PERBANDINGAN *CYBER SECURITY* TIONGKOK DAN AMERIKA SERIKAT TERKAIT *CYBER WARFARE*, 2016–2021

(Skripsi)

Oleh

SHINDI PHILADELPIA

1816071012

FAKULTAS ILMU SOSIAL DAN ILMU POLITIK
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG
2024

ABSTRAK

PERBANDINGAN *CYBER SECURITY* TIONGKOK DAN AMERIKA SERIKAT TERKAIT *CYBER WARFARE*, 2016–2021

Oleh

SHINDI PHILADELPIA

Cyberwarfare antara Tiongkok dan Amerika Serikat mencerminkan ketegangan dalam politik global saat ini. Penelitian ini bertujuan untuk mendeskripsikan konflik *cyber* antara kedua negara besar tersebut dan menganalisis strategi mereka dalam penyelesaian konflik melalui keamanan *cyber* dan kerja sama internasional. Dengan menggunakan metodologi penelitian kualitatif dan deskriptif, dengan strategi yang diambil oleh masing-masing negara dalam menangani ancaman *cyber*.

Amerika Serikat telah mengedepankan kolaborasi internasional dan transparansi, dengan menekankan pentingnya tindakan pencegahan serta strategi respons yang efektif terhadap ancaman *cyber*. Di sisi lain, Tiongkok telah memfokuskan strateginya pada pengendalian domestik, pengembangan kemampuan *cyber*, serta melancarkan serangan *cyber* yang terukur untuk mempengaruhi negara lain sesuai dengan kepentingan strategisnya.

Perbedaan dalam pendekatan keamanan *cyber* antara Tiongkok dan Amerika Serikat memiliki dampak signifikan tidak hanya pada keamanan *cyber* nasional, tetapi juga pada dinamika global. *Cyber defense* muncul sebagai area potensial untuk kolaborasi, kedua negara memiliki kepentingan bersama dalam melindungi infrastruktur kritis dan meningkatkan kesiapsiagaan terhadap ancaman *cyber*. Serta keterlibatan kedua negara dalam forum internasional dapat mempengaruhi norma global cybersecurity dan menciptakan tantangan serta peluang untuk kolaborasi di masa depan.

Kata kunci: *cyberwarfare*, *cyber*, Tiongkok, Amerika Serikat

ABSTRACT

COMPARISON OF CYBER SECURITY BETWEEN CHINA AND THE UNITED STATES RELATED TO CYBER WARFARE, 2016–2021

By

SHINDI PHILADELPIA

Cyberwarfare between China and the United States reflects the tensions in current global politics. This study aims to describe the cyber conflict between these two major nations and analyze their strategies in conflict resolution through cybersecurity and international cooperation. Using qualitative and descriptive research methodologies, this study examines the strategies adopted by each country in addressing cyber threats.The United States has emphasized international collaboration and transparency, highlighting the importance of preventive measures and effective response strategies to cyber threats. In contrast, China has focused its strategy on domestic control, the development of cyber capabilities, and conducting measured cyberattacks to influence other countries in line with its strategic interests.The differences in cybersecurity approaches between China and the United States have significant impacts not only on national cybersecurity but also on global dynamics. Cyber defense emerges as a potential area for collaboration, as both countries share common interests in protecting critical infrastructure and enhancing preparedness against cyber threats. Furthermore, the engagement of both nations in international forums can influence global cybersecurity norms and create both challenges and opportunities for future collaboration.

Key words: *cyberwarfare*, *cyber*, China, United States

PERBANDINGAN *CYBER SECURITY* TIONGKOK DAN AMERIKA SERIKAT TERKAIT *CYBER WARFARE*, 2016–2021

Oleh

SHINDI PHILADELPIA

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	:	**PERBANDINGAN *CYBER SECURITY* TIONGKOK DAN AMERIKA SERIKAT TERKAIT *CYBER WARFARE*, 2016–2021**
Nama Mahasiswa	:	***Shindi Philadelpia***
Nomor Pokok Mahasiswa	:	**1816071012**
Jurusan	:	**Hubungan Internasional**
Fakultas	:	**Ilmu Sosial dan Ilmu Politik**

MENYETUJUI

1. Komisi Pembimbing

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

Indra Jaya Wiranata, S.IP., M.A
NIP. 199212192022031011

2. Ketua Jurusan Hubungan Internasional

Simon Sumajoyo H. S.A.N., M.PA.
NIP. 198106282005011003

MENGESAHKAN

1. **Tim Penguji**

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

Sekretaris : Indra Jaya Wiranata, S.IP., M.A

Penguji Utama : Hasbi Sidik, S. IP., MA.

2. **Dekan Fakultas Ilmu Sosial dan Ilmu Politik**

Dr. Anna Gustina Zainal, S.Sos., M.Si
NIP. 197608212000032001

Tanggal Lulus Ujian Skripsi: **16 Oktober 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 sebutkan 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.

Bandarlampung, 16 Oktober 2024
Yang membuat pernyataan,

Shindi Philadelpia

NPM 1816071012

RIWAYAT HIDUP

Penulis bernama lengkap Shindi Philadelpia lahir di Bandar Lampung pada 28 Februari 2000. Penulis adalah anak pertama dari tiga bersaudara, dari pasangan yang berbahagia yaitu bapak Suheri dan ibu Khelsi Sarie.

Penulis menyelesaikan Pendidikan di TK IKI PTPN 7, SDN 2 Labuhan Ratu tahun 2012, SMPN 22 Bandar Lampung tahun 2015, SMAN 3 Bandar Lampung tahun 2018.

Pada tahun 2018, penulis diterima sebagai mahasiswa program S-1 di Jurusan Hubungan Internasional Fakultas Ilmu Sosial dan Politik melalui jalur SNMPTN. Selama menempuh studi, saya beberapa kali ikut aktif terlibat dalam penyelenggaraan kegiatan kampus. Selain itu, dalam berbagai kesempatan saya ikut ke dalam seminar yang diadakan oleh kampus maupun luar kampus. Pada tahun 2021, saya berkesempatan magang di Divisi Hubungan Internasional Kepolisian Republik Indonesia dan juga melaksanakan Kuliah Kerja Nyata (KKN) yang bertempat di Kelurahan Metro Barat pada tahun 2020.

MOTTO

"*Maka sesungguhnya, bersama kesulitan ada kemudahan. Sesungguhnya, bersama kesulitan ada kemudahan."*

(Q.S Al – Inshirah 94:5-6)

"She believed in the beauty of her dreams and the power of her heart, embracing life with a calm spirit."

(Audrey Hepburn)

PERSEMBAHAN

Saya persembahkan skripsi ini sebagai bentuk hasil dari usaha, tanggung jawab dan rasa terima kasih untuk:

Segala puji bagi Allah SWT yang telah memberikan segala kemudahan, kelancaran, dan ketabahan dalam setiap langkah penyusunan skripsi ini. Dengan izin-Nya, penulis dapat menyelesaikan tugas akhir ini dengan penuh kelancaran dan meraih hasil yang memuaskan.

Kedua orang tuaku yang sangat saya sayangi,

Bapak Suheri dan Ibu Khelsi Sarie

Tulisan ini merupakan ungkapan terimakasih yang mungkin tidak pernah cukup untuk membalas limpahan kasih sayang dari kedua orang tua yang selalu mendoakan. Segala pencapaian ini tidak terlepas dari lantunan doa, usaha keras, dan semangat. Saya selalu bersyukur kepada Tuhan karena dilahirkan dari orangtua yang hebat seperti Bapak dan Ibu.

Kedua saudaraku dan segenap keluarga besar yang selalu mendukung.

Diri Sendiri,

karena telah menjaga harapan dan cita-cita dengan tidak menyerah, bahkan di saat-saat sulit demi masa depan yang sedangku perjuangkan.

SANCAWACANA

Puji Syukur tak hentinya saya ucapkan kepada Allah SWT karena berkah dan karunia-Nya penelitian dengan judul Strategi penyelesaian konflik Tiongkok dan Amerika Serikat terhadap *cyber warfare* 2016 – 2021 ini dapat diselesaikan, sebagai syarat untuk dapat meraih gelar sarjana Hubungan Internasional di Universitas Lampung. Penulis mengucapkan terima kasih kepada semua pihak yang telah berperan dalam memberikan doa, dukungan, dan bantuan kepada penulis, yaitu:

1. Tuhan Yang Maha Esa, Allah SWT Yang Maha Pengasih, Maha Penyayang atas segala karunia dalam hidup serta Nabi Muhammad SAW sebagai utusan Allah SWT.
2. Prof. Dr. Ir. Lusmeiila Afriani, D.E.A., I.P.M., selaku Rektor Universitas Lampung.
3. Dr. Anna Gustina Zainal, S.Sos, M.Si., selaku Dekan Fakultas Ilmu Sosial dan Ilmu Politik Universitas Lampung.
4. Bapak Simon Sumanjoyo Hutagalung, S.A.N., M.P.A., selaku Ketua Jurusan Hubungan Internasional Universitas Lampung.
5. Bapak Iwan Sulistyo S.Sos., M.A. selaku Dosen Pembimbing Akademik dan Dosen Pembimbing Skripsi atas segala kesediaan, kesabaran, dan keikhlasannya dalam memberikan bimbingan dan ilmu kepada penulis selama perkuliahan hingga saat ini.
6. Bapak Indra Jaya Wiranata S.IP., M.A. selaku Dosen Pembimbing Pembantu Skripsi dalam membantu memberikan kritik, saran, dan nasihat kepada penulis selama pengerjaan skripsi ini.
7. Bapak Hasbi Sidik, S.IP., M.A., selaku Dosen Penguji Skripsi, yang telah memberikan banyak bantuan, motivasi, dan juga saran yang membangun agar skripsi penulis dapat lebih baik lagi.

8. Seluruh jajaran Dosen Hubungan Internasional Universitas Lampung beserta Staff Jurusan yang telah membantu dan memberikan ilmu yang bermanfaat.
9. Untuk kedua orang tuaku tercinta, papa dan mama yang selalu memberikan semangat dan bekerja keras untuk selalu memenuhi segala kebutuhan penulis, terima kasih telah menjadi sumber inspirasi dan kekuatan dalam hidup penulis. Kalian adalah alasan penulis bertahan dan terus melangkah dalam proses penyelesaian skripsi ini, terima kasih telah menjadi orang tua yang hebat, yang selalu percaya dan mendukung penulis di setiap langkah perjalanan hidup ini. Keyakinan kalian bahwa penulis mampu mencapai impian telah memberi semangat yang tiada henti. Penulis merasa sangat beruntung memiliki orang tua seperti kalian. Jika ada kehidupan selanjutnya, penulis akan tetap memilih untuk menjadi anak kalian. Terima kasih atas semua cinta dan kasih sayang yang telah kalian berikan.
10. Kedua saudara penulis, Shakia Adira dan Shandi Alditya Ardana yang selalu memberikan dukungan dan warna dalam hidup penulis. Kehadiran kalian membuat setiap tantangan dalam proses penyelesain skripsi ini terasa lebih ringan dan penulis sangat bersyukur mempunyai saudara seperti kalian. Semoga kita terus saling mendukung dan menginspirasi satu sama lain dalam setiap langkah yang kita ambil.
11. Teman- teman seperjuangan rahasia negara: Titis Pratita Pambayun, Awalia Sukma Chantika, Diajeng Bella Puspita dan Febrina Septiana Putri. Terimakasih telah menjadi teman terbaik dari awal hingga akhir. Dapat berteman dengan kalian menjadi hal yang penulis amat syukuri dan *one of the best things that ever happened in university life.* Setiap tawa, cerita, dan perjuangan yang telah kita bagi membuat perjalanan ini terasa lebih mudah. Semoga kita terus saling mendukung di masa depan. *My go-to person, my ride or die, my partner in crime,* terima kasih untuk semuanya.
12. Teman-teman cgalxy dan chewy, yang dalam segala kondisi selalu mengerti dan memberikan semangat penulis dalam proses penyelesaian skripsi ini. Bahkan di saat-saat tersulit, kalian selalu membuat penulis tersenyum. Terima kasih penulis sangat menghargai kehadiran kalian.

13. Teman seperjuangan penulis, M. Calakdo Islami, Putranda Satria dan M. Ghazi Ramadhan Jauhari yang selalu membantu dan menjadi pendengar yang baik dalam hal perkuliahan. Terima kasih telah menemani dan selalu ada di setiap penulis merasa butuh.
14. Teman-teman jurusan Hubungan Internasional angkatan 2018 yang telah saling memberikan bantuan dan dukungan selama perkuliahan. Semoga kita semua selalu diberikan perlindungan oleh Allah dan dituntun jalannya menuju kesuksesan.
15. Terakhir kepada diri sendiri, yang telah berjuang meskipun banyak tantangan menghadang. Di setiap langkah perjalanan ini, ada saat-saat lelah dan putus asa, namun tetap memilih untuk melanjutkan. Terima kasih telah berani menghadapi kesulitan. Setiap halaman skripsi yang ditulis adalah bukti kerja keras dan dedikasi. Bangga telah sampai di titik ini, meskipun banyak rintangan. Berbahagialah selalu dimanapun berada, Shindi. Apapun kurang dan lebihmu mari merayakan diri sendiri.

Akhir kata, penulis menyadari bahwa dalam penyusunan skripsi ini masih terdapat kekurangan karena keterbatasan dan pengetahuan yang penulis miliki. Oleh karena itu, segala bentuk kritik, saran, dan masukan yang membangun dari seluruh pihak sangat diharapkan untuk pengembangan dan kesempurnaan skripsi ini.

Bandar Lampung, 16 Oktober 2024

Penulis,

Shindi Philadelpia

DAFTAR ISI

Halaman

DAFTAR GAMBAR

DAFTAR SINGKATAN

APEC	: *Asia-Pacific Economic Cooperation*
CAC	: *Cyberspace Administration of China*
CDM	: *Continuous Diagnostics and Mitigation*
CISA	: *Cybersecurity and Infrastructure Security Agency*
CNCI	: *Comprehensive National Cybersecurity Initiative*
CPR	: *Cyberspace Policy Review*
CSL	: *Cyber Security Law*
DSL	: *Data Security Law*
FOCAC	: *China-Africa Cooperation*
GFW	: *Great Firewall*
MSS	: *Ministry of State Security*
NCC	: *National Cybersecurity Center*
PIPL	: *Personal Information Protection Law*
PRC	: *People's Republic Of China*
SSTC	: *State Science and Technology Commission*
TIK	: Teknologi Informasi dan Komunikasi
UN GGE	: *United Nations Group of Governmental Experts*
WIC	: *World Internet Conference*

I. PENDAHULUAN

Skripsi ini akan meneliti tentang dinamika konflik antara Tiongkok dan Amerika Serikat terhadap penyelesaian *cyber warfare* dalam rentang waktu 2016—2021. Penelitian terdapat landasan teoretis, empiris dan metodologis, serta adanya kebaruan. Sehingga pada latar belakang penelitian ini, peneliti akan memaparkan sejarah *cyber* di Tiongkok dan Amerika Serikat, permulaan awal terjadi konflik *cyber* dengan Amerika Serikat, kecurigaan kedua negara tersebut dan serangan yang terjadi serta justifikasi teoritis dan empiris menggunakan konsep terkait, yaitu konsep *cyber security*, *cyber warfare* dam kerja sama Internasional. Dalam bab ini juga, peneliti akan menyajikan penelitian-penelitian terdahulu, rumusan masalah, tujuan penelitian, serta manfaat penelitian ini.

1.1. Latar Belakang

Cyber warfare merupakan perang yang terjadi di *cyberspace* yang melalui sistem jaringan dan komputer. *Cyberspace* atau dunia maya berperan besar dalam menyempitkan ruang, jarak, dan waktu sehingga seluruh orang yang ada dunia bisa saling terkoneksi satu sama lain. Maka dari itu, *cyberspace* menjadi ruang sekaligus sarana baru dalam hubungan antar negara dapat menjadi pilihan lain aktor untuk mencapai kepentingan. Perkembangan *cyberspace* mengakibatkan *power* tidak hanya lagi diukur melalui kekuatan fisik saja namun dapat dilihat juga dari kemampuan *cyberpower*-nya. Namun, sistem *cyber* sendiri merupakan hal yang kompleks sehingga menciptakan adanya kerentanan baru yaitu sistem *cyber* dapat di eksploitasi aktor negara maupun non-negara untuk tujuan yang tidak baik dan merugikan pihak lain seperti penyusupan, peretasan, *cyber espionage*, dan *cyber crime* (Haaster, 2016). Hal itu menyebabkan banyak aktor yang berusaha untuk memajukan kemampuan *cyber power*-nya.

Salah satu negara yang ikut mengembangkan *cyberpower* adalah Tiongkok dan Amerika Serikat. Untuk Tiongkok sendiri bermula pada tahun 1980 melalui *People's Republic of China* (PRC) mulai memusatkan perhatian pada perkembangan teknologi dan informasi. Selanjutnya Tiongkok mendirikan *State Science and Technology Commission* (SSTC) di tahun 1986 yang menjadi awal keseriusan Tiongkok dalam memperkuat teknologinya serta memfasilitasi penciptaan perkembangan teknologi dan informasi (Cheng, 2017). Peningkatan kapabilitas *cyber warfare* Tiongkok terus menjadi salah satu fokus pemerintahan dalam upaya untuk meningkatkan militer dan keamanan *cyber*-nya. Dalam pidato Presiden Xi Jinping bahkan mengumumkan reformasi pada tahun 2015 dan 2016 yang berada di kelembagaan *Chinese People's Liberation Army* (PLA) untuk menandai era baru kecanggihan dunia maya serta untuk mengatur kembali layanan operasi menangani domain *cyberspace* dalam artian untuk memperkuat *cyber security* Tiongkok dari ancaman negara lain (Williams, 2021). Hingga selama beberapa dekade terakhir, Tiongkok melakukan peningkatan *cyberpower*, setidaknya pada tahun 2021 ada 40,000 *technology companies* yang aktif (Statista number of companies in the software industry China, 2021). Tiongkok pada abad ke-21 menjadi salah satu negara yang mengalami pertumbuhan yang signifikan dan memiliki skala kapabilitas yang baik dalam *cyberpower*.

Dilain sisi *cyber* juga telah menjadi salah satu fokus utama dalam pemerintahan Amerika Serikat sejak serangan teroris 11 September 2001 (Tirrell, 2012). Pemerintahan Obama memulai tinjauan kebijakan keamanan *cyber* yang dilakukan oleh pemerintahan Bush sebelumnya. Hasil dari tinjauan ini adalah *Cyberspace Policy Review* (CPR) yang diterbitkan 90 hari kemudian. CPR ini mencakup berbagai kekhawatiran keamanan *cyber* dan memberikan rekomendasi untuk memperkuat keamanan *cyber*nya (Baylon, 2014). Selain itu, Amerika Serikat juga meluncurkan *Comprehensive National Cybersecurity Initiative* (CNCI) yang masih dirahasiakan. CNCI adalah inisiatif yang dimulai oleh pemerintahan Bush dan dilanjutkan oleh pemerintahan Obama. CNCI bertujuan untuk menciptakan kemampuan respons yang terkoordinasi dan kooperatif dengan komunitas internasional terhadap ancaman

keamanan *cyber* (Spade C. J., 2011). Dan kebijakan kerja sama lainnya seperti mengeluarkan International Strategy for *Cyber*space pada tahun 2011. Dapat dikatakan bahwa Amerika Serikat mempunyai kelebihan kekuatan yang tinggi di *cyberspace*, dan batasan geografis tidak mempengaruhi proyeksi kekuatannya. Amerika Serikat memiliki pengaruh yang signifikan dalam penciptaan serta perkembangan Internet, memungkinkannya untuk mempertahankan dominasi dalam pengelolaan dan pengoperasian infrastruktur tersebut. Saat ini, dari 13 root server yang mengatur fungsi Internet global, sebanyak 10 berlokasi di Amerika Serikat, menunjukkan posisi sentral negara ini dalam arsitektur dan kontrol jaringan global (Haizler, The United States' *cyber* warfare history: Implications on modern *cyber* operational structures and policymaking, 2017). Hal itu menjadikan Amerika Serikat masih memiliki pengaruh yang besar di dalam *cyberspace* dan banyak negara lain masih bergantung pada teknologi yang disediakan oleh perusahaan-perusahaan teknologi informasi Amerika Serikat.

Eskalasi *cyber warfare* oleh Tiongkok menyebabkan negaranya memiliki potensi untuk mendominasi *cyberspace* sehingga Tiongkok mampu melakukan *cyber attack* negara dengan *cyberpower* terbaik. Amerika Serikat berada di urutan teratas pada daftar dan menempati peringkat pertama dari tahun 2020 hingga kini. Index tersebut memberikan 30 peringkat teratas negara sesuai dengan kemampuannya berdasarkan 8 index yaitu *financial, surveillance, intelligence, commerce, defense, information control, destructive* dan *norms* (National Index *Cyber*power, 2022). Tiongkok memiliki kecenderungan menggunakan kapabilitas *cyber* secara ofensif berupa tindakan spionase dan peretasan terhadap Amerika Serikat. Lembaga Intelijen Amerika Serikat menyebutkan operasi spionase tersebut sebagai "*Titan rain*" kasus pertama spionase *cyber* pada tahun 2003, dimana peretasan yang terjadi dilakukan Tiongkok terhadap target militer dan pemerintah untuk mendapatkan informasi (Rubenstein, 2014). Pada tahun 2013, Amerika Serikat mengajukan tuduhan spionase *cyber* secara hukum terhadap individu yang termasuk dalam unit militer Tiongkok dan menuduh mereka mencoba meretas sejak tahun 2006 terhadap beberapa perusahaan besar dalam negeri (CNBC, 2013). Menurut Jaksa Agung Amerika Serikat Eric Holder, surat

dakwaan telah diajukan di Kantor Kejaksaan Amerika Serikat menyebutkan spionase *cyber* ekonomi dilakukan terhadap perusahaan dalam bidang industri baja, tenaga surya, tenaga nuklir dan logam khusus. Penyerangan ini memiliki niat untuk mencuri rahasia dagang atau strategi perusahaan yang berupa data penetapan harga, teknik manufaktur, dan posisi negosiasi perusahaan-perusahaan Amerika Serikat.

Kekhawatiran akan tindakan yang dilakukan oleh Tiongkok membuat Amerika Serikat melakukan kerja sama dalam bidang *cyber security* dengan Tiongkok. Di tahun 2013, Amerika Serikat mengeluarkan *International Strategy for Cyberspace* adalah sebuah strategi kebijakan Amerika Serikat melalui diplomasi untuk memperkuat kerja sama internasional serta pertahanan keamanan *cyber* dari ancaman *cyber* secara internasional (Washington Post, 2011). Sehingga dalam hal ini, untuk pertama kalinya isu *cyber* masuk kedalam agenda penting hubungan bilateral antara Tiongkok dan Amerika Serikat. Pada perjanjian *cyber* pertama tersebut tidak berjalan dengan baik karena Tiongkok melakukan lagi kegiatan spionase yang dinamakan operasi beebus yang ditujukan kepada Departemen Pertahanan Amerika Serikat pada tahun 2013 (Security affairs, 2013). Setahun setelahnya Amerika Serikat membalas dengan melakukan spionase terhadap kepada perusahaan asal Tiongkok yaitu Huawei yang dijuluki operasi Shotgiant (BBC News, 2014). Yang menyebabkan kerja sama pertama tersebut pun berakhir dengan buruk.

Selanjutnya, di tahun 2015 Amerika Serikat berhasil melakukan pendekatan yang baik lagi dengan Tiongkok sehingga terjalin perjanjian kerja sama. Dalam konferensi pers di Rose Garden, Presiden Obama mengumumkan telah terjalin perjanjian kerja sama yang dinamakan *US-China Agreement* yang berisikan kesepakatan bersama yang mengatur tentang tidak diperbolehkannya melakukan kegiatan spionase yang dapat merugikan dan mencuri informasi khususnya pencurian data informasi rahasia dagang, keamanan dan informasi penting lainnya seperti spionase terhadap komersial dan ekonomi. Menurut Mandiant, setelah *US-China agreement* dilakukan pada tahun 2015 telah mengurangi sejumlah serangan terhadap perusahaan Amerika Serikat. Laporan yang dirilis FireEye mengklaim jika kelompok peretas Tiongkok yang dilacak menurun dari 60 pada Februari 2015 menjadi kurang dari 10 pada bulan Mei 2016 (FireEye

Isight Intelligence, 2016). Namun uniknya, walaupun kerja sama tersebut menghasilkan hal yang baik tetap saja kerja sama itu hanya bertahan tidak lama karena kerja sama tersebut dilanggar oleh Tiongkok yang tetap melakukan kegiatan spionase *cyber* terhadap Amerika Serikat. Hal itu cukup mengherankan dikarenakan kerja sama yang dilakukan Tiongkok dan Amerika Serikat yang lainnya seperti kerja sama ekonomi dan kerja sama untuk menangani krisis iklim berjalan dengan baik (Dewan, 2021).

1.2. Rumusan Masalah

Pertumbuhan dan kemajuan Tiongkok dalam *cyberspace* mengalami kemajuan dan hal ini tentu menjadi perhatian Amerika Serikat khususnya dalam konteks potensi dampak dari aktivitas *cyber* warfare yang terjadi atas eskalasi *cyber warfare* Tiongkok. Hubungan Amerika dan Tiongkok sudah sejak lama ditandai dengan perlombaan dan rivalitas yang kompetitif. Tindakan yang dilakukan Tiongkok berupa spionase dan peretasan terhadap target militer dan pemerintah untuk mendapatkan informasi. Situasi tersebut terjadi berulang kali yang menyebabkan Amerika Serikat menjadi salah satu negara yang mendapatkan *cyber attack* terbanyak dari Tiongkok. Kekhawatiran tersebut menyebabkan Amerika Serikat merespon dengan melakukan perjanjian kerja sama *cybersecurity* dengan Tiongkok beberapa kali diantaranya adalah *US-China Agreement* pada tahun 2015. Perjanjian tersebut berawal dengan baik terbukti dengan penurunan angka penyusupan diantara kedua belah pihak. Tetapi sayangnya, *US-China agreement* tidak bertahan lama karena Tiongkok melanggar perjanjian tersebut dengan cara terus melakukan spionase terhadap Amerika Serikat. Berdasarkan latar belakang masalah yang telah disampaikan, peneliti kemudian mengajukan pertanyaan penelitian yaitu: **“Bagaimana Perbandingan *Cyber Security* Tiongkok dan Amerika Serikat Terkait *Cyber Warfare*, 2016—2021?”**

1.3. Tujuan Penelitian

Sesuai dengan latar belakang dan rumusan masalah yang ada, tujuan penelitian yang ingin dicapai peneliti adalah:

1. Mendeskripsikan *cyberwarfare* yang terjadi antara Tiongkok dan Amerika Serikat tahun 2016-2021.
2. Mendeskripsikan *cyber security* Tiongkok dan Amerika Serikat terkait *cyber warfare* dengan menggunakan *cyber security dan* kerja sama internasional.

1.4. Manfaat Penelitian

Adapun manfaat yang diharapkan dapat diperoleh melalui penelitian yang dilakukan yaitu:

1. Untuk meningkatkan pemahaman dan kemampuan berpikir secara akademis dalam memandang *cyber warfare* sebagai salah satu konsep dan fenomena internasional.
2. Dapat menambah ilmu dan dapat menjadi acuan referensi bagi penelitian lain terkait konsep *cyber warfare* dan *cyber security* dalam hubungan internasional.

II. TINJAUAN PUSTAKA

Bab ini akan berisi tinjauan pustaka yang memiliki dua bagian. Yang pertama adalah menjelaskan landasan konseptual yang terdiri dari konsep *cyber* warfare, konsep *cyber* security, dan kerja sama internasional. Bagian kedua mengembangkan kerangka pemikiran yang bertujuan untuk merangkai pemikiran yang digunakan dalam penelitian ini, serta memberikan gambaran mengenai konflik yang terjadi antara Tiongkok dan Amerika Serikat terkait *cyber* warfare 2016—2021.

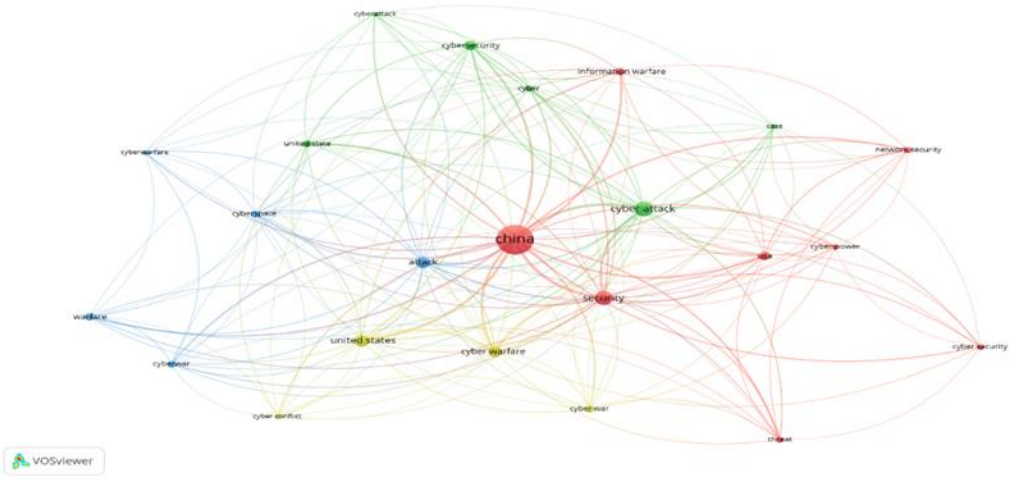
2.1 Penelitian Terdahulu

Penelitian terdahulu untuk membantu penulis memahami masalah yang diteliti, mengamati fenomena yang diteliti secara lebih luas, membantu dalam proses analisis yang berkaitan dengan topik kajian. Secara khusus, penelitian yang diambil oleh peneliti belum banyak dilakukan. Namun, kajian ini juga yang bersinggungan dilakukan oleh akademisi dari berbagai bidang. Penelitian yang tersebut antara lain memiliki fokus pembahasan tentang Operasi *cyber* China dan implikasinya (Wortzel, 2010);China *cyber power* dan Amerika *national security* (Spade J. , 2011); Kompetisi *cyber war* dan Hubungan China dan US (Lewis, 2010), (Lee J. , 2019), (Qobo, 2022), (Ardita, Prakoso, Putra, Sulistiobudi, & Satria, 2023); Perbandingan *Cybersecurity* US-China (Cai, 2016), (Akdag, 2017); *Cyber warfare* US-China secara umum (Manson, 2011), (Sergeevna, 2017), (Khan & Abbasi, 2023).

Dalam penulisan ini peneliti menggunakan beberapa penelitian sebelumnya untuk membentuk kerangka pemikiran, termasuk mengidentifikasi konsep atau teori yang akan digunakan peneliti ketika mempelajari kasus ini. Untuk melakukan novelty, penulis menggunakan metode bibliometrik yang dilakukan dengan *Publish Or Perish* untuk mendapatkan database dan *Vosviewer* yang digunakan untuk memetakan hasil penelitian. Peneliti menggunakan kata kunci *cyber warfare*, *cyber*, China, Amerika Serikat dan *conflict*. Peneliti menemukan banyaknya data terkait dan sesuai dengan hasil dari pemetaan tersebut dan dapat dilihat jika peneliti yang membahas strategi yang terjadi antara tiongkok dan Amerika secara spesifik masih sedikit dan berada di cluster

dua. Sehingga, penulis memfokuskan topik kepada perbandingan *Cyber Security* Tiongkok dan Amerika Serikat Terkait *Cyber Warfare*, 2016—2021.

Gambar 1 Hasil pemetaan VosViewer peneliti (berbagai sumber, diolah oleh peneliti)



Penelitian pertama merupakan jurnal ilmiah karya Dewi Triwahyuni, yang berjudul **"*The Impact of China's Cyberpower Development on The Interest of The United States"*** (Triwahyuni, 2018)**.** Penelitian ini berisikan agresivitas Tiongkok di *cyberspace* selama 10 tahun terakhir dan juga membahas tentang strategi Tiongkok di dunia maya menggunakan *cyber* yang bertujuan membangun teknologi informasi Tiongkok tahun ke depan sehingga Tiongkok dapat menjadi negara yang memiliki kekuatan *cyber*. Penelitian ini juga menjelaskan bagaimana Tiongkok dengan perilakunya dan ambisinya di dunia maya memicu reaksi yang kurang baik dari Amerika Serikat karena dianggap merugikan kepentingan negaranya. Mengusung konsep *cyberpower* sebagai salah satu konsep dasarnya yang membahas tentang sebuah perangkat sumber daya yang berkaitan dengan manufaktur elektronik untuk melakukan pemantauan dan komunikasi serta jaringan yang tidak terbatas ruang dan waktu. Berfokus pada impact yang diberikan Tiongkok dalam usaha meningkatkan kekuatan militernya terhadap Amerika Serikat sedangkan penelitian saya berfokus pada strategi

cyber security yang dilakukan Tiongkok untuk menghadapi *cyber warfare* Amerika Serikat.

Penelitian kedua merupakan sebuah jurnal karya Ramadani Pasaribu dengan judul "**Strategi Amerika Serikat Dalam Menghadapi Eskalasi *Cyber*power China Tahun 2015-2019"** (Pasaribu, 2021). Artikel jurnal tersebut membahas tentang perkembangan teknologi *cyberpower* yang dimiliki oleh Tiongkok, karena dalam beberapa dekade terakhir Tiongkok menjadi sangat agresif dalam kemajuan teknologinya dan mempunyai keinginan untuk memiliki *cyberpower* sebagaimana yang dipidatokan oleh Xi Jinping pada tahun 2013. Eskalasi *cyber*power yang telah dilakukan oleh China menyebabkan dampak tersendiri untuk Amerika Serikat hal itu dianggap merugikan pihak Amerika Serikat karena banyaknya serangan *cyber* yang ditujukan kepadanya. Upaya yang dilakukan Tiongkok untuk memiliki *cyberpower* yang kuat menjadikan Amerika serikat juga harus menanggapi kondisi tersebut dengan upaya merilis strategi pertahanan baru yang dikenal dengan istilah *defence-forward strategy*.

Melalui *defend forward strategy* Amerika Serikat mampu menempatkan posisi yang seimbang dimana Amerika Serikat dapat bertahan dari segala ancaman maupun serangan yang ditujukan kepada mereka serta di lain sisi tetap dapat mempunyai kemampuan ofensif dengan melakukan serangan balik kepada negara yang mengincarnya. Memiliki fokus terhadap kemajuan Amerika Serikat dan strateginya dalam *cyber warfare* dan menunjukan cara kerjanya sebagai pemikiran dari strategi tersebut. Sedangkan penelitian penulis berfokus kepada sisi Tiongkok melakukan strategi *cyber security* dan bagaimana strategi tersebut digunakan untuk melakukan menghadapi *cyber warfare* dengan Amerika Serikat.

Penelitian ketiga merupakan literatur jurnal yang berjudul "**Pengaruh *Cyber* Security Strategy Amerika Serikat Menghadapi Ancaman *Cyber* Warfare"** oleh Moehammad Yuliansyah Saputera (Saputera, 2015). Jurnal ini berfokus kepada pengaruh *cyber security strategy* terhadap ancaman *cyber warfare* yang dipandang sama bahayanya dengan ancaman perang fisik untuk Amerika Serikat. *Cyber warfare* mampu melakukan serangan jarak jauh yang dilakukan melalui ruang *cyber* dan dapat

melumpuhkan infrastruktur vital, segala sistem informasi bahkan dapat mengancam kepercayaan akan pemerintah yang akhirnya dapat mengancam kedaulatan negara. Akibat dampak besar yang dapat dihasilkan *cyber warfare* menyebabkan tuntunan akan keamanan *cyber* meningkat sehingga terciptalah *cybersecurity* yang diperlukan strategi dalam penggunaanya. Amerika Serikat sebagai negara besar pun tidak mau terlihat lemah dan kehilangan pamor akan kegagalan mereka dalam menjaga keamanan *cyber*.

Pemerintah Amerika Serikat kemudian melakukan peningkatan teknologi Informasi dan Komunikasi (TIK) underground atau teknologi jaringan deep web didukung dengan fasilitas yang mumpuni. Bahkan Amerika Serikat juga dapat dengan baik melakukan serangan balasan dengan menerapkan TIK underground sebagai alat dari *cybersecurity strategy* untuk melakukan serangan balasan berupa spionase dari agensi intelijen negara Amerika Serikat. Perbedaan dengan penelitian penulis adalah membahas di sisi Tiongkok tentang bagaimana mereka menjalankan strategi untuk mempertahankan kekuatan *cyber*-nya.

Penelitian keempat yang digunakan merupakan karya Dean Cheng yang berjudul "***Cyber Dragon Inside China's Information Warfare and Cyber Operations"*** (Cheng D. , 2016)**.** Tiongkok yang merupakan kekuatan finansial terbesar kedua di dunia sehingga dengan berkembangnya zaman membuat Tiongkok memperkuat pasukan militer modernnya yang mampu bersaing di lingkungan darat, laut, dan udara tetapi dapat bersaing di domain dunia maya. Tidak hanya itu, penelitian ini menggunakan sumber yang berbahasa Tiongkok untuk memberikan wawasan yang relevan tentang bagaimana orang Tiongkok memandang perkembangan melalui teknologi untuk mendapatkan informasi dan isu-isu serta peperangan yang dapat terjadi dari jaringan komputer. Literatur ini juga ditulis oleh seorang ahli militer Tiongkok dan memahami mengenai perkembangan keamanan yang terjadi di negeri tirai bambu tersebut. Buku ini menjelaskan secara detail tentang bagaimana tahapan dan pemikiran dari gambaran besar mengapa Tiongkok sangat termotivasi untuk melakukan *cyber warfare*.

Operasi *cyber* yang dilakukan Tiongkok secara bertahap terus menjadi lebih baik karena mereka memperjuangkan dan memberikan pengetahuan tentang *cyber* serta bagaimana orang Tiongkok melihat dunia maya sebagai tempat penyebaran informasi

yang menguntungkan. Dikarenakan hal itu. Di dalam literatur ini juga dibahas upaya Tiongkok untuk mengimbangi kekuatan *cyber* Amerika Serikat dan ambisi Tiongkok dapat menjadi ancaman dalam dunia maya dan informasi terutama untuk Amerika Serikat. Literatur ini terdapat konsep *active defense* yang diterapkan oleh Tiongkok dalam usahanya untuk menjaga stabilitas militernya. Konsep ini bermaksud untuk menunjukan militer Tiongkok yang berperan dengan aktif ke dunia. Perbedaan penelitian dengan penulis adalah penulis membahas strategi dan upaya Tiongkok untuk melakukan penyelesaian *cyber warfare* dengan Amerika Serikat.

Penelitian kelima berjudul **"The Impact Of China on *Cyber*security"** merupakan karya yang ditulis oleh Jon R. Lindsay (Lindsay, 2015). Membahas tentang keamanan dunia maya menjadi tantangan tersendiri untuk Tiongkok yang pada dasarnya merupakan salah satu negara yang memiliki ekonomi internet dengan pertumbuhan tercepat di dunia dan salah satu penggunaan dunia maya yang paling aktif. Semakin tingginya penggunaan dunia maya di Tiongkok menciptakan tingginya insentif untuk peretasan pula yang menyebabkan ketidakamanan *cyber* Tiongkok. Literatur ini juga membahas hubungan pelik Tiongkok dengan Amerika Serikat. Hal itu terlihat dalam ranah politik, dimana *cyber security* mencerminkan hubungan saling ketergantungan ekonomi serta persaingan dan ketidakpercayaan satu sama lain di bidang *cyber security*. Penelitian ini memiliki fokus pada kemampuan dan usaha Tiongkok untuk mengevaluasi dan mengatasi kekurangan mereka dalam kekuatan *cyber* sedangkan penelitian saya berfokus pada bagaimana Tiongkok menjalankan strateginya untuk tetap menguatkan keamanan militer *cyber* dan melakukan penyelesain *cyber warfare* yang sudah terjadi dengan Amerika Serikat.

Keseluruhan studi pustaka yang penulis jabarkan mempunyai kesamaan mengenai dinamika hubungan antara Tiongkok dengan Amerika Serikat dalam hal *cybersecurity*. Dalam penelitian ini, penulis akan melakukan pembahasan dengan fokus berbeda untuk memperbaharui penelitian-penelitian terdahulu dengan konsep *cyber security* dan *cyber warfare* juga beberapa konsep yang sesuai lainnya agar dapat menganalisis secara detail mengenai strategi *cybersecurity* oleh Tiongkok untuk menghadapi *cyber warfare* Amerika Serikat.

2.2 Landasan Konseptual

2.2.1 *Cyber* Security

Menurut Nazri Choucri, jika konsep keamanan terbagi menjadi empat dimensi yaitu *External Security*, *Internal Security*, *Environmental security*, *cyber security*. Dalam buku tersebut *cyber security* merupakan dimensi keempat dari keamanan nasional, yang mana merupakan salah satu dimensi paling penting dalam keamanan nasional. *Cyber* security adalah kemampuan untuk melindungi negara dari berbagai ancaman, termasuk spionase, sabotase, hacking, dan kejahatan *cyber* lainnya, melalui serangkaian langkah dan teknologi yang dirancang untuk menjaga keamanan sistem, jaringan, dan data. (Choucri, 2012). *Cyber* security ada dikarenakan munculnya ketidakamanan di *cyber*space dan dibentuk untuk membuatnya praktik atau proses *cyber*space lebih aman. Myriam Dunn Cavelty berpendapat jika dalam *cyber* security jaminan informasi merupakan konsep proteksi utama dalam keamanan *cyber*. Karena masalah umum yang ada pada ancaman *cyber* adalah menyerang jaminan informasi dan sistem informasi.

Jaminan informasi merupakan konsep kunci dalam keamanan *cyber*, yang menerapkan standar untuk mengurangi risiko yang terkait dengan penggunaan, pemrosesan, penyimpanan, dan pengiriman informasi atau data, serta sistem dan proses yang digunakan untuk tujuan tersebut. Perlindungan informasi adalah Langkah paling mendasar dan penting yang perlu dilakukan suatu negara guna menjaga keamanan jaringan. Hal ini dikarenakan informasi fundamental seperti keuangan, militer, strategi pemerintah, dan bahkan jaringan komputer dapat menjadi target serangan sewaktu-waktu. Serangan semacam itu dapat menciptakan kerentanan dalam sistem informasi dan komputasi, yang berpotensi mengancam stabilitas keamanan jaringan. (Cavelty, 2012).

Model dari jaminan keamanan mempunyai tiga tujuan yaitu; *confidentiality*, yang mengacu pada perlindungan informasi dari bahaya pengungkapan kepada pihak yang tidak berwenang. Selanjutnya ada *integrity*, yang dimaksudkan untuk melindungi informasi sehingga tidak dapat diubah oleh pihak yang tidak berwenang. Dan yang terakhir *availability*, yang berarti ketersediaan informasi harus ada ketika pihak berwenang ingin informasi tersebut (Cavelty, 2012). Tujuan dasar dari jaminan informasi merupakan pencegahan terhadap ancaman-ancaman *cyber* dengan membuat strategi jaminan informasi menjadi dua tingkatan yaitu:

1. Tingkat Nasional
    a. *Cyber Deterrence*

    Konsep *deterrence* sendiri didasarkan pada kemampuan untuk mencegah lawan mengambil tindakan sebelum perang terjadi, dalam hal ini suatu negara tidak harus berada dalam situasi konflik dan dapat dilakukan saat situasi damai. Dilakukan dengan memperlihatkan kapabilitas militer yang dimiliki suatu negara sehingga hal itu dapat mempengaruhi dan menyebabkan kekhawatiran kepada lawan. Ciri utama *cyber deterrence* adalah jelasnya implikasi risiko yang didapat, kemampuan dan kapabilitas teknologi, serta tanggung jawab pemerintah (Cavelty, 2012).

    b. *Cyber Offense*

    Strategi ini seringkali digunakan untuk menyerang musuh seperti melakukan kegiatan hacking, malware dan sabotase lainnya untuk melemahkan sistem komputer dan jaringan sehingga akan memperoleh informasi yang dibutuhkan. Operasi *cyber offense* cenderung membutuhkan koordinasi yang lebih sedikit dan oleh karena itu operasi ini berbiaya rendah namun memiliki hasil yang tinggi untuk mendapatkan pelanggaran (Slayton, 2017). *Cyber offense* sendiri sudah lazim untuk digunakan dalam militer dan strategi keamanan nasional dengan melakukan peningkatan kapabilitas offensenya.

c. *Cyber Defense*

Merupakan strategi yang memiliki fokus terhadap pencegahan, pendeteksian dan respon terhadap ancaman yang merugikan untuk infrastruktur penting dan jaminan informasi sehingga dapat dilindungi secara penuh. *Cyber defense* adalah bentuk suatu usaha pertahanan negara dengan memperkuat pertahanan *cyber*, mencari kerusakan dan memperbaiki kerusakan pada sistem. Secara umum bentuk *cyber defense* terbagi menjadi dua yaitu, menerapkan sistem resiliensi agar stabilitas pertahanan *cyber* terjaga dan pertukaran informasi yang dilakukan agar memperoleh hubungan kerja sama dengan sektor privat, negara serta organisasi internasional (Vazquez, Acosta, Spirito, Brown, & Reid, 2012).

d. Perlindungan Infrastruktur Penting

Organisasi yang memiliki jaringan komputer bertanggung jawab untuk melindungi jaringan mereka sendiri seperti pemerintah menjaga jaringan pemerintahnya, militer menjaga jaringan militer, dan perusahaan menjaga jaringan mereka sendiri. Tetapi, ada beberapa aset yang sangat penting bagi masyarakat, terutama di sektor swasta, sehingga pemerintah juga terlibat untuk memastikan perlindungan yang cukup (Cavelty, 2012). Dalam laporannya *Presidential Policy Directive 21 (PPD-21)* disimpulkan bahwa masyarakat maju bergantung pada infrastruktur penting seperti energi listrik, komunikasi dan komputer yang saling terkait. (Cavelty, 2012) Namun sektor tersebut sangat rentan terhadap gangguan fisik dan ancaman virtual lainnya. Sehingga infrastruktur penting menjadi topik utama keamanan *cyber* di banyak negara. Tantangan utama untuk melindungi infrastruktur penting muncul dari privatisasi dan deregulasi masyarakat di sektor tersebut sejak tahun 1980. Tetapi dengan adanya globalisasi pada tahun 1990 an menyebabkan banyak infrastruktur dialihkan ke tangan swasta. Akibatnya aktor negara saja tidak mampu untuk menyediakan tingkat keamanan yang diperlukan untuk melindungi infrastruktur penting tersebut. Oleh sebab itu, munculah *Public-Private Partnership (PPP)* dimana hal itu merupakan

bentuk kerja sama antara negara yang dilakukan dengan sektor swasta sebagai upaya mengatasi masalah perlindungan infrastruktur yang penting. Kerja sama ini saling menguntungkan satu sama lain karena terjalinnya pertukaran informasi untuk sektor swasta oleh layanan Intelijen dan sektor negara mendapatkan pengetahuan teknologi maju. (Cavelty, 2012)

2. Tingkat Internasional

a. Konstruksi Norma *Cyber*

Banyak organisasi internasional dan badan internasional yang telah mengambil langkah-langkah untuk meningkatkan kesadaran, menjalin kerja sama dan menyepakati aturan bersama. Hal itu disebabkan oleh efektivitas *cyber deterrence* yang mengharuskan adanya skala lebih luas lagi dari kapabilitas *cyber* suatu negara baik ofensif dan defensif yang didukung juga dengan kemampuan negara untuk menyerang penyerang tanpa pandang bulu (Cavelty, 2012). Setelah terjadi kasus stuxnet, banyak negara meningkatkan kewaspadaan dan berusaha untuk mengendalikan penggunaan eksploitasi komputer untuk tujuan militer melalui kontrol senjata serta pembentukan norma dan aturan yang disepakati bersama (Cavelty, 2012). Adanya norma tersebut memiliki maksud untuk melindungi hak asasi manusia dan kedaulatan negara, dengan harapan negara akan sadar bahwa negara memiliki batasan dalam melakukan kegiatan yang ada di *cyberspace.*

2.2.2 *Cyber* Warfare

Cyberwarfare adalah situasi konflik antara dua negara atau lebih yang melakukan serangan jaringan komputer untuk menyerang infrastruktur sipil, warga sipil dan militer dimaksudkan untuk melemahkan pertahanan musuh (Liff, 2012). Menurut Clarke dan Knake, *cyberwarfare* sebagai perang yang dilakukan melalui serangan *cyber* yang dirancang untuk merusak, memanipulasi, atau menghancurkan infrastruktur vital suatu negara dengan memanfaatkan teknologi informasi dan komunikasi. Berdasarkan definisi ini, jelas bahwa *cyberwarfare* tidak hanya melibatkan upaya untuk menyerang sistem komputer atau jaringan tetapi juga

mempengaruhi struktur sosial dan keamanan nasional (Clarke & Knake, 2010). Untuk menghadapi ancaman ini secara efektif, diperlukan pemahaman mendalam tentang bagaimana *cyberwarfare* dapat memengaruhi struktur sosial dan ekonomi serta strategi yang terintegrasi untuk melindungi dan memperkuat keamanan nasional. Oleh karena itu, kegiatan *cyber* antara kedua negara ini mencerminkan cara modern dalam berkonflik yang memerlukan pendekatan komprehensif dan adaptif untuk mengelola dan mengurangi risiko yang ada (Clarke & Knake, 2010).

Ancaman yang diberikan oleh *cyberspace*, membuat negara juga mulai bereksperimen dan mengeksplorasi kapasitas dan peluang yang terbuka. Namun selagi *cyberspace* tidak diatur maka akan tetap sulit untuk mendefinisikan jenis serangan dunia maya tertentu dalam hubungan internasional dikarenakan negara cenderung tidak ingin berbagi informasi tentang kapasitas dan aktivitas mereka di *cyberspace*. Untuk mengatasi hal itu, negara mencoba untuk membentuk unit militer *cyber* yang berfokus kepada pertahanan dan ancaman keamanan nasional terhadap internet yang harus diatur dan diawasi (Novakovic & Rizmal, 2019).

2.2.3 Kerja Sama Internasional

Menurut James E. Dougherty dan Robert L. Pfaltzgraff, definisi kerja sama adalah hubungan antar negara ataupun orang perorangan yang dilakukan tanpa adanya paksaan dan disahkan secara hukum. Kerja Sama terjadi karena adanya sebuah komitmen untuk mencapai kesejahteraan bersama dan memenuhi sebuah kepentingan. Hal utama yang harus dimiliki dari perilaku kerja sama didasari oleh kepercayaan aktor satu sama lain bahwa mereka akan bekerja sama. Dimana akan ada hasil yang menguntungkan kedua belah pihak melalui kerja sama daripada usaha sendiri atau persaingan (Doughtery & Pfaltzgraff, 1997).

Kerja sama internasional diartikan sebagai bentuk tentang dua atau lebih kepentingan, nilai, dan tujuan yang memiliki tujuan untuk dapat menghasilkan sesuatu dalam bentuk pertemuan, ditaati oleh setiap pihak yang bersangkutan, pandangan kebijakan yang akan membantu negeri tersebut mencapai kepentingan dan nilai-nilainya serta adanya persetujuan aturan resmi dan tidak resmi mengenai

kerja sama yang akan dilakukan di masa depan. Holsti juga menjelaskan, ada beberapa faktor yang mendorong negara-negara melakukan kerja sama dengan negara lain dalam skala global, antara lain: mendorong kesejahteraan ekonomi dengan biaya minimal dan kendala produksi berbagai produk yang dibutuhkan masyarakat, penggunaan biaya efisien untuk kesejahteraan bersama, dan meminimalkan kerugian yang diakibatkan oleh dampak setiap tindakan suatu negara terhadap negara lain (Holsti, 1994). Negara atau aktor tidak dapat menghindari akan adanya kerja sama internasional. Kebutuhan ini disebabkan oleh saling ketergantungan hubungan antara aktor-aktor internasional dan meningkatnya kompleksitas kehidupan manusia dan selain itu, sumber daya yang dibutuhkan oleh berbagai pihak tidak merata.

Menurut Chris Brown dan Kirsten Ainley, kerja sama internasional ada dua pendekatan yang memiliki fungsi dan peran dalam tata kelola global, serta saling berinteraksi dalam konteks dinamika internasional yang kompleks yaitu bilateral dan multilateral (Brown & Chris, 2020).

1. Kerja Sama Bilateral

Kerja sama bilateral melibatkan hubungan langsung antara dua negara atau entitas internasional. Dalam konteks ini, negara-negara terlibat dalam negosiasi dan perjanjian yang secara khusus ditujukan untuk memenuhi kepentingan masing-masing. Kerja sama bilateral sering kali merupakan solusi yang dipilih ketika dua negara memiliki kepentingan yang saling berkaitan atau ketika mereka perlu menyelesaikan isu-isu yang hanya melibatkan kedua belah pihak. Pendekatan ini memungkinkan fleksibilitas tinggi dalam negosiasi, karena hanya melibatkan dua aktor, sehingga proses pengambilan keputusan bisa dilakukan dengan lebih cepat dan lebih terfokus.

Salah satu kelebihan utama dari kerja sama bilateral adalah kemampuannya untuk mencapai kesepakatan yang sangat spesifik sesuai dengan kebutuhan kedua negara. Hal ini membuatnya sangat efisien dalam menangani masalah-masalah yang langsung mempengaruhi kedua negara tersebut. Namun, kerja sama bilateral juga memiliki beberapa kekurangan. Pertama, cakupan dari perjanjian bilateral

sering kali terbatas, yang berarti bahwa isu-isu yang lebih luas atau yang melibatkan banyak negara mungkin tidak tertangani dengan baik. Kedua, jika salah satu negara memiliki kekuatan ekonomi atau politik yang jauh lebih besar, perjanjian bilateral dapat mengarah pada ketidakseimbangan kekuatan dan hasil yang kurang adil bagi negara yang lebih kecil atau kurang berkuasa. Ketergantungan pada pendekatan bilateral juga bisa membuat negara-negara lebih terisolasi dari forum internasional yang lebih luas, yang membatasi potensi mereka untuk berkolaborasi dalam skala global (Brown & Chris, 2020).

2. Kerja Sama Multilateral

Kerja sama multilateral melibatkan banyak negara atau entitas internasional dan biasanya dilakukan melalui organisasi internasional atau forum global. Dalam buku ini, Brown dan Ainley menekankan pentingnya kerja sama multilateral untuk menangani isu-isu yang bersifat global dan melibatkan banyak negara, seperti perubahan iklim, terorisme, dan perdagangan internasional (Brown & Chris, 2020). Pendekatan multilateral dapat membuat negara-negara untuk berkolaborasi dalam tentang hal yang lebih luas, membentuk aturan dan norma yang berlaku secara global, dan mengatasi tantangan yang tidak bisa diselesaikan hanya melalui interaksi bilateral.

Keuntungan utama dari kerja sama multilateral adalah cakupannya yang luas Melalui forum multilateral, negara-negara dapat mengembangkan dan menerapkan kebijakan yang berlaku untuk semua anggota, menciptakan kerangka kerja yang lebih terkoordinasi untuk menangani masalah internasional. Namun, kerja sama multilateral juga menghadapi tantangan. Proses negosiasi dalam forum multilateral sering kali lebih kompleks karena melibatkan banyak negara dengan kepentingan yang beragam. Hal ini dapat memperlambat proses pengambilan keputusan dan menambah ketidakpastian. Selain itu, dengan banyaknya aktor yang terlibat, terdapat potensi untuk ketidaksetujuan dan konflik di antara negara-negara anggota, yang dapat menghambat pencapaian kesepakatan yang efektif.

Brown dan Ainley juga menjelaskan bahwa kerja sama bilateral dan multilateral tidak saling eksklusif, melainkan dapat saling melengkapi (Brown &

Chris, 2020). Negara-negara seringkali menggabungkan kedua pendekatan ini untuk mencapai tujuan mereka. Sebagai contoh, negara-negara dapat menggunakan forum multilateral untuk menetapkan aturan umum yang berlaku secara global, sambil juga melakukan perjanjian bilateral untuk menangani isu-isu yang spesifik dan langsung mempengaruhi kedua negara. Dalam prakteknya, negara-negara dapat menciptakan keseimbangan antara pendekatan bilateral dan multilateral untuk mengoptimalkan hasil diplomasi mereka (Brown & Chris, 2020).

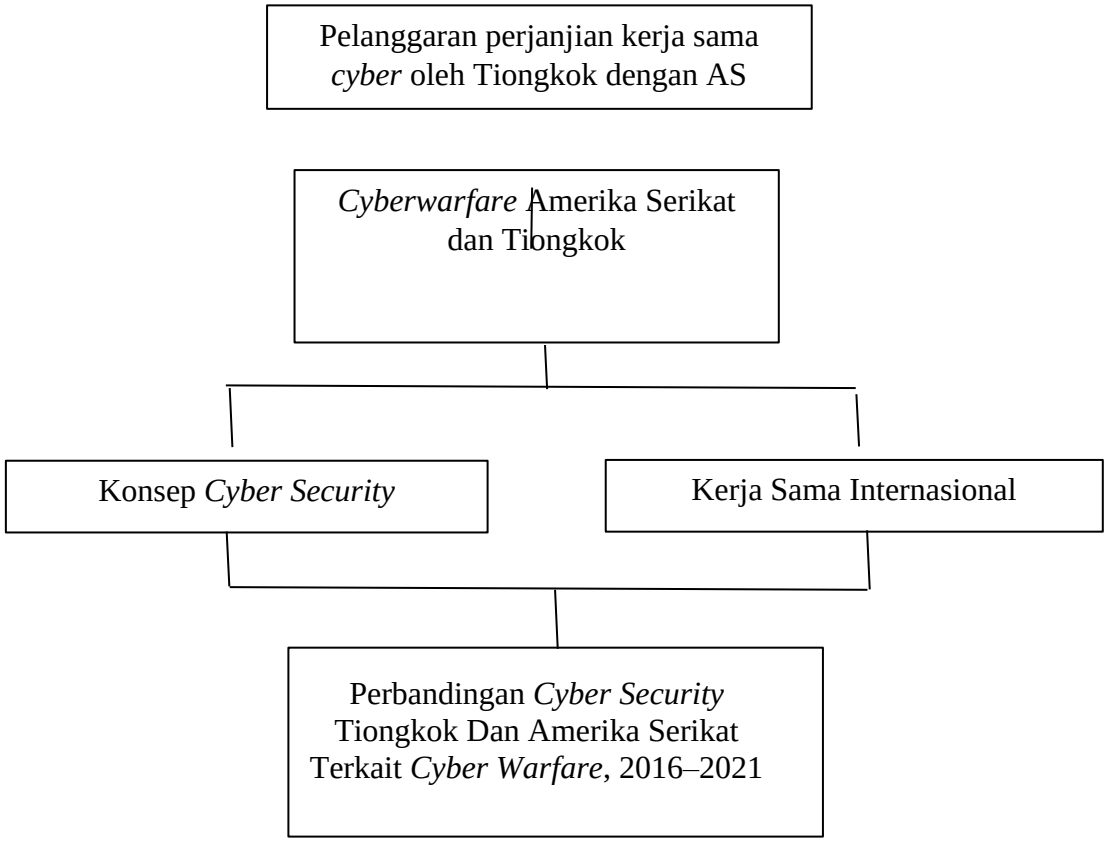
2.3 Kerangka Pemikiran

Bagian kerangka pemikiran ini membantu penulis dalam menganalisa masalah utama dalam penelitian ini. Awal pemikiran ini adalah pertumbuhan dan perkembangan internet menciptakan *cyberspace*. Hal ini menjadikan *power* tidak hanya diukur melalui kekuatan fisik saja namun dapat dilihat dari kemampuan *cyberpower*. Menyebabkan Tiongkok secara konsisten untuk meningkatkan *cyberpower*-nya. Namun, *cyberspace* mempunyai kerentanan dan masalah terkait penyalahgunaan teknologi komputer untuk tujuan yang tidak baik seperti penyusupan, peretasan, *cyber espionage*, dan *cybercrime*. Eskalasi *cyberpower* Tiongkok membuatnya mampu untuk memiliki potensi menguasai *cyberspace* dan melakukan *cyber attack* ke negara lain.

Tindakan yang dilakukan Tiongkok berupa spionase dan peretasan terhadap target militer dan pemerintah untuk mendapatkan informasi. Situasi tersebut terjadi berulang kali yang menyebabkan Amerika Serikat menjadi salah satu negara yang menjadi sasaran *cyber attack* terbanyak dari Tiongkok. Kekhawatiran tersebut menyebabkan Amerika Serikat merespon dengan melakukan perjanjian kerja sama *cybersecurity* dengan Tiongkok beberapa kali diantaranya adalah *US-China Agreement* pada tahun 2015. Perjanjian tersebut berawal dengan baik terbukti dengan penurunan angka penyusupan diantara kedua belah pihak. Tetapi sayangnya, *US-China agreement* tidak bertahan lama karena Tiongkok melanggar perjanjian tersebut dengan cara terus melakukan spionase terhadap Amerika Serikat. Kondisi hubungan yang pelik membuat kedua negara melakukan peningkatan keamanan *cyber* untuk

melindunginya dari ancaman yang dilakukan sehingga meminimalisir kerugian yang diberikan dengan adanya penyerang *cyber*. Dalam hal ini penulis melihat bagaimana konflik yang terjadi di antara Tiongkok dan Amerika Serikat untuk menganalisa penyelesaian seperti apa yang dikiranya tepat untuk digunakan oleh Tiongkok dan Amerika Serikat dalam menghadapi ancaman keamanan *cyber* dan menghadapi *cyber warfare* yang terjadi.

Gambar 2 Kerangka Pemikiran



III. METODE PENELITIAN

Bab ini menguraikan metode penelitian yang diterapkan oleh peneliti. Bab ini terdiri dari lima bagian utama, yakni jenis penelitian, fokus penelitian, sumber data, teknik pengumpulan data, dan teknik analisis data. Dalam penelitian ini, peneliti menggunakan pendekatan kualitatif dengan analisis deskriptif, yang difokuskan pada perbandingan *cyber security* Tiongkok dan Amerika Serikat terkait *cyber warfare* dari tahun 2016—2021. Sumber data yang digunakan utama bersifat sekunder, yang diperoleh melalui studi kepustakaan yang mencakup buku, jurnal ilmiah, laporan tahunan, berita terbitan, dan situs web relevan.

1.1. Jenis Penelitian

Metode penelitian yang peneliti gunakan adalah metode kualitatif dengan tipe penelitian deskriptif. Metode ini akan memperoleh data deskriptif yang berupa kata-kata tertulis atau lisan dari hal yang dapat diamati (Lexy J, 2006). Penelitian deskriptif adalah metode memberikan gambaran kuat dan terperinci tentang data serta keadaan subjek objek penelitian kemudian setelah itu di analisa dan dibandingkan sehingga dapat memberikan data yang baru yang berbeda dari data sebelumnya sesuai dengan kenyataan yang berlangsung pada fenomena yang ingin diteliti (Newman, 2000).

Metode kualitatif ini digunakan karena pada penelitian ini menggunakan data yang diperoleh berdasarkan fakta yang harus dianalisis secara mendalam. Sesuai dengan penelitian penulis yang berjudul perbandingan *cyber security* Tiongkok dan Amerika Serikat terkait *cyber warfare* dari tahun 2016—2021 maka dibutuhkannya analisis serta pengumpulan data di penelitian ini yang dilakukan dengan studi kepustakaan dan bersumber dari literatur-literatur, jurnal ilmiah, dokumen online serta adanya sumber lain yang relevan. Penelitian kualitatif deskriptif membantu penulis untuk dapat mencari dan membantu untuk menganalisa strategi apa saja yang dilakukan Tiongkok dan informasi-informasi penting yang berkaitan tentang penelitian penulis.

1.2. Fokus Penulisan

Fokus dalam penelitian sangat diperlukan sehingga tidak membuat penelitian mengalami perluasan serta dapat membantu agar tetap terarah dalam proses analisis. Fokus penelitian penulis adalah melihat bagaimana strategi *cybersecurity* yang diadopsi oleh AS dan Tiongkok dalam menghadapi ancaman *cyberwarfare* selama periode tersebut. Penelitian ini mengeksplorasi bagaimana masing-masing negara merespons ketidakberhasilan perjanjian yang ada. Konflik antara Tiongkok dan Amerika Serikat terjadi dalam waktu yang cukup lama bermula dari perkembangan teknologi yang terjadi menyebabkan Tiongkok menjadi memiliki keinginan untuk menjadi negara yang memiliki posisi dengan *cyber power* yang mampu menyaingi kemampuan posisi negara adidaya yang menguasai *cyberspace* yaitu Amerika Serikat. Dinamika konflik antara kedua negara tersebut sejalan dengan kemampuan *cyber* nya yang terus menjadi fokus utama pemerintahan negara masing-masing dengan menerapkan strategi-strategi yang membantu meningkatkan kapabilitas kemampuan kekuatan *cyber*nya serta fokus akan membuat kebijakan *cyber security* yang tepat untuk menghadapi ancaman dari *cyber* warfare. Maka dari itu, penulis berfokus pada perbandingan *cyber security* Tiongkok dan Amerika Serikat terkait *cyber warfare* dari tahun 2016—2021

1.3. Sumber Data

Penelitian ini menggunakan data kualitatif sekunder sebagaimana jenis data yang diperoleh melalui studi kepustakaan yang mencakup di dalamnya buku, jurnal ilmiah, laporan tahunan, terbitan berita dan situs web yang relevan. Penulis melakukan pengumpulan data yang berisi informasi-informasi yang berkaitan dengan sejarah *cyber*, dinamika konflik *cyber*, strategi *cyber security* Amerika Serikat dan Tiongkok serta penyelesaian *cyber* warfare yang akan penulis gunakan untuk mengetahui apa saja dinamika konflik antara Tiongkok dan Amerika Serikat dalam usahanya untuk menghadapi *cyber* warfare yang terjadi. Sumber-sumber data diatas membantu penulis untuk menganalisis dan menemukan hasil dari penelitian.

1.4. Level dan Unit Analisis Penelitian

Untuk memberikan pusat atau inti dalam suatu analisis pada teori Hubungan Internasional. Langkah yang bisa dilakukan yaitu menemukan tujuan penelitian yang tepat dan terfokus pada satu hal, dan memiliki pemilihan tingkat analisis yang berbeda. Sehingga, pada pemilihan tingkat penyidikan, penulis akan memilih atau menetapkan kesatuan unit pemeriksaan.

Level / Tingkat Analisis: Nation-State	
Unit Analisis	**Unit Eksplanasi**
Cyber security yang dilakukan Tiongkok dan Amerika Serikat.	*cyber warfare* Tiongkok dan Amerika Serikat serta potensi ancaman *cyber* akibat dari konflik yang terjadi.

1.5. Teknik Analisa Data

Dalam penelitian ini, penulis menggunakan teknik analisis data kualitatif untuk mengeksplorasi dan mengolah data yang telah kumpulkan. Teknik analisis ini penulis terapkan sebagai langkah-langkah sistematis untuk mengubah data yang kami temukan menjadi jawaban yang mengarah pada pemahaman yang lebih baik dan berguna dalam menyelesaikan masalah penelitian yang penulis hadapi. Pendekatan kualitatif penulis berfokus pada analisis data berupa informasi numerik dan teks, dengan tujuan utama menjawab pertanyaan penelitian yang telah dirumuskan. Selaras dengan Flick yang berpendapat, Analisis data dalam penelitian kualitatif adalah proses memahami materi berupa kata-kata atau gambar untuk menghasilkan pernyataan mengenai makna yang tersirat dan tersurat. Analisis ini bertujuan untuk menjelaskan bagaimana makna tersebut terbentuk dan apa yang diwakili oleh materi yang dianalisis (Flick, 2013).

V. PENUTUPAN

5.1 Kesimpulan

Berdasarkan pemaparan diatas, hubungan antara Amerika Serikat dan Tiongkok dalam bidang *cyberwarfare* mencerminkan tidak hanya persaingan teknologi yang intensif, tetapi juga dampak yang luas terhadap geopolitik global, keamanan nasional, dan stabilitas internasional. Perkembangan teknologi *cyber* telah mengubah keamanan global dengan memperkenalkan dimensi baru dari konflik dan strategi militer yang tidak terlihat sebelumnya. Amerika Serikat mengadopsi pendekatan terintegrasi yang menggabungkan *cyber deterrence, cyber offense,* dan *cyber defense*. AS cenderung menyeimbangkan ketiga pendekatan ini dengan fokus yang kuat pada *cyber defense* dan *cyber deterrence* untuk melindungi aset kritis. Negara ini menginvestasikan sumber daya yang signifikan dalam melindungi infrastruktur kritis dan data sensitif dari serangan *cyber* dengan memperkuat sistem keamanan, menerapkan teknologi canggih seperti firewall, sistem deteksi intrusi, dan enkripsi, serta membangun mekanisme pemantauan dan respons yang efektif. Meskipun *cyber offense* juga merupakan bagian dari strategi keamanan *cyber* AS, namun cenderung memiliki peran yang lebih terbatas.

Di sisi lain, Tiongkok telah mengembangkan pendekatan yang menekankan penguatan kontrol domestik dan memusatkan kemampuan ofensif dan defensif *cyber*. *Cyber* offense adalah area dimana Tiongkok menunjukkan aktivitas yang paling menonjol. Negara ini secara aktif terlibat dalam operasi *cyber* yang berfokus pada spionase dan pencurian data, dengan tujuan utama mengakses informasi sensitif dari negara lain. Ini termasuk kegiatan seperti peretasan, penggunaan malware, dan eksploitasi kerentanan sistem untuk mencuri data militer, teknologi, dan rahasia dagang. Penekanan pada spionase *cyber* mencerminkan kepentingan Tiongkok dalam mendapatkan keuntungan strategis melalui pengumpulan intelijen yang penting. Dalam *cyber defense*, Tiongkok berinvestasi besar dalam perlindungan infrastruktur kritis dan

pengembangan teknologi *cyber* canggih, mencerminkan upaya mereka untuk mempertahankan jaringan domestik dari ancaman eksternal. Strategi keamanan *cyber* antara AS dan Tiongkok mencerminkan pendekatan yang berbeda terhadap tantangan yang sama. AS menekankan kolaborasi internasional dan transparansi dalam kebijakan pencegahan dan respons, sedangkan Tiongkok fokus pada pengendalian domestik dan pengembangan kemampuan *cyber* yang lebih terintegrasi dengan kebijakan nasionalnya. Dengan mengedepankan dialog dan kerja sama, AS berupaya menciptakan norma dan standar internasional yang dapat mencegah konflik *cyber*. Di sisi lain, pendekatan Tiongkok yang lebih bersifat defensif dan ofensif berpotensi menciptakan ketegangan yang lebih besar, mengingat fokusnya ada pada kontrol domestik. Dalam hal ini, upaya untuk mengurangi ketegangan melalui diplomasi dan kolaborasi internasional menjadi sangat penting.

Dampak dari perbedaan ini tidak hanya mempengaruhi keamanan *cyber* di tingkat nasional tetapi juga berkontribusi pada dinamika global dalam keamanan *cyber*. Dengan meningkatnya ketergantungan pada teknologi digital dan ancaman yang terus berkembang, pendekatan yang diambil oleh kedua negara akan terus mempengaruhi kebijakan dan praktik internasional di bidang keamanan *cyber*. Berdasarkan pemaparan diatas dari hubungan *cyberwarfare* antara Amerika Serikat dan Tiongkok, *cyber defense* adalah area di mana kedua negara mungkin menemukan titik temu untuk kolaborasi dan penyelesaian, karena keduanya memiliki kepentingan bersama dalam melindungi infrastruktur kritis dan meningkatkan kesiapsiagaan terhadap ancaman *cyber*. Sebaliknya, *cyber* deterrence dan *cyber offense* cenderung lebih kontroversial dan berisiko, membuatnya sulit untuk disepakati atau diterapkan secara bersama. Oleh karena itu, fokus pada *cyber defense* memiliki peluang yang lebih besar untuk kerja sama dan penyelesaian yang efektif antara Amerika Serikat dan Tiongkok dalam menghadapi tantangan *cyber* bersama. Kerja sama internasional yang telah dilakukan, seperti partisipasi dalam forum-forum multilateral, menjadi platform penting bagi kedua negara untuk berbagi informasi dan pengalaman dalam *cyber defense.*

5.2 Saran

Berdasarkan hasil penelitian ini, beberapa saran penting dapat disampaikan kepada para akademisi dan penggiat dalam studi hubungan internasional terkait dengan *cyber* warfare antara Tiongkok dan Amerika Serikat:

1. Para akademisi di bidang hubungan internasional diharapkan untuk memperluas kajian mereka dengan mengembangkan penelitian yang lebih mendalam dan komprehensif mengenai dampak dari *cyber* warfare antara Tiongkok dan Amerika Serikat terhadap stabilitas keamanan global. Penelitian yang lebih rinci mengenai bagaimana persaingan *cyber* ini mempengaruhi hubungan internasional, keamanan nasional, serta kebijakan luar negeri di berbagai kawasan akan memberikan wawasan yang sangat berharga. Melalui analisis mendalam tentang dampak persaingan *cyber* ini, akademisi dapat membantu merumuskan strategi dan kebijakan yang lebih efektif untuk menghadapi tantangan *cyber* yang semakin kompleks. Penelitian ini dapat membantu para pembuat kebijakan dalam merancang strategi yang lebih baik untuk melindungi infrastruktur *cyber* dan menangani ancaman yang muncul dari kompetisi *cyber* antara kekuatan besar. Dengan menerapkan saran ini, komunitas akademis dan para peneliti dapat lebih efektif dalam mengidentifikasi risiko, mengembangkan solusi yang inovatif, serta memanfaatkan peluang yang timbul dari persaingan global dalam *cyberwarfare*. Dengan memperluas dan mendalami kajian mengenai *cyberwarfare*, akademisi dapat memberikan kontribusi yang lebih besar dalam memahami dan menangani tantangan *cyber* yang semakin berkembang, serta membantu menciptakan kebijakan yang lebih adaptif dan responsif terhadap dinamika internasional di era digital ini.

DAFTAR PUSTAKA

Akdag, Y. (2017). *Cyber* deterrence against *cyber*war between the United States and China: A power transition theory perspective.

Allen, G. C. (2021). *Cyber Conflict and Cooperation between the United States and China: A Comparative Analysis*.

APEC. (2019). *APEC Cybersecurity Strategy.*

Ardita, N. D., Prakoso, S. G., Putra, F. A., Sulistiobudi, A., & Satria, R. (2023). *Cyber*warfae between United States and China 2014-202.

Attorney General: Eric H. Holder, J. (2015, August 18). *The United States Department of Justice*. Retrieved Oktober 02, 2022, from Justice Government: https://www.justice.gov/opa/speech/attorney-general-eric-holder-delivers-remarks-supreme-court-decision-shelby-county-v

Ball, D. (2011). *China's cyber warfare capabilities*. *Security Challenges, 7*(2), 81-103.

BBC. (2014, March 24). *China wants explanation on allegations of US spying*. Retrieved Oktober 3, 2022, from BBC News: https://www.bbc.com/news/world-asia-26712564

Brown, & Chris, A. K. (2020). *Understanding International Relations.* London: Palgrave Macmillan.

Cai, C. (2016). Global *Cyber*security Environment: Perspectives of the US and China in Comparison. SECURING *CYBER*SPACE.

Carry, D. (2021, July). A Base for Military-Civil Fusion in the *Cyber* Domain. *China's National Cybersecurity Center*. Retrieved from China's National *Cyber*security Center.

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

Cheng, D. (2016). *Cyber Dragon: Inside China's Information Warfare and Cyber Operations: Inside China's Information Warfare and Cyber Operations*. ABC-CLIO.

Cheng, E. (2022, Maret 4). *China will raise defense spending by 7.1% in 2022, faster than last year*. Retrieved September 12, 2022, from CNCB: https://www.cnbc.com/2022/03/05/china-*defense*-spending-to-rise-by-7point1percent-in-2022-says-finance-ministry.html

Choucri, N. (2012). *Cyberpolitics in International Relations* . London: The Mitt Press.

CISA. (2020). *Critical Infrastructure Sectors*. Retrieved from America *Cyber Defense* Agency: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Clarke, R. A., & Knake, R. K. (2010). *Cyber War: The Next Threat to National Security and What to Do About It.* HarperCollins.

Companies Market Cap. (2022). *Largest internet companies*. Retrieved from Companies Market Cap: https://companiesmarketcap.com/internet/largest-internet-companies-by-market-cap/

Corera, G. (2021, July 21). *China accused of cyber-attack on Microsoft Exchange servers*. Retrieved from BBC News: https://www.bbc.com/news/world-asia-china-57889981

Countries With The Highest Number Of Internet Users. (2019, June 30). Retrieved September 17, 2022, from Internet World Stats: https://www.internetworldstats.com/top20.htm

Cuihong, C. (2021). *Cyber Politics in US–China Relation.* World Scientific.

*Cyber*security Administration of China. (2019, September 20). *筑牢"防火墙"！网络安全高峰论坛"火花"碰撞　多名专家学者献智开讲！*. Retrieved from *Cyber*security Administration of China: https://www.cac.gov.cn/2019-09/20/c_1570519394003406.htm

DeNardis, L. (2014). *The Global War for Internet Governance.* Connecticut: Yale University Press.

Department of Homeland Security. (2021). *DHS Has Made Limited Progress Implementing the Continuous Diagnostics and Mitigation Program.* Washington, DC.

Dewan, A. (2021, November 11). *CNN*. Retrieved from CNN website: https://edition.cnn.com/2021/11/10/world/china-us-climate-cop26-joint-agreement-intl/index.html

Dilanian, K., Ainsley, J., & Kosnar, M. (2020, May 13). *Feds warn that Chinese attempts to hack health care, drug firms threaten U.S. COVID-19 response*. Retrieved from NBC News: https://www.nbcnews.com/politics/national-security/feds-warn-chinese-attempts-hack-health-care-drug-firms-threaten-n1206151

Doughtery, J. E., & Pfaltzgraff, R. L. (1997). *Contending Theories of International Relation: A Comprehensive Survey.* New York: Addison Wesley Longman.

EU *Cyber* Direct. (2020, April 2). *European Cyber Diplomacy Dialogue 2020*. Retrieved from EU *Cyber* Direct: https://eu*cyber*direct.eu/events/european-*cyber*-diplomacy-dialogue-2020

Flick, U. (2013). Mappung the Field. In *The SAGE Handbook of Qualitative Data Analysis* (p. 3). London: SAGE Publications.

FORUM ON CHINA-AFRICA COOPERATION. (2018). *RECOMMENDATIONS BY THE PARTICIPANTS OF THE REGIONAL AWARENESS AND CAPACITY BUILDING WORKSHOP TOWARDS THE FORUM ON CHINA-AFRICA COOPERATION (FOCAC).* NAIROBI.

Goldman, D. (2019, February 25). *What is 5G?* Retrieved Agustus 19, 2022, from CNN: https://edition.cnn.com/2019/02/25/tech/what-is-5g/index.html

Greenleaf, G., & Livingston, S. (2021). *China's New Cybersecurity Law – Also a Data Privacy Law?*

Haizler, O. (2017). The United States' *cyber* warfare history: Implications on modern *cyber* operational structures and policymaking. *The United States' cyber warfare history: Implications on modern cyber operational structures and policymaking*.

Hjortdal, M. (2011). China's use of *cyber* warfare: Espionage meets strategic deterrence. *Journal of Strategic Security*, *4*(2), 1-24.

Holsti, K. J. (1994). *International Politics: A Framework for Analysis.* Pearson College Div.

Index, I. F. (2022). *Internet Freedom Scores*. Retrieved Agustus 21, 2022, from Freedom House: https://freedomhouse.org/countries/freedom-net/scores

Inkster, N. (2018). *China's cyber power*. Routledge.

internet world stats. (2019). Retrieved from internet world stats: https://www.internetworldstats.com/emarketing.htm

Isachenkov, V. (2022, September 19). *Russia Seeks Closer Security Ties With China as Key Goal*. Retrieved from The Diplomat: https://thediplomat.com/2022/09/russia-seeks-closer-security-ties-with-china-as-key-goal/

Khan, S. A., & Abbasi, S. N. (2023). *The Us-China Warfare in the 21st Century.* Insight Turkey.

Lee, & John. (2017, May 4). *The rise of China's tech sector; The Making Of An Internet Empire*. Retrieved from Lowy Institute: https://www.lowyinstitute.org/the-interpreter/rise-china-s-tech-sector-making-internet-empire

Lee, J. (2019). Shifting IP battlegrounds in the US-China trade war.

Lendon, B. (2018, March 5). *China boosts military spending 8% amidst ambitious modernization drive*. Retrieved September 4, 2022, from CNN: https://edition.cnn.com/2018/03/04/asia/chinese-military-budget-intl/index.html

Lewis, J. (2010). *Cyber war and competition in the China-US relationship. Remarks delivered at the China* .

Lieberthal, k., & Singer, P. W. (2012). *Cybersecurity and U.S -China Relations*.

Lin, H. (2018). *Konflik cyber dan Hukum Humaniter Internasional*.

Liff, A. P. (2012). *Cyber*war: a new 'absolute weapon'? The proliferation of *cyberwarfare* capabilities and interstate war. 401-428.

Lindsay, J. R. (2015). *The Impact Of China on Cybersecurity*.

Mayer, B. S. (2010). *The dynamics of conflict resolution: A practitioner's guide.* John Wiley & Sons.

Manson, G. (2011). *Cyber*war: The United States and China prepare for the next generation of conflict.

Mishra, N. (2020). *The trade:(cyber) security dilemma and its impact on global cybersecurity governance*, 54.

Nakashima, E. (2011, May 16). *Obama administration outlines international strategy for cyberspace*. Retrieved September 27, 2022, from The Washington Post: https://www.washingtonpost.com/world/obama-administration-outlines-international-strategy-for-*cyber*space/2011/05/16/AFokL54G_story.html

Noah, B., Maizlan, L., & Chatzky, A. (2023, February 8). *Is China's Huawei a Threat to U.S. National Security?* Retrieved from Council On Foreign Relations: https://www.cfr.org/backgrounder/chinas-huawei-threat-us-national-security

North Atlantic Treaty Organization. (2016, July 8). *Cyber Defence Pledge*. Retrieved from North Atlantic Treaty Organization: https://www.nato.int/cps/en/natohq/official_texts_133177.htm

Novakovic, I., & Rizmal, I. (2019). *CYBER* WARFARE: NEW TYPE OR WARFARE OR ADDITIONAL ELEMENT OF CONVENTIONAL WARFARE.

Nye, J. S. (2011). Nuclear Lessons for *Cyber*security. Strategic Studies Quarterly. 21.

Paganini, P. (2013, February 7). *Operation Beebus, another chinese cyber espionage campaign*. Retrieved from Security Affair: https://securityaffairs.co/wordpress/12216/hacking/operation-beebus-another-chinese-*cyber*-espionage-campaign.html

Paganini, P. (2013, February 7). *Operation Beebus, another chinese cyber espionage campaign*. Retrieved from Security Affairs: https://securityaffairs.com/12216/hacking/operation-beebus-another-chinese-*cyber*-espionage-campaign.html

Park, C. H. (2020). *cybersecurity Policies and Strategies: A Comparative Study of the United States and China*.

Pasaribu, R. Strategi Amerika Serikat Dalam Menghadapi Eskalasi *Cyber*power China Tahun 2015-2019. *Jurnal Online Mahasiswa (JOM) Bidang Ilmu Sosial dan Ilmu Politik*, *8*(2), 1-14.

Personal Information Protection Law. (2021). *Personal Information Protection Law of the People's Republic of China*. Retrieved from Personal Information Protection Law: https://personalinformationprotectionlaw.com/

Petallides, C. J. (2012). "*Cyber* Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat." *Inquiries Journal/Student Pulse*, *4*(03)

Qobo, M. (2022).). US–China Tech Wars: Shaping Africa's Agency. The Political Economy of China—US Relations.

Robertson, J., & Riley, M. (2018, October 4). *The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies*. Retrieved from Bloomberg: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Rubenstein, D. (2014). Nation state *cyber* espionage and its impacts. *Dept. of Computer Science and Engineering WUSTL, Saint Louis*.

Saputera, M. Y. (2015). *Pengaruh Cyber Security Strategy Amerika Serikat Menghadapi Ancaman Cyber Warfare*.

Schmidt, M. S., & Sanger, D. E. (2014, May 19). *5 in China Army Face U.S. Charges of Cyberattacks*. Retrieved from The New York Times: https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-*cyber*spying.html

Security Consultative Committee. (2019, April 19). *Joint Statement of the Security Consultative Committee*. Retrieved from U.S Department of State: https://2017-2021.state.gov/u-s-japan-joint-press-statement/

Segal, A. (2016, September 28). *The U.S - China Cyber Espionage Deal One Year Later*. Retrieved from Council on Foreign Relations: https://www.cfr.org/blog/us-china-*cyber*-espionage-deal-one-year-later

Segal, A. (2019). *US-China Cybersecurity Relations: The Interplay Between Politics, Technology, and Policy*.

Sergeevna, V. (2017). USA, China and essential Focus on strategic *cyberwarfare*.

Singer, P. W., & Friedman, A. (2014). *Cyber*security and *Cyber*war. What everyone needs to know. 124.

Slayton, R. (2017). What Is the *Cyber* Offense-*Defense* Balance? *Conceptions, Causes, and Assessment*, 72-109.

Slotta, D. (2022, Maret 11). *Number of companies in the software industry in China from 2009 to 2021*. Retrieved Agustus 21, 2022, from Statista: https://www.statista.com/statistics/276633/companies-in-the-software-industry-in-china/

Spade, C. J. (2011). *China's cyber power and America's national security.* U.S. Army War College.

Tirrell, W. K. (2012). *United States Cybersecurity Strategy, Policy, and Organization: Poorly Postured to Cope with a Post-9/11 Security Environment?*, 144.

The Mandiant. (2019). *APT1: Exposing One of China's Cyber Espionage Units.* Mandiant.

The Mandiant. (2022). *APT41, A DUAL ESPIONAGE AND CYBER CRIME OPERATION.* Mandiant.

The White House. (2011). *International Strategy for Cyberspace.* Washington D.C: U.S. Department of State.

The White House. (2021, September 24). *FACT SHEET: The United States and India – Global Leadership in Action*. Retrieved from The White House: https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/fact-sheet-the-united-states-and-india-global-leadership-in-action/

Tiezzi, S. (2014, February 28). *Xi Jinping Leads China's New Internet Security Group*. Retrieved from The Diplomat: https://thediplomat.com/2014/02/xi-jinping-leads-chinas-new-internet-security-group/

Triwahyuni, D. (2018). The Impact of China's *Cyber*power Development on The Interest of The United States

U.S *Cyber* Command. (2018). *History of U.S. Cyber Command*. Retrieved from U.S. *Cyber* Command: https://www.*cyber*com.mil/About/History/

U.S Department Of State. (2018). *Release of the 2018 National Cyber Strategy.* Washington, DC: Office of the Spokesperson.

U.S. Department of the Treasury's Office of Foreign Assets Control. (2018, March). *Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks*. Retrieved from U.S. Department of the Treasury's Office of Foreign Assets Control: https://home.treasury.gov/news/press-releases/sm0312

U.S.-China Relations. (2020). Retrieved from Council On Foreign Relations: https://www.cfr.org/timeline/us-china-relations

Vazquez, D. F., Acosta, O. P., Spirito, C., Brown, S., & Reid, E. (2012). Conceptual Framework for *Cyber Defense* Information Sharing. *4th International Conference on Cyber Conflict (CYCON 2012)*.

Voo, J. (2022). *National Cyber Power Index 2022.* Cambridge: Belfer Center for Science and International Affairs.(n.d.).

Wagner, J. (2017, June 01). *China's Cybersecurity Law: What You Need to Know*. Retrieved from The Diplomat: https://thediplomat.com/2017/06/chinas-*cyber*security-law-what-you-need-to-know/

Wang, A. (2020). *Cyber* Sovereignty at Its Boldest: A Chinese Perspective. 395.

WIC. (2020, November). *Highlights of the 2020 World Internet Conference*. Retrieved from The State Council Information Office The People's Republic of China: http://english.scio.gov.cn/WIC2020/2020-11/20/content_76930988.htm

Wortzel, L. (2010). China's approach to *cyber* operations: implications for the United States.

Young, G. B. (2017, January 19). *Cybersecurity Agreement, Part 1: The US Approach to Cyberspace*. Retrieved October 10, 2022, from The Diplomat: https://thediplomat.com/2017/01/evaluating-the-us-china-*cyber*security-agreement-part-1-the-us-approach-to-*cyber*space/