DIALOG KEAMANAN SIBER AMERIKA SERIKAT-TIONGKOK GUNA PENANGGULANGAN KEJAHATAN SIBER 2018-2022

(Skripsi)

Oleh

MUHAMMAD MUHAGAM

NPM 1816071045

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

2024

ABSTRAK

DIALOG KEAMANAN SIBER AMERIKA SERIKAT-TIONGKOK GUNA PENANGGULANGAN KEJAHATAN SIBER 2018-2022

Oleh

Muhammad Muhagam

Cyber security mulai menjadi perhatian PBB pada tahun 1998, pada saat Rusia pertama kalinya memberikan draf resolusi mengenai *cyber security* dan di ikuti oleh negara-negara lain, termasuk Amerika Serikat dan Tiongkok yang juga menjalin kesepakatan agar setiap negara wajib mematuhi hukum internasional dalam *cyber security*. Pemerintah Amerika Serikat dan Tiongkok menjalin dialog untuk secara bersama-sama melakukan penanggulangan kejahatan *cyber* yang terus meningkat.

Penelitian ini menggunakan pendekatan kualitatif dengan analisis deskriptif, untuk mendeskripsikan dialog keamanan Amerika Serikat Dengan Tiongko guna penanggulangan kejahatan *cyber* 2018-2022. Dengan menggunakan teknik studi literatur, berbagai sumber data, utamanya dari laman resmi dan sumber-sumber terkait lainnya, dianalisis dengan metode analisis interstate. Data tersebut kemudian dianalisis menggunakan kondensasi data, penyajian data dan penarikan kesimpulan.

Hasil dari penelitian ini menunjukkan bahwa kerja sama keamanan *cyber* yang dilaksanakan oleh Amerika Serikat dengan Tiongkok guna penanggulangan kejahatan *cyber* dilakukan melalu berbagai forum dialog untuk mengangkat isu-isu *cyber* termasuk permasalahan kerugian akibat kejahatan *cyber*. Aktivitas dialog yang dilakukan oleh Amerika Serikat dengan Tiongkok terbagi menjadi dua bentuk, yaitu dialog sebelum tercapainya kesepakatan *cyber security* antara Amerika Serikat dengan Tiongkok, keduanya berupaya untuk menyamakan pandangan dalam forum *US-China Cyber security Dialogue* dan .*S.-China High-Level Joint Dialogue on Cybercrime and Related Issues* didalamnya terdapat sebuah *cyber working group* yang dikhususkan untuk membahas permasalahan *cyber space* guna penanggulangan kejahatan *cyber*.

Kata Kunci: Dialog, Keamanan, Kejahatan, *Cyber*

ABSTRACT

UNITED STATES CYBER SECURITY DIALOGUE WITH CHINA TO OVERCOME CYBER CRIME 2018-2022

By

Muhammad Muhagam

Cyber security began to come to the attention of the UN in 1998, when Russia first submitted a draft resolution regarding cyber security and followed by other countries, including the United States and China, which also entered into an agreement that every country is obliged to comply with international law cyber security. The governments of the United States and China are establishing dialogue to jointly combat crime cyber which continues to increase.

This research uses a qualitative approach with descriptive analysis, to describe A's security dialogueiAmericai Governmentit Listenin China to tackle cyber crime 2018-2022. Using literature study techniques, various data sources, mainly from official websites and other related sources, were analyzed using the interstate analysis method. The data is then analyzed using data condensation, data presentation and drawing conclusions.

The results of this research show that the cyber security cooperation carried out by the United States and China to tackle cyber crime is carried out through various dialogue forums to raise cyber issues, including the problem of losses due to cyber crime. Dialogue activities carried out by the United States and China are divided into two forms, namely dialogue before reaching a cyber security agreement between the United States and China, both of which seek to equalize views in the US-China Cyber security Dialogue and S.S.-China High-Level Joint forums. Dialogue on Cybercrime and Related Issues includes a cyber working group specifically to discuss cyber space issues in order to tackle cyber crime

Keywords: *Dialogue, Security, Crime, Cyber*

DIALOG KEAMANAN SIBER AMERIKA SERIKAT-TIONGKOK GUNA PENANGGULANGAN KEJAHATAN SIBER 2018-2022

Oleh

MUHAMMAD MUHAGAM

NPM 1816071045

Skripsi

Sebagai Salah Satu Syarat untuk Mencapai Gelar

SARJANA HUBUNGAN INTERNASIONAL

Pada

Jurusan Hubungan Internasional

Fakultas Ilmu Sosial dan Ilmu Politik

JURUSAN HUBUNGAN INTERNASIONAL
FAKULTAS ILMU SOSIAL DAN ILMU POLITIK
UNIVERSITAS LAMPUNG
2024

Judul Skripsi	:	**DIALOG KEAMANAN SIBER AMERIKA SERIKAT-TIONGKOK GUNA PENANGGULANGAN KEJAHATAN SIBER 2018-2022**
Nama Mahasiswa	:	*Muhammad Muhagam*
Nomor Pokok Mahasiswa	:	**1816071045**
Jurusan	:	**Hubungan Internasional**
Fakultas	:	**Ilmu Sosial dan Ilmu Politik**

MENYETUJUI,

1. Komisi Pembimbing

Iwan Sulistyo, S.Sos., M.A.
NIP. 198604282015041004

Roby Rakhmadi, S.Sos., M.Si.
NIP. 199006062019031019

2. Ketua Jurusan Hubungan Internasional

Simon Sumanjoyo Hutagalung, S.A.N., M.P.A.
NIP. 19810628 200501 1 003

MENGESAHKAN

1. Tim Penguji

   Ketua : **Iwan Sulistyo, S.Sos., M.A.** .....

   Sekretaris : **Roby Rakhmadi, S.Sos., M.Si.** .....

   Penguji Utama : **Gita Karisma, S.IP., M.Si** .....

2. Dekan Fakultas Ilmu Sosial dan Ilmu Politik

Dra. Ida Nurhaida, M.Si.
NIP. 19610807 198703 2 001

Tanggal Lulus Ujian Skripsi : **16 Juli 2024**

PERNYATAAN

Dengan ini saya menyatakan bahwa

1. Karya tulis saya, skripsi ini adalah asli dan belum pernah diajukan untuk mendapatkan 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 disebutkan nama pengarang dan dicantumkan dalam daftar pustaka
4. Pernyataan ini saya buat dengan sesungguhnya dan apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah berlaku di Universitas Lampung.

Bandar Lampung, 16 Juli 2024

Yang membuat pernyataan,

Muhammad Muhagam

NPM.1816071045

RIWAYAT HIDUP

Muhammad Muhagam lahir pada tanggal 6 November 2000 di Bandar Lampung, seorang anak bungsu dari Affandi dan Maria. Bersaudara kandung dengan kakaknya yakni Muhammad Mugadam yang lahir pada tahun 1997.

Penulis memulai edukasinya di TK Mutiara Adinda Bandar lampung dan lulus pada tahun 2006. Memasuki SDN 2 Sawah Lama dan pindah ke SD 2 Kartika Jaya lulus pada tahun 2012. Melanjutkan ke SMP AR-Raihan lulus pada tahun 2015, dan kemudian melanjutkan edukasinya di SMAN 2 Bandar Lampung dan selesai pada tahun 2018 di tahun yang sama, dirinya diterima di jurusan Hubungan Internasional Fakultas Ilmu Sosial dan Ilmu Politik Universitas Lampung.

Pada tahun 2019, penulis aktif dalam berorganisasi di kampus dari keikutsertaannya dalam kepanitiaan acara ataupun di dalam himpunan jurusannya sendiri, pada tahun 2020 penulis juga menyelesaikan program KKN di Bumi Kedamaian, Bandar Lampung. Dari tahun 2021. Selain melaksanakan aktivitas perkuliahan penulis juga bekerja dengan perusahaan-perusahaan luar negeri yang berfokus di Amerika Serikat hingga saat ini dengan memegang tanggung jawab di tiga perusahaan yang berbasis di Amerika Serikat secara bersamaan.

MOTTO

If you don't believe you are the best, then you will never achieve all that you are capable of
"Cristiano Ronaldo"

PERSEMBAHAN

Dengan menyebut nama Allah Yang Maha Pengasih lagi Maha Penyayang,
Kupersembahkan skripsi ini untuk:

"Keluargaku"

Ayah dan Bunda, Serta Keluarga Besarku

Sebagai wujud rasa terima kasihku yang telah memberi motivasi serta semangat untuk terus pantang menyerah dalam melakukan sesuatu dan bangkit dari kegagalan. Terima kasih atas dukungan sehingga aku dapat menyelesaikan skripsi ini.

SANWACANA

Puji syukur penulis ucapkan atas kehadirat Allah SWT, karena berkat rahmat dan hidayah-Nya penulis dapat menyelesaikan skripsi dengan judul "*DIALOG KEAMANAN SIBER AMERIKA SERIKAT-TIONGKOK GUNA PENANGGULANGAN KEJAHATAN SIBER 2018-2022*". Skripsi ini disusun sebagai syarat untuk memperoleh gelar Sarjana Hubungan Internasional dari Universitas Lampung. Pada kesempatan ini penulis mengucapkan terima kasih kepada:

1. Ibu Dra. Ida Nurhaida M.Si., selaku Dekan Fakultas Ilmu Sosial dan Ilmu Politik Universitas Lampung
2. Bapak Simon Sumanjoyo Hutagalung, S.A.N., M.P.A. selaku Ketua Jurusan Hubungan Internasional Universitas Lampung
3. Mas Iwan Sulistyo S.Sos., M.A., selaku Dosen Pembimbing Utama yang selalu memberikan ilmu, waktu, masukan, bimbingan, nasihat, serta motivasi dan pengalaman kepada penulis selama menjadi mahasiswa pada Jurusan Hubungan Internasional
4. Bang Roby Rakhmadi, S.Sos., M.Si., selaku dosen pembimbing yang telah memberikan banyak ilmu dan membantu penulis dalam menyelesaikan skripsi serta meluangkan waktunya untuk membimbing, memberikan nasihat dan masukan kepada penulis
5. Mba Gita Karisma, S.IP., M.Si., selaku dosen pembahas yang sudah membantu penulis dalam menyelesaikan skripsi serta meluangkan waktunya untuk membimbing dan membantu saya
6. Seluruh dosen Jurusan Hubungan Internasional serta staf jurusan atas ilmu, pelajaran, dan pengalaman yang diberikan kepada penulis
7. Terima kasih kepada Ayah dan Bunda, yang terus memberikan doa, perjuangan dan dukungan kepada penulis. Penulis sangat bersyukur karena mempunyai

orang tua yang selalu mendukung penulis untuk bisa menyelesaikan stu Universitas Lampung

8. Terima kasih kepada teman-teman KKN yang telah membantu penulis dalam melaksanakan kegiatan KKN UNILA, semoga sukses dan sehat selalu
9. Seluruh pihak yang mendoakan dan membantu penulis selama proses penyusunan skripsi ini.

Bandar Lampung,16 Juli 2024

Muhammad Muhagam
NPM.1816071045

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR SINGKATAN

BEC	: Business Email Compromise
CBM	: Confidence Building Measures
CCCI	: Central Commission for Cyber security and Informatization
CERT	: Computer Emergency Response Team
CGI	: Cyber Global Index
CNNIC	: China Internet Network Information Center
CNCERT/CC	: Computer Network Emergency Response Technical Team/Coordination Center of China
CICIR	: China Institutes of Contemporary Internationa Relations
CSIS	: Centre for Strategic and International Studies
CWG	: Cyber Working Group
EMCE	: Economic Motive Cyber Espionage
FBI	: Federal Bureau of Investigation
GGE	: Group of Governmental Experts
ICANN	: Internet Corporation for Assigned Names and Numbers
IMF	: International Monetary Fund
LECD	: Law Enforcement and Cyber Security Dialogue
LOAC	: Laws of Armed Conflict
NATO	: North Atlantic Treaty Organization
NSA	: National Security Agency
MLAA	: Mutual Legal Assistance Agreement
MLAA	: Mutual Legal Assistance Agreement
NATO	: North Atlantic Treaty Organization
NSA	: National Security
PBB	: Perserikatan Bangsa-Bangsa
SD	: United States Dollar
USA	: United States of America
S&ED	: Strategic and Economic Dialogue
SSD	: Strategic Security Dialogue
US-CERT	: United States Computer Emergency Readiness Team
TI	: Teknologi Informasi

I. PENDAHULUAN

Skripsi ini akan menguraikan kerja sama antara Amerika Serikat dengan Tiongkok terkait dengan keamanan siber sebagai upaya penanggulangan kejahatan yang selama ini menjadi target sasaran kejahatan siber. Penelitian ini penting dan layak untuk dilakukan atas landasan justifikasi teoretis dan empiris, justifikasi metodologis, serta kebaruan yang ditemukan oleh peneliti. Maka dari itu, pada latar belakang penelitian ini, peneliti menyajikan riwayat singkat tentang kejahatan siber di sektor keuangan masing-masing negara yaitu Amerika Serikat dan Tiongkok, kerja sama yang di bangun oleh Amerika Serikat dengan Tiongkok, permasalahan yang di hadapi oleh masing-masing negara dalam melakukan kerja sama keamanan siber sebagai upaya penanggulangan kejahatan. Dalam bab ini pula, peneliti menyajikan penelitian-penelitian terdahulu, rumusan masalah, tujuan penelitian, serta manfaat penelitian ini.

1.1 Latar Belakang

Kemajuan sebuah teknologi saat ini membawa perkembangan yang cukup signifikan sehingga menjadikan penggunaan teknologi dan informasi sebagai kebutuhan utama masyarakat modern saat ini. Dampak dari pesatnya penggunaan teknologi informasi dan komunikasi adalah banyaknya penemuan-penemuan baru pada media teknologi informasi dan komunikasi salah satunya adalah penemuan jaringan internet. Jaringan internet setiap tahun juga mengalami perkembangan yang juga signifikan hal itu terlihat dari internet sudah menjadi kebutuhan masyarakat dalam menjalankan aktivitas sehari-hari. Pengembangan teknologi komunikasi dan informasi tersebut tidak terlepas dari upaya untuk melakukan perubahan di masa depan sehingga apa yang menjadi keinginan masyarakat bisa di jalankan dengan cepat, mudah, efisien, efektif dan nyaman (Geng, 2018).

Walaupun demikian kemajuan teknologi informasi tidak hanya memberikan manfaat secara positif namun juga memberikan pengaruh kurang baik, pengaruh kurang baik tersebut adalah munculnya kejahatan *cyber* (*cyber crime*). *Cyber crime* kini tidak hanya menyerang perusahaan atau personal melainkan sudah menyerang negara bahkan negara-negara maju juga menjadi sasaran kejahatan *cyber*. Oleh karena itu *cyber security* mulai menjadi sorotan sebagai isu keamanan non-tradisional. Isu keamanan tidak lagi hanya berada pada keamanan tradisional seperti peperangan maupun penggunaan senjata nuklir (Kshetri, 2013). Setiap negara berupaya meningkatkan strategi keamanan nasional di bidang *cyber security*. Pada saat ini, sebanyak 82 negara di dunia telah memiliki strategi *cyber security* nasional (NATO *Cooperative Cyber Defence Centre of Excellence*, 2018). Kesadaran akan ancaman dalam *cyber security* memunculkan alat negosiasi dan perjanjian sebagai pendekatan baru untuk menghadapi permasalahan *cyber security* secara internasional sehingga dalam perjanjian internasional yang di bangun oleh negara-negara di dunia terfokus pada pembentukan norma dan nilai dalam tata kelola internet serta pentingnya kerja sama antar negara.

Cyber security mulai menjadi perhatian PBB pada tahun 1998, pada saat Rusia pertama kalinya memberikan draf resolusi mengenai *cyber security* dan di ikuti oleh 15 negara, termasuk Amerika Serikat dan Tiongkok yang menjalin kesepakatan. Setiap negara wajib mematuhi hukum internasional dalam *cyber security*, dan menghormati kedaulatan negara begitu juga dengan prinsip dan norma yang dianut satu sama lain (Segal, 2017).

Pentingnya *cyber security* menjadi *wake-up call* bagi berbagai negara di dunia salah satunya adalah Amerika Serikat, Amerika Serikat menganggap *cyber security* sebagai prioritas keamanan nasional dan bahkan mencoba untuk mendominasi ranah *cyber space*. Amerika Serikat menempati posisi ke-2 dalam *Cyber Security Global Index* (CGI), Amerika Serikat memiliki tingkat keamanan dan pertahanan Amerika Serikat yang dominan (Assembly, 2010). Selain itu Amerika Serikat juga berperang aktif dalam tata kelola internet global di mana Amerika Serikat menekankan peran yang dimiliki oleh multi-*stakeholder*, yaitu seluruh entitas yang menjadi *stakeholder* dalam *cyber security* memiliki

kewenangan yang sama dalam menentukan kebijakan tata kelola internet, (Xinbao, 2016).

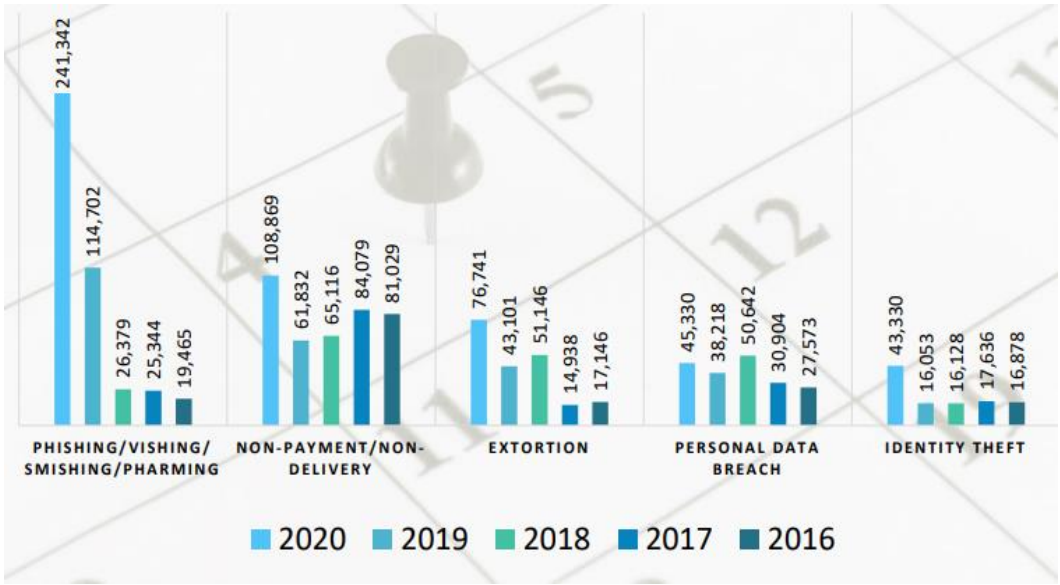
Berdasarkan hal tersebut maka Amerika Serikat dianggap sebagai negara pelopor perkembangan teknologi serta memiliki posisi yang diperhitungkan dalam *Internet Corporation for Assigned Names and Numbers* (ICANN) sebagai organisasi internasional yang mengontrol domain strategis *cyber space*. Oleh karena itu pada tahun 2021 Amerika Serikat mengeluarkan *action plan* kebijakan mulai dari *The National Strategy to Secure Cyberspace, Cyberspace Policy Review, International Strategy for Cyberspace, Departement of Defense Stratey for Operating Cyberspace, The Departement of Defense Cyber Strategy* dan *Departement of State International Cyberspace Policy Strategy*. Kebijakan tersebut di keluarkan oleh Amerika Serikat sebagai upaya untuk menghadapi persoalan yang menyangkut kejahatan *cyber* (The White House, 2022).

Kejahatan *cyber* melumpuhkan dan merusak sistem jaringan komputer maupun internet sehingga berdampak besar bagi kelangsungan operasional lembaga-lembaga besar baik milik negara maupun swasta. Sehingga kejahatan *cyber* di Amerika Serikat telah mengakibatkan kerugian ratusan miliar dolar, dan mengancam keselamatan publik dan keamanan ekonomi. Korban dari kejahatan *cyber* di Amerika Serikat tersebar cukup luas mulai dari individu, lembaga pendidikan, dunia usaha, utilitas, dan pemerintah (GAO, 2023). Hal itu terlihat pada tahun 2022 warga Amerika Serikat terdampak kejahatan *cyber* mencapai 53,35 juta, sedangkan antara bulan Juli 2020 dan Juni 2021, Amerika Serikat adalah negara yang paling menjadi sasaran serangan siber, menyumbang 46% serangan secara global (AAG, 2024).

Akibat dari kejahatan tersebut warga Amerika Serikat kehilangan $6,9 miliar pada tahun 2021 karena kejahatan terkait dunia maya, termasuk penipuan percintaan ($956 juta), penipuan investasi ($1,4 miliar), dan penyusupan email bisnis ($2,39 miliar). Bagi dunia bisnis ini adalah ancaman serius terhadap keamanan, dengan 60% organisasi di Amerika Serikat datanya dienkripsi dalam serangan *ransomware* yang berhasil. Biaya untuk memperbaiki serangan ini menelan biaya rata-rata $1,08 juta pada tahun 2021, turun 49% dari tahun 2020 ($2,09 juta (AAG, 2024).

Lembaga atau organisasi yang paling terdampak dari kejahatan *cyber* di Amerika Serikat adalah lembaga keuangan. Sektor keuangan menjadi fokus utama pemerintah Amerika Serikat memberikan perlindungan dari kejahatan *cyber*, dikarenakan berdasarkan informasi dari *International Monetary Fund* (IMF) sektor keuangan 300 kali lebih rentan terhadap kejahatan *cyber* (*Federal Bureau of Investigation*, 2021). Rawannya kejahatan pada sektor keuangan tersebut membuat Amerika Serikat menjadikan keamanan *cyber* pada sektor keuangan prioritas utama hal itu tidak terlepas dari besarnya kerugian pada sektor keuangan akibat kejahatan *cyber*. Diketahui bahwa Amerika Serikat sejak tahun 2016 sampai dengan 2020 serangan kejahatan 27% tertuju pada industri keuangan di susul oleh wilayah pemerintahan sebesar (25%), (*Federal Bureau of Investigation*, 2021).

Berdasarkan data *International Monetary Fund* (IMF) tahun kejahatan pada sektor industri jasa keuangan dari tahun 2016 sampai dengan tahun 2020 terus mengalami peningkatan diketahui bahwa kejahatan pada jasa keuangan akibat serangan *cyber* sebesar USD 1.5 milyar meningkat signifikan pada tahun 2020 menjadi USD 4.2 milyar (Internet Crime Report, 2020). Berikut ini adalah 5 bentuk kejahatan serangan *cyber* pada bidang keuangan di Amerika Serikat. Hal tersebut dapat dilihat alam gambar di bawah ini:



Gambar 1. 1 Bentuk Kejahatan Serangan *Cyber* pada Jasa Keuangan di Amerika Serikat

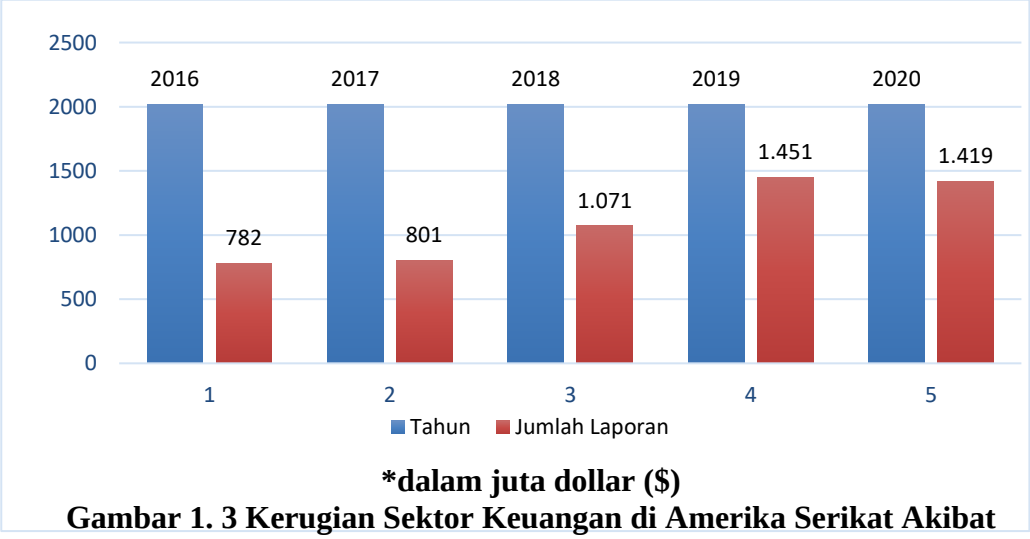
Sumber: Federal Bureau of Investigation, 2021

Jika melihat grafik di atas maka dari tahun 2016 sampai dengan 2020 angka kejahatan *cyber* pada bidang keuangan di Amerika Serikat terus mengalami peningkatan cukup signifikan. Data di atas juga dikuatkan oleh banyaknya keluhan atau laporan oleh masyarakat Amerika Serikat terkait dengan kejahatan *cyber* pada bidang keuangan, yang bisa dilihat dalam grafik di bawah ini:

Gambar 1. 2 Laporan oleh Masyarakat Amerika Serikat Terkait dengan Kejahatan *Cyber* pada Bidang Keuangan Tahun 2016-2020

Sumber: www.ic3.gov, 2022

Berdasarkan grafik di atas, jumlah laporan kerugian di bidang keuangan terus naik sepanjang tahun 2016-2020, tahun 2016 ada sebanyak 262,213 laporan, meningkat pada tahun 2017 menjadi 269,422, tahun 2018 naik kembali menjadi 298,728, 2019 ada sebanyak 288, kenaikan laporan kerugian di bidang keuangan meningkat signifikan pada tahun 2020 menjadi 301,580. Jika di total ada sebanyak 1,420,555 lapangan yang diterima oleh IC3. Sementara itu jumlah kerugian di sektor keuangan yang disebabkan oleh kejahatan *cyber* juga mengalami kenaikan, hal itu terlihat dalam grafik di bawah ini:



***dalam juta dollar ($)**

Gambar 1. 3 Kerugian Sektor Keuangan di Amerika Serikat Akibat Kejahatan *Cyber* Tahun 2016-2020

Sumber: www.ic3.gov, 2022

Gambar di atas menunjukkan bahwa dari tahun 2016 sampai dengan tahun 2020 serangan kejahatan *cyber* di Amerika Serikat di sektor keuangan cenderung mengalami kenaikan, hal itu terlihat dari besarnya kerugian pada sektor ini yang mencapai 5,52 milyar dallar Amerika Serikat dalam kurun waktu 2016-2020. Selain Amerika Serikat negara lainnya yang juga menganggap *cyber security* sebagai prioritas keamanan nasional adalah Tiongkok. Tiongkok memiliki penduduk sebanyak 1,4 milyar. Tidak hanya itu, setengah dari populasi tersebut dapat membawa Tiongkok dengan jumlah pengguna internet terbesar mencapai 772 juta masyarakat Tiongkok sudah menggunakan internet, (*China Internet Network Information Center* (CNNIC), 2018). Kedua angka tersebut cukup besar apabila dilihat sebagai potensi sumber daya manusia dalam ranah *cyber space*.

Secara ekonomi, Tiongkok adalah negara raksasa yang berada di posisi kedua perekonomian dunia. Tiongkok memiliki karakteristik perekonomiannya sendiri yang menjadikannya sebagai kekuatan ekonomi. Selain memiliki kekuatan dari jumlah populasi, Tiongkok memanfaatkan tingkat penggunaan internet yang tinggi sebagai alat pertumbuhan bagi bisnis dan perkembangan pasar oleh karena itu jumlah pengguna internet di Tiongkok berkorelasi dengan meningkatnya pertumbuhan ekonomi negara Tiongkok (*United Nations Department of Economic and Social Affairs*, 2018).

Perekonomian Tiongkok sangat bergantung dengan teknologi informasi. *Cyber space* memberikan nyawa dalam kemajuan sektor industri dan pengembangan ekonomi digital. Pada tahun 2021, pendapatan yang berasal dari perdagangan elektronik mengalami peningkatan sebanyak 43.4% per tahunnya, dengan total pendapatan 218.8 miliar RMB (*China Internet Network Information Center* (CNNIC), 2021).

Tingginya tingkat pengguna internet di Tiongkok menjadi potensi ancaman bagi stabilitas domestik, terlebih lagi negara Tiongkok merupakan negara dengan sistem satu partai. Ancaman tersebut dapat berasal dari pihak asing ataupun domestik. *Cyber space* memiliki kapasitas sebagai sarana untuk melakukan serangan yang ditujukan kepada pemerintah. Untuk mengantisipasi kerentanannya, pemerintah Tiongkok lalu memberlakukan pengawasan terhadap aktivitas internet domestik, dan memperjuangkannya sebagai ranah kedaulatan teritorial secara internasional (Austin, 2018). Berdasarkan hal tersebut maka Tiongkok memperjuangkan peran negara sebagai aktor utama yang berpengaruh dalam tata kelola internet global melalui *cyber sovereignty* atau kedaulatan internet, yaitu legitimasi atas kontrol dan manajemen konten internet yang ada di wilayahnya (Schia and Gjesvik, 2017).

Cyber security Tiongkok lalu memiliki *action plan* pada penguatan *cyber* yang dilakukan dalam bentuk peningkatan pengembangan teknologi, peningkatan keamanan internet, dan penguatan posisi Tiongkok dalam tata kelola internet global. Presiden Xi Jinping kemudian berambisi menjadikan Tiongkok sebagai *cyber power* oleh karena itu Presiden Xi Jinping membuat dua kebijakan yaitu *Central Commission for Cyber security and Informatization (CCCI)* dan *Strategic Thinking on Building China into a Cyber Super Power*. Tujuan dari kebijakan ini adalah untuk mewujudkan Tiongkok sebagai *cyber sovereignty* dalam tata kelola internet global serta untuk memberikan perlindungan pada sektor-sektor industri seperti keuangan, asuransi dan infrastruktur penting lainnya (Brown and Yung, 2017).

Prioritas perlindungan keamanan pada industri keuangan, asuransi dan infrastruktur penting lainnya menjadi fokus utama Presiden Xi Jinping melalui *cyber security*, hal itu dikarenakan serangan *cyber* di Tiongkok 70% ditujukan

kepada perbankan, 16% perusahaan asuransi dan 14% sektor lainnya, dengan rata-rata kerugian tahunan dari kejahatan siber (*cyber crime*) sektor keuangan Tiongkok telah mencapai US$600 miliar (CSIS, 2020).

Besarnya kerugian baik negara Amerika Serikat maupun Tiongkok akibat kejahatan *cyber*, membuat kedua negara ini melakukan upaya dialog di bawah kerangka *community of common destiny*. Hubungan antara Amerika Serikat dengan Tiongkok di mulai dari dialog bilateral yang dilakukan oleh perwakilan pemerintah dari bersama dengan pakar *cyber security* Tiongkok maupun Amerika Serikat (Fang, 2018).

Amerika Serikat dengan Tiongkok lalu bertemu pada tahun 2015 untuk membahas perihal isu *cyber security*. Walaupun sempat menandakan sinyal positif namun belum membuahkan hasil yang signifikan. Tidak terlihat adanya perubahan perilaku keduanya yang masih saling tidak percaya terhadap satu sama lain. Forum dialog *cyber security* berakhir dengan pernyataan Tiongkok yang memutuskan untuk menunda forum dialog bilateral Amerika Serikat dengan Tiongkok dalam kurun waktu yang tidak dapat ditentukan (Kuehl, 2019). Kemudian pada tanggal 24-25 September 2020, Amerika Serikat dengan Tiongkok melahirkan kesepakatan bilateral dengan nama *US-China Cyber Agreement* 2020 yang berbunyi:

> *Both sides agree to step up crime cases, investigation assistance and information-sharing. And both government will not be engaged in or knowingly support online theft of intellectual properties.*

Kutipan di atas mengatakan bahwa kedua belah pihak sepakat untuk menghentikan segala kegiatan *spionase cyber* dengan motif ekonomi atau bisnis, dan tidak terlibat maupun mendukung aktivitas pencurian kekayaan negara. Kesepakatan tersebut menandai dimulainya dialog antara Amerika Serikat dengan Tiongkok dalam menghadapi ancaman kejahatan *cyber* (Libicki dan Cevallos, 2020). Setelah tercapainya kesepakatan dalam *cyber security*, perjanjian yang telah disepakati pada tahun 2020 dilanjutkan dengan dialog tingkat tinggi dengan nama *U.S.-China Law Enforcement and Cyber Security Dialogue* (LECD), sebuah kerangka meningkatkan hubungan Amerika Serikat dengan Tiongkok (*Department of Justice United States of America*, 2021).

Dilihat dari sudut padang dialog internasional tercapainya kesepakatan antara Amerika Serikat dengan Tiongkok menjadikan penelitian ini menarik untuk

di kaji lebih mendalam. Dialog antara Amerika Serikat dengan Tiongkok di pilih dengan alasan pertama kedua negara memiliki kerugian cukup besar akibat dari, kejahatan *cyber* di semua sektor baik negara maupun swasta dan angka kerugian akibat kejahatan *cyber* di setiap tahun mengalami kenaikan yang menunjukkan bahwa kedua negara menjadi target sasaran dari kejahatan *cyber*. Kedua, kerugian terbesar akibat dari kejahatan *cyber* di kedua negara adalah pada sektor keuangan karena sektor keuangan memiliki dampak yang cukup besar pada sektor infrastruktur penting lainnya bahkan mempengaruhi kehidupan warga negara baik warga negara Amerika Serikat maupun Tiongkok. Ketiga, Amerika Serikat dengan Tiongkok adalah dua negara dengan kepentingan yang saling bertolak belakang dalam tata kelola internet. Amerika Serikat adalah negara demokratis yang mendukung nilai kebebasan dalam berinternet, dan bertolak belakang dengan Tiongkok yang berpegang teguh pada kedaulatan internet. Selain itu juga untuk pertama kalinya, kesepakatan mengenai *cyber security* untuk penanggulangan kejahatan berhasil dicapai oleh Amerika Serikat dengan Tiongkok. Dialog *cyber security* Amerika Serikat dengan Tiongkok menjadi sebuah sinyal yang baik dalam perkembangan hubungan di ranah *cyber*.

Peneliti membatasi tahun penelitian pada tahun 2018 sampai dengan tahun 2022 dengan alasan kesepakatan dialog antara Amerika Serikat dengan Tiongkok pada tahun 2018 yang sebelumnya sudah di lakukan pada tahun 2015 namun terhenti karena adanya kasus *spionase* yang dilakukan oleh warga Tiongkok ke Amerika Serikat sehingga menimbulkan saling ke tidak percayaan di kedua negara akibatnya dialog terhenti, kemudian dialog di lanjutkan kembali pada tahun 2018 sampai dengan 2022 ketika kedua negara sama-sama menjadi target kejahatan *cyber* dan besarnya kerugian akibat dari kejahatan *cyber*.

Ketiga alasan tersebut membuat peneliti tertarik untuk peneliti terkait dengan kerja sama yang dibangun Amerika Serikat dengan Tiongkok, oleh karena itu peneliti mengambil judul: “DIALOG KEAMANAN SIBER AMERIKA SERIKAT-TIONGKOK GUNA PENANGGULANGAN KEJAHATAN 2018-2022”.

1.2 Penelitian Terdahulu

Dalam menyusun penelitian ini, peneliti menggunakan beberapa penelitian terdahulu dalam membentuk sebuah kerangka pemikiran, termasuk dalam menentukan konsep atau teori yang akan peneliti gunakan dalam penelitian ini. Secara spesifik dalam penelitian ini menekankan pada Kerja sama keamanan siber Amerika Serikat dengan Tiongkok guna penanggulangan kejahatan pada sektor industri keuangan. Meski demikian, penelitian lainnya yang bersinggungan dengan topik ini telah cukup banyak dilakukan oleh para akademisi dari berbagai disiplin ilmu namun hanya sebatas kerja sama untuk memperkuat keamanan siber negara secara umum belum ada yang secara spesifik membahas tentang dialog keamanan *cyber* dalam bidang tertentu seperti dalam penelitian ini yaitu keamanan siber guna menanggulangi kejahatan *cyber*. Penelitian-penelitian terdahulu yang menekankan pada kerja sama keamanan siber antara Amerika Serikat dengan Tiongkok untuk mengurangi ketegangan diantara kedua negara (Liaropoulos, 2015), kerja sama antara Amerika Serikat dengan Tiongkok untuk mempertahankan keamanan *cyber*-nya dengan berbagai strategi (Shi, 2015), kerja sama antara Amerika Serikat dengan Tiongkok untuk mencegah terjadinya *spionase* (Baezner, 2018), kerja sama antara Amerika Serikat dengan Tiongkok untuk menciptakan peraturan terkait dunia siber (Geng, 2018), kerja sama antara Amerika Serikat dengan Tiongkok untuk menghadapi menghadapi ancaman *cyber warfare* global (Saputera, 2015).

Penelitian pertama adalah penelitian yang di lalakukan oleh Andrew Liaropoulos (Liaropoulos, 2015), penelitian ini berjuduk *Great Power Politicssin Cyber Space: U.S. anddChina are Drawing the Ines Between Confrontation and Cooperation oleh Andrew Liarpoulos dalam jurnal Panorama of Global Security Environtment*, ditulis oleh Andrew Liaropoulos, dari Sociology Study, tahun 2015. Dalam penelitian ini menggunakan metode penelitian kualitatif serta teknik deskriptif, dan menggunakan landasan teori *cyber diplomacy*. Andrew Liaropoulos menjelaskan mengenai politik dalam dunia siber antara dua negara yang notabenenya merupakan negara *great power* yakni Amerika Serikat dan Tiongkok. Selain itu, dalam tulisan ini juga menjelaskan mengenai hubungan kedua negara yang berada diantara konfrontasi dan kerja sama. Dalam hal untuk mengurangi

ketegangan antara Amerika Serikat dan Tiongkok dan membangun jaringan komunikasi merupakan tugas yang tergolong sulit, menurut Andrew Liarpoulos, hal tersebut disebabkan oleh dua alasan *pertama* adalah mencapai kemajuan dalam kebijakan *cyber détente* (perubahan kebijakan dari konfrontasi kepada kerja sama) adalah tugas yang sulit karena sifat dunia maya yang kompleks. *Kedua* ialah kedua negara (Amerika Serikat dan Tiongkok) masih melihat masing–masing sebagai musuh dan masih ada ketidak percayaan diantara keduanya. Terkait hal tersebut, penulis menyatakan bahwa *cyber diplomacy* harus bekerja keras dalam hal untuk menurunkan saling curiga diantara keduanya dengan membangun norma-norma dan mengkoodinasikan mekanissme.

Penelitian kedua, penelitian yang dilakukan oleh Bowei Shi (Shi, 2015), dengan judul penelitian adalah *National Cyber Security Strategy of the Usand Its Constructivel mplications for China,* yang ditulis oleh Bowei Shi pada tahun 2015. Jurnal ini diterbitkan di Washington, DC, USA dari penerbit Taylor & Francis. Dalam penelitian ini, Bowei Shi menggunakan metode penelitian yang salah satunya ialah kualitatif dengan teknik deskriptif, serta konsep strategi. Bowei Shi, menjelaskan bahwa fokus utama Amerika Serikat dalam mempertahankan keamanan sibernya dengan beberapa strategi–strategi yang secaras eksplisit dimulai sejak pemerintahan Presiden Georgew Bush. Konsep yang digunakan penulis terkait dengan tulisan tersebut ialah konsep strategi. Komponen – komponen strategi dalam strategi keamanan siber nasional Amerika Serikat ialah; (1) membangun organisasi pemerintah yang relevan, (2) Undang – undang hukum domestik terkait dunia maya, (3) kolaborasi antara pemerintah dengan perusahaan internet swasta, (4) memfasilitasi penelitian dan pembangunan jaringan teknologi yang mumpuni dan pelatihan komputer profesional, (5) melakukan kerja sama dengan komunitas internasional.

Penelitian ketiga, adalah penelitian yang dilakukan oleh Marie Baezner (Baezner, 2018) dengan judul: *Cyber Security in Sino Americana Relations*. Jurnal ini diteliti oleh Marie Baezner dari *CSS Analyses in Security Policy*, yang diterbitkan pada tahun 2018. Penelitian ini menggunakan konsep *cyber warfare*, serta metode penelitian kualitatif. Baezner menjelaskan bahwa faktor–faktor yang membuat kedua negara saling tidak percaya sehingga melakukan *spionase*. Selama

beberapa tahun terakhir, ketegangan antara kedua negara ini secara khusus meningkat terkait masalah keamanan siber. Tiongkok dan Amerika Serikat telah melakukan *spionase* siber satu sama lain. Hal yang mempengaruhi tindakan saling tidak percaya diantara kedua negara ini ialah Tiongkok tidak setuju dengan model tata kelola global internet yang diajukan oleh Amerika Serikat dalam pembentukkan Zona Anti-Akses, ada dua faktor yang menjadi penyebab kedua negara saling melakukan *spionase*. *Pertama* adalah masalah tata kelola global internet. Hal ini disebabkan Amerika Serikat yang mana merupakan negara yang menginisiasi pembentukkan tata kelola global dalam hal siber. Internet dikelola oleh organisasi non profit yang bernama *Internet Cooperation for Assigned Names and Numbers* (ICANN), (ICANN adalah lembaga atau organisasi yang dibentuk oleh pemerintah yang bertanggung jawab untuk melakukan pengelolaan infrastruktur internet inti). Faktor yang kedua adalah zona anti akses di bangun oleh Tiongkok di kawasan Laut Cina Selatan. Zona anti akses merupakan pendekatan pertahanan asimetris yang digunakan untuk mencegah dan menghalangi musuh memasuki zona tersebut dengan meningkatkan kemampuan siber untuk mengendalikan ruang informasi jika terjadi konflik tujuannya adalah menganggu sistem komunikasi dan GPS musuh.

Penelitian keempat adalah penelitian yang dilakukan oleh Zhao Geng, (Geng, 2018), dengan judul, *Analysis of Cyberspace Rule-Makingin China-US Relations*. Jurnal ini diterbitkan oleh Internasional Relations and Diplomacy pada tahun 2018, alam penelitian ini menggunakan teori *cyberspace*. Zhao Geng dalam penelitiannya menjelaskan bahwa bahwa pembuatan peraturan terkait dunia siber dalam hubungan Tiongkok dan Amerika Serikat. Kedua negara tersebut saling bernegosiasi untuk menciptakan peraturan terkait dunia siber agar terciptanya keamanan dan kestabilan dunia siber secara global. Kedua negara mampunyai kepentingan nasionalnya masing–masing dalam pembuatan peraturan siber ini. Dengan adanya landasan norma dalam tata kelola dunia siber ditujukan untuk membatasi perilaku setiap aktor internasional dengan norma – norma yang efektif.

Penelitian kelima adalah penelitian yang dilakukan oleh Moehammad Yuliansyah Saputera (Saputera, 2015) yang berjudul *Pengaruh Cyber Security Strategy Amerika Serikat Menghadapi Ancaman Cyber Warfare*, yang di tulis oleh Moehammad Yuliansyah Saputera pada tahun 2015 pada jurnal Jom FISIP Jurusan

Ilmu Hubungan Internasional Universitas Riau, dalam jurnal ini mengunakan metode kualitatif yang bersifat deskriptif, dengan menggunakan teori *cyber warfare*. Moehammad Yuliansyah Saputera, menjelaskan bahwa penguasaan dan pemanfaatan Teknologi Informasi (TI) yang destruktif merupakan ancaman bagi keamanan dan ketahanan nasional suatu negara. Penggunaan Teknologi Informasi (TI) sebagai eksploitasi dapat menciptakan ancaman perang informasi atau *cyber warfare* (perang dunia maya). Ketergantungan pada jaringan *cyber* dapat memiliki celah kerentanan dalam kemanan *cyber*. Amerika Serikat merupakan salah satu negara yang memiliki kapabilitas dalam menguasai dan memanfaatkan Teknologi Informasi (TI) untuk kehidupan masyarakat dan negara dari sektor kecil sampai infrastruktur vital. Dalam penelitian yang juga menjelaskan bahwa kerentanan jaringan dapat memberikan celah masuknya *cyber attack* (serangan siber/serangan dunia maya) dan menjadi ancaman bagi keamanan *cyber* Amerika Serikat, sebab, informasi-informasi rahasia yang di simpan secara digital dapat di curi, dimata-matai, di ubah ataupun dihancurkan. Menghadapi ancaman *cyber warfare* global, Amerika Serikat telah menggunakan *ICT underground* atau *deep web* (merupakan bagian dari *word, wide, web* namun tidak dapat di akses dengan mudah) sehinga sistem *deep web* dijadikan sebagai bentuk *cyber security strategy* dalam menjaga keamanan *cyber*. *Cyber security strategy* merupakan upaya yang dakukan oleh pemerintah untuk melindungi dari adanya *cyberwwarfare* (perang dunia maya) yang di khawatirkan akan menganggu keamanan, kerahasiaan, integritas serta ketersedian informasi. *Cyber security strategy* tersebut untuk mengamankan dan mempertahankan data-data digital penting serta menjaga infrastruktur vital Amerika Serikat.

1.3 Rumusan Masalah

Kejahatan *cyber* yang ditujukan kepada sebuah negara memiliki dampak yang cukup berbahaya karena dampaknya yang begitu besar pada kemajuan sebuah negara hal itu dikarenakan dampak yang dirasakan tidak hanya pada pemerintah saja melainkan kepada seluruh penduduk sebuah negara. Oleh karena itu kejahatan *cyber* menjadi fokus utama pemerintah ataupun sebuah negara karena akibat

kejahatan tersebut dapat merugikan semua pihak khususnya sektor keamanan negara.

Selain itu kejahatan *cyber* tidak hanya menyerang negara-negara berkembang namun negara-negara maju seperti Amerika Serikat dan Tiongkok juga menjadi sasaran kejahatan *cyber*. Salah satu yang paling banyak mendapatkan serangan *cyber* baik Amerika Serika maupun Tiongkok. Pemerintah Amerika Serikat dan Tiongkok menjalin dialog *cyber security* dengan nama *U.S.-China Law Enforcement and Cyber Security Dialogue* (LECD) yang salah satu isinya adalah menghentikan segala kegiatan *spionase cyber* dengan motif ekonomi atau keuangan.

Dialog Amerika Serikat dengan Tiongkok sebagai mitra di sektor *cyber* juga ditandai dengan penandatanganan nota kesepakatan atau *common understanding* antara Presiden Amerika Serikat dengan Presiden Tiongkok. Pemilihan Tiongkok sebagai mitra di sektor *cyber* dengan pertimbangan Tiongkok merupakan negara maju di kawasan ASIA yang mampu menciptakan kekuatan dan kecanggihan teknologi serta melakukan inovasi pembaharuan terhadap *teknologi cyber.*

Berdasarkan uraian pada latar belakang di atas maka pertanyaan yang akan di uraikan dan dijawab dalam penelitian ini adalah: “Bagaimanakah dialog keamanan *cyber* Amerika Serikat dengan Tiongkok guna penanggulangan kejahatan 2018-2022?”

1.4 Tujuan Penelitian

Berdasarkan uraian yang yang di paparkan dalam latar belakan dan rumusan masalah di atas maka penelitian ini memiliki dua tujuan, yakni:

1. Untuk menyajikan pelaksanaan dialog keamanan *cyber* Amerika Serikat dengan Tiongkok guna penanggulangan kejahatan 2018-2022
2. Menganalisis bentuk dialog keamanan *cyber* Amerika Serikat dengan Tiongkok guna penanggulangan kejahatan 2018-2022.

1.6 Manfaat Penelitian

Manfaat dalam penelitian ini dijabarkan menjadi, kegunaan teoritis dan praktis:

1. Secara teoritis, diharapkan turut berkontribusi dalam pengembangan teori dan konsep dalam studi hubungan internasional, terutama terkait dengan dialog keamanan *cyber* Amerika Serikat dengan Tiongkok guna penanggulangan kejahatan.
2. Secara praktik, diharapkan penelitian ini mampu berkontribusi memberi informasi deskriptif tentang keamanan *cyber* yang dilaksanakan oleh Amerika Serikat dengan Tiongkok guna penanggulangan kejahatan *cyber*. Selain itu, ditujukan pula dapat berguna sebagai informasi bagi negara-negara untuk terus memaksimalkan keamanan *cyber* dengan menjalin dialog dengan berbagai negara-negara yang sudah memiliki keamanan lebih baik dan maju.

II. TINJAUAN PUSTAKA

Bab ini menyajikan tinjauan pustaka yang terbagi ke dalam dua bagian yang akan menguraikan tentang landasan konseptual yang terdiri dari dialog keamanan dan konsep *cyber security*, serta teori *cooperation security* dan *collective security*, pada bagian kedua akan dipaparkan kerangka pemikiran yang bertujuan untuk menciptakan alur pikir yang diterapkan dalam penelitian ini serta memberikan gambaran mengenai DIALOG KEAMANAN SIBER AMERIKA SERIKAT-TIONGKOK GUNA PENANGGULANGAN KEJAHATAN.

1.5 Landasan Konseptual

Konsep serta teori yang digunakan oleh peneliti dalam landasan konseptual tentunya menjadi modal bagi peneliti dalam membingkai kerangka analisis dalam penelitian ini. Adapun poin-poin dalam konsep pengertian keamanan, dialog keamanan atau *defence cooperation,* tujuan dialog keamanan. Selain itu konsep *cyber security* juga akan menguraikan tentang pengertian *cyber security*, tujuan kerja sama *cyber security* dan elemen pokok *cyber security*. Konsep-konsep tersebut peneliti jelaskan karena tidak semua pembaca memahami terkait dengan keamanan atau *defence cooperation* serta *cyber security*, selain itu sebagai langkah agar tidak terjadi kesalahan informasi dalam penelitian ini.

2.1.1 Konsep Dialog Keamanan

Dialog dikatakan sebagai sebuah keterbukaan pandangan yang berbeda, tetapi memiliki kepedulian terhadap satu dan yang lainnya. Dialog yang dilakukan antar negara adalah wujud dari sebuah keharmonisan sebuah negara. Cara efektif dalam melaksanakan sebuah dialog antar negara adalah dengan mengupayakan

dialog itu menjadi dialog yang bertanggungjawab secara global. Dialog bukan untuk saling mengalahkan akan tetapi untuk saling memahami antara satu pihak lain dengan baik, untuk mencapai kesepakatan penuh secara universal. Dialog berorientasi sebagai sebuah sarana komunikasi untuk menjembatani kesalahpahaman dalam budaya yang berbeda, mengungkapkan pandangan dalam bahasa masing-masing (Knitter, 2010).

Berdasarkan penjelasan tersebut maka dialog dapat dilakukan untuk mencapai sebuah kesepakatan antar pihak termasuk antar negara, salah satu bentuk dialog yang sering digunakan oleh negara adalah untuk mencapai kesepakatan tentang keamanan. Keamanan (*security*) secara etimologi berasal dari bahasa latin yaitu dari kata *securus* (*se + cura*) yang memiliki arti kebebasan dari hal yang membahayakan, terbebas dari rasa takut (*free from donger, free from fear*) selain itu jika melihat kata *se* yang memiliki makna tanpa/*without*. Sementara itu *curus* memiliki makna *liberation from uneasiness* secara keseluruhan menjadi *liberation from uneasiness without any risks or threats* (Liofa, 2002).

Sedangkan jika dilihat dari pendekatan tradisional konsep keamanan adalah keadaan sebuah negara yang terbebas dari berbagai ancaman dari pihak-pihak yang berkepentingan. Selain itu keamanan juga bisa di maknai sebagai cara sebuah negara dalam memberikan perlindungan kepada rakyatnya atau negaranya dari serangan negara lain (*the absence of a militery threat or with the nation external overthow ar attact*) (Haftendorn, 1991).

Penjelasan tersebut di kuatkan oleh Arnold Wolfers menjelaskan bahwa secara objektif keamanan dapat di ukur dari negara yang tidak mendapatkan ancaman selain itu negara juga tidak merasa takut dengan berbagai ancaman penyerangan dari negara lain (Baylis dan Smith, 1997). Walter Lippmann juga mengungkapkan bahwa negara dikatakan memiliki keamanan yang tinggi jika tidak memiliki ancaman serta negara memiliki kemampuan untuk mempertahankan kemenangan dari berbagai ancaman negara lain yang selalu mengancam (Jackson-Preece, 2011).

Keamanan dalam sebuah negara terbagi dalam lima bidang yaitu militer, politik, ekonomi dan sosial. Bidang militer hanya sebagai satu aspek penting dalam sebuah keamanan negara sedangkan politik, ekonomi dan sosial memiliki aspek

yang lebih luas yang juga disebut dengan aspek non militer. Walaupun demikian aspek ini memiliki pengaruh besar pada sebuah negara dalam mempertahankan keamanan (Buzan, 1991). Untuk mewujudkan keamanan di bidang non militer tersebut negara akan selalu aktif melakukan kerja sama dengan negara lain yang juga sama-sama memiliki kekuatan yang besar seperti yang dilakukan oleh Amerika Serikat yang memilih melakukan kerja sama dengan Tiongkok untuk memperkuat keamanan siber di bidang keuangan.

Kerja sama keamanan harus memiliki tujuan yang jelas, karena kerja sama keamanan sangat penting apabila memiliki arti ganda dan tidak memiliki arah yang sama. Hal ini dapat digunakan sebagai celah untuk melakukan tindakan yang tidak diinginkan oleh para pihak. Secara formal tujuan kerja sama akan tertulis pada perjanjian, antara lain untuk:

1. Mempromosikan hubungan perdamaian dan menciptakan stabilitas bisang keamanan di regional dan dunia
2. Mempromosikan hubungan yang ramah dan bersahabat
3. Mempererat dan meningkatkan kerja sama bilateral
4. Mengebangkan hubungan kerja sama antar kedua negara
5. Menetapkan suatu kerangka kerja guna meningkatkan hubungan bilateral di antara badan keamanan.

Kerja sama keamanan yang dilakukan oleh Amerika Serikat di bidang non militer sebagai langkah Amerika Serikat untuk mencapai hegemoni global, sebab akan sangat sulit bagi negara mencapai keamanan yang maksimal di semua sektor khususnya di bidang non militer jika memiliki keterpisahan jarak oleh karena itu untuk mencapai keamanan terbaik sebagaimana negara yang memiliki kekuatan untuk melakukan hegemoni. Amerika Serikat melakukan kerja sama di kawasan Asia dengan negara yang juga memiliki kekuatan besar yaitu Tiongkok. Agar kerja sama berjalan dengan baik dan tepat serta tidak merugikan sesalah satu negara maka Amerika Serikat melakukan pembagian kekuasaan. Tujuannya adalah untuk mewujudkan *great power security cooperation* agar negara-negara lain tidak berani untuk melakukan gangguan atau ancaman tidak hanya dari sektor militer namun juga sektor non militer (Toft, 2005).

Mearsheimer menjelaskan bahwa *great power security cooperation* dapat di formulasikan dalam dua bidang pertama adalah *latent power* (ekonomi dan populasi atau non militer) dan *actual power* (militer). Kedua bidang tersebut di wujudkan untuk memaksimalkan *great power security cooperation* agar sebuah negara mampu dengan efektif menguasai sebuah wilayah oleh karena itu negara akan mempertimbangkan berbagai strategi yang tepat tujuannya adalah untuk mencapai hegemoni. Mearsheimer juga membagi strategi tersebut dalam dua bentuk yaitu strategi langsung untuk mencapai power relatif dan tindakan tidak langsung untuk mengetahui tindakan yang akan dilakukan oleh negara *agresor* (*checking*) (Mearsheimer, 2001).

Tiongkok merupakan salah satu negara yang memaksimalkan *great power security cooperation* di kawasan Asia Timur, namun Tiongkok enggan untuk memaksimalkan kekuatan realtifnya saat ini. Hal itu dikarenakan Tiongkok lebih memilih menciptakan kemampuan sumber daya manusia sebagai basis kekuatan negara sehingga sumber daya manusia di Tiongkok rata-rata melebihi kemampuan sumber daya manusia negara tetangga khususnya di bidang militer dan ekonomi. Mearsheimer menjelaskan bahwa apa yang dilakukan oleh Tiongkok karena Tiongkok selalu memperhatikan kemampuan yang dimiliki oleh sumber daya manusia yang ada di negara persaingan terdekatnya yaitu Amerika Serikat, oleh karena itu perhatian Tiongkok terhadap sumber daya manusia dinilai cukup rasional untuk memaksimalkan kekuatan relatifnya untuk bisa bersaingan dengan negara Amerika Serikat. Untuk mendukung tindakan tersebut Tiongkok terus berusaha meningkatkan kekuatan ekonominya kemudian menyusun strategi yang tepat agar mampu bekerja sama dengan negara-negara kuat seperti Amerika Serikat yang saat ini Amerika Serikat berusaha untuk melakukan hegemoni di kawasan Asia (Mearsheimer, 2001).

Mearsheimer mencontohkan *great power security cooperation* yang dilakukan oleh Amerika Serikat pasca merdeka tahun 1783 yang diketahui adalah negara kecil yang ada di kawasan Lautan Atlatis. Namun setelah 115 tahun kemudian Amerika Serikat mampu membuat sebuah formulasi *great power security cooperation* untuk dijadikan hegemoni regional, yang ditandai dengan ekspansi Amerika Serikat di daratan atlatis hingga lautan pasifik. Agar bisa bersaingan

dengan negara tetangga yaitu Mexico yang di huni oleh rata-rata penduduk Amerika Serikat, ekspansi yang dilakukan tidak hanya pada sebatas Mexico namun juga sampai dengan daratan Kanada dan Karabia. Amerika Serikat berusaha menyingkirkan *great power security cooperation* di wilayah ini dan memastikan mereka tidak lagi kembali. Formulasi ini di kenal dengan *Doktrin Monroe* dan Amerika Serikat dikenal sebagai negara dengan hegemoni pertama dalam sejarah dunia modern (Mearsheimer, 2001).

Begitu juga dengan Tiongkok yang meniru Amerika Serikat dalam melakukan hegemoni, Tiongkok selalu memperlihatkan kekuatan (power) kepada negara lain khususnya negara tetangga. Namun Tiongkok dalam melakukan tindakan hegemoni cenderung lebih *offensive* hal itu dilakukan Tiongkok agar lebih mudah melakukan hegemoni regional (Mearsheimer, 2001).

Berdasarkan penjelasan di atas maka dapat diketahui bahwa perilaku Amerika Serikat dengan Tiongkok dalam mengimplementasikan *great power security cooperation* untuk mencapai maksimal relatif power, sehingga kedua negara tersebut akan melakukan kerja sama keamanan dengan cara melaksanakan empat strategi *great power security cooperation*. Strategi tersebut antara lain: *pertama, great power security cooperation* akan dijadikan sebagai hegemoni dalam regional kedua negara hal itu dikarenakan kedua negara tersebut akan kesulitan memproyeksikan power jika terbatas jarak. *Kedua, great power security cooperation* yang dilakukan oleh kedua negara akan memaksimalkan kekayaan di kedua negara agar negara-negara lain tidak mampu menyaingi baik ekonomi, militer, politik dan sosial.

Ketiga, great power security cooperation selalu memproyeksikan kekuatan ekonomi selaku kekuatan non militer dan militer baik darat, laut dan udara. *Keempat, great power security cooperation* akan di wujudkan melalui kerja sama membangun kekuatan militer, hal itu dikarenakan kekuatan militer menjadi kekuatan utama karena dengan adanya kekuatan militer seluruh kekayaan dapat dialokasikan serta dapat menjaga wilayah dari serangan musuh. Selain itu dengan kekuatan militer yang dimiliki oleh masing-masing negara yaitu Amerika Serikat dengan Tiongkok negara-negara lain akan merasa takut karena kedua negara

menjadikan *great power security cooperation* akan memproyeksikan keunggulan nuklir sebagai pertahanan pada masing-masing negara (Mearsheimer, 2001).

Great power security cooperation tidak hanya mengandalkan power sebagai kekuatan utama, *great power security cooperation* juga sebagai langkah utama negara dalam menghentikan hegemoni negara lain untuk mencapai power di negara atau kawasan dalam negaranya. Walaupun demikian *great power security cooperation* dilaksanakan juga sebagai salah satu strategi mempertahankan hegemoni di sebuah negara, maka negara yang berhasil melakukan hegemoni akan selalu mengedepankan strategi agar tidak tercipta hegemoni lain atau hegemoni baru, sejauh hal yang dilakukan adalah *balancing* dan atau *buckpussing* (Mearsheimer, 2001).

2.1.2 Konsep *Cyber Security*

Cyber security adalah kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan *cyber* dan organisasi dan aset pengguna. Organisasi dan aset pengguna dalam *cyber security* termasuk perangkat yang terhubung komputasi, personil, infrastruktur, aplikasi, layanan, sistem telekomunikasi dan totalitas informasi yang dikirimkan dan/atau disimpan dalam lingkungan maya (Choucri, 2012).

Cyber security merupakan upaya untuk memastikan pencapaian dan pemeliharaan sifat keamanan organisasi dan aset pengguna terhadap risiko keamanan yang relevan dalam lingkungan *cyber*. Tujuan keamanan umum terdiri dari ketersediaan, integritas termasuk didalamnya keaslian dan kemungkinan upaya mengurangi terjadinya penolakan serta terakhir kerahasiaan (Valeriano at al, 2021). *Cyber security* dibangun di atas lima bidang kerja antara lain kepastian hukum (undang-undang *cyber crime*), teknis dan tindakan prosedural (pengguna akhir dan bisnis (pendekatan langsung dan penyedia layanan dan perusahaan perangkat lunak), struktur organisasi (struktur organisasi sangat berkembang, menghindari tumpang tindih). *Capacity building* dan pendidikan pengguna (kampanye publik dan komunikasi terbuka dari ancaman *cyber crime* terbaru),

kerjasama internasional (termasuk didalamnya kerjasama timbal balik dalam upaya mengatasi ancaman *cyber*) (undang-undang *cyber crime*) (Choucri, 2012).

Cyber security lebih lanjut dimaknai sebagai semua mekanisme yang dilakukan untuk melindungi dan meminimalkan gangguan kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi. Mekanisme ini harus bisa melindungi informasi baik dari *physical attack* maupun *cyber attack*. *Cyber security* merupakan upaya untuk melindungi informasi dari adanya *cyber attack*, adapun elemen pokok *cyber security* adalah:

1. Dokumen *security policy* merupakan dokumen standar yang dijadikan acuan dalam menjalankan semua proses terkait keamanan informasi
2. *Information infrastructure* merupakan media yang berperan dalam kelangsungan operasi informasi meliputi *hardware* dan *software*. Contohnya adalah *router*, *switch*, server, sistem operasi, database, dan *website*
3. *Perimeter defense* merupakan media yang berperan sebagai komponen pertahanan pada infrastruktur informasi misalnya IDS, IPS, dan *firewall*
4. *Network monitoring system* merupakan media yang berperan untuk memonitor kelayakan, *utilisasi*, dan *performanc*e infrastruktur informasi
5. *System information and event management* merupakan media yang berperan dalam memonitor berbagai kejadian di jaringan termasuk kejadian terkait pada insiden keamanan
6. *Network security assessment* merupakan elemen *cyber security* yang berperan sebagai mekanisme kontrol dan memberikan measurement level keamanan informasi
7. *Human resource dan security awareness* berkaitan dengan sumber daya manusia dan *awareness*-nya pada keamanan informasi (Cavelty, 2012).

2.2 Kerangka Teori

Kerangkan teori dalam penelitian ini akan peneliti bagi ke dalam dua teori yaitu teori *cooperation security* dan teori *collective security*, kedua teori ini digunakan sebagai upaya untuk melihat kerja sama yang di bangun oleh Amerika Serikat dengan Tiongkok guna penanggulangan kejahatan *cyber*. Kedua teori ini

cukup relevan digunakan untuk menganalisis hasil penelitian karena *cooperation security* sebagai upaya untuk melihat strategi yang digunakan oleh negara Amerika Serikat dengan Tiongkok guna menanggulangi kejahatan *cyber*. Sedangkan *collective security* digunakan karena Amerika Serikat dengan Tiongkok yang ingin meningkatkan keamanan secara bersama-sama. Hal itu dilakukan oleh Amerika Serikat dengan Tiongkok mengingat kejahatan *cyber* di dua negara ini cukup tinggi oleh karena itu meningkatkan keamanan secara bersama-sama sebagai langkah untuk memperkuat keamanan *cyber* di masing-masing negara sehingga kejahatan *cyber* dapat di tanggulangi dengan cepat dan tepat.

.

2.2.1 *Cooperation Security*

Pendekatan yang bisa di capai dalam sebuah organisasi tanpa ada sebuah gangguan setingkat internasional adalah melalui kerja sama keamanan (*cooperation security*). *Cooperation security* telah di jalankan dalam beberapa tahun yang lalu, *cooperation security* merupakan cara atau strategi sebuah negara agar dalam melakukan kerja sama bisa mencapai sebuah persetujuan tanpa harus memberikan paksaan ataupun tekanan (Schou at al, 2015).

Cooperation security adalah kerangka kerja sama melalui dialogis yang dianggap mampu menciptakan keamanan dengan cukup stabil sehingga proses kerja sama ini mampu memberikan rasa saling percaya, oleh karena itu *cooperation security* sering dilakukan melalui berbagai pendekatan khususnya pendekatan institusi karena kerja sama ini di lakukan antara negara satu dengan negara yang lain yang bersifat formal (*formal institusional*). *Cooperation security* jika dipahami lebih mendalam adalah sebuah kerangka yang lebih mengedepankan sinergisitas atas dasar kebersamaan agar keamanan sebuah negara tidak terganggu, hal itu tidak terlepas dari masing-masing sektor memiliki peran dan tanggung jawabnya secara internasional (Acharya, 2021).

Cooperation security juga sebagai cara negara untuk memperkuat keamanan secara lebih menyeluruh dengan jangka waktu yang cukup lama. Oleh karena itu dalam *cooperation security* bagian dari strategi pilihan yang cukup inovatif karena model keamanan yang dipilih lebih fleksiber dan bersahabat tanpa

paksaan dan tekanan sehingga mampu menggantikan *security againts adversary or enemy* dalam konsep *patnership security dialogue with enemy or adversary* dengan cara melakukan kerja sama keamanan dengan pihak lawan sekalipun melalui dialog kemanan multileteral dan bilateral (Schou at al, 2015). Dengan demikian *cooperation security* merupakan strategi jaminan keamanan dengan mengedepankan dialogis sebagai langkah pendekatan preventif sebagai upaya agar tidak terjadi konflik baik antara negara musuh maupun negara pesaing

Berdasarkan penjelasan tersebut maka konsep dari *cooperation security* menjadi rancangan keamanan yang pantas diperhitungkan sebab banyak perihal. Alibi kuncinya merupakan di masa kemajuan garis besar semacam saat ini ini, banyak kasus yang terletak di luar capaian serta kapasitas dari suatu negeri buat dituntaskan dengan cara tunggal.

Tantangan kontemporer yang telah nyata nampak serta butuh menemukan atensi merupakan isu- isu transnasional semacam bahaya terorisme, kasus area, evakuasi, kesalahan terencana, serta perdagangan obat. Namun, apalagi rumor keamanan konvensional juga saat ini sudah berganti jadi lingkungan yang menimbulkan tampak tak mungkin untuk sesuatu negeri buat mencegah kebutuhan nasionalnya tanpa terdapatnya kerja sama dengan negeri lain. Sebab seperti itu, banyak negeri yang melaksanakan kegiatan serupa bersumber pada rancangan dari *cooperative security* ini, dengan harapan semua pihak yang bertugas serupa bersama mempunyai kebutuhan buat melindungi keamanan bersama (Moodie, 2020).

Cooperative security di lakukan oleh banyak negara melalui sebuah kerja sama hal itu dikarenakan sebuah negara ingin mencapai keamanan secara bersama. Keamanan bersama (*common security*) dipublikasikan oleh Komisi Palme pada tahun 1980- 1989, keamanan ini berdialog kalau mereka yakin ikatan dampingi bintang film yang silih berselisih dapat diubah dengan menghasilkan kebijaksanaan keamanan yang silih tembus pandang serta tidak kasar. Tujuan kuncinya merupakan buat melenyapkan rasa silih berprasangka hendak arti pihak lain buat menghindari bentrokan bersenjata (Hechter, 2020).

Common security adalah pendekatan untuk mencapai keamanan nasional, regional, dan internasional dengan memperhatikan kebutuhan keamanan negara

lain, termasuk musuh, serta kebutuhan keamanan sendiri. Hal ini didasarkan pada keamanan yang berkelanjutan sehingga tidak dapat diperoleh dengan merusak atau mengancam keamanan negara lain, melainkan pada penyelesaian konflik dengan negara pesaing atau negara musuh serta memastikan keamanan di semua negara dapat di jalankan dengan tepat (*Policies for Common Security*, 2015).

Common security bergantung pada diplomasi, negosiasi, mediasi, dan bentuk penyelesaian konflik lainnya yang dilakukan oleh masing-masing negara, serta penerapan hukum internasional, untuk memastikan perdamaian, keadilan, dan keamanan bagi semua. Oleh karena itu dalam *common security* dijadikan sebuah pendekatan untuk menjalin hubungan antar negara (sebagai upaya untuk menyelesaikan masalah sehingga masing-masing negara yang menjalin kerja sama mendapat manfaat) (Threats, 2022).

Dalam *common security* tidak mengesampingkan pertahanan negara dan kekuatan militer sebagai komponen keamanan nasional. Namun, kerangka *common security* lebih menekankan pada penyelesaian konflik dan hukum internasional, dan mencadangkan pendekatan militer sebagai upaya terakhir untuk mengatasi agresi, jika semua metode lain gagal, dan selama penggunaan kekuatan tersebut sesuai dengan hukum internasional, oleh karena itu dalam *common security* tercipta *Confidence Building Measures* (CBM).

Confidence Building Measures (CBM) berdasarkan *United Nations Office of Disarmament Affairs* (UNODA) didefinisikan sebagai prosedur terencana untuk mencegah terjadinya perselisihan, mencegah terjadinya eskalasi, mengurangi ketegangan militer, serta membangun rasa percaya di antara negara-negara (UNODA, 2019). Sementara Marie-France Desjardin mendefinisikan CBM sebagai kumpulan aksi penguatan komunikasi dua arah berupa kunjungan maupun inspeksi ke negara lain, penerapan peraturan-peraturan atas berbagai latihan militer, termasuk juga dalam bidang sosial dan budaya, serta kerja sama dalam berbagai bidang (Haider dan Azad, 2021). Dari adanya dua definisi tersebut maka dapat digarisbawahi bahwa *Confidence Building Measures* (CBM) adalah serangkaian kegiatan terencana untuk mengurangi ketegangan militer dengan melakukan penguatan komunikasi dan pembagian informasi militer antar negara yang sedang mengalami perselisihan.

Mekanisme dari *Confidence Building Measures* (CBM) terdiri dari 3 yakni, *information* CBM yang merupakan pelaporan ke PBB dalam pembelian senjata, pertukaran personil militer dan lain sebagainya. Kemudian *constraint* CBM yang merupakan aspek untuk menumbuhkan kepercayaan di antara negara-negara melalui transparansi dan pembatasan kapabilitas militer dan *unilateral* CBM yang merupakan langkah negara secara sukarela untuk mendeklarasikan sesuatu untuk menumbuhkan kepercayaan dengan negara lainnya (Callabero, at al, 2016). Contoh dari *unilateral* CBM ini yakni Tiongkok yang mengemukakan tiga prinsip dalam pengembangan ekonomi, yakni tidak menggunakan *cyber power* untuk melakukan *spionase cyber* dengan motif ekonomi atau keuangan, tidak menggunakan *cyber power* yang di bangun hanya untuk kegiatan perlindungan domestik atau nasional dan *cyber power* yang di bangun juga tidak negara lain khususnya negara-negara mitra kerja sama di bidang *cyber* seperti Amerika Serikat.

2.2.2 Keamanan Kolektif (*Collective Security*)

Collective security adalah sebuah usaha beberapa negara yang bertindak bersama dengan rencana untuk meningkatkan keamanan mereka bersama. *Collective security* adalah bagian dari studi keamanan dan konsep keamanan secara umum. Untuk memahami kompleksifikasi konsep keamanan terdapat dua pendekatan yang mempelajari studi keamanan, yaitu cara pandang sempit dan luas. Untuk pendekatan dalam jangkauan yang sempit, para tradisionalisme memberikan pendapat bahwa konsep keamanan fokus pada kemampuan material dan isu-isu seputar penggunaan, ancaman, dan kontrol terhadap kekuatan militer, serta hal-hal yang menyangkut subjek politik sebagai fokus dari studi keamanan. Namun pada tahun 1970-1980-an agenda internasional mengenai ekonomi dan lingkungan mulai meningkat, disusul pada tahun 1990 dengan meningkatnya isu seputar identitas dan kejahatan internasional. Membuat definisi dari konsep keamanan menjadi sangat berbeda khususnya pada era *euroatlantic*. Perubahan definisi dari konsep keamanan membuat pendekatannya mulai terkonsentrasi pada cangkup yang lebih luas tidak hanya pada sektor Militer namun juga pada sektor politik, ekonomi, lingkungan, dan sosial (Andrew, 2014).

Collective security adalah prinsip hubungan internasional yang mendasarkan keamanan negara pada kerja sama antara negara-negara yang memiliki tujuan yang sama untuk mencapai keamanan bersama. Konsep keamanan kolektif adalah keamanan suatu negara dapat dipertahankan dengan menggabungkan kekuatan antar negara-negara. Dalam konsep *collective security*, negara-negara yang tergabung dalam suatu aliansi atau organisasi bekerja sama untuk menjamin keamanan bersama dan melindungi diri serta memiliki tanggung jawab bersama untuk melindungi negara dari ancaman (Mwagwabi, 2010).

Prinsip *collective security* mengandung asumsi bahwa keamanan internasional tidak dapat dicapai hanya dengan mengendalikan kekuatan militer dan tindakan unilateral dari satu negara saja, tetapi harus melibatkan kerja sama antara banyak negara yang berbeda. Dalam hal ini, setiap negara memiliki tanggung jawab untuk membantu melindungi keamanan dan kepentingan negara-negara lain, serta memperoleh dukungan dari mereka ketika menghadapi ancaman bersama. Konsep *collective security* ini bertujuan untuk mengurangi kemungkinan terjadinya perang dan meningkatkan stabilitas internasional melalui kerja sama antara negara-negara. Namun, implementasi dari prinsip ini tidak selalu mudah dan sering kali terkendala oleh perbedaan pandangan dan kepentingan negara anggota (Buzan et al., 1998).

Collective security dapat dilihat dalam bentuk sistem aliansi, aliansi juga berbasis pada prinsip satu untuk semua dan semua untuk satu seperti dalam prinsip *collective security*. Lebih spesifiknya, Aliansi berfungsi sebagai badan pertahanan kolektif yang melindungi anggotanya dari ancaman keamanan langsung dan lebih terfokus pada ancaman dari luar, sedangkan keamanan di dalam diurus secara kolektif oleh anggota. Bentuk lain yang mengilustrasikan pengaturan keamanan yang melawan balik ancaman internal yang datang dari anggota sebuah *collective security* hal ini didefinisikan sebagai *security community*. Prasyarat pembentukan *security community* sangat berbeda dan dapat dikatakan sangat luas. Selain itu negara-negara yang bergabung ke dalam *security community* memiliki hubungan yang sangat baik satu dengan yang lainnya, dalam sektor perekonomian, sosial dan politik, serta saling ketergantungan yang tinggi. Logika dasar dari sebuah *collective security* terletak pada dua hal. Pertama, mekanisme *balancing* yang diberlakukan di bawah *collective security* dapat mencegah perang dan menghentikan agresi, jauh

lebih efektif dibandingkan dengan mekanisme yang dilakukan dalam *setting* yang anarki. Kedua, *collective security* terinstitusi dengan pemikiran *all against one*, untuk berkontribusi dalam sistem internasional yang mana dalam keadaan stabil dapat menciptakan suatu hubungan kerja sama, bukan kompetisi (Aleksovski et al., 2014).

2.3 Kerangka Pemikiran

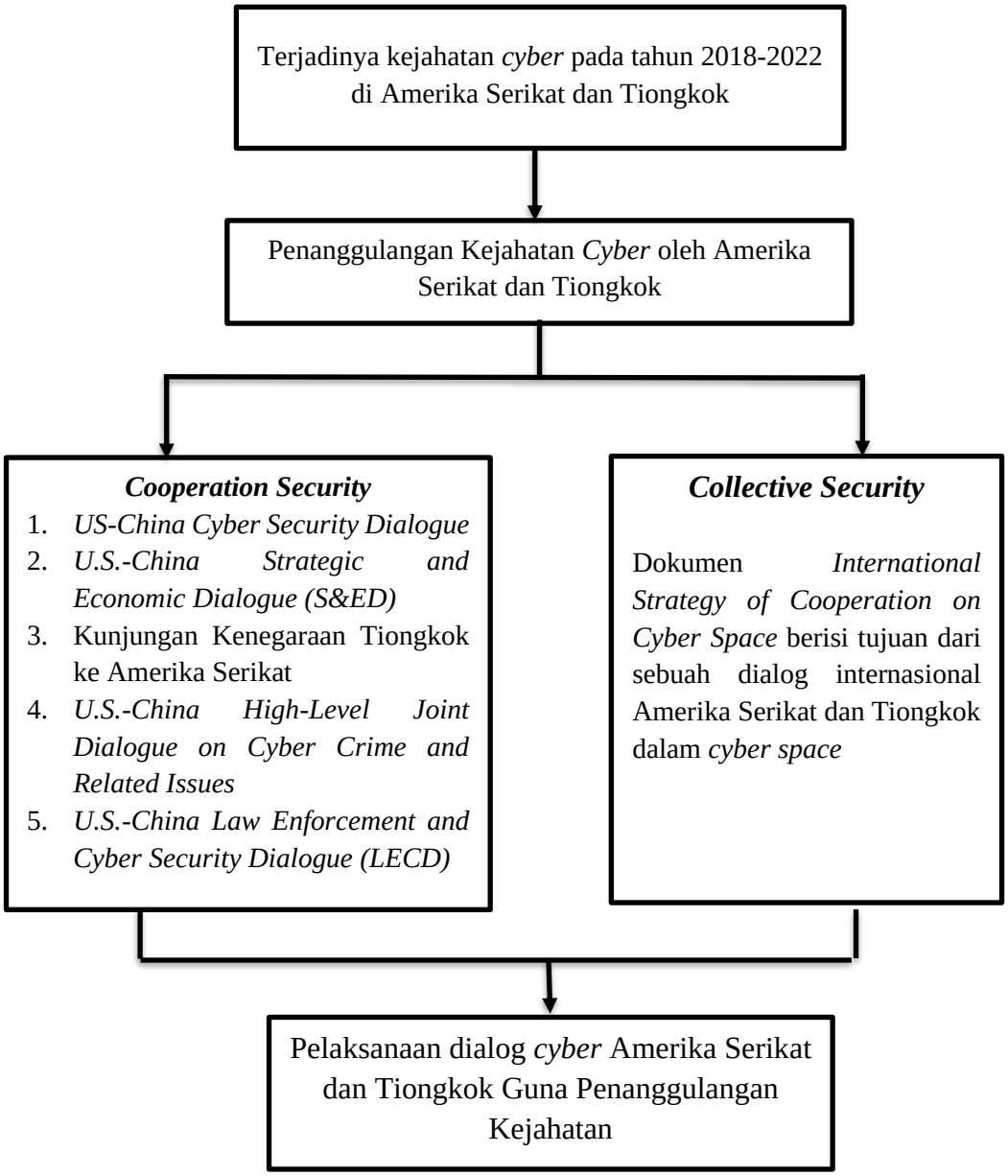
Kerja sama keamanan *cyber* Amerika Serikat dengan Tiongkok dilihat melalui aktivitas hubungan bilateral yang dilakukan oleh Amerika Serikat dengan Tiongkok untuk menangani permasalahan *cyber security*. Dalam proses kerja sama antara Amerika Serikat dengan Tiongkok pembahasan tentang *cyber space*, *cyber issues*, yaitu isu-isu dalam konteks *cyber* dalam penanggulangan kejahatan *cyber* yang diangkat dalam aktivitas dialog tersebut, dan dialog sebagai representasi negara yang membawa kepentingan politik. Dialog *cyber security* yang tercapai atau disepakati dilanjutkan dengan dialog tingkat tinggi dengan nama *U.S - China Law Enforcement and Cyber Security Dialogue* (LECD), sebuah kerangka kerja sama Amerika Serikat dengan Tiongkok.

Dialog yang di bangun oleh Amerika Serikat dengan Tiongkok merupakan langkah awal dari kedua negara untuk mencapai *cyber sovereignty*. Sesuai dengan politik luar negerinya dalam *cyber space*, dengan cara meningkatkan intensitas dialog *cyber security* baik Amerika Serikat dengan Tiongkok, untuk memaksimalkan dialog tersebut baik Amerika Serikat maupun Tiongkok memiliki *action plan*. *Action plan* sebagai upaya untuk memaksimalkan kerja sama antara Amerika Serikat dengan Tiongkok, *action plan* tersebut antara lain *US-China Cyber Security Dialogue, U.S.-China Strategic and Economic Dialogue (S&ED), U.S.-China High-Level Joint Dialogue on Cyber Crime and Related Issues* dan *U.S.-China Law Enforcement and Cyber Security Dialogue (LECD).*

Dilihat dari *action plan* kebijakan baik pemerintah Amerika Serikat maupun Tiongkok secara keseluruhan sebagai langkah untuk menjaga infrastruktur penting nasional. Kebijakan tersebut juga menunjukkan keseriusannya terhadap kebijakan *cyber security* untuk melindungi keamanan guna menanggulangi kejahatan *cyber* baik Amerika Serikat maupun Tiongkok tujuannya adalah untuk melakukan

pencegahan kerugian yang semakin besar akibat kejahatan *cyber* serta semakin memperkuat *cyber security* pada semua sektor baik pemerintah maupun swasta.

Untuk lebih jelas maka dapat dilihat dalam gambar kerangka analisis dan kerangka pikir seperti di bawah ini:



Gambar 2.1 : Kerangka Pemikiran

Sumber: diolah sendiri untuk keperluan penelitian

III. METODOLOGI PENELITIAN

Bab ini menyediakan penjelasan metodologis yang digunakan oleh peneliti. Bab ini terbagi ke dalam enam bagian, yaitu: tipe penelitian, tingkat analisis, fokus penelitian, jenis dan sumber data, teknik pengumpulan data dan teknik analisis data. Dalam penelitian ini, peneliti menggunakan jenis penelitian kualitatif dengan analisis deskriptif, dengan fokus penelitian yaitu pada pelaksanaan dialog keamanan *cyber* Amerika Serikat dengan Tiongko guna penanggulangan kejahatan 2018-2022. Sumber data yang dijadikan acuan oleh peneliti dalam penelitian ini ialah sumber-sumber sekunder. Data dan fakta dikumpulkan dengan menggunakan teknik studi literatur yang kemudian dianalisis menggunakan analisis interstate, untuk kemudian disajikan dan ditarik kesimpulannya berdasarkan data yang diperoleh.

3.1 Tipe Penelitian

Peneliti menggunakan metode penelitian kualitatif dengan teknik deskriptif, karena masalah yang dikaji berupa fenomena yang kompleks baik mencakup tempat, waktu, dan dinamika kejadian di dalamnya. Penelitian kualitatif lebih menekankan pada pernyataan dan data berbentuk teks daripada numerik secara pengumpulan maupun pengamatan data (Albarran, 2013). Maka, metode kualitatif yang dasarnya berbentuk data teks dikira menjadi pilihan yang cocok. Bahwa menurut Cresswell, penelitian kualitatif merupakan gambaran secara umum yang dianalisis mengenai fenomena dan kejadian secara historis (Creswell, 2014). Oleh karena itu demi memahami pelaksanaan dialog keamanan *cyber* Amerika Serikat dengan Tiongko guna penanggulangan kejahatan sehingga cenderung mengarah pada penggunaan kualitatif deskriptif.

3.2 Tingkat Analisis

Tingkat analisis disebut juga dengan level analisis yang digunakan untuk tujuan identifikasi cakupan dari sebuah penelitian. Berdasarkan pendapat dari Mochtar Masoed dalam buku Ilmu hubungan internasional disiplin dan metodologi bahwa terdapat kebutuhan penelitian yang mana penulis perlu menentukan unit analisis dan variabel dependen sehingga nantinya memberikan dampak yang diharapkan dari objek penelitian yang sedang diamati (Mas'oed, 2019). Dalam pemahaman lain**,** unit analisis adalah objek yang hendak dianalisis. Sedangkan unit eksplanasi adalah objek yang mempengaruhi unit analisis.

Kedua hal ini penting ketika hendak melakukan penelitian karena dengannya kita dapat mengetahui apa yang harus dianalisis dan diamati dalam mempelajari hubungan internasional. Dalam penelitian ini tingkat analisis memfokuskan pada pelaksanaan dialog keamanan *cyber* Amerika Serikat dengan Tiongko guna penanggulangan kejahatan 2018-2022. Oleh karena itu dalam tingkat analisis ini terbagi dalam tiga level, pertama level analisis sistem pada tahap ini peneliti akan menjelaskan distribusi kekuatan antar negara Amerika Serikat dengan Tiongkok sebagai negara *super power* yang melakukan dialog keamanan di bidang *cyber* guna penanggulangan kejahatan *cyber* oleh karena itu dalam level ini antar sesama pihak atau aktor yang terlibat dalam kerja sama saling mempengaruhi.

Level kedua adalah keterlibatan negara *(state-level-analysis*) pada tahap ini akan menjelaskan perilaku negara baik internal maupun eksternal dalam menjalin kerja sama antar negara *super power*, tingkat level analisis negara ini akan menghasilkan berbagai penjelasan yang tidak terlalu besar seperti pada tahap analisis sistem namun tidak juga terlalu kecil seperti dalam penelitian ini yang di wujudkan dalam kunjungan kenegaraan presiden Tiongkok ke Amerika Serikat untuk membahas berbagai guna penanggulangan kejahatan *cyber*. Leven analisis ketiga atau yang terakhir adalah level individu (*individual-level-analysis*) pada level ini peneliti lebih fokus pada pihak-pihak yang terlibat dalam pelaksanaan dialog keamanan *cyber* Amerika Serikat dengan Tiongko guna penanggulangan kejahatan yaitu dengan melihat keterlibatan seperti Sekretaris Keamanan Dalam Negeri Amerika Serikat dan Jaksa Agung Amerika Serikat serta partisipasi dari

perwakilan *Federal Bureau of Investigation* (FBI), badan-badan intelijen Amerika Serikat, *Centre for Strategic and International Studies* (*CSIS)* sedangkan dari Tiongkok mulai dari keterlibatan perwakilan Kementerian Keamanan Publik, Kementerian Keamanan Negara, Kementerian Kehakiman serta Kantor Internet dan Informasi Negara Tiongkok serta *China Institutes of Contemporary International Relations* (*CICIR*). Untuk lebih jelas tingkat analisis dapat dilihat dalam tabel di bawah ini:

Tabel 3.1 Level dan Unit Analisis Penelitian

Tingkat Analisis: Hubungan Amerika Serikat dengan Tiongkok	
Unit Analisis	Unit Eksplanasi
Dialog keamanan *cyber* yang dilaksanakan oleh Amerika Serikat dengan Tiongkok guna penanggulangan kejahatan	Analisis kejahatan *cyber* pada Amerika Serikat dengan Tiongkok

Sumber : Diolah oleh Peneliti untuk Kepentingan Penelitian

3.3 Fokus Penelitian

Fokus dibutuhkan dalam suatu penelitian supaya karya ilmiah mendapatkan spesifikasi yang jelas dan tidak begitu luas. Maka, fokus penelitian ini bertumpu pada:

1. Pelaksanaan dialog keamanan *cyber* Amerika Serikat dengan Tiongko guna penanggulangan kejahatan 2018-2022
2. Bentuk dialog keamanan *cyber* Amerika Serikat dengan Tiongko guna penanggulangan kejahatan 2018-2022.

3.4 Jenis dan Sumber Data

Dalam penelitian ini jenis datanya dipilih berdasarkan kondisi peneliti yang sedang menelaah objek penelitian yang jauh, oleh karena itu jenis sekunder lebih dipilih oleh peneliti. Data sekunder merupakan data yang didapatkan melalui

himpunan data yang diambil dari penelitian terdahulu, jurnal ilmiah, laman berita terpercaya, dan bahan pustaka lain.

Data sekunder yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Publikasi data terkait kerugian pada sektor keuangan oleh *Federal Bureau of Investigation Internet Crime Report United States of America*
2. GAO *Report of US-CERT*
3. *Cyberspace Policy Review*
4. Publikasi data terkait dengan *operating cyberspace* oleh *The Department of Defense (DoD) Cyber Strategy*
5. Publikasi data terkait dengan intelejensi *cyber* oleh *US Strategic Command* (Badan Intelijen) *United States of America*
6. Publikasi data serangan *cyber* oleh *US Cyber Command* (USCYBERCOM) sebagai Badan Pertahanan *Cyber* Militer
7. Publikasi data terkait dengan perIndungan informasi dan infrastruktur vital khususnya keuangan dari *National Security Agency* (NSA).

3.5 Teknik Pengumpulan Data

Peneliti memilih menggunakan data sekunder maka teknik dalam mengoleksi data yang cocok melalui studi literatur dan dokumentasi. Dengan kajian pustaka akan dilakukan riset melalui studi pustaka yang telah diklasifikasikan dan disinkronkan dengan kebutuhan. Terdapat beberapa tempat untuk mengumpulkan data dari studi pustaka, yaitu termasuk dengan buku, jurnal penelitian, situs yang kredibel, serta dokumen-dokumen resmi yang ditelusuri di internet.

Kemudian pada dokumentasi akan dilakukan pengambilan data seperti merekam histori dari peristiwa terdahulu. Oleh karena itu, data yang akan diperoleh akan dihimpun dari laman resmi yang terpercaya, misalnya website resmi Pemerintah Amerika Serikat dan dokumen dari Departemen Pertahanan Amerika Serikat.

3.6 Teknik Analisis Data

Teknik analisis sekunder merupakan teknik yang dipilih oleh peneliti dalam penelitian ini. Menurut Huberman dan Miles, aktivitas analisis data sekunder merupakan teknik yang menggunakan data yang telah ada, tersedia, dan telah diteliti sehingga sumber data yang diperoleh dapat dikembangkan dan disesuaikan dengan yang dibutuhkan dalam penelitian ini.

Dalam suatu kutipan, Miles dan Huberman mengemukakan bahwa terdapat sejumlah tiga teknik analisis data dalam penelitian kualitatif, yakni (Huberman, 2005), **Kondensasi data** yaitu seleksi data yang dipilih berdasarkan prioritas yang paIng relevan dan cocok dalam penelitian. Lalu, **Penyajian data** yaitu aktivitas menganalisis data kualitatif yang dilakukan dengan menyusun informasi yang telah dikumpulkan, lalu menarik kesimpulan. Bentuk penyajian data kualitatif dapat disajikan berupa grafik, gambar, dan himpunan data teks. Kemudian, **Penarikan kesimpulan** yaitu hasil akhir kumulasi data dan penyajian serta analisis yang dapat ditarik kesimpulannya oleh peneliti. Data yang akan dianalisis dalam penelitian ini terkait dengan strategi keamanan siber Amerika Serikat melalui kerja sama dengan Tiongkok guna Penanggulangan kejahatan pada sektor industri keuangan.

V. SIMPULAN DAN SARAN

Bab ini akan menguraikan tentang simpulan dan saran sesuai dengan pertanyaan yang diajukan dalam penelitian ini, penelitian ini akan menguraikan jawaban sesuai dengan tujuan penelitian oleh karena dalam penelitian ini juga akan menguraikan poin-poin utama dari setiap dialog keamanan Amerika Serikat Dengan Tiongko guna penanggulangan kejahatan *cyber*. Selanjutnya juga akan menguraikan saran yang di tunjukan kepada pihak-pihak terkait khususnya kepada negara yang menjalin dialog keamanan siber yaitu Amerika Serikat dan Tiongkok.

5.1 Simpulan

Dialaog keamanan yang dilaksanakan oleh Amerika Serikat dengan Tiongkok guna penanggulangan kejahatan *cyber* dilakukan melalu berbagai forum dialog. Didalam forum dialog tersebut diangkat isu-isu *cyber* termasuk permasalahan kerugian perusahaan akibat kejahatan *cyber.* Aktivitas dialog yang dilakukan oleh Amerika Serikat dengan Tiongkok terbagi menjadi dua bentuk, yaitu dialog sebelum tercapainya kesepakatan *cyber security* antara Amerika Serikat dengan Tiongkok, keduanya berupaya untuk menyamakan pandangan dalam *US-China Cyber security Dialogue*. Jalur dialog resmi antar pemerintah pertama untuk membahas persoalan *cyber security* adalah *U.S.-China Strategic and Economic Dialogue*. Didalamnya terdapat sebuah *cyber working group* yang dikhususkan untuk membahas permasalahan *cyber space* pada Amerika Serikat dengan Tiongkok.

Pelaksanaan dari dialog tersebut berupaya untuk diwujudkan melalui forum dialog *U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues*, pada akhirnya isu *cyber security* dalam kerja sama Amerika Serikat dengan Tiongkok tergabung dalam kerangka U*.S.- China Law Enforcement and Cyber*

Security Dialogue dalam agenda tersebut terlihat adanya beberapa isu *cyber* yang menjadi agenda di dalam aktivitas dialog keamanan *cyber* yang dilakukan oleh Amerika Serikat dengan Tiongkok. Isu-isu siber tersebut antara lain adalah isu *cyberse curity* pada perusahaan atau industri komersil, *cyber crime* pada perusahaan atau industri komersil, *confidence building*, dan *internet governance*.

5.2 Saran

Berdasarkan hasil penelitian yang sudah di uraikan di atas maka dapat penulis berikan saran antara lain:

1. Setiap negara diharapkan untuk mengembangkan, memperkuat dan juga meningkatkan kapasitas keamanan *cyber* negara sebagai upaya penanggulangan kejahatan *cyber* yang saat ini menjadi target utama *cyber crime*. Hal itu dikarenakan keamanan internasional sedang tidak kondusif dengan terus terjadinya serangan *cyber* baik melalui aktor individu, kelompok *hacker* baik secara mandiri maupun disponsori oleh negara, murni serangan *cyber* dari negara, dan berbagai macam aktor lainnya yang tidak bisa dipastikan kapan dan siapa yang akan melakukan serangan *cyber*
2. Negara harus memainkan peran dalam organisasi internasional untuk mencapai konsensus bersama terkait norma *cyber* yang sedang dibahas melalui forum Perkembangan Informasi dan Telekomunikasi dalam Konteks Keamanan Internasional (UNGGE) dan *Open-Ended Working Group* (*OEWG*). Tatanan internasional membutuhkan norma yang mengatur perilaku dan batasan dalam ruang *cyber*. Hal itu dikarenakan berdasarkan data yang ditemukan dalam penelitian, serangan *cyber* mengakibatkan perusahaan-perusahaan swasta mengalami kerugian dan ketidak stabilan dalam menjalankan bisnis
3. Amerika Serikat dengan Tiongkok hendaknya terus melakukan dialoh keamanan *cyber* baik bilateral maupun multilateral karena dialog ini memberikan manfaat dan keuntungan dari adanya dialog tersebut.

DAFTAR PUSTAKA

Albarran, A. B. (2013). *The Social Media Industries*, New York: Routledge.

Austin, G. (2018). *Cybersecurity in China The Next Wave*, Springer.

Acharya, A. (2021). *Constructing a security community in Southeast Asia: ASEAN and the problem of regional order: Second edition*.

Assembly, G. (2010). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/65/201, 2010, http://www.unidir.org/files/medias/pdfs/final-report-eng-0-189.pdf, diakses pada 07 April 2023.

Baezner, M. (2018). *Cybersecurity in Sino-American Relations*, CSS Analyses in Security Policy, No.224

Baylis, J., dan Smith, S. (1997). *The Globalization of Word Politics an Introduction to Internasional Relations*, New York: Oxford University Press

Buzan, B. (1991). *People, States and Pear: An Agenda for Internasional Security Studies in the Post Cold War*, Bunder: Lynne Rinner Publishers

Brown. G., Yung. C.D. (2017). *Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace*. Melalui https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurityagreement-part-1-the-us-approach-to-cyberspace/, diakses pada 07 April 2023

Callabero, M., Anthony and Emmers, Ralf. (2016). *Understanding the Dynamic of Securitizing Non TraditionalSecurity dalam Non-Traditional Security in Asia*, Singapore: Nanyang Technological University, Ashgate.

Cavelty, M.D. (2012). *Cyber Security*, Oxford:Oxford University Press.

Center For Strategic and International Studies (CSIS). (2022). *Significant Cyber Incidents*, dalam https://www.csis.org/programs/strategic-technologiesprogram/significant-cyber-incidents

China Internet Network Information Center (CNNIC). (2021). *Statistical Report on Internet Development in China*..

Choucri, N. (2012). *Cyberpolitics in International Relations*, Cambridge : MIT Press.

China Daily. (2018). Summary of outcomes of First China-US Law Enforcement and Cybersecurity Dialogue, 2018, http://www.chinadaily.com.cn/world/2017-10/06/content_32924234.htm

China Institute of Contemporary International Relations (CICIR) and Center for Strategic and International Studies (CSIS). (2022). *Bilateral Discussions on Cooperation in Cybersecurity*, https://www.thecre.com/fnews/?p=1105

Center for Strategic and International Studies (CSIS). (2022). *Deep Comprehension of the Global Security Initiative: Coordinating Our Own Security and Common Security*, https://interpret.csis.org/translations/deep-comprehension-of-the-global-security-initiative-coordinating-our-own-security-and-common-security/

Creswell, J.W. (2016). *Research Design Pendekatan Kualitatif, Kuantitatif, dan Mixed.* Yogyakarta: Pustaka Pelajar.

Chris Ott. (2022). *What You Should Know About The 24/7 Cybercrime Network*, https://www.dwt.com/files/uploads/documents/publications/What%20You%20Should%20Know%20About%20The%2024.pdf

Cohen, R., and Mihalka, M. (2021). *Cooperative Security: New Horizons for International Order*, Marshall Center Paper No. 3, Garmish-Partenkirchen, Germany: George C. Marshall European Center for Security Studies.

Davila, J.M. D.L.T. (2023). *Cybersecurity and United States-China Relations: A Theoritical Perspective*, International Master's Program in International Studies National Chengchi University

Department of Justice United States of America. (2017). *First U.S.-China Law Enforcement and Cybersecurity Dialogue Summary of Outcomes*. Available from.

Department Of Defense Cyber Strategy. (2021). *Summary DoD_Cyber_Strategy*, https://www.defense.gov/Portals/1/features/0415_cyber-strategy/Final_DoD_CYBER_STRATEGY_for_web.pdf

Embassy of the People's Republic of China in the United States of America. (2021). *U.S.-China Strategic and Economic Dialogue Outcomes of the Strategic Track*, http://www.china-embassy.org/eng/zmgxss/t1058593.htm

Embassy of the People's Republic of China in the Republic of Kenya, The Third China-U.S. (2021). *Strategic Security Dialogue Held in Washington, D.C*, http://us.china-embassy.gov.cn/eng/zmgx/zxxx/201307/t20130711_4908623.htm

Embassy of the People's Republic of China in the United States of America. (2021). *U.S.-China Strategic and Economic Dialogue Outcomes of the Strategic Track*, http://us.china-embassy.gov.cn/eng/

Fang, B. (2018). *Cyberspace Sovereignty Reflections on Building a Community of Common Future in Cyberspace*, Springer.

Federal Bureau of Investigation. (2021). *Internet Crime Report. 2021*

Finnermore, M., dan Hollis, D.B. (2016). *Constructing Norms for Global Cybersecurity*, The American Journal of International Law, Vol.110, No.3.

Geng, Z. (2018). *An Analysis of Cyberspace Rule-Making in China-US Relations*, International Relations and Diplomacy, Vol. 6, No.1

Gertz, B. (2023). *Obama Rejected Tough Options for Countering Chinese cyber Attacks Two Years Ago*, https://www.washingtontimes.com/news/mar/10/Biden-rejected-tough-options-countering-chinese-cy

Goldstein, J.S., and Jon C.P. (2020.) *International Relations Tenth Edition*. United States of America: Pearson Education Limited.

Harold, S.W., Libicki, Martin. C., Cevallos, A.S. *Getting to Yes with China in Cyberspace*, tt, Getting to Yes with China in Cyberspace, https://www.rand.org/pubs/research_reports/RR1335.html

Haftendorn, H. (1991). *The Security Puzzer: Theory Bulding and Discipline in Internasional Security*, Internasional Studies Quarterly, Vol. 35, No.1

Hechter, M. (2020). *Nationalism and Rationality*, Journal of World System Research, Vol. VI, No. 2

Huberman, M. (2005). *Qualitative Data Analysis*. Jakarta : UI Press.

Interpol. (2022). *Cybercrime*, https://www.interpol.int/Crimes/CybercrimeCybercrime

Jackson-Preece, J. (2011) *Security in International Relations*, London: University of London.

Kshetri, N. (2013). *Cybercrime and cyber-security issues associated with China: some economic and institutional considerations*, Electronic Commerce Research no. 13 (2013), pp. 41–69 (p.42).

Kuehl, D.T. (2009). *From Cyberspace to Cyberpower: Defining the Problem*, *Cyberpower and National Security*, Washington, D.C: National Defense UP.

Liaropoulos, A. (2013). *Great Power Politics in Cyberspace: U.S. and China are Drawing the Ines Between Confrontation and Cooperation*, PANORAMA of Global Security Environment.

Liofa, P.H. (2002). *Boomerang Effect: The Convergence of Nationnal and Human Security*, Security Dialogue, Vol.33, No.4

Louie, C. (2021), U*.S.-China Cybersecurity Cooperation*, https://jsis.washington.edu/news/u-s-china-cybersecurity-cooperation/

Mearsheimer, J.J. (2001). *The Tragedy of Great Power Politics*, New York: Norton.

Moodie, M. (2020). *Cooperative Security: Implications for National Security and International Relations dalam Cooperative Monitoring Center Occasional Paper/14*. Albuquerque; Sandia National Laboratories.

Mihalka, M., dan Cohen, R. (2021). *Cooperative Security: New Horizons for International Order*, Marshall Center Paper No. 3, Garmish-Partenkirchen, Germany: George C. Marshall European Center for Security Studies.

Muladi. (2012). *Pemanfaatan Kerjasama Keamanan (Cooperative Security) untuk Menghadapi Bahaya Keamanan Komprehensif (Comphrehensive Security Threat) dalam Rangka Ketahanan Nasional dan Memperkokoh NKRI*. Jakarta: Bahan Ceramah PPRA dan PPSA Lemhannas

NATO Cooperative Cyber Defence Centre of Excellence. (2018). *Cyber Security Strategy Documents*.

Policies for Common Security. (2015). *Papers from the SIPRI Conference on Common Security*, Published by Taylor & Francis.

Qingchuan, Y. (2013). *Commentary: China-U.S. dialogue to Transcend Talks of Cyber Security*, China Central Television, http://english.cntv.cn/20130710/103009.shtml

Saputera, Y. (2015). *Pengaruh Cyber Security Strategy Amerika Serikat Menghadapi Ancaman Cyber Warfare*, Jom FISIP Volume 2 No.2

Segal, A. (2017). *Chinese Cyber Diplomacy in a New Era of Uncertainty', Hoover Working Group on National security*, Technology, and Law, Aegis Paper Series No. 1703, Stanford University.

Schia, N.N., and Gjesvik, L. (2017). *China's Cyber Sovereignty,* The Norwegian Institute of International Affairs.

Schou, Corey D., Trimmer., dan Kenneth J. (2015). *Information Assurance and Security*, Journal of Organizational and End User Computing on Information Security.

Shi, B. (2015). *National Cybersecurity Strategy of the US and Its Constructive Implications for China*, Sociology Study, Vol.5, No.11

Simamora, H. (2013). *Manajemen Sumberdaya Manusia*. Yogyakarta: Sekolah Tinggi Ilmu Ekonomi YKPN.

Tiezzi, S. (2015). *A delegation of Chinese officials visited the U.S. For Talks on Cybersecurity Issues*, https://thediplomat.com/2015/09/us-china-hold-cyber-talks-before-xis-visit/

The Ministry of Foreign Affairs of the People's Republic of China, (2015). *Full Text: Outcome list of President Xi Jinping's state visit to the United States*, https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1300771.shtml

The State Council The People's Republic of China. (2016) *China, US urge maintenance of bilateral dialogue mechanism to combat cybercrime*, http://english.www.gov.cn/state_council/state_councilors/2016/12/08/content_281475510995959.htm

Threats, N. (2020). *Common Security And Disarmament, A Reflection on The 35th Anniversary of New Zealand's Nuclear Weapons Ban, and What We Can Do Now to Prevent Nuclear War and Achieve Global Nuclear Abolition*. Alyn Ware.

T. Stevens. (2012). *A cyberwar of ideas?: Deterrence and norms in cyberspace.* Contemporary Security Policy, Vol. 33, No.1.

The White House. (2021). *Remarks by President Obama and President Xi Jinping of the People's Republic of China After Bilateral Meeting*, https://obamawhitehouse.archives.gov/the-press-office/2013/06/08/remarks-president-obama-and-president-xi-jinping-peoples-republic-china-

The White House. (2021). *FACT SHEET: President Xi Jinping's State Visit to the United States***,** https://whitehouse.archives.gov/the-press-office/fact-sheet-president-xi-jinpings-state-visit-united-states

The White House. (2022). *The National Strategy to Secure Cyberspace*, Washington, diakses di https://georgewbush-whitehouse.archives.gov/pcipb/.

Toft, P. (2005). *John J. Mearsheimer: an Offensive Realist Between Geopolitics and Power*, Journal of International Relations and Development, https://www.researchgate.net/publication/263323588

United Nations Department of Economic and Social Affairs. (2018). *Population And Vital Statistics Report Statistical Papers Series A Vol. LXX*.

Usito (United States Information Tecnology Office, (tt), *US-China S&ED, CWG and SSD Key Outcame*, https://usito.org/news/us-china-sed-cwg-and-ssd-key-outcomes

U.S. Department of Justice. (2020). *Second U.S.-China Cybercrime and Related Issues High Level Joint Dialogue*, https://www.justice.gov/opa/pr/second-us-china-cybercrime-and-related-issues-high-level-joint-dialogue

U.S. Department of the Treasury. (2023). *U.S. Fact Sheet – Economic Track Fifth Meeting of the U.S.- China Strategic and Economic Dialogue*, https://www.treasury.gov/press-center/press releases/Pages/.aspx

U.S. Department of Justice. (2020). *First U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues Summary of Outcomes*, https://www.justice.gov/opa/pr/first-us-china-high-level-joint-dialoguecybercrime-and-related-issues-summary-outcomes-0

Valeriano, B, Maness., dan Ryan. C. (2021). *The Dynamics of Cyber Conflict between Rival Antagonist*, Journal of Peace Research, Vol.51, No.3

www.statista.com/statistics/1310985/number-of-cyber-incidents-in-financial-industry-worldwide

Xinbao, Z. (2016). *The Governance Model of Cyberspace Sovereignty and Its System Construction*, Chinese Social Sciences, No. 8.

Yildirim, E.Y. (2016). *The Importance of Risk Management in Information Security*, IIER International Conference, ISBN: 978-93-86083-34-0

Ziolkowski, K. (2013). *Confidence Building Measures for Cyberspace', in K. Ziolkowski (Ed.), Peacetime regime for state activities in cyberspace: International law, international relations and diplomacy*, Tallinn: NATO Cooperative Cyber Defence Centre of Excelle.