KEBIJAKAN TIONGKOK DALAM MENGHADAPI *CYBER WARFARE* PASCA SERANGAN AMERIKA SERIKAT TAHUN 2013

(Skripsi)

Oleh

ABDURAHMAN WAHID
1516071087

JURUSAN HUBUNGAN INTERNASIONAL
FAKULTAS ILMU SOSIAL DAN ILMU POLITIK
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG
2022

ABSTRAK

KEBIJAKAN TIONGKOK DALAM MENGHADAPI *CYBER WARFARE* PASCA SERANGAN AMERIKA SERIKAT TAHUN 2013

Oleh

ABDURAHMAN WAHID

Penelitian ini merupakan penelitian pengembangan dari sejarah konflik dunia maya antara Tiongkok dan Amerika Serikat pada tahun 2009 dengan pencurian data perusahaan Google. Penelitian ini bertujuan untuk mengetahui tentang keamanan *cyber* negara Tiongkok dalam menghadapi ancaman *cyberwarfare*. Penelitian ini menggunakan teori kebijakan publik, kebijakan nasional, dan kebijakan luar negeri dan dilakukan melalui tiga tahapan utama, yaitu (1) proses (*process*) untuk mengetahui kebutuhan awal dalam mengembangkan sistem pertahanan dunia maya. (2) Implementasi (*implementation*) merupakan rancangan kegiatan dan penyusunan soal. (3) Dampak (*impact*), pengujian hasil akhir yang diterapkan dan dilaksanakan. Sumber data dalam penelitian ini adalah jenis data sekunder melalui dokumen, jurnal dan *website* resmi negara. Teknik analisis data menggunakan model Miles dan Huberman dengan tiga tahapan, (1) kondensasi data, (2) penyajian data dan (3) penarikan kesimpulan. Hasil penelitian menunjukkan bahwa tahapan kebijakan dan pelaksanaan kepentingan nasional Tiongkok berdampak positif serta efisien dalam menghadapi ancaman *cyber* khususnya Amerika Serikat. Kebijakan kepentingan luar negeri Tiongkok yang melalui sebuah perjanjian berdampak negatif, pelanggaran tetap berlanjut dan tidak memberikan dampak positif didalam hubungan internasional.

Kata Kunci: *Cyberwarfare*, Tiongkok, Pertahanan Dunia Maya, Kebijakan Nasional

ABSTRACT

CHINA POLICY IN DEALING WITH CYBER WARFARE POST ATTACK IN THE UNITED STATES OF 2013

By

ABDURAHMAN WAHID

This research is a development study of the history of cyber conflicts between China and the United States in 2009 with the theft of Google company data. This study aims to find out about China's cyber security in dealing with the threat of cyberwarfare. This research uses public policy theory, national policy, and foreign policy and is carried out through three main stages, namely (1) the process to determine the initial needs in developing a cyber defense system. (2) Implementation is the design of activities and preparation of questions. (3) Impact, the final result test that is applied and implemented. The source of data in this study is secondary data through documents, journals and official state websites. The data analysis technique uses the Miles and Huberman model with three stages, (1) data condensation, (2) data presentation and (3) conclusion drawing. The results show that the stages of policy and implementation of China's national interests have a positive and efficient impact in dealing with cyber threats, especially the United States. China's foreign policy, which through an agreement has a negative impact, continues to violate and does not have a positive impact on international relations.

Keywords: Cyberwarfare, China, Cyber Defense, National Policy

KEBIJAKAN TIONGKOK DALAM MENGHADAPI *CYBER WARFARE* PASCA SERANGAN AMERIKA SERIKAT TAHUN 2013

Oleh

ABDURAHMAN WAHID

Skripsi

Sebagai Salah Satu Syarat untuk Mencapai Gelar
SARJANA HUBUNGAN INTERNASIONAL

Pada

Program Sarjana Ilmu Hubungan Internasional
Fakultas Ilmu Sosial dan Ilmu Politik

FAKULTAS ILMU SOSIAL DAN ILMU POLITIK
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG
2022

Judul Skripsi	:	**KEBIJAKAN TIONGKOK DALAM MENGHADAPI *CYBER WARFARE* PASCA SERANGAN AMERIKA SERIKAT TAHUN 2013**
Nama	:	**Abdurahman Wahid**
NPM	:	**1516071087**
Jurusan	:	**Hubungan Internasional**
Fakultas	:	**Ilmu Sosial Ilmu Politik**

MENYETUJUI

1. Komisi Pembimbing

Drs. Agus Hadiawan, M.Si.	**Gita P Djausal, S.IP., M.A.B.**
NIP 195801091986031002	NIP 198412162019032004

2. Ketua Jurusan Hubungan Internasional

Dr. Ari Darmastuti, M.A.
NIP 196004161986032002

MENGESAHKAN

1. Tim Penguji

Ketua : **Drs. Agus Hadiawan, M.Si.** .....

Sekretaris : **Gita P Djausal, S.IP., M.A.B.** .....

Penguji
Bukan Pembimbing : **Hasbi Sidik, S.IP., M.A.** .....

2. Dekan Fakultas Ilmu Sosial Ilmu Politik

Dra. Ida Nurhaida, M.Si.
NIP 196108071987032001

Tanggal Lulus Ujian Skripsi : **22 Juli 2022**

PERNYATAAN

Dengan ini saya menyatakan bahwa:

1. Karya tulis saya, skripsi ini adalah asli dan belum pernah diajukan untuk mendaftar gelar akademik (sarjana), baik di Universitas Lampung maupun di perguruan tinggi lain.
2. Karya tulis ini murni gagasan, rumusan, dan penelitian saya sendiri, tanpa bantuan pihak lain, kecuali arahan komisi pembimbing dan penguji.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan sebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
4. Pernyataan ini saya buat dengan sesungguhnya dan apabila di kemudian hari terdapat penyimpangan dan ketidak benaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah berlaku di Universitas Lampung.

Bandar Lampung, 22 Juli 2022
Yang membuat pernyataan

Abdurahman Wahid
1516071087

RIWAYAT HIDUP

Abdurahman Wahid lahir di Bandar Lampung pada tanggal 15 Juli 1995. Penulis merupakan anak pertama dari dua bersaudara pasangan Bapak Moh. Ali dan Ibu Jamaliyah. Penulis menempuh pendidikan di TK Al-Azhar pada tahun 2000, kemudian Sekolah Dasar di SD 1 Al-Azhar lulus pada tahun 2001 hingga 2007, kemudian penulis melanjutkan pendidikan di Sekolah Menengah Pertama di SMPN 4 Bandar Lampung pada tahun 2007 hingga 2010. Kemudian penulis melanjutkan pendidikan di Sekolah Menengah Atas di SMA Al-Kautsar Bandar Lampung tahun 2010 hingga 2013. Pada tahun 2015, penulis dinyatakan berhasil diterima sebagai mahasiswa Jurusan Hubungan Internasional Universitas Lampung.

MOTTO

"Allah tidak membebani seseorang melainkan sesuai dengan kesanggupannya. Ia mendapat pahala (dari kebajikan) yang diusahakannya dan ia mendapat siksa (dari kejahatan) yang dikerjakannya."

(QS. Al-Baqarah: 286)

"Be a strong wall in the hard times, and be smiling sun in the good times."

(ARW)

PERSEMBAHAN

Dengan Segala Kerendahan Hati Kupersembahkan Karya Kecilku ini Kepada :

Kedua orang tua tercinta
Bapak Moh. Ali dan Ibu Jamaliyah

Terimakasih Untuk Semua Kasih Sayang Dan Pengorbanannya Selama Ini.

Serta Almamater tercinta
Universitas Lampung

SANWACANA

Puji syukur kepada Allah SWT yang selalu memberikan rahmat dan hidayah-Nya terhadap penulis selama masa perkuliahan, sehingga dapat menyelesaikan skripsi yang berjudul **"Kebijakan Tiongkok Dalam Menghadapi *Cyber Warfare* Pasca Serangan Amerika Serikat Tahun 2013"**.

Skripsi ini disusun sebagai syarat untuk memperoleh gelar sarjana Hubungan Internasional di Universitas Lampung. Selama proses penyusunan skripsi ini penulis banyak mendapatkan bimbingan dan bantuan dari berbagai pihak. Dalam kesempatan ini penulis ingin mengucapkan terima kasih kepada :

1. Allah SWT, atas segala kemudahan, kelancaran, dan kekuatan yang telah Engkau berikan dalam melancarkan skripsi ini.
2. Ibu Dra. Ida Nurhaida, M.Si. Selaku Dekan Fakultas Ilmu Sosial dan Ilmu Politik Universitas Lampung.
3. Ibu Dr. Ari Darmastuti, M.A Selaku Ketua Jurusan Ilmu Hubungan Internasional Fakultas Ilmu Sosial dan Ilmu Politik Universitas Lampung.
4. Bapak Drs. Agus Hadiawan, M.Si., Selaku pembimbing Utama Skripsi yang telah berkenan meluangkan waktu, tenaga dan pikiran dalam membimbing penulis hingga dapat menyelesaikan skripsi ini.
5. Mba Gita P Djausal, S.IP., M.A.B., Selaku dosen pembimbing skripsi yang dengan sabar telah membimbing, memberikan arahan serta masukannya selama proses penyelesaian skripsi ini.
6. Bang Hasbi Sidik, S.IP., M.A, selaku dosen penguji dalam setiap bimbingan, saran, maupun kritik yang membangun bagi kelancaran skripsi penulis.

7. Adik yang penulis sayangi. Siti Aisyach Nursyachbani yang selalu mendukung, menyayangi dan selalu memberikan yang terbaik untuk keberhasilanku.
8. Donna Exsanti Charinda, Maya Novita, Ayu Selviani, Intan Permata, M Firly Ramadan, Intan Nata Sasmita dan Chaindra Adityas R. selaku "Nayah Wacana" yang memberikan canda tawa selama perkuliahan serta semangat dan dukungan.
9. Seluruh jajaran Dosen FISIP Universitas Lampung, khususnya jurusan Hubungan Internasional yang telah memberikan seluruh ilmu yang bermanfaat.
10. Teman-teman Hubungan Internasional angkatan 2015. Terima kasih sudah menjadi bagian dari perjalanan perkuliahan penulis. Terima kasih sudah berbagai tawa, cerita dan kesulitan bersama.
11. Seluruh pihak yang memberikan doa, dukungan dan bantuan kepada penulis yang tidak dapat disebutkan satu-persatu.

Akhir kata, penulis menyadari bahwa penelitian ini masih jauh dari kata kesempurna, akan tetapi sedikit harapan semoga skripsi ini dapat berguna dan bermanfaat bagi semua. Amiinn.

Bandar Lampung, 22 Juli 2022
Penulis,

Abdurahman Wahid

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Gambar Halaman

DAFTAR TABEL

Tabel Halaman

DAFTAR SINGKATAN

AMSC	: *American Superconductor*
AS	: Amerika Serikat
CIA	: *Central Intelligence Agency*
CNCERT	: *China National Network Emergency Response Technical*
CPPCC	*: Chinese People's Political Consultative Conference*
DARPA	: *The Defense Advanced Research Projects Agency*
DDoS	: *Distributed Denial of Service*
DHS	: *Department of Homeland Security*
DISA	: *Defense Information Systems Agency*
DoD	: *Department of Defense*
FBI	: *Federal Bureau of Investigation*
FYP	: *Five-Year Plan*
HUMINT	: *Human Intelligence*
IP	: *Internet Protocol*
ISP	: *Internet Service Provider*
ITU	: *International Telecomunication Union*
NDRC	: *National Development and Reform Commission*
NPC	: *National People's Congress*
NSA	: *National Security Agency*
NSC	: *National Supervisory Commission*
PLA	: *People's Liberation Army*
SC	: *State Council*
SIGINT	: *Signal Intelligence*
SPC	: *Supreme People's Court*

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada dunia moderen, keberadaan sebuah informasi memiliki peran penting dalam perjalanan dari tujuan-tujuan kehidupan. Informasi sebagai sarana utama bagi setiap manusia dalam berkomunikasi, dan dilakukan antar individu maupun kelompok dan organisai. Dengan demikian, dapat dikatakan bahwa informasi dalam kehidupan manusia berperan sebagai aliran darah sebagai bentuk sumber kekuatan tubuh (Anne, 1986: 1). Pengembangan di era ini melahirkan tahapan baru yang lebih kompleks yaitu melalui internet. Teknologi ini menciptakan jaringan komunikasi untuk dapat menjelajah antar wilayah yang tidak dapat dijangkau secara langsung. Dengan kata lain, teknologi ini membantu mempersingkat waktu dalam melakukan komunikasi maupun memperoleh informasi dan data agar lebih akurat.

Hadirnya internet menyebabkan masyarakat mengalami tingkat ketergantungan yang tinggi, karena menurut pendapat Young (1998) yang di kutip dari Noviana Dewi dalam jurnal Psikologi Universitas Gajah Mada (UGM) bahwa internet bisa menjadi salah satu sarana yang tidak baik jika penggunanya tidak mampu mengendalikan jumlah kegiatan di dunia nyata ke dalam bentuk dunia maya. Jika seseorang yang pada dasarnya mudah dalam berkomunikasi di kehidupan nyata dan masuk ke dalam dunia internet, maka hal ini terjadi karena hadirnya internet yang menawarkan kenyamanan dan membuat komunikasi lebih cepat dan praktis. Arus komunikasi yang dilakukan secara berkala serta kebutuhan dalam mengakses data akan tetap menjadi prioritas yang utama. Dunia internet bukan berarti secara keseluruhan dapat dikatakan baik, karena hadirnya internet sebagai sarana perubahan teknologi

moderen, dapat menjadi lebih efektif bila kegunaannya dapat dikontrol penuh oleh pemerintah sebagai bentuk perhatian khusus. Sehingga pengelolaan dunia internet dapat di sesuaikan melalui nilai-nilai sosial maupun secara pribadi. Pemerintah menciptakan dan merealisasikan peraturan untuk melindungi seluruh masyarakatnya dari dampak yang buruk.

Dunia maya (*cyberspace*) adalah bagian dari internet, menurut Major Graham H. Todd di dalam buku *The Air Force Law Review* (vol. 64, (2009: 68) *Armed Attack in Cyberspace*: *Deterring Asymmetric Warfare with an Asymmetric Definition*, mendefinisikan *cyberspace* sebagai domain buatan manusia yang berkembang untuk organisasi dan *transfer* data menggunakan berbagai panjang gelombang dari spektrum elektromagnetik. Domain itu adalah kombinasi dari properti pribadi dan publik yang di atur oleh aturan teknis dan di rancang, terutama untuk memfasilitasi aliran informasi. Era digital menjadi salah satu arena baru bagi setiap negara dunia, karena selain dunia digital seperti darat, laut, udara maupun luar angkasa sudah diperebutkan oleh negara-negara *super power* untuk kepentingan dan tujuan-tujuan politik.

Perkembangan besar teknologi memasuki beberapa aspek seperti (ekonomi, transportasi, medis, pendidikan), salah satu aspek yang paling besar pengaruhnya yaitu adalah aspek keamanan. Menurut Kshetri (2014: 2), penyebab pesatnya perkembangan teknologi tersebut dikarenakan sebagai salah satu arena terakhir yang meiliki kemampuan secara menyeluruh lebih cepat dan praktis dalam menghubungkan kepentingan dan tujuan-tujuan sebuah negara baik dalam sektor keamanan nasional maupun dalam hubungan internasional. Kshetri juga menambahkan melalui pemahaman Adam Cobb (1999), jika terjadi suatu konflik di arena dunia digital, maka dampak dan ancaman yang dapat ditimbulkan akan jauh lebih besar dibandingkan dengan adanya persenjataan nuklir seperti kisaran tahun 1940.

Pengguna internet global mengalami peningkatan yang signifikan, dan proses perubahan yang terjadi tapatnya pada tahun (2000-2019), seperti tabel berikut:

Tabel 1.1

WORLD INTERNET USAGE AND POPULATION STATISTICS 2019 Mid-Year Estimates						
World Regions	Population (2019 Est.)	Population % of World	Internet Users 30 June 2019	Penetration Rate (% Pop.)	Growth 2000-2019	Internet World %
Africa	1,320,038,716	17.1 %	522,809,480	39.6 %	11,481 %	11.5 %
Asia	4,241,972,790	55.0 %	2,300,469,859	54.2 %	1,913 %	50.7 %
Europe	829,173,007	10.7 %	727,559,682	87.7 %	592 %	16.0 %
Latin America	658,345,826	8.5 %	453,702,292	68.9 %	2,411 %	10.0 %
Middle East	258,356,867	3.3 %	175,502,589	67.9 %	5,243 %	3.9 %
North America	366,496,802	4.7 %	327,568,628	89.4 %	203 %	7.2 %
Australia	41,839,201	0.5 %	28,636,278	68.4 %	276 %	0.6 %
WORLD TOTAL	7,716,223,209	100.0 %	4,536,248,808	58.8 %	1,157 %	100.0 %

Menurut *Miniwatts Marketing Group* (internetworldstats), jumlah pengguna internet di seluruh dunia yang terdata pada 30 Juni 2019 mencapai 4,5 Milyar pengguna. Penyumbang pengguna internet terbesar yakni dari wailayah Asia dengan jumlah 2,3 Milyar pengguna, atau setengah dari jumlah total pengguna internet di seluruh dunia. Dalam hal ini wilayah Asia di pimpin oleh Tiongkok dalam pengguna terbesarnya yaitu:

Tabel 1.2

-CHINA *internetworldstats*
CN - **1,420,062,022(*) population (2019) - Area: 9,806,391 sq km**
Cap. city: Beijing - Pop. 22,063,000 (2017) - Median Age: 37.4 years
GNI (per capita): $8,690 (2017) per World Bank.
829,000,000 Internet users, June/2019, 58.4% pen., per CNNIC
1,800,000 Facebook subscribers in Dec/2018, 0.1% penetration.
Local Time and Weather in Beijing, China

Dengan jumlah 800 juta pengguna internet, Tiongkok mengungguli India yang berada di peringkat kedua dengan jumlah 500 juta pengguna. Jaringan internet (*cyberspace*) saat ini di nilai sebagai sumber informasi universal bagi masyarakat global, dengan menghadirkan inovasi-inovasi baru membuat dorongan pertumbuhan ekonomi mengalami perubahan. Namun

inovasi yang di timbulkan tidak dapat dengan mudah memberikan efek yang baik dari segi ekonomi global, karena di sisi lain *cyberspace* membawa efek buruk dengan meningkatnya serangan kejahatan dunia maya (*cybercrime*). Serangan *cybercrime* yang terus berevolusi dan meningkat telah memberi efek (*negative*) yang cukup besar dalam segi ekonomi.

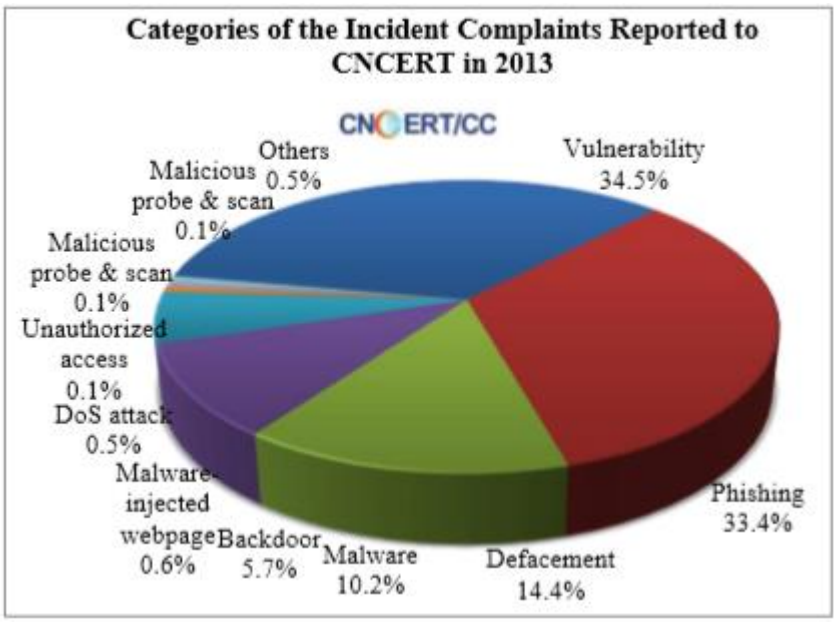
Pencurian data, gangguan terhadap transaksi online (*e-commerce*), pembajakan, dan menjadi salah satu jalan alternatif kegiatan pasar gelap (*black market*). Tidak hanya itu, *cybercrime* juga akan berdampak pada negara, salah satunya dapat mengancam stabilitas negara seperti pencurian data-data penting negara yaitu seperti data lembaga negara, data infrastruktur nasional, data pribadi penduduk, data keamanan dan data kekuatan negara. Kejahatan dunia maya seperti ini menjadi kompleks karena kegunaan internet yang notabene tanpa batas. Sehingga dapat di jadikan alat suatu negara untuk dapat memata-matai negara lain dalam hal apapun guna meraih tujuan-tujuan yang di inginkan, walaupun jika penyerangan di lakukan bukan oleh negara yang bersangkutan melainkan hanya kegiatan individu, tentu akan mengakibatkan ketegangan antar negara yang berkaitan serta dapat merusak hubungan bilateral maupun multilateral jika kasus-kasus tersebut tidak tertangani dengan cepat dan akurat. Karena dapat menjadi asumsi negatif, baik itu dari pandangan nasional maupun dari sudut pandang internasional.

Tiongkok memimpin sebagai jumlah populasi pengguna internet dunia dan telah mengklaim bahwasannya seperti yang dikutip Yan Jie dalam chinadaily pada tahun 2010 mereka telah mendapatkan serangan *cyber* sebanyak 21.618 laporan yang telah diterima oleh CNCERT/CC (*China National Computer Network Emergency Response Technical Team*). Menurut Zhou Yonglin wakil kepala departemen CNCERT, peretasan dilakukan dari luar negeri terutama di kendalikannya dari Amerika Serikat yang secara ilegal merusak melalui program jahat trojan dan program zombie. Kemudian tahun sebelumnya Tiongkok mengalami serang virus *trojan* dengan jumlah sasaran tujuan sebanyak kurang lebih 300.000 alamat IP (*internet protocol*) yang berasal dari 170.000 alamat IP luar negeri yang dimana Amerika Serikat sebagai pengirim serangan dengan memperoleh 16,61% terbanyak. Keterangan

tersebut juga di dukung oleh perusahaan terbesar keamanan *cyber* yaitu *symantec* dengan menyatakan laporan 33% server *zombie* dunia berada di Amerika Serikat.

Kementerian keamanan publik Tiongkok juga telah mencatat bahwa jumlah serangan siber pada komputer Tiongkok dan situs *website* telah melonjak lebih dari 80% setiap tahun, dan yang terbanyak terjadi pada sektor jaringan keamanan seperti *website* sosial media, game online, dan perdagangan elektronik pada tahun 2011, dengan hasil 100 juta username beserta *e-mail* dan kata sandinya (Lieberthal, 2012: 4).

Pada beberapa kasus tersebut sudah membuat Tiongkok dan Amerika Serikat menjadi tidak harmonis dan ketegangan kedua negara terhadap kegiatan *cyber* memuncak pada tahun 2013. Menurut CNCERT Annual report 2013, dalam lima bulan pertama di tahun 2013, terdapat 13.408 *trojan horse* luar negeri dan robot pengontrol server yang membajak sekitar 5,63 juta *mainframe* di Tiongkok. Dari jumlah tersebut menyangkut adanya 4.062 server kontrol yang berbasis di Amerika Serikat dengan berhasil membajak 2,91 juta *mainframe* di Tiongkok.



Gambar 1.1

Pada periode yang sama, 249 *website* organisasi penting Tiongkok yang juga termasuk departemen pemerintah, sistem informasi utama dan lembaga penelitian di tanamkan dengan program *backdoor*. Terdapat 54 situs *website* di bajak oleh alamat IP yang berbasis di Amerika Serikat dengan berhasil mencuri data informasi *website* tersebut.

Direktur tim teknis tanggap darurat jaringan komputer nasional / pusat koordinasi Tiongkok (CNCERT) yaitu Huang Chengqing menyatakan: "*We have mountains of data, if we wanted to accuse the United States, but it's not helpful in solving the problem. Besides, we have smooth communication at the civil level. I don't understand why all levels of the United States government are accusing China of cybersecurity recently. I felt it is driven by some political intentions, though I don't know what the intentions.*" ("Kami memiliki banyak data, jika kami ingin menuduh Amerika Serikat, tetapi itu tidak membantu dalam menyelesaikan masalah. Selain itu, kami memiliki komunikasi yang lancar di tingkat sipil. Saya tidak mengerti mengapa semua tingkat pemerintah Amerika Serikat menuduh Tiongkok melakukan *cybersecurity* baru-baru ini. Saya rasa itu di dorong oleh beberapa elit politik, meskipun saya tidak tahu apa niatnya.") (chinadaily, 2013). Pernyataan Huang muncul setelah banyak laporan yang menuduh Tiongkok melakukan peretasan yang dirilis di Amerika Serikat pada tahun yang sama.

Sejumlah besar aktivitas internet yang berbahaya berasal dari atau setidaknya bergerak melalui Amerika Serikat, sebagai contoh dari peneliti keamanan di *HostExploit* telah menemukan bahwa 20 dari 50 ISP (*internet service provider*) yang menyebarkan kejahatan di dunia khususnya (*cyberspace*) adalah orang Amerika Serikat dan juga para agen pemerintah A.S. seperti NSA (*National Security Agency*) turut aktif dalam melakukan operasi *cyber* tersebut (Lieberthal, 2012: 5). Hal ini yang membuat dampak dari era informasi tentang stabilitas keamanan *cyber* dan bahkan dapat menimbulkan perang *cyber*, karena telah menjadi isu utama selama dua dekade terakhir ketika para pembuat kebijakan, baik juga militer, para ahli strategi, dan aktor non-negara mempertimbangkan cara terbaik bagaimana untuk menggunakan dan melindungi diri dari ancaman perang *cyber* (*cyberwar*).

Frederik Kremer & Benedikt Müller (2014: 22) mengatakan bahwa: ”*Unlike weapons of the past, the technology necessary for waging cyber war are not restricted to particular actors within the system. The capacity to assault important systems exists both in state and non-state actors and could possibly cripple whole societies that have become reliant on information. Over the last several years the world has seen examples of cyber war*.” (“Tidak seperti senjata masa lalu, teknologi yang diperlukan untuk menciptakan perang siber tidak terbatas pada aktor tertentu di dalam sebuah sistem. Kapasitas untuk menyerang sistem penting, terdapat pada aktor negara maupun non-negara dan juga bisa melumpuhkan masyarakat yang telah bergantung pada suatu informasi. Dan dalam beberapa tahun terakhir dunia telah memperlihatkan contoh perang siber tersebut").

Cyber warfare atau perang *cyber*, Frederik Kremer & Benedikt Müller (2014: 62) juga menjelaskan bahwa hal ini adalah kelanjutan dari strategi masa lalu untuk dapat menghancurkan suatu negara dari dalam. Di masa lalu, kerajaan selama perang, mengirim mata-mata untuk menyusup ke tembok kerajaan lain agar dapat menghancurkan atau melumpuhkan para penjaga. Algojo melemparkan mayat di dinding benteng dan membuat kekacauan di dalamnya. Langkah-langkah ofensif ini mirip dengan serangan *cyber*, mereka ingin melemahkan suatu negara dari dalam. Seperti halnya *trojan horse* yang digunakan sebagai salah satu strategi di masa perang siber dan karenanya, perang siber bukanlah hal yang baru, tetapi perpanjangan dari *new season of war* atau teknik inovatif yang berupaya melemahkan negara dari interiornya, dari pada melalui cara yang normal.

Perang *cyber* adalah sesuatu yang dapat di harapkan, mengingat struktur dunia yang anarkis, karena itu bukan sepenuhnya fenomena baru. Sebaliknya, itu hanyalah arena politik yang telah di militerisasi guna memastikan keamanan dengan cara membatasi keamanan orang lain. Ini menghadirkan peluang untuk menghancurkan keamanan dan otonomi nasional suatu negara untuk menciptakan kerentanan yang sangat berbahaya, sehingga kelangsungan hidup dan rakyatnya di pertaruhkan.

Serangan dunia maya terhadap Estonia pada tahun 2007 adalah sebagai contoh *cyber warfare* yang lebih mutakhir dari praktik kontemporer yang muncul di negara bagian. Pada akhir April 2007, pemerintah Estonia berupaya untuk merelokasi patung era Soviet di ibu kota mereka, Tallinn, dan menyebabkan gangguan yang signifikan pada Internet lalu layanan berbasis *Web* yang berlangsung selama beberapa minggu serta terdiri dari 128 serangan unique DDOS *cyber warfare*. Pada puncaknya, lalu lintas yang berasal dari luar Estonia 400 kali lebih tinggi dari kecepatan normalnya dan melibatkan sekitar 100 juta komputer lebih dari 50 negara (Bradley, 2015: 17).

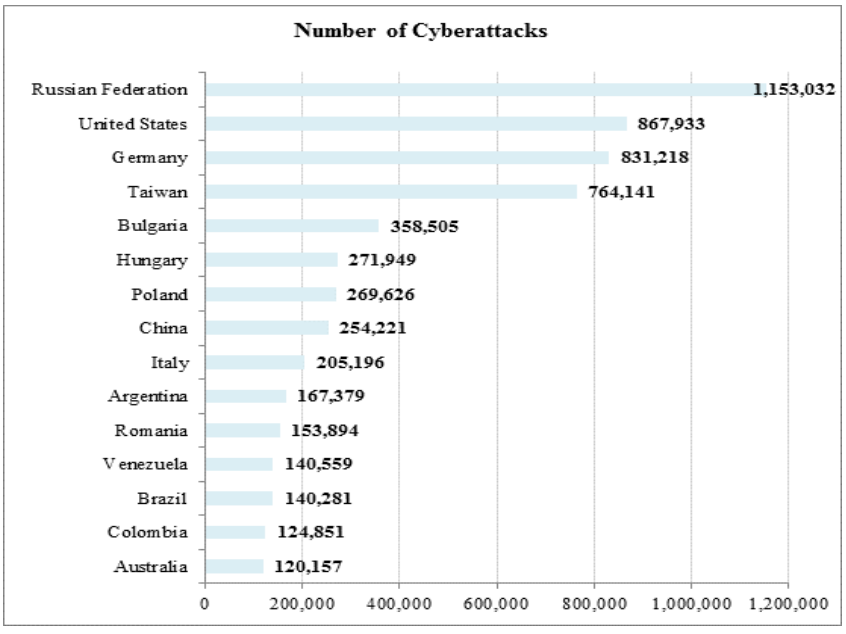
Para penyerang mengeksekusi serangan menggunakan serangkaian "*botnet*" dan penyelidik menentukan bahwa serangan itu adalah dikoordinasikan dengan hati-hati sebelumnya, karena fakta bahwa serangan itu tidak jadi menyebar dan nampaknya tidak dikendalikan secara terpusat melalui pusat komando dan kendali yang dapat diidentifikasi. Untuk meredakan serangan, Estonia perusahaan telekomunikasi dan ISP (*internet service provider*) bekerja dengan cepat untuk mengembangkan kapasitas jaringan dan memindahkan situs pemerintah ke server alternatif. Contoh serangan *cyber warfare* lain dintaranya (Nicholas, 2019: 42):

Tabel 1.3

Year	Preparator	Target	Summary of cyber-attacks
2007	Russian Federation (alleged*)	Estonia	Series of cyber-attacks first against Estonian government agencies, and then private sites and servers.
2007	China (alleged)	United-Kingdom, France, Germany	Intrusions into government networks.
2008	Russian nationalist hackers	Lithuania	Hacking of hundreds of Lithuanian government and corporate websites.
2008	Russian Federation	Georgia	Cyber-attack directly coordinated with a kinetic land, sea and air attack.
2009	Russian Federation (alleged)	Kyrgyzstan	Cyber-attacks focused on Internet Service Providers in Kyrgyzstan disrupting all internet traffic.
2009-2010	Unknown	Iran	Stuxnet, a cyber-worm, designed specifically to sabotage Iran's nuclear reactors.
2012	Unknown	Saudi Arabia's State oil company	The Sharmoon virus infected 30000 ARAMCO computers
2012	Unknown	Qatar	Sharmoon virus (oil company RasGas)

'*alleged*', this reflects the difficulty in ascertaining responsibility.
Source: Flowers and Zeadally (2014).

Tabel 1.4



Source: Flowers and Zeadally (2014)

The Wall Street Journal (WSJ) dalam artikelnya tentang "kekuatan dunia maya" menyatakan bahwa "Tiongkok sering menggunakan serangan

bervolume tinggi dengan jumlah yang banyak melalui operasi di militer atau kelompok luar yang terkait dengan pemerintah untuk membombardir target-tergetnya". Menurut WSJ, daftar dugaan tindakan oleh Tiongkok dalam beberapa tahun terakhir yaitu:

1. 2009: Pencurian data dari Google Inc.
2. 2009: Penemuan rencana pencurian proyek Joint Strike Fighter AS.
3. 2010: Serangan terhadap eksekutif Inggris
4. 2011: Serangan di portal Internet Korea Selatan.
5. 2013: Perusahaan media besar AS diretas (Liudmyla, 2018: 143).

Sementara itu Amerika Serikat menurut WSJ, jika berbicara tentang kemampuan perang dunia maya Amerika Serikat yang dipimpin oleh NSA dan Komando Siber. Serangan Amerika Serikat dikenal karena kompleksitas dan tekniknya yang canggih, karena negara tersebut telah aktif di lapangan selama hampir dua dekade. Daftar tindakan yang dicurigai diantaranya:

1. 2010: Worm komputer di Pembangkit nuklir Iran.
2. 2010: Pengawasan (memata-matai) kantor Uni Eropa.
3. 2011: Serangan pada Gemalto, pembuat kartu SIM seluler Eropa.

Pra Konflik Tiongkok dan Amerika Serikat terjadi karena di awali adanya ancaman terhadap keamanan nasional Amerika Serikat. Sejumlah contoh spionase dunia maya Tiongkok yang menargetkan pada program keamanan nasional AS telah di identifikasi dalam beberapa tahun terakhir. Pada Mei 2013, *Washington Post* menggambarkan laporan rahasia oleh Defense Science Board, yang mencantumkan lebih dari 24 desain sistem senjata AS diakses oleh penyusup dunia maya. *The Washington Post* melaporkan, "Pejabat senior militer dan industri yang mengetahui pelanggaran tersebut mengatakan bahwa sebagian besar adalah bagian dari kampanye spionase Tiongkok yang semakin meluas terhadap kontraktor pertahanan dan

lembaga pemerintah AS." Daftar tersebut termasuk sistem rudal Patriot *(Patriot missile system*), sistem pertahanan rudal balistik Aegis *(Aegis ballistic missile defense system*), pesawat tempur F / A-18, pesawat tempur multiperan V-22 Osprey, dan Kapal Tempur Littoral.

Ancaman selanjutnya di tujukan terhadap industri Amerika Serikat, Jenderal Keith Alexander, komandan Komando Siber AS, menilai biaya kerugian dari pencurian kekayaan intelektual perusahaan AS sekitar 250 miliar dollar pertahun, meskipun tidak semua kerugian tersebut di sebabkan oleh aktivitas Tiongkok. Entitas Tiongkok yang terlibat dalam dunia maya dan bentuk spionase ekonomi lainnya kemungkinan besar menyimpulkan bahwa dengan cara mencuri kekayaan intelektual dan informasi kepemilikan jauh lebih hemat biaya daripada berinvestasi dalam waktu lama. Namun demikian, jelas bahwa Tiongkok bukan hanya pemimpin global dalam menggunakan metode dunia maya untuk mencuri kekayaan intelektual, tetapi juga bertanggung jawab atas sebagian besar pencurian kekayaan intelektual global. Aktor Tiongkok dalam kurun waktu beberapa tahun terakhir memanfaatkan aktivitas dunia maya untuk mendapatkan informasi sensitif atau hak kepemilikan dari perusahaan AS, diantaranya yaitu:

1. Dalam laporan Mandiant yang disebutkan, terdapat bukti sejak 2006 *People's Liberation Army* (PLA) Unit 61398 setidaknya telah menembus jaringan 141 organisasi, termasuk perusahaan, organisasi internasional, dan pemerintah asing. Organisasi-organisasi ini berlokasi atau memiliki kantor pusat di 15 negara dan mewakili 20 sektor utama, dari teknologi informasi hingga layanan keuangan. Dari organisasi-organisasi itu yang ditembus, 81 persen berlokasi di Amerika Serikat atau memiliki kantor pusat yang berbasis di AS. Unit 61398 adalah Biro kedua dari departemen pengintaian teknis *People's Liberation Army* (PLA), yang berbasis di Shanghai (Larry, 2014: 15).
2. *Departemen Kehakiman atau Department of Justice* (DoJ) pada Juni 2013 mengajukan tuntutan terhadap Sinovel Wind

> Group, sebuah perusahaan energi Tiongkok, dengan tuduhan Sinovel mencuri kekayaan intelektual dari perusahaan *American Superconductor* (AMSC) yang berbasis di Massachusetts. Setelah Sinovel dapat mereproduksi teknologi AMSC dan mencuri kode sumber miliknya, perusahaan Tiongkok tersebut memutuskan kemitraan, membatalkan pesanan yang ada, dan menghancurkan pendapatan AMSC. AMSC telah meminta kompensasi dari Sinovel melalui tuntutan hukum di Tiongkok, dan atas upaya yang sedang berlangsung telah menghasilkan biaya hukum untuk AMSC melebihi 6 juta dollar. Sementara tuntutan hukum ini terus bergerak perlahan melalui sistem hukum Tiongkok, sehingga menambah biaya hukum AMSC, dan Sinovel terus meraup keuntungan dari teknologi yang mereka curi.

Pasukan *cyber warfare* adalah orang-orang yang terlatih dan memahami dunia internet secara kompleks, atau biasa disebut juga dengan istilah *hacker*. Selaras dengan pandangan Klimburg & Manson dalam buku Kremer & Benedikt (2014: 24) yang mengatakan: "*The literature and occurrences in the system show that non-state actors are significantly involved in conducting cyber war.*" ("Literatur dan kejadian dalam sistem menunjukkan bahwa aktor non-negara terlibat secara signifikan dalam melakukan perang *cyber*"). Untuk menyempurnakan tindakan *cyber*, mereka melengkapi diri dengan "senjata pribadi" yang meliputi: kecerdikan, ketangkasan dan kecerdasan. Mereka menggunakan keterampilan ini untuk menyusup / menyelinap, mencuri dan menghancurkan, menggunakan program seperti virus dan teknik seperti perangkap (*phishing*) (Kremer & Benedikt, 2014: 62).

Serangan-serangan ini bisa untuk tujuan spionase, sabotase, dan destruktif. Mereka dapat mematikan jaringan listrik, menyedot uang, mengganggu komunikasi, membatalkan pengiriman, transportasi, bahan bakar dan air, mengganggu pasar saham dan bahkan membajak drone. Ini pada

akhirnya akan menghancurkan stabilitas domestik suatu negara dan menciptakan kekacauan. Namun yang lebih relevan adalah dapat memutuskan komunikasi negara untuk mendapatkan keuntungan strategis dan taktis sebelum invasi skala penuh dimulai.

Oleh karena itu negara diperlukan adanya sistem pengembangan yang khusus untuk teknologi *cyber* ini, yaitu di antaranya ialah peningkatan *cyber* security dan *cyber defense*. *Cyber security* atau keamanan dunia maya adalah bentuk dari proses atau upaya melindungi jaringan informasi dan komunikasi dengan suatu sistem perangkat komputer, berupa program yang diolah untuk mencari, mendata, merekam, memproses dan menyimpan serangkaian informasi dari tindakan ilegal (Touhill, 2014: 2). Di sederhanakan seperti proteksi atau perlindungan dunia maya dari sumber-sumber ancaman salah satunya adalah virus. Sedangkan *cyber defense* atau pertahanan dunia maya adalah semacam bentuk usaha untuk mempertahankan keamanan *cyber* atau dunia maya melalui cara memperkuat sistem *cyber* sebagai contoh dengan melakukan lapisan-lapisan *coding* algoritma.

Cyber security itu sendiri sangat berbeda dengan security atau keamanan biasa karena ancaman cyber tidak bisa di-masukkan begitu saja ke dalam kategori keamanan tradisional (Wallace, 2013). Dan mengutip dari (Kremer & Benedikt, 2014: 22) Geers (2011) mengatakan “Perang *cyber* adalah peperangan yang terjadi tidak menggunakan alat berat, perang ini biasanya sangat diminati oleh negara-negara yang perekonomian militernya rendah. Karena sebagai tindakan investasi jangka panjang guna mengimbangi kerugian konvensional”.

Sun Tzu adalah ahli strategi dan cendekiawan Tiongkok dalam risalahnya yang terkenal "*the art of war*" mengungkapkan salah satu gagasan utama dalam *attack by stratagem* yaitu adalah "keunggulan tertinggi bukanlah terletak pada saat dapat menaklukan disemua medan pertempuran, akan tetapi pencapaian yang paling terbaik adalah bisa menghancurkan pertahanan dan perlawanan musuh tanpa adanya tindakan pertempuran”.

Terkait ungkapan Sun Tzu tersebut, peneliti mengisyaratkan bahwasannya Tiongkok dapat mengendalikan dunia hanya dengan melalui jaringan teknologi informasi dan teknologi tanpa harus bersusah payah melakukan kontak fisik dengan para musuh yang dapat mengganggu kepentingannya. Akan tetapi guna menghadapi peningkatan di dalam perkembangan dunia maya, Tiongkok tentunya memiliki sejumlah strategi / kebijakan khusus, karena pada akhirnya bukan hanya Amerika Serikat yang dapat mengganggu kedaulatan mereka, melainkan negara-negara besar dan maju lain dapat menjadi ancaman selanjutnya.

Karena itu peneliti ingin lebih lanjut melihat bagaimana perkembangan dan penanganan *cyber* Tiongkok dalam menghadapi keadaan yang sulit, serta kebijakan apa yang akan menjadi langkah tepat guna memperbaiki sistem *cyber* yang ada. Dalam pembahasan ini peneliti akan menggunakan kajian-kajian studi hubungan internasional yang secara tidak langsung sudah berkaitan dengan permasalahan di dalam penelitian ini.

1.2 Rumusan Masalah

Tiongkok untuk dapat mewujudkan kepentingannya banyak hal yang harus mereka lakukan, karena dengan dapat menguasai dunia maya, maka dapat dengan mudah Tiongkok mengontrol dan membaca pergerakan lawan. Sehingga memunculkan keuntungan yang dapat diperoleh Tiongkok dalam keseluruhan sektor, terutama dalam sektor ekonomi dan juga sektor kedaulatan mereka dalam menjadikan negara super power yang baru.

Berdasarkan latar belakang di atas, maka peneliti merumuskan satu permasalahan yang akan dibahas dalam penelitian yaitu:

“Bagaimana kebijakan Tiongkok dalam menghadapi cyber warfare pasca serangan Amerika Serikat pada tahun 2013?”

1.3 Tujuan Penelitian

Penulis memiliki dua tujuan dari penulisan ini adalah sebagai berikut:

1. Untuk mendeskripsikan kebijakan Tiongkok dalam menghadapi perkembangan dunia *cyber*; dan
2. Untuk menganalisis berbagai upaya menghadapi ancaman *cyber warfare*.

1.4 Manfaat Penelitian

Penulis berharap penelitian ini memiliki dua kegunaan.

1. Secara teoritis, penelitian ini diharapkan dapat menjadi referensi dan ilmu tambahan dalam fokus kajian Internasional. Dalam penerapan teori kebijakan publik, teori kebijakan luar negeri, dan konsep kepentingan nasional.
2. Secara praktis, penelitian ini diharapkan dapat memberikan pengetahuan dan wawasan bagi masyarakat, khusus pemerintah Indonesia untuk meningkatkan keamanan di *cyber*.

BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Penelitian mengenai kebijakan Tiongkok dalam menghadapi *cyber warfare* pasca serangan Amerika Serikat pada tahun 2013, secara eksplisit tidak ditemukan. Namun, terdapat peneliti yang mengerjakan topik serupa, dari unit analisis dan fokus penelitian, mempunyai kesamaan dengan penelitian yang dilakukan. Penelitian sebelumnya kemudian menjadi salah satu acuan penulis dalam mengkonstruksi kerangka berpikir dari rumusan masalah yang diteliti. Terdapat empat penelitian terdahulu yang dijadikan dasar dalam penelitian ini.

Penelitian pertama berjudul "Motivasi China menguasai cyber teknologi" ditulis oleh Nadya Vira Meisitha yang berasal dari jurnal Ilmu Hubungan Internasional, FISIP, Universitas Jember (UNEJ). Jenis pada penelitian ini ialah kualitatif dengan menggunakan pengumpulan data dan metode analisis data. Untuk teori atau konsep yang digunakan dalam penelitian ini yaitu menggunakan konsep keamanan nasional.

Tiongkok menjadi salah satu di antara beberapa negara pengguna teknologi modern yang sangat baik dalam tahap-tahapannya. Hal ini tidak lepas dari banyak proses yang mereka tempuh hingga saat ini. Motivasi Tiongkok dalam pengembangan dan penguasaan teknologi tidak lepas dari awal terjadinya aksi penyerangan Tiongkok kepada badan pertahanan Amerika Serikat beberapa tahun silam. Sebagaimana yang dijelaskan di dalam penelitian tersebut, Tiongkok melakukan serangan pertamanya pada 4 Mei 2001 (Nadya Vira Meisitha, 2014), yang membuat jaringan gedung putih mengalami lumpuh sesaat. Serangan itu ditujukan dengan menggunakan metode *attacking* DDoS (*distributed denial-of-service*). Sejak saat itu mulai banyak serangan cyber

yang ditargetkan kepada AS secara bertahap, sehingga menimbulkan beberapa penyidikan dan penelusuran terkait permasalahan tersebut. Amerika Serikat memastikan bahwasannya hal itu dilakukan oleh Tiongkok, dengan terus-menerus menunjukkan bukti Tiongkok sebagai dalang dari semua penyerangan tersebut.

Fokus pada penelitian ini untuk dapat membuktikan motivasi apa yang membuat Tiongkok ingin menguasai teknologi *cyber*. Terungkapnya motif utama Tiongkok bahwa mereka melakukan *cyber attack* guna memata-matai dan memproses data peralatan perang milik Amerika Serikat yang kemudian ditiru jenis pembuatan senjatanya, bahkan agar dapat lebih melampaui batas dari negara tersebut. Penelitian ini menjelaskan juga mengenai isu-isu yang menimbulkan awal mula konflik perang antara Tiongkok dan Amerika Serikat salah satunya adalah berkaitan dengan zona laut Tiongkok.

Penelitian ini Nadya menyimpulkan bahwa perang antara Tiongkok dengan Amerika Serikat diprediksikan akan terjadi di laut, atas potensi perang yakni isu-isu yang berada di wilayah laut Tiongkok. Karena Tiongkok harus memperketat strategi dengan membentuk aliansi jika perang benar terjadi.

Berkaitan dengan hal tersebut, peneliti menemukan bahwa di dalam penelitian ini masih kurang terperinci terkait dengan data-data teknologi *cyber* yang Tiongkok inginkan seperti halnya, berapa jumlah armada *cyber* yang akan dibuat Tiongkok atau adanya perkembangan hasil riset Tiongkok dengan berapa jumlah dana yang dikeluarkan untuk dapat merealisasikan kekuatan *cyber* yang ideal. Akan tetapi dalam penelitian ini, selaras dengan apa yang ingin peneliti gunakan terkait dengan keamanan nasional Tiongkok terhadap ancaman-ancaman yang ada di *cyberspace*.

Penelitian yang ke-dua yaitu berjudul “Penanganan *cyber attacks* oleh pemerintah Tiongkok melalui kebijakan network security tahun 2000-2015” ditulis oleh Nadia Talita Putri yang berasal dari jurnal Hubungan Internasional Fakultas Ilmu Sosial dan Ilmu Politik Universitas Udayana. Jenis pada penelitian ini ialah kualitatif dengan menggunakan analisa deskriptif. Teori atau konsep yang digunakan dalam penelitian ini menggunakan konsep *network security* dan konsep *cyber security cooperation*.

Keamanan jaringan *cyber* adalah salah satu prioritas utama dalam hal kenyamanan dan keamanan setiap para pengguna internet yang ingin melakukan hal apapun di dunia maya. Namun berjalannya waktu dan kegunaannya, dunia *cyber* tidak luput dari yang namanya tindakan kejahatan seperti halnya *cyber attack*. *Cyber attack* itu sendiri adalah gangguan yang dapat terjadi atas aktivitas jaringan komunikasi dan informasi digital maupun data di suatu negara dengan melalui target serangan kepada infrastruktur penting, seperti alat radio komunikasi, aliran listrik, kontrol limbah beracun, industri kimia, operasi komando militer, kontrol bursa saham negara, dan beberapa aktivitas umum untuk mengatur kebutuhan kehidupan pada warga negara (Nadia Talita Putri, 2017).

Berdasarkan hukum *network security*, upaya penanganan *cyber attack* yang dilakukan untuk kepentingan nasional pemerintah Tiongkok adalah melalui tahapan strategis, seperti membuat undang-undang dalam mengatur masyarakat untuk beberapa tindakan yang diperbolehkan seperti mengakses dan mengelola demi menjaga stabilitas keamanan, yang dikenal juga sebagai kontrol akses isolasi jaringan. Lembaga khusus dibentuk dan ditujukan hanya untuk mengatasi permasalahan *cyberspace* dan juga sebagai wadah pemberi sanksi bagi para pelaku yang melanggar aturan-aturan hukum dari *network security* seperti masyarakat sipil, pegawai, maupun departemen yang bertugas menjaga keamanan *cyber*.

Fokus penelitian ini terdapat pada bagaimana bentuk tahapan pemerintah Tiongkok untuk memproteksi jaringan informasi beserta data digital dari ancaman cyber attack domestik maupun internasional.

Kesimpulan dari penelitian ini, secara domestik pemerintah Tiongkok membentuk, (1) CCERT sebagai lembaga CERT nasional di bidang pendidikan, (2) CNCERT/CC sebagai lembaga monitoring, *early warnings*, dan *emergency responses nasional*, dan (3) polisi internet yang bertugas untuk menginvestigasi penyalahgunaan dan kejahatan TIK. Sedangkan secara internasional, melakukan diplomasi dan kerjasama atas dasar hukum dari *network security*, (1) membuat aturan legal (*legal measure*) untuk mengatur

cyberspace, (2) melakukan *sharing information*, dan (3) melakukan *capacity building*.

Terkait kesimpulan tersebut, peneliti akan menggunakan beberapa pendekatan diantaranya guna memperkuat data-data mengenai kebijakan Tiongkok.

Penelitian yang ke-tiga yaitu berjudul "Pengaruh *cyber security strategy* Amerika Serikat menghadapi ancaman *cyber warfare*" ditulis oleh Moehammad Yuliansyah Saputera yang berasal dari jurnal Jurusan Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Riau. Jenis pada penelitian ini ialah kualitatif dengan menggunakan pengumpulan data dan analisa deskriptif. Teori atau konsep yang digunakan dalam penelitian ini yaitu perspektif Konstruktivisme, teori Sekuritisasi dan teori Strategi.

Pada bagian penelitian ini, *cyber security strategy* Amerika Serikat sebagai pemilik dan penyedia teknologi informasi digital terbesar dunia, sangat baik dalam mengelola jaringan informasi dalam kehidupan sehari-hari. Tetapi dengan hadirnya teknologi tidak sepenuhnya berjalan dengan sempurna, terdapat sedikit banyak kekurangan dunia maya yang sewaktu-waktu dapat disusupi oleh individu, kelompok bahkan negara (Moehammad Yuliansyah Saputera, 2015).

Fokus penelitian ini adalah memberikan proteksi infrastruktur *cyber* dan dunia digital dalam negeri. Infrastruktur tersebut meliputi sektor layanan darurat, pemerintahan, publik, industri, swasta, pangkalan pertahanan, telekomunikasi, trasnportasi, perbankan, pos pengiriman, jaringan internet, bahan zat kimia, pusat energi, air dan layanan kesehatan masyarakat.

Kesimpulannya yaitu, perbedaan jumlah serangan *cyber* pada sektor pemerintah dengan sektor swasta dikarenakan proses tahapan selalu dimulai dan dikomando dari pemerintah pusat. Sehingga dapat dikatakan bahwa negara Amerika Serikat lemah, jika hanya dengan melalui tekanan serangan *cyber* negara mudah dikendalikan dan tidak patut lagi disebut sebagai negara *superpower*.

Terkait tinjauan pustaka ketiga, peneliti akan menggunakan metode tahapan yang sama seperti halnya rangkaian tata kelola pengembangan yang

dilakukan Amerika Serikat terhadap kualitas teknologi *cyberspace* yang mereka terapkan dalam menghadapi ancaman *cyber warfare*.

Penelitian yang ke-empat yaitu berjudul "*Warring State: China's Cybersecurity Strategy*" ditulis oleh Amy Chang (2014). Penelitian Chang ini menjelaskan perilaku kebijakan luar negeri Tiongkok termasuk kebijakan aktivitas dunia maya, terutama didorong oleh imperatif politik domestik untuk melindungi Partai Komunis Tiongkok (PKT). Dengan memastikan stabilitas domestik, integritas wilayah, modernisasi, dan pertumbuhan ekonomi, dan secara bersamaan mempersiapkan kemungkinan *cyber* konflik di masa depan. Dan pembahasan ini menggunakan konsep *network security*. Selain itu, penelitian ini juga memberikan pemahaman yang cukup baik dan terstruktur dalam menggambarkan karakteristik Tiongkok dari tahapan kebijakan hingga bentuk pola kerjasama yang direalisasikan dengan negara kompetitornya.

Fokus penelitian ini diantaranya terkait *stakeholders* di Tiongkok dalam kebijakan dan strategi *network security*. Dan Amy Chang menyimpulkan bahwa Tiongkok merumuskan strategi tetap untuk pemeliharaan kekuatan nasional. Dan Tiongkok sedang mengembangkan strategi keamanan jaringan dengan memiliki manifestasi ekonomi, politik, dan militer, dan sangat erat terkait dengan prioritas keamanan nasional lainnya seperti integritas wilayah, ketertiban politik dan sosial domestik, pertumbuhan ekonomi, dan modernisasi militer.

Pada penelitian ini, peneliti akan menggunakan beberapa pandangan Amy Chang seperti literature network security strategy guna melengkapi data-data Tiongkok dalam perkembangan Teknologi dunia maya.

Penulis membuat tabel agar mempermudah dalam melihat perbedaan dan kesamaan dari sejumlah penelitian terdahulu dengan penelitian ini, berikut adalah rangkaian tabel dari jenis penelitian, objek penelitian, konsep, teori, kesamaan dan kesimpulan dalam **Tabel 2.1**

Tabel 2.1 Perbandingan Penelitian Terdahulu

Penelitian Terdahulu	**Nadya Vira Meisitha (2014)**	**Nadia Talita Putri (2017)**	**Moehammad Yuliansyah Saputera (2015)**	**Amy Chang (2014)**
Topik Penelitian	*Motivasi China menguasai cyber teknologi*	*Penanganan cyber attacks oleh pemerintah Tiongkok melalui kebijakan network security tahun 2000-2015*	*Pengaruh cyber security strategy Amerika Serikat menghadapi ancaman cyber warfare*	*Warring State: China's Cybersecurity Strategy*
Jenis Penelitian	Kualitatif	Kualitatif	Kualitatif	Kualitatif
Objek Penelitian	Menentukan motivasi China untuk mendominasi *cyber* teknologi	Menggambarkan upaya untuk mengatasi serangan cyber oleh pemerintah Tiongkok melalui kebijakan keamanan jaringan	Pengaruh *cyber security strategy* Amerika Serikat menghadapi ancaman *cyber warfare*	Motivasi dan pandangan Tiongkok terhadap aktivitas *cyberspace* yang dilakukan oleh Amerika Serikat
Teori dan Konsep	Keamanan Nasional	Keamanan Nasional	Perspektif Konstruktivisme, Teori Sekuritisasi, dan Teori Strategi	Konsep *Network Security*
Kesimpulan	Perang antara China dengan Amerika Serikat diprediksikan akan terjadi di laut, atas potensi perang yakni isu-isu Taiwan, Semenanjung Korea dan Kepulauan Diayou	Memproteksi jaringan informasi serta data digitalnya, tidak lepas dari kontrol PKT dan prinsip Konfusian yang harmoni dan menerapkan *network security*	Amerika Serikat berhasil mengamankan data-data digital dari berbagai infrastruktur vital. Hal ini dapat dibuktikan dengan tidak adanya kepanikan besar (*big chaos*)	Tiongkok mengembangkan strategi keamanan jaringan dengan manifestasi ekonomi, politik, dan militer, dan sangat erat terkait dengan prioritas keamanan nasional

Sumber: diolah oleh peneliti

2.2 Landasan Konseptual

Penulis menganalisis penelitian ini dengan menggunakan beberapa konsep dan teori yang mampu untuk menjelaskan terkait kebijakan Tiongkok, diantaranya yaitu teori kebijakan publik, konsep kepentingan nasional dan teori kebijakan luar negeri.

2.2.1 Teori Kebijakan Publik

Kebijakan publik menurut Charles L. Cochran dan Eloise F.Malone (1995) yang dikutip oleh Irfan Islamy (2014) mengatakan bahwa, kebijakan publik adalah serangkaian keputusan politik dalam melaksanakan kepentingan dan program-program untuk memenuhi kebutuhan serta tujuan masyarakat. Kebijakan publik dirancang melalui sebuah tindakan yang diprogram dengan tampilan berupa tujuan yang akan dicapai, dengan contoh melakukan konservasi didalam kegiatan menggunakan seluruh data dan sumber yang diperlukan sehingga kegiatan dapat berjalan dengan baik dan seusai dengan tujuan hasil akhir yang diinginkan.

Larry N. Gerston (2002) mengungkapkan bahwa, kebijakan publik adalah kombinasi dari keputusan, komitmen dan tindakan yang dibuat dan dilaksanakan oleh mereka yang memegang kekuasaan dalam pemerintahan atau mempengaruhi pemerintahan. Artinya mereka yang mengambil keputusan harus memiliki komitmen yang kuat terhadap keputusannya, keputusan tersebut harus dibuat dengan benar, berisi substansi yang sangat baik mengenai kepentingan masyarakat, dan bersifat nyata bagi masyarakat umum.

Di dalam kutipan Irfan Islamy (2014), terdapat 10 macam kategori penggunaan istilah '*policy*' yang di jelaskan oleh Brian W. Hogwood dan Lewis A.Gunn (1984), yaitu:

1. *Policy as a label for afield of activity*. Kebijakan sebagai sebuah sebutan untuk medan atau wilayah kegiatan tertentu dan keterlibatan pemerintah dalam proses kebijakannya.
2. *Policy as an expression of general purposes or desired state of affairs*. Kebijakan merupakan pernyataan tentang tujuan dan keinginan negara secara umum. Pernyataan kebijakan sering kali disampaikan oleh pejabat negara misalnya eksekutif yang menyangkut hal-hal yang besar dan strategis.
3. *Policy as specific proposals*. Kebijakan publik dipandang sebagai usulan kegiatan atau tindakan yang akan diambil oleh pemerintah. Usulan kegiatan ini bisa bersifat adhoc (sementara).
4. *Policy as decisions of government*. Kebijakan publik sebagai keputusan yang dibuat oleh pemerintah. Kebijakan publik sebagian besar merupakan usulan pemerintah setelah memperhatikan dengan seksama adanya masalah yang sangat urgen dan menyentuh kepentingan rakyat banyak.
5. *Policy as formal authorization*. Kebijakan publik adalah merupakan salah satu bentuk produk dari kewenangan formal pemerintah untuk merumuskan, melaksanakan dan menilai kebijakan tersebut.
6. *Policy as programme*. Kebijakan publik sebagai program mempunyai arti bahwa kebijakan itu terdiri dari banyak program, atau dikatakan dengan kata lain bahwa program itu bagian dari kebijakan.
7. *Policy as output*. Kebijakan publik sebagai keluaran. Hal ini berarti bahwa kebijakan itu adalah merupakan produk dari proses mengubah "masukan" menjadi "keluaran" atau hasil.
8. *Policy as outcome*. Kebijakan publik sebagai dampak. Artinya, bahwa kebijakan publik yang telah dilaksanakan membuahkan dampak (pengaruh) baik yang positif maupun

negatif kepada pihak yang menjadi sasaran kebijakan tersebut.

9. *Policy as a theory or model*. Semua kebijakan mengandung asumsi tentang apa yang dilakukan pemerintah dan apa konsekuensi (dampak) dari tindakan pemerintah tersebut. Dan asumsi-asumsi tersebut membentuk teori kausalitas atau model sebab-akibat.
10. *Policy as process*. Kebijakan publik sebagai proses. Artinya, setiap kebijakan itu terdiri dari bermacam-macam kegiatan yang prosesnya menyangkut waktu yang panjang dan sangat kompleks.

Menyikapi dari keseluruhan tentang kebijakan publik, Hogwood dan Gunn (1984) menegaskan bahwa semua kebijakan publik didefinisikan secara subyektif oleh pengamat sesuai dengan kepentingan diri mereka sendiri, dan biasanya terdiri dari serangkaian pola pengambilan keputusan yang saling terkait dimana lingkungan, individu, kelompok, dan organisasi memiliki pengaruh yang signifikan.

2.2.2 Konsep Kepentingan Nasional

Penelitian ini menggunakan konsep kepentingan nasional yang dimana dalam diskursus politik internasional, konsep kepentingan nasional dapat digunakan di dua hal berbeda. Pertama, kepentingan nasional digunakan sebagai *shape political behaviour* (pembentukan perilaku politik), sebagai cara untuk mempertahankan, menentang atau mengajukan kebijakan-kebijakan politik. Kedua, kepentingan nasional digunakan oleh mahasiswa hubungan internasional sebagai alat analisis untuk menggambarkan, menjelaskan, dan menilai kelayakan kebijakan luar negeri suatu negara (Scott Burchill, 2005: 23).

Morgenthau mengatakan bahwa, kepentingan nasional adalah suatu upaya negara untuk mencapai dan mengembangkan power dalam dunia internasional. Morgenthau menyatakan bahwa kepentingan nasional setiap

negara adalah mengejar kekuasaan, yaitu apa saja yang bisa membentuk dan mempertahankan pengendalian suatu negara atas negara lain. Hubungan kekuasaan atau pengendalian ini bisa diciptakan melalui teknik-teknik paksaan maupun kerjasama (Mohtar Mas'oed, 1994: 140).

Donald E. Nuechterlein mendefinisikan kepentingan nasional sebagai kebutuhan dan keinginan suatu negara berdaulat untuk bekerjasama dengan negara berdaulat lainnya berdasarkan pertimbangan lingkungan eksternal. Definisi ini menguraikan perbedaan antara lingkungan eksternal dan internal suatu negara. Lingkungan internal diartikan sebagai kepentingan umum rakyat negara, sedangkan lingkungan eksternal adalah pengaruh dari sistem internasional. Donald juga mengungkapkan bahwa kepentingan suatu negara bangsa berarti kepentingan kesuluruhan masyarakat dan bukan hanya kepentingan kelompok dan elit-elit politik (Donald E Nuechterlein, 1976: Vol 2). Lalu Donald E. Nuechterlein menjelaskan bahwa terdapat 4 basic national interest yaitu sebagai berikut:

(i) *Defence interests* (kepentingan pertahanan) : Kepentingan untuk memberikan perlindungan kepada warga negara, wilayah serta ancaman kekerasan fisik yang berasal dari negara lain dan ancaman eksternal terhadap sistem pemerintahan.

(ii) *Economic interests* (kepentingan ekonomi) : Kepentingan negara dalam menjalin hubungan ekonomi yang baik dengan negara lain demi peningkatan kesejahteraan.

(iii) *World Order interests* (kepentingan tatanan dunia) : Kepentingan mempertahankan kestabilan sistem politik internasional dan sistem ekonomi internasional yang memberikan keuntungan bagi negara.

(iv) *Ideological interests* (kepentingan ideologi): Kepentingan untuk mempertahankan atau melindungi ideologi negaranya dari ancaman ideologi negara lain.

Kepentingan nasional dapat di simpulkan sama dengan usaha negara untuk mengejar power atau kekuasaan, dimana power ini bertujuan untuk mendapatkan segala sesuatu dalam mengontrol dan mempertahankan satu negara atas yang lain. Kepentingan nasional juga merupakan interaksi yang dilakukan oleh negara untuk memenuhi kebutuhan yang seharusnya mereka penuhi, dengan menggunakan kekuasaan sebagai bentuk realisasinya. Hubungan internasional digunakan sebagai wadah untuk memajukan kepentingan nasional bangsa-bangsa dengan menggunakan kekuatan dan kekuasaannya. Sehingga dapat dengan mudah suatu negara menguasai sektor-sektor yang di-inginkan melalui besarnya jangkauan kekuasaan yang dapat mempengaruhi berbagai kebijakan.

2.2.3 Teori Kebijakan Luar Negeri

Kebijakan luar negeri adalah strategi atau rencana tindakan yang secara khusus dirumuskan oleh para pengambil keputusan negara dalam hubungannya dengan negara lain atau entitas politik internasional, dan dikendalikan untuk mencapai tujuan nasional tertentu, sebagaimana dinyatakan dalam istilah kepentingan nasional. Oleh karena itu, untuk memenuhi kepentingan nasionalnya, negara-negara dan aktor-aktor di dalamnya melakukan berbagai bentuk kerjasama, antara lain kerjasama bilateral, trilateral, regional dan multilateral. Plano dan Olton berpendapat bahwa semua kebijakan luar negeri dirancang untuk mencapai tujuan nasional. Tujuan nasional yang ingin dicapai melalui politik luar negeri merupakan formula khusus dan dirancang dengan menyelaraskan kepentingan nasional dengan situasi internasional saat ini dan menggunakan kekuatan yang dimiliki untuk mencapainya (Perwita & Yani, 2005: 49-51).

K.J. Holsti mendefiniskan kebijakan luar negeri sebagai suatu tindakan dan gagasan, yang dirancang oleh pembuat kebijakan untuk memecahkan masalah atau mempromosikan suatu perubahan dalam

lingkungan, yaitu dalam kebijakan, sikap atau tindakan negara lain (K.J. Holsti, 1988: 136). Sedangkan menurut Robert Jackson dan Georg Sorensen memaknai kebijakan luar negeri sebagai tujuan-tujuan dan tindakan tindakan yang dimaksudkan untuk memandu keputusan dan tindakan pemerintah menyangkut urusan-urusan eksternal, terutama hubungan dengan negara lain (Georg Sorensen, 2013: 262). Sehingga dapat disimpulkan bahwa kebijakan luar negeri adalah upaya suatu negara dalam menjalin hubungannya dengan negara lain guna terciptanya kepentingan nasional.

K.J. Holsti mengemukakan bahwa terdapat tujuan khusus negara dalam kebijakan luar negerinya dengan menggunakan tiga kategori yaitu:

(i) Tujuan inti: Tujuan inti dari kebijakan luar negeri adalah menjamin kedaulatan dan kemerdekaan wilayah nasional dan mengekalkan sistem politik, sosial dan ekonomi tertentu berdasarkan wilayah itu (K.J. Holsti, 1988).

(ii) Tujuan Jangka Menengah:

1. Mencakup usaha pemerintah memenuhi tuntutan dan kebutuhan perbaikan ekonomi melalui tindakan internasional. Kesejahteraan sosial dan pembangunan ekonomi merupakan tujuan utama dari pemerintahan suatu negara.
2. Meningkatkan prestise negara dalam sistem. Prestise diukur dengan tingkat perkembangan industri dan keterampilan ilmiah serta teknologi.
3. Mencakup banyak bentuk perluasan diri atau imperialisme. Negara melakukan perluasan wilayah, walaupun wilayah tersebut tidak memiliki kepentingan strategis, ekonomi dan sosial

(iii) Tujuan Jangka Panjang: Tujuan ini berisi rencana, impian dan pandangan mengenai organisasi politik atau ideologi terakhir sistem internasional, aturan yang mengatur hubungan dalam sistem itu dan peran negara tertentu di dalamnya.

2.3 Kerangka Pemikiran

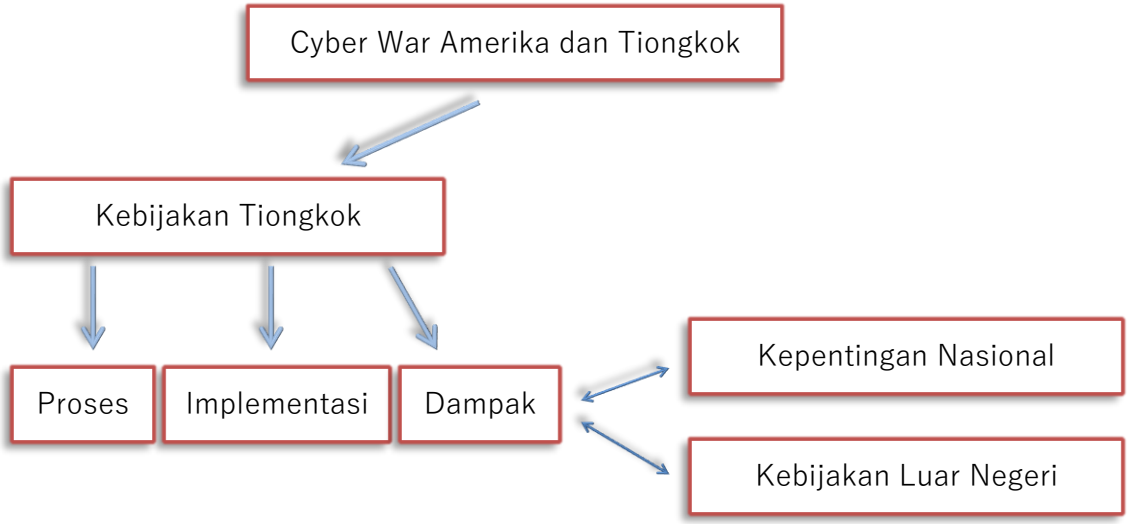
Teknologi semakin pesat perkembangannya dan membuat negara-negara di dunia berlomba-lomba dalam kemajuan teknologi. Hal ini menimbulkan adanya sisi negatif dari persaingan yang ada, sehingga muncul yang namanya kejahatan dunia maya. Karena hal ini terjadi diawali dari individu ke kelompok dan negara menggunakannya untuk kepentingan yang secara menyeluruh. Seperti untuk kemajuan ekonomi, keamanan, dan pada akhirnya untuk menjadi negara yang sangat kuat dan paling dominan dari setiap kemajuan melalui teknologi *cyber*.

Tiongkok secara garis besar di dalam penelitian ini mengalami motivasi khusus untuk dapat memperbaiki keadaan dunia maya nasionalnya guna mencapai kekuatan baru di dunia modern saat ini. Oleh karena itu Tiongkok rela melakukan perubahan besar terkait dengan jaringan teknologi *cyber*, karena dengan dapat menguasai dunia maya Tiongkok akan lebih leluasa mengontrol perkembangan cyberspace global. Sehingga keamanan nasional Tiongkok dapat dengan mudah teratasi jika mereka memiliki banyak "perlengkapan" perang di dunia maya.

Kerangka berfikir dimulai dengan pembahasan serangan yang dilakukan Amerika Serikat terhadap Tiongkok pada tahun 2013 beserta data yang sesuai, lalu menjelaskan mengenai langkah-langkah dan kebijakan Tiongkok dalam menangani kasus serangan tersebut. Dengan melalui berbagai kebijakan luar negeri sebagai landasan kepentingan Tiongkok dalam tatanan global.

Pada penelitian tersebut, peneliti akan menggunakan 3 tahapan utama dalam merumuskan kebijakan-kebijakan yang akan dilakukan Tiongkok dalam penanganan teknologi dunia maya. Tahapan itu di antaranya ialah dengan tahapan proses kebijakan, implementasi kebijakan dan dampak kebijakan yang pemerintah lakukan. Ketiga elemen tersebut akan peneliti gunakan dari total 10 elemen yang dikemukakan oleh Brian W. Hogwood dan Lewis A.Gunn (1984).

Untuk mempermudah dalam menjawab pertanyaan penelitian, maka berikut merupakan kerangka pemikiran dalam penelitian ini:



Gambar 1.1 Kerangka Berpikir

Sumber: Diolah Oleh Peneliti

BAB III
METODOLOGI PENELITIAN

3.1 Metode Penelitian

Penelitian ini penulis akan menggunakan tipe penelitian kualitatif deskriptif untuk memahami langkah-langkah dan kebijakan Tiongkok dalam mengendalikan teknologi *cyber*. Di dalam penelitian kualitatif bertujuan untuk dapat memahami fenomena tentang apa yang dialami subjek penelitian, baik dalam perilaku, persepsi, motivasi maupun tindakannya secara deskripsi dalam bentuk kata-kata dan bahasa. Penelitian ini menggunakan desain studi kasus deskriptif agar dapat memperoleh informasi dari data penelitian secara menyeluruh, luas, dan mendalam. Tipe penelitian kualitatif deskriptif akan signifikan dalam menganalisis masalah pada penelitian ini berdasarakan karakteristik yang diungkapkan oleh Creswell (2014: 189-191) yaitu di antaranya ialah, penelitian kualitatif dalam teknik pengumpulan datanya di ajukan, di mana peneliti tersebut mengalami permasalahan yang ingin diteliti lebih lanjut. Lalu menggunakan berbagai macam data yang dapat diperoleh melalui dokumentasi, observasi maupun secara informasi *audiovisual*.

Metode kualitatif menekankan pada pencarian makna di balik realitas empiris dari realitas sosial yang sudah ada sebelumnya sehingga dapat dicapai pemahaman yang mendalam tentang realitas sosial. Karena penelitian kualitatif menjadi lebih mudah dipahami sebagai suatu metode, datanya dapat berupa pernyataan, dan data yang dihasilkan dapat berupa data deskriptif tentang subjek penelitian, yaitu dalam bentuk kata-kata tertulis dan lisan (Matthew, 1992: 15).

3.2 Fokus Penelitian

Pada penelitian ini akan berfokus pada 3 tahapan utama dalam merumuskan kebijakan-kebijakan yang akan dilakukan Tiongkok dalam penanganan teknologi dunia maya. Tahapan itu di antaranya ialah:

1. Proses : Tahapan dalam perancangan pembuat kebijakan, dengan melibatkan para petinggi, pejabat negara dan warga negara.
2. Implementasi : Pembentukan, dan pelaksanaan dari kebijakan yang telah di terapkan dalam jangka waktu yang sudah ditentukan.
3. Dampak : Kebijakan yang sudah pemerintah lakukan dapat menghasilkan dampak positif dan dampak negatif dari kebijakan tersebut, serta apakah kebijakan itu berhasil atau tidak berhasil dalam pelaksanaannya.

3 tahapan tersebut dapat membantu melihat perkembangan Tiongkok dalam upaya melakukan strategi kebijakan khusus untuk membekali negaranya agar dapat bersaing dan memenuhi kebutuhan lain seperti menggapai kepentingan tertentu baik dari sektor utama perekonomian negara maupun dalam sektor keamanan teritorialnya.

3.3 Jenis dan Sumber Data

Jenis data yang digunakan dalam penelitian ini adalah jenis data sekunder. Adapun data yang dicari merupakan data mengenai Kebijakan dan langkah strategis Tiongkok dalam mengelola keamanan cyber nasionalnya. Peneliti memperoleh data tersebut melalui sumber-sumber baik berupa jurnal-jurnal ilmiah, buku, laporan tertulis, situs internet dan dokumen-dokumen berkaitan dengan objek penelitian (Bakry, 2016: 17).

Sumber data yang digunakan yaitu salah satunya ialah *The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies.* Dan situs resmi penanganan *cyber* Tiongkok "*Office of the Central Cyberspace Affairs Commission / Cyberspace Administration of China*" http://www.cac.gov.cn/

3.4 Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini ialah dengan menggunakan cara studi pustaka dan studi dokumentasi. Studi pustaka adalah adalah teknik pengumpulan data yang mengkaji literatur dari buku-buku fisik dan non-fisik dengan tema-tema yang memuat kasus-kasus tertentu atau tentang kronologis kejadian (Earl, 2014: 490-496). Dalam hal ini penulis berkunjung ke perpustakaan fakultas dan juga perpustakaan universitas dan mengakses *e-book* maupun jurnal online. Dan studi dokumentasi adalah berkaitan dengan data yang tidak dipublikasikan secara umum. Sehingga dengan melalui studi tersebut data yang akan didapatkan cenderung lebih spesifik dan informasi yang didapat lebih kompleks. Seperti halnya mengakses langsung laman resmi pemerintah Tiongkok yang menangani sektor keamanan dunia maya, yaitu:

1. http://www.cac.gov.cn/
2. https://www.cert.org.cn/

3.5 Teknik Analisis Data

Berdasarkan metode studi pustaka yang digunakan peneliti, maka analisis data yang digunakan oleh peneliti adalah teknik analisis data model Miles & Huberman (1994) dalam Sugiyono (2014: 247-249) yaitu:

1. Kondensasi data pada penelitian kualitatif merupakan proses menyederhanakan, memproses, mengabstraksi, menyeleksi,

serta mentransformasi atau pergantian data yang terdapat pada dokumen, data empiris, transkip dan catatan lapangan.

2. Penyajian data, data yang telah melalui proses reduksi dapat ditampilkan dalam bentuk berupa catatan lapangan, grafik, bagan, matrik, jaringan, bagan, dan tabel untuk memudahkan penelitian.
3. Penarikan kesimpulan / Verfikasi, Hal ini dilakuakan sebagai tahapan akhir peneliti dalam memaparkan temuan baru yang sebelumnya belum pernah ada, serta deskripsi atau gambaran objek yang sebelumnya masih bias.

BAB V
SIMPULAN DAN SARAN

5.1 Simpulan

Kebijakan Tiongkok dalam menghadapi *cyber warfare* pasca serangan Amerika Serikat tahun 2013 dapat dilihat melalui 2 tahapan yaitu proses implementasi pembuatan kebijakan dan dampak. Tahapan dari proses dan implementasi menghadirkan kepentingan nasional serta kebijakan luar negeri Tiongkok, yang dimana dengan disahkannya undang-undang untuk memperkuat keamanan *cyber* dalam negeri, menjadikan masyarakat lebih aman dan nyaman untuk dapat mengakses internet tanpa harus khawatir data pribadi dicuri dan disalahgunakan, sesuai dengan pendapat Morgenthau bahwa, kepentingan nasional adalah bentuk upaya negara untuk memperoleh dan mengembangkan kekuasaan di dunia internasional. Robert Jackson dan Georg Sorensen mengungkapkan bahwa kebijakan luar negeri adalah tindakan yang memiliki unsur tujuan tertentu yang artikan sebagai alat untuk memandu setiap keputusan pemerintah dalam menyangkut urusan-urusan eksternal, seperti menjalin kerjasama antar negara.

Pemerintah Tiongkok menyikapi permasalahan luar negeri dengan mengupayakan kerjasama ataupun melalui serangkaian negosiasi untuk dapat tercapainya tujuan-tujuan yang diinginkan, akan tetapi malah menimbulkan dampak yang kurang baik, karena pada tahap ini kebijakan luar negeri antara Tiongkok dan Amerika Serikat tidak patuh dan tunduk dengan yang telah disepakati, kedua negara malah tetap melanjutkan tujuan-tujuan dan kepentingan negaranya masing-masing dengan melakukan serangkaian serangan *cyber*, seperti spionase maupun pencurian kekayaan intelektual. Pemerintah Tiongkok juga mendapatkan dampak terkait kebijakan nasionalnya, mengingat jika

masyarakat ingin aman dan nyaman dalam melakukan aktifitas di dunia maya, maka pemerintah Tiongkok menggunakan karya dalam negeri sebagai kendaraan mandiri negara tersebut, yaitu dengan didorongnya "*Baidu*" sebagai mesin pencari utama untuk menggantikan "*Google*", sehingga masyarakat tidak mudah untuk dapat mengakses dunia internasional. Tidak hanya itu, organisasi global ikut berdampak dengan kebijakan yang Tiongkok terapkan, data-data yang diperlukan untuk mengakses dan menggambarkan situasional negara menjadi lebih tertutup dan tidak efektif.

5.2 Saran

Hasil penelitian menunjukkan bahwa kebijakan Tiongkok yang menggunakan "*Baidu*" sebagai mesin pencari utama adalah tindakan yang tepat jika untuk kepentingan dalam negeri, namun tidak untuk sudut pandang dunia internasional karena Tiongkok sulit untuk ditinjau lebih detail terkait data maupun fakta yang ingin diperoleh oleh masyrakat global. Pemerintah Tiongkok telah menciptakan jaringan internet yang cukup kuat dan dapat dikendalikan secara mandiri oleh negara tanpa harus mengandalkan bantuan negara asing, tetapi Tiongkok harus meyakinkan bahwa mereka layak bersaing dalam dunia internet yang dikelola mandiri untuk menggapai kesepakatan kerjasama dan berhubungan baik dengan dengara lain.

Harapan penelitian ini bisa bermanfaat dan dilanjutkan agar dapat ditemukan konsep baru maupun tujuan lebih lanjut dari serangkaian kebijakan Tiongkok. Hendaknya peneliti selanjutnya lebih untuk mengembangkan ruang lingkup penelitian, mengingat penelitian ini belum sepenuhnya menjabarkan tentang dana yang digunakan dalam pelaksanaan kebijakan.

DAFTAR PUSTAKA

Buku

A.A, Perwita., & Y. M., Yani., (2005). "Pengantar Ilmu Hubungan Internasional". Bandung: PT Remaja Rosdakarya.

Babbie, Earl. 2014. The Basics of Social Research. Wadsworth, Cengage Learning. Wadsworth.

Bakry, Suryadi U. 2016. Metode Penelitian Hubungan Internasional. Pustaka Pelajar.

Balke, Liudmyla (2018). China's New Cybersecurity Law and U.S-China Cybersecurity Issues. 58 Santa Clara L. Rev. 137.

Branscomb, Anne W., ed., 1986. Toward A Law of Global Communication Network. New York: Longman.

Burchill, Scott. 2005. The National Interest inInternational Relations Theory. Palgrave Macmillan. New York.

Chang, Amy (2014). Warring State: China's Cybersecurity Strategy. New American Security.

Creswell, W John. 2014. Research Design: qualitative, quantitative, and mixed method approaches, 4th, New York: SAGE Publication, Inc.

Daras, J. Nicholas. 2019. Cyber Security and Information Warfare, New York: Nova Science Publishers, Inc.

Graham H. Todd, (2009). Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition. Air Force Law REV. 65, vol 64.

Gregory J. Touhill and C. Joseph Touhill (2014). Cybersecurity for Executives, A Practical Guide. New Jersey: Published by John Wiley & Sons, Inc.

Guion, Lisa A. 2002. Triangulation: Establishing the Validity of Qualitative Studies. University of Florida. Florida.

ITU. (2008). Overview of cybersecurity, Recommendation ITU–T X.1205 (http://tinyurl.com/boys7dj). The ITU Plenipotentiary Conference 2010 held in Guadalajara, Mexico, approved the definition of cybersecurity.

J.-F. Kremer and B. Müller (eds.), 2014. Cyberspace and International Relations. Heidelberg: Springer-Verlag.

Janczewski, Lech J & Andrew M. Colarik (2008): Cyber Warfare and Cyber Terrorism, IGI Global

Kshetri, N. (2014). Cybersecurity and International Relations: The U.S. engagement with China and Rusia.

Kshetri, N. (2016). The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies. Springer

Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. In F. D. Kramer, S. Starr, & L. K. Wentz (Eds.), Cyberpower and national security (p. 38). Washington, DC: Center for Technology and National Security, National Defense University.

Lieberthal, K., & Singer, P. W. (2012). Cybersecurity and U.S.-China Relations. Brookings: The John L. Thornton China Center and the 21st.

Lindsay, Jon. R (2015). China and Cyber Security: Espionage, Strategy, and Politics in the Digital Domain. Oxford University.

Mas'oed, Mohtar. 1994. Ilmu Hubungan Internasional Displin dan Metodologi. Pustaka LP3ES Indonesia. Jakarta.

Nuechterlein, Donald E. 1976. National Interests and Foreign Policy: A Conceptual Framework for Analysis and Decision-Making. British Journal of International Studies. Vol 2.

Sorensen, Georg & Robert Jackson. 2013. Introduction Tointernational Relations Theories And Approaches Fifth Edition. Oxford University Press Inc. New York.

Springer, J. Paul 2017. Encyclopedia of Cyber Warfare. ABC-CLIO, LLC. Denver, Colorado.

Sugiyono, 2014. Metode Peneliteian Kuantitatif, Kualitatif dan R&D. Alfabeta. Bandung.

Sun Tzu, The Art of War.
Nine99 Innovation Lab (OPC) Pvt Ltd, 1 Jul 2019.

Thayer, A. Bradley (2015). Deterring Cyber Warfare.
Palgrave Macmillan. New York.

Wortzel M. Larry, (2014). China's Military Modernization and Cyber Activities. Strategic Studies Quarterly, Vol. 8, No. 1.

Jurnal dan Skripsi

Dewi, Noviana. 2016. "Bahaya Kecanduan Internet dan Kecemasan Komunikasi terhadap Karakter Kerja Sama pada Mahasiswa". Jurnal Psikologi UGM. Volume 43, Nomor 3.

Islamy, Irfan. "Definisi dan Makna Kebijakan Publik". ADPU4410 / Modul 1, dalam http://repository.ut.ac.id/3993/1/ADPU4410-M1.pdf, di akses pada 2 November 2019

Meisitha, Nadya Vira. 2014. "Motivasi China menguasai cyber teknologi". Jurnal Ilmu Hubungan Internasional. Universitas Jember.

Putri, Nadia Talita. 2017. "Penanganan cyber attacks oleh pemerintah Tiongkok melalui kebijakan network security tahun 2000-2015". Jurnal Ilmu Hubungan Internasional. Universitas Udayana.

Saputera, Moehammad Yuliansyah. 2015. "Pengaruh cyber security strategy Amerika Serikat menghadapi ancaman cyber warfare". Jom FISIP Hubungan Internasional Volume 2 No.2. Universitas Riau.

Situs Resmi

Center For Strategic & International Studies (CSIS), "Significant Cyber Incidents", dalam https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents, di akses pada 7 Februari 2020.

Chinadaily, "China 'biggest victim' of cyber attacks", dalam http://www.chinadaily.com.cn/china/2010-01/25/content_9368402.htm, di akses pada 24 September 2018.

Chinadaily, "China is victim of hacking attacks", dalam http://www.chinadaily.com.cn/china/2013-06/05/content_16567174.htm, di akses pada 3 Oktober 2018.

CNCERT (China National Computer Network Emergency Response Technical Team), "Annual report 2013" dalam

https://www.cert.org.cn/publish/english/115/2014/20140612094831200399105_.html, di akses pada 3 Oktober 2018.

CNCERT (China National Computer Network Emergency Response Technical Team), "Annual report 2017" dalam https://www.cert.org.cn/publish/english/115/2018/2018041008343902511 9420/20180410083439025119420_.html, di akses 15 November 2019.

International Comparative Legal Guides (ICLG), "Cybersecurity Laws and Regulations China", dalam https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/china, di akses pada 27 November 2020.

International Telecommunication Union (ITU), "Global Cybersecurity Index", dalam https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx, di akses pada 11 Desember 2019.

KPMG, "Overview of China's Cybersecurity Law 2017", dalam https://home.kpmg/cn/en/home/insights/2017/02/overview-of-chinas-cybersecurity-law.html, di akses pada 8 November 2019.

Miniwatts Marketing Group, "World Internet Usage and Population Statistics 2019", dalam https://www.internetworldstats.com/stats.htm, di akses pada 10 November 2019.

NPC China, "Cybersecutiry law of the People's Republic of China", dalam http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm, di akses pada 14 September 2020.

Supreme People's Court, "Criminal law of the People's Republic of China", dalam http://english.court.gov.cn/2015-12/01/content_22595464_26.htm, di akses pada 14 September 2020.

Trivium China, "Intro to China's policymaking process", dalam https://triviumchina.com/2018/09/03/an-intro-to-chinas-policymaking-process/, di akses pada 24 Juni 2020.

Wallace, I. 2013. The Military Role In National Cybersecurity Governance. Brookings, dalam https://www.brookings.edu/opinions/the-military-role-in-national-cybersecurity-governance/ di akses pada 11 Maret 2019.