BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan globalisasi di abad ke-21 memunculkan kehadiran internet dan meningkatnya penggunaan sistem informasi sehingga membawa perubahan terhadap kehidupan manusia. Pada tahun 1997, Pemerintahan Tiongkok, mencantumkan internet sebagai bagian dari Rencana Lima Tahunan dalam infrastruktur informasi negara, dan menjadikannya sebagai tujuan untuk mendorong kemajuan informasi ekonomi nasional.[1] Tahun 1997 hingga 2009, tercatat jumlah netizen Tiongkok telah mencapai 384 juta, 618 kali lipat dan mengalami peningkatan tahunan sebesar 31,95 juta pengguna internet.[2] Inilah yang membuktikan tingginya ketergantungan Pemerintahan Tiongkok dan warga negaranya terhadap dunia siber yakni internet.

Tiongkok mulai memberlakukan langkah-langkah untuk memastikan keamanan jaringan informasi komputer secara internasional pada tahun 1997 untuk perlindungan hukum terhadap kebebasan dan kerahasiaan dalam konstitusi negara.[3] Perlindungan tersebut dicantumkan dalam Undang-Undang Sementara Republik Rakyat Tiongkok tahun 1997 di era Jiang Zemin tentang Tindakan Penyelenggaraan Jaringan Internasional Jaringan Informasi Komputer Republik Rakyat Tiongkok yang dikeluarkan oleh Kementerian Keamanan Publik

[1] " Internet in China," Information Office of the State Council of the People's Republic of China, June 8, 2010, diakses pada January 18, 2024, http://iq.china-embassy.gov.cn/ara/zt/zgzfbps/201206/t20120621_2518854.htm.
[2] Internet in China, *Information Office of the State Council of the People's Republic of China*.
[3] "China's Law-Based Cyberspace Governance in the New Era," *The State Council Information People's Republic of China*, March 16, 2023, diakses pada February 27, 2024, http://www.scio.gov.cn/zfbps/ndhf/49551/202303/t20230320_709284.html.

Tiongkok.[4] Pentingnya keamanan siber menjadi perhatian bagi Tiongkok sehingga Tiongkok menetapkan sistem hukum untuk melindungi hak dan kepentingan masyrakat dalam dunia siber.

Dalam perkembangan hubungan kerja sama antara Amerika Serikat dengan Tiongkok, Amerika Serikat melakukan tuduhan terhadap Tiongkok atas kegiatan spionase yang dilakukan terhadap negaranya, di mana Amerika Serikat dengan Tiongkok pernah terlibat dalam konflik siber yakni Operasi Titan Rain dan Shady RAT sejak tahun 2003. Kedua operasi siber ini merupakan bagian dari operasi serangan spionase yang dilakukan oleh Tiongkok terhadap lembaga pemerintahan resmi maupun swasta milik Amerika Serikat.[5] Departemen Keamanan Dalam Negeri sekaligus Departemen Pertahanan Amerika Serikat juga menjadi terkena dampak dari serangan siber yang dilakukan Tiongkok.

Pada tahun 2011, Tiongkok mengajukan draft *International Code of Conduct for Information Security* ke Perserikatan Bangsa-Bangsa (PBB) bersama Rusia, Tajikistan, dan Uzbekistan sebagai bentuk kerja sama terkait keamanan siber.[6] Pada 19 Januari 2011, Presiden Hu Jintao melakukan kunjungan kenegaraan atas undangan dari Presiden Barack Obama, kedua negara melakukan kerja sama keamanan siber yakni *Joint Statement* untuk melakukan dialog strategis terkait keamanan siber yang ditujukan pada pemahaman terkait isu-isu keamanan siber dan

[4] "Tindakan Penyelenggaraan Perlindungan Jaringan Internasional Jaringan Komputer Republik Rakyat Tiongkok," Network Information Center of Lanzhou Jiaotong University, December 30, 1997, diakses pada March 1, 2024, https://nic.lzjtu.edu.cn/info/1101/1547.htm.
[5] " Computer Espionage, Titan Rain and China," Center for Strategic and International Studies-Technology and Public Policy Program, December 2005, diakses 19 January, 2024, http://cybercampaigns.net/wp-content/uploads/2013/05/Titan-Rain-Moonlight-Maze.pdf.
[6] Adam Segal, "Chinese Cyber Diplomacy in a New Era of Uncertainty," *Hoover Institution*, no. 1703 (2017): 1-5.

dialog terbuka antara kedua negara.[7] Kesepakatan *Joint Statement* ini menekankan pada komitmen antara Tiongkok dan Amerika Serikat untuk bekerja sama dalam menghadapi serangan siber. Ini membuktikan kerja sama pertama antara Tiongkok dan Amerika Serikat menjalin kesepakatan dunia siber. *The Cyber Working Group* dibentuk pada 8 Juli 2013. Dalam pertemuan tersebut kedua negara memutuskan untuk mengambil langkah-langkah praktis untuk meningkatkan dialog tentang norma dan prinsip internasional untuk memandu tindakan dalam dunia siber. Selain itu, kedua negara juga sepakat untuk memperkuat koordinasi dan kerjasama antara US Computer Emergency Readiness Team (CERT) dan The National Computer Network Emergy Response Technical Team/Coordination Center of China (CNCERT/CC).

Pada tahun 2011 hingga 2013 setelah adanya kerja sama Tiongkok dengan Amerika Serikat, Tiongkok dilaporkan atas operasi siber yang dilakukannya terhadap Departemen Pertahanan Amerika Serikat yakni Operasi Beebus.[8] Namun, pada tahun 2010 hingga 2014 diketahui bahwa Amerika Serikat juga melakukan operasi siber pada perusahaan Tiongkok yakni Huawei yang disebut dengan Operasi Shotgiant.[9] Adapun hubungan antara Tiongkok dengan Amerika Serikat memburuk akibat penjelasan Edward Snowden yang merupakan salah satu mantan agen National Security Agency (NSA) sekaligus mantan agen Central Intelligence Agency (CIA) dari Amerika Serikat terkait program pengawasan internet massal

[7] " U.S. – China Joint Statement," *The White House Office of the Press Secretary*, January 19, 2011, diakses pada 22 Januari 2024, https://obamawhitehouse.archives.gov/the-press-office/2011/01/19/us-china-joint-statement.
[8] "Operation Beebus, Another Chinese Cyber Espionage Campaign," Security Affairs, February 7, 2013, diakses pada February 11, 2024, https://securityaffairs.com/12216/hacking/operation-beebus-another-chinese-cyber-espionage-campaign.html.
[9] "NSA Infiltrates Servers of China Telecom Giant Huawei," Reuters, March 24, 2014, diakses pada February 1, 2024, https://reuters.com/article/idUSBREA2L0PD/.

yang dilakukan Amerika Serikat sekaligus menjelaskan terkait kampanye aktivitas spionase siber Amerika Serikat menghadapi serangan Tiongkok serta terkait pernyataannya bahwa Amerika Serikat telah melakukan spionase dalam teknologi informasi Tiongkok, perbankan, serta Ketua dari Partai Komunis Tiongkok.[10]

Pada *World Internet Conference* 2015, Presiden Tiongkok Xi Jinping mengungkapkan bahwa Tiongkok menerapkan *Cyber Diplomacy* untuk mendorong kerja sama, yang berakar pada prinsip non-intervensi dalam urusan internalnya, partisipasi aktif, bantuan pembangunan, peningkatan kapasitas, dan dukungan terhadap Perserikatan Bangsa-Bangsa (PBB).[11] Pada September 2015, Presiden Xi Jinping melakukan kunjungan negara ke Amerika Serikat untuk berdiskusi dengan Presiden Barack Obama terkait dunia maya, kedua pihak mencapai kesepakatan kerja sama yang dinamakan US-China Cyber Agreement 2015 yang menyatakan bahwa kedua negara tidak akan melakukan aktivitas spionase apapun khususnya pada bidang ekonomi. Kesepakatan ini berfokus pada penegakan hukum dan tindak lanjut terhadap serangan siber yang dilakukan kedua negara.[12] Sekaligus, kesepakatan ini merupakan kesepakatan internasional pertama dalam bidang keamanan siber yang dilakukan secara perdana oleh Tiongkok dan Amerika Serikat sebagai negara adidaya untuk tidak menggunakan serangan siber dalam maksud apapun.

[10] Adrian Adzanas, Bambang Cipto, "Edward Snowden's Communication Strategy Against Information Domination Government of The United States," *Jurnal Administrasi Publik* 20, no. 1 (2022): 130-132.
[11] Adam Segal, "Bridging the Cyberspace Gap," PRISM 7, no. 2 (2013): 67–77.
[12] Marie Baezner, "Cybersecurity in Sino-American Relations," *Cyberespionage Campaigns*, no. April (2018): 1-4.

Adapun pasca kesepakatan di September 2015, kedua negara berlomba-lomba dalam membuat program AI pada Desember 2015, di mana Tiongkok tengah mengembangkan program *Internet Plus* terkait *Made in China* 2025, sedangkan perusahaan Amerika Serikat yakni *Google* tengah mengembangkan program *DeepMind*.[13] Dengan demikian, berangkat dari permasalahan yang terjadi antara Amerika Serikat dengan Tiongkok yang mengalami kerumitan. Mulai dari konflik yang berujung pada kerja sama hingga terjadi konflik kembali yang kemudian pada akhirnya Tiongkok dan Amerika Serikat berujung pada kesepakaan untuk menandatangani perjanjian terkait siber, maka tulisan ini akan menganalisis faktor pendorong Tiongkok melakukan kerja sama keamanan siber dengan Amerika Serikat pada tahun 2015.

1.2 Rumusan Masalah

Internet menjadi bagian penting dalam infrastruktur informasi negara Tiongkok tahun 1997. Pada kesepakatan *Joint Statement*, Tiongkok ikutserta menjadi salah satu mitra kerja sama dalam keamanan siber Amerika Serikat terkait isu siber yang menjadi bagian penting dalam kerja samanya pada tahun 2011. *The Cyber Working Group* mulai dibentuk pada 8 Juli 2013 untuk mengambil langkah-langkah praktis untuk meningkatkan dialog tentang norma dan prinsip internasional untuk memandu tindakan dalam dunia siber. Namun kerja sama tersebut tidak berjalan lancar. Tercatat dari tahun 2011 hingga 2014 setelah adanya kerja sama, Tiongkok dengan Amerika Serikat kembali melakukan kegiatan spionase. Pada tahun 2015, Amerika Serikat melakukan kerja sama kembali, di mana Presiden

[13] "The Top A.I. Breakthroughs of 2015," *Future of Life Institute*, December, 2015, accessed on September 15, 2024, https://futureoflife.org/ai/the-top-a-i-breakthroughs-of-2015/.

Obama dan Presiden Xi Jinping mencapai kesepakatan untuk tidak melakukan kegiatan spionase khususnya dalam bidang ekonomi yakni *US-China Agreement 2015*. Dengan demikian, penelitian ini menganalisis terkait faktor pendorong Tiongkok melakukan kerja sama keamanan siber dengan Amerika Serikat tahun 2015.

1.3 Pertanyaan Penelitian

Berdasarkan latar belakang dan rumusan masalah, maka penelitian ini akan menjawab pertanyaan penelitian terkait Apa faktor yang mendorong Tiongkok melakukan kerja sama keamanan siber dengan Amerika Serikat 2015?

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk mendeskripsikan dan menganalisis faktor pendorong Tiongkok melakukan kerja sama keamanan siber dengan Amerika Serikat tahun 2015.

1.5 Manfaat Penelitian

Adapun manfaat yang didapatkan dari penelitian ini sebagai berikut:

a. Penelitian ini diharapkan bermanfaat secara praktis, dapat dijadikan sebagai bahan pertimbangan dan evaluasi oleh pihak-pihak berkepentingan dalam memahami faktor-faktor yang mendorong kerja sama dalam bidang keamanan siber antara Tiongkok dengan Amerika Serikat tahun 2015.
b. Dari segi akademis, penelitian ini bermanfaat untuk menambah wawasan dan informasi terkait faktor yang mendorong Tiongkok melakukan kerja sama dengan Amerika Serikat terkait keamanan siber.

1.6 Studi Pustaka

Dalam rangka menganalisis penelitian terkait faktor pendorong Tiongkok melakukan kerja sama kemanan siber dengan Amerika Serikat tahun 2015, penulis mencoba untuk menemukan berbagai referensi yang relevan dari penelitian-penelitian yang telah dilakukan sebelumnya dan memungkinkan untuk dapat gunakan sebagai telaah dalam menyelesaikan permasalahan dalam penelitian ini. Dalam pengangkatan terkait topik ini, tidak ada yang membahas mengenai peristiwa yang sama, namun terdapat beberapa referensi dari karya ilmiah, buku, ataupun jurnal relevan yang bisa dijadikan sebagai acuan bagi peneliti dalam melakukan penelitian. Berikut tercantum beberapa referensi antara lain:

Dalam artikel jurnal yang berjudul *"Cyberspace Security and U.S.-China Relations"* yang ditulis oleh Xuming Qian pada tahun 2019.[14] Jurnal ini membahas mengenai aspek keamanan dunia maya yang merupakan bagian penting dalam hubungan bilateral Tiongkok dan Amerika Serikat. Dalam dunia maya hubungan bilateral Tiongkok-Amerika Serikat, konflik dan kerja sama terbatas saling berkaitan, dan hubungan Tiongkok dengan Amerika Serikat atas dasar kedaulatan, peretasan dunia maya, spionase dunia maya, dan keamanan dunia maya tercermin dalam perbedaan pandangan mengenai batasan-batasan hubungan bilateral Tiongkok dan Amerika Serikat. Dalam jurnal ini juga menjelaskan bagaimana Amerika Serikat membatasi hubungan bilateral dalam perdagangan dengan Tiongkok. Jurnal ini membantu peneliti memperoleh informasi tentang bagaimana hubungan Tiongkok-AS dengan dunia maya sejak tahun 1990-an hingga 2019.

[14] Xuming Qian, "Cyberspace Security and U . S . - China Relations," *AICS*, (2019): 709-712.

Dalam artikel jurnal yang berjudul "*An Analysis Cyberspace Rule-Making in China-Us Relations*" yang ditulis oleh Zhao Geng pada tahun 2018.[15] Jurnal ini menyajikan analisis terkait proses penciptaan peraturan dan kebijakan terkait dunia maya dalam hubungan Tiongkok dan Amerika Serikat pada tahun 2015. Kedua negara juga memperlihatkan saling ketergantungan yang dilihat dari pembentukan negosiasi untuk menciptakan aturan terkait dunia maya agar terciptanya keamanan dan kestabilan dunia siber secara global yang tentunya didasarkan pada kepentingan nasional negara masing-masing. Adanya landasan normatif dalam tata kelola dunia siber bertujuan untuk membatasi tindakan para aktor internasional melalui norma-norma efektif yang hendak dibentuk.[16] Artikel jurnal ini juga menjelaskan pentingnya menciptakan peraturan mengenai dunia maya bagi Tiongkok maupun Amerika Serikat. Hal ini dilakukan untuk mencegah terjadinya serangan jaringan siber seperti pencurian data dan serangan spionase. Kedua negara memanfaatkan *soft power* yang dicapai melalui negosiasi dan diplomasi untuk menetapkan norma dan membuat peraturan terkait dunia maya. Dengan demikian, selain melindungi kepentingan kedua negara, keamanan dan stabilitas juga terjamin.

Selanjutnya ada artikel jurnal berjudul "*Cybersecurity in Sino-American Relations*" yang ditulis Marie Baezner tahun 2018.[17] Jurnal ini menjelaskan mengenai alasan mengapa kedua negara mengalami dilemma dalam kepercayaan sehingga beralih pada serangan siber atau memata-matai. Ketegangan terjadi pada Tiongkok dan Amerika Serikat selama beberapa tahun terakhir akibat aktivitas siber

[15] Zhao Geng, "An Analysis of Cyberspace Rule-Making in China-U.S. Relations" *International Relations and Diplomacy* 06, no. 01 (2018): 16-23.
[16] Zhao Geng, An Analysis of Cyberspace Rule-Making in China-U.S. Relations, 6.
[17] Marie Baezner, "Cybersecurity in Sino-American Relations," *Center for Security Studies*, no. 224 (2018): 1-4.

yang tidak terbendung, yang menyebabkan Tiongkok dan Amerika Serikat telah melakukan spionase siber satu sama lain selama beberapa periode. Ketidakpercayaan tersebut terjadi karena Tiongkok tidak mengikuti pola tata kelola global internet yang diusulkan Amerika Serikat sehingga menciptakan kapabilitas militer siber yang meningkat dari Tiongkok yang dilakukan dengan pembentukkan Zona Anti-Akses. Terdapat dua faktor yang menyebabkan kedua negara saling melakukan spionase. Pertama, terkait permasalahan tata kelola global internet. Hal ini disebabkan Amerika Serikat yang mana merupakan negara yang menginisiasi pembentukkan tata kelola global bernama Internet Cooperation for Assigned Names and Numbers (ICANN) mengatur kelola internet di Tiongkok.[18]

Namun, negara-negara seperti Tiongkok dan Rusia menduga bahwa pembentukan tata kelola global internet ini hanya digunakan untuk memajukan kepentingan nasional Amerika Serikat saja serta untuk mendapatkan akses penuh dalam mendapatkan rahasia negara lain melalui jejaring siber Tiongkok. Faktor yang kedua adalah zona larangan akses yang ditetapkan oleh Tiongkok untuk keperluan di Laut China Selatan (Zona Anti Akses). Pembentukan zona ini merupakan bagian dari pendekatan pertahanan secara asimetris yang dirancang untuk mencegah dan menghalangi infiltrasi musuh ke dalam zona dengan meningkatkan kemampuan dunia maya untuk mengontrol ruang informasi jika terjadi konflik yang bertujuan untuk mengganggu sistem komunikasi dan *Global Positioning System* (GPS) musuh.[19] Jurnal ini membantu penulis mmperoleh berbagai informasi terkait proses Tiongkok menjaga keamanan siber negaranya.

[18] Marie Baezner, Cybersecurity in Sino-American Relations, 3.
[19] Marie Baezner, Cybersecurity in Sino-American Relations, 4.

Selanjutnya ada artikel jurnal yang berjudul "*Chinese Cyber-diplomacy in a New Era of Uncertainty*" yang ditulis oleh Adam Segal dari Hoover Institution tahun 2015.[20] Artikel jurnal ini berisikan tentang hubungan yang terjalin kurang baik antara Tiongkok dengan Amerika Serikat pasca peristiwa 9/11. Segal menjelaskan diplomasi siber terutama hubungan tiongkok dengan amerika serikat yang dapat dijadikan rujukan dalam penelitian ini. Kedaulatan siber yang diperlihatkan oleh tiongkok sebagai bentuk dari diplomasi siber. Dalam tulisannya menjelaskan bahwa diplomasi siber memiliki pengaruh besar terhadap hubungan Tiongkok dengan Amerika Serikat. World Internet Conference (WIC) merupakan langkah awal bagi hubungan kedua negara terkait dunia maya. Perbedaan penelitian yang akan diteliti dengan penelitian sebelumnya yakni pada konsep yang dipakai penulis. Jurnal ini juga membantu penulis dalam mendapatkan informasi terkait dasar kepentingan dari Tiongkok untuk menjalin hubungan baik dengan Amerika Serikat dalam keamanan siber.

Artikel jurnal selanjutnya berjudul "*Great Power Politics in Cyberspace: U.S. and China are Drawing the Lines Between Confrontation and Cooperation*" yang ditulis Andrew Liarpoulos tahun 2013 dalam sesi buku berjudul *Panorama of Global Security Environment*.[21] Artikel jurnal ini menjelaskan politik yang terjadi dalam dunia siber yang terjadi antara Tiongkok dan Amerika Serikat yang merupakan dua kekuatan besar. Selain itu, jurnal ini menjelaskan tentang hubungan konflik dan kerja sama kedua negara.

[20] Adam Segal, Chinese Cyber Diplomacy in a New Era of Uncertainty, 4-5.
[21] Andrew Liaropoulos, "Great Power Politics In Cyberspace: U.S. And China Are Drawing The Lines Between Confrontation And Cooperation," *Panorama of Global Security Environment*, (2013): 155–165.

Berdasarkan tulisan Andrew Liapoulos, ketegangan kerja sama kedua negara terjadi karena dua faktor yang mempengaruhi. Pertama, terjadinya kompleksitas dunia maya yang menyulitkan kemajuan dalam mengurangi konflik di dunia siber ini.[22] Dalam hal ini penting rasanya membangun hubungan komunikasi dalam bentuk dialog kerja sama antar perusahaan, masyarakat sipil, dan pemerintahan mengenai ketidaksesuaian kerangka hukum internasional yang ada, terkait realisasi tujuan kebebasan sipil dan perlindungan priasi warga negara itu penting. Melihat permasalahan dunia maya sangat sulit dialami kedua negara yang memiliki perspektif berbeda.[23] Faktor selanjutnya karena kedua negara masih memandang satu sama lain sebagai musuh dan masih adanya rasa ketidakpercayaan antara kedua negara. Dalam hal tersebut, artikel ini juga menekankan bahwa diplomasi siber perlu dibangun oleh kedua negara melalui penciptaan norma dan mekanisme koordinasi.[24]

Terakhir ada jurnal yang berjudul "*The United States Motivation in Having Cyber Security Cooperation with China"* yang ditulis oleh Devi Purwanti. "Motivasi Amerika Serikat dalam Melakukan Kerja sama Keamanan Siber dengan Tiongkok" oleh Devi Purwanti pada tahun 2021.[25] Penelitian memaparkan tentang alasan yang mendorong Amerika Serikat menjalin kemitraan siber dengan Tiongkok. Penelitian ini menemukan hasil di mana pada tingkat nasional, Amerika Serikat berupaya mencapai jaminan informasinya melalui strategi pertahanan siber

[22] Andrew Liaropoulos, Great Power Politics In Cyberspace: U.S. And China Are Drawing The Lines Between Confrontation And Cooperation, 155.
[23]Andrew Liaropoulos, Great Power Politics In Cyberspace: U.S. And China Are Drawing The Lines Between Confrontation And Cooperation, 163.
[24] Andrew Liaropoulos, Great Power Politics In Cyberspace: U.S. And China Are Drawing The Lines Between Confrontation And Cooperation, 164.
[25] Devi Purwanti, "The United States Motivation in Having Cyber Security Cooperation With China," *Journal of International Studies on Energy Affairs* 2, no. 1 (2021): 105-122.

dengan memperkuat kolaborasi. Sementara itu, pada tingkat internasional pembangunan norma melalui kerja sama bilateral telah menjadikan Amerika Serikat sebagai peran yang memiliki pengaruh besar dalam keamanan siber internasional. Rencana aksi yang dikembangkan berfokus pada perlindungan pada infrastruktur informasi dan komunikasi, perlindungan informasi terkait warga negara, perusahaan bisnis, hingga negara, serta membangun posisi Amerika Serikat dalam ruang lingkup internasional. Membangun kerangka politik dan memperkuat kerja sama internasional dalam aspek keamanan siber serta pengembangan rancangan strategis untuk memerangi ancaman dan serangan siber. Berawal dari konflik yang terjadi antara Tiongkok dan Amerika Serikat, kemudian berakhir dengan kedua negara menjalin kesepakatan untuk kerja sama yang menimbulkan konflik, namun kembali menjalin kerja sama lewat perjanjian keamanan siber 2015.

Perbedaan dalam Penelitian sebelumnya dengan penelitian ini yakni terletak pada objek penelitian yang diteliti. Pada penelitian sebelumnya meneliti dari segi Amerika Serikat, sedangkan penelitian ini menjelaskan faktor pendorong dari segi Tiongkok. Penelitian ini membantu penulis dalam memperoleh serangkaian informasi mengenai hubungan bilateral seperti apa yang dilakukan kedua negara dalam konteks keamanan siber yang menyebabkan pada akhirnya terjadinya konfrontasi yang berujung pada kerja sama.

1.7 Kerangka Konseptual

Dalam pandangan neorealisme, berangkat dari asumsi dasar bahwa konflik atau peperangan yang terjadi karena sifat anarki struktur internasional. Konsep anarki dari sudut neorealisme menurut Kenneth Waltz yang menyatakan bahwa

dinamika internasional yang mengalami perubahan dalam distribusi kapabilitas. Distribusi kapabilitas yang dimaksud yakni distribusi kekuatan ekonomi dan militer karena sifatnya yang struktural menyebabkan neorealisme justru cenderung melakukan Kerja sama dengan negara-negara besar saja. Hal ini karena negara-negara besar memiliki kapasitas untuk mengubah sistem internasional.

Realisme klasik memandang bahwa tujuan negara yaitu memiliki kekuasaan, namun neorealisme memandang bahwa keamanan merupakan tujuan negara. Waltz menyatakan bahwa kekuasaan merupakan bagian dari alat negara dalam mencapai tujuan karena dengan adanya kekuasaan, negara akan mengejar keamanan negaranya.

1.7.1 Cyber Security

Dalam buku yang ditulis oleh Nazri Choucri berjudul *Cyber Politics in International Relations* membagi keamanan nasional dalam empat kategori yaitu keamanan eksternal, keamanan internal, keamanan lingkungan, serta keamanan siber. Keamanan siber menjadi salah satu keamanan utama dalam konsep keamanan nasional di era globalisasi.[26] Keamanan jenis ini merujuk pada kemampuan negara untuk melindungi negaranya dari spionase, sabotase, ancaman, pencurian data, hingga transaksi elektronik yang merusak. Tindak kejahatan dunia maya atau yang dikenal dengan istilah *cybercrime* yang bersifat tidak mengenal batas merupakan suatu bentuk tindakan ancaman terhadap keamanan individu hingga global. Ancaman siber seperti spionase, sabotase, pencurian data negara merupakan bagian dari bentuk *security*

[26] Nazli Choucri, "Cyberpolitics in International Relations," *Oxford University*, London, England: *The MIT Press*, (2012): 38-39.

dilemma.[27] Dengan demikian, negara memerlukan keamanan siber di mana ruang siber perlu mendapatkan perlindungan yang layak dengan tujuan untuk menghindari terjadinya kerugian, baik itu pribadi, organisasi maupun negara.[28]

Tulisan Myriam Dunn Cavelty dan Andreas Wenger tentang *Cyber Security* dalam artikel jurnal yang berjudul *The Ambiguity of Cyber Security Politics in Context of Multidimensional Uncertainty*, Keadaan politik keamanan siber saat ini merupakan gambaran dari interaksi antara kekuatan-kekuatan yang mendasari persaingan negara-negara besar dan dinamika proses globalisasi sosio-teknis dan sosio-ekonomi. Terdapat dua faktor utama yang menjadi ciri konteks politik keamanan siber saat ini, yaitu ketidakpastian multidimensi (*Multidimensional uncertainty*) dan ambiguitas sosial-politik (*socio-political ambiguity*).[29] Menurut Myriam Dunn Cavelty dan Andreas Wenger, keamanan siber atau *cyber security* merupakan masalah keamanan nasional di abad ke-21, dimana terdapat interaksi dinamis antara kerentanan teknologi dan kemungkinan terjadi penyalahgunaan politik yang menimbulkan ruang maslah dengan sedikitnya stabilitas karena terjadinya ketidakpastian terkait ruang lingkup ntara sosial dan teknologi yang menigkatkan keinginan untuk menggunakan alat siber yang mengganggu dalam konteks kekuatan besar dan peleburan otoritas pada tingkat yang berbeda.

Ketidakpastian tersebut menyebabkan pengelolaan ketidakamanan siber terus menjadi salah satu masalah tata kelola yang paling menantang dalam era

[27] Nazli Choucri, "Theory Matters in International Relations,"*Cyberpolitics in International Relations*: 43.
[28] Monica Romauly Weu, "Kerja sama Pemerintah Indonesia Dan Pemerintah Kerajaan Inggris Dalam Bidang Keamanan Siber," *Global Political Studies Journal* 4 (2020): 159.
[29] Myriam Dunn Cavelty, and Andreas Wenger, "The ambiguity of cyber security politics in the context of multidimensional uncertainty." *Contemporary Security Policy* 41, (2019): 239.

politik kontemporer. Keamanan siber bersifat lintas batas yang terjadi di berbagai tingkat lintas sektor yang akan berdampak pada semua aktor baik publik maupun privat. Masalah terkait keamanan siber, menghindari definisi langsung dan tidak mungkin dapat dipecahkan dengan cara sederhana karena terdiri banyak faktor yang saling bergantung yang sering berubah.[30] Selain itu aktor yang berperan dalam keamanan siber memiliki nilai, tujuan, hingga motivasi yang berbeda dalam masalah ini. Keamanan siber yang berkembang dipersimpangan anara teknologi yan serba cepat, penggunaan politik oleh aktor negara dan non-negara yang menentukan ikatan tanggung jawab, batasan hukum hingga aturan perilaku yang dapat diterima dalam ruang keamanan siber. inilah yang mendasari pemikiran Myriam Dunn Cavelty dan Andreas Wenger terkait keamanan siber yang mengembangkan dua dimensi yakni ketidakpastian multidimensi dan ambiguitas politik.

Kerangka konseptual ini menyoroti pentingnya mempertimbangkan ketidakpastian multidimensi dan ambiguitas politik dalam mencapai keamanan siber. Pemahaman tentang ketidakpastian multidimensi dan ambiguitas politik memiliki keterkaitan dalam mencapai keamanan siber, di mana ketidakpastian multidimensi memainkan peran kuncinya dalam memunculkan ketidakamanan siber sebagai masalah hingga menimbulkan ambiguitas politik dalam keamanan siber. Elemen-elemen ini mampu memberikan penjelasan terkait faktor yang mendorong Tiongkok melakukan kerja sama siber dengan Amerika Serikat. Berikut penjelasan terkait elemen yang relevan dalam kerangka konseptual, diantaranya;

[30] Myriam Dunn Cavelty, and Andreas Wenger, "Cyber security between socio-technological uncertainty dan political fragmentation." *Contemporary Security Policy* 41, (2019): 1-3

1. Ambiguitas Politik

Ambiguitas sosial-politik dalam politik keamanan siber mengacu pada ketidakjelasan dan ketidakkonsistenan proses pembuatan kebijakan politik dan implikasi dari berbagai entitas politik seperti pemerintah dan lembaga. Aspek-aspek utama di dalam faktor ini, meliputi:

a. **Kepentingan Pemangku Kepentingan yang Beragam (*Diverse Stakeholder Interests*):** Pemangku kepentingan yang berbeda (pemerintah, perusahaan, masyarakat sipil) memiliki prioritas dan tujuan yang berbeda-beda, sehingga menyebabkan pendekatan yang bertentangan terhadap keamanan siber. Keamanan siber melibatkan berbagai pemangku kepentingan karena ini dapat menciptakan situasi di mana kebijakan dan tindakan sering kali dipengaruhi oleh kepentingannya yang saling bertentangan. Dalam proses pengambilan keputusan kebijakan tentunya tergantung pada kepentingan pemangku politik.[31]

b. **Fragmentasi Kebijakan (*Policy Fragmentation*):** Pengaruh negara dan organisasi yang kuat dapat membentuk norma dan praktik keamanan siber, yang sering kali menyebabkan ketidakseimbangan dan ketegangan dalam hubungan internasional. Pengaruh tersebut menciptakan kebijakan yang tidak konsisten dan tumpang tindih antar yurisdiksi menciptakan kebingungan dan menghambat strategi keamanan siber yang kohesif. Poin ini merujuk pada situasi di mana kebijakan di dalam suatu bidang mengalami peleburan, tidak ada koordinasi yang baik, atau tidak konsisten antara lembaga-lembaga yang

[31] Myriam Dunn Cavelty, and Andreas Wenger, The ambiguity of cyber security politics in the context of multidimensional uncertainty, 244

bersangkutan.[32] Poin ini difokuskan untuk menganalisis bagaimana Tiongkok dalam melakukan proses pengambilan keputusan untuk membuat kebijakan negara.

2. Ketidakpastian Multidimensional

Ketidakpastian multidimensi dalam politik keamanan siber merujuk pada kompleksitas dan ketidakpastian yang ada dalam ranah keamanan siber serta interaksinya dengan politik yang mempengaruhi kemampuan negara dan aktor internasional dalam mengantisipasi dan memahami ancaman siber. Mulai dari ketidakpastian yang terjadi dalam teknologi, hukum, dan politik yang mempengaruhi keputusan negara untuk melakukan kerja sama dengan negara lain. Pada poin ini menjelaskan tentang ketidakpastian terkait ruang lingkup dan tempo dalam melakukan inovasi teknologi yang ditujukan untuk mengejar ketertinggalan negara dalam berevolusi. Keterlibatan aspek-aspek mendorong terjadinya pengambilan keputusan dalam membuat kebijakan untuk melakukan kerja sama dengan negara lain. Berikut merupakan aspek-aspek dalam ketidakpastian multidimensi:

a. **Ketidakpastian Teknologi (*Technology Uncertainty*):** Kemajuan teknologi yang pesat dan munculnya ancaman siber baru mempersulit prediksi dan persiapan menghadapi tantangan keamanan siber di masa depan. Inovasi dapat melampaui pengembangan langkah-langkah dan peraturan keamanan, sehingga menciptakan kerentanan.Tantangan Atribusi yang menentukan sumber atau aktor sebenarnya di balik serangan siber bisa sulit karena faktor-faktor seperti spoofing, operasi bendera palsu, dan

[32] Myriam Dunn Cavelty, and Andreas Wenger, The ambiguity of cyber security politics in the context of multidimensional uncertainty, 270.

penggunaan proksi, menyebabkan ketidakpastian tentang siapa yang bertanggung jawab atas suatu insiden.

b. **Ketidakpastian Kebijakan dan Peraturan (*Policy and Regulatory Uncertainty*):** Kurangnya kebijakan dan peraturan keamanan siber yang konsisten dan komprehensif di berbagai negara dan wilayah menyebabkan pendekatan keamanan siber yang terfragmentasi. Hal ini dapat mengakibatkan kesenjangan dalam perlindungan, standar yang bertentangan, dan tantangan dalam kerja sama internasional. Ambiguitas Hukum dan Regulasi: Kurangnya norma dan perjanjian internasional yang jelas mengatur dunia maya berkontribusi pada ketidakpastian tentang legalitas aktivitas siber tertentu dan tanggapan yang tepat terhadap insiden siber.

c. **Ketidakpastian Ekonomi (*Economic Uncertainty*):** Insiden keamanan siber dapat menimbulkan dampak ekonomi yang besar, termasuk kerugian finansial, gangguan layanan, dan rusaknya reputasi. Dimensi ekonomi juga mencakup biaya penerapan dan pemeliharaan langkah-langkah keamanan siber dan potensi dampak perubahan peraturan terhadap dunia usaha.

d. **Ketidakpastian Intelijen dan Atribusi (*Intelligence and Attribution Uncertainty*):** Mengidentifikasi sumber serangan siber dan memahami motifnya sering kali merupakan suatu tantangan. Kesulitan atribusi dapat menghambat respons terhadap insiden dunia maya dan mempersulit hubungan internasional.

Berdasarkan penjelasan terkait kerangka konsep di atas, peneliti menggunakan konsep cyber security yang ditulis oleh Andreas Wenger dan Myriam Dunn Cavelty karena terdapat kecocokan untuk membantu menganalisis faktor pendorong Tiongkok melakukan kerja sama keamanan siber dengan Amerika Serikat tahun 2015, dikarenakan terdapat beberapa hal dari komponen cyber security yang mempengaruhi terbentuknya kebijakan Tiongkok sehingga mendorong terjadinya kerja sama keamanan siber dengan Amerika Serikat tahun 2015.

1.8 Metodologi Penelitian

1.8.1 Pendekatan dan Jenis Penelitian

Dalam melakukan penelitian terkait Faktor pendorong Tiongkok melakukan kerja sama Keamanan siber dengan Amerika Serikat, penulis menggunakan pendekatan kualitatif yang berfokus pada menjelaskan dan menganalisis data untuk mendapatkan hasil dari penelitian yang baik. Penelitian ini nantinya dikaitkan dengan konsep, teori, maupun persepsi sehingga menghasilkan data yang bersifat deskriptif.

Peneliti kemudian mengembangkan dan mengumpulkan informasi berupa data sekunder terkait dengan topik penelitian. Dengan demikian, jenis penelitian

yang dilakukan yakni penelitian eksplanatif kualitatif. Penelitian eksplanatif dilakukan untuk memberikan penjelasan terkait mengapa sebuah fenomena terjadi. Berdasarkan penggunaan pendekatan deskriptif kualitatif, peneliti dapat menganalisis penyebab Tiongkok menjalin kerja sama kembali dengan Amerika Serikat setelah kasus siber yang terjadi kisaran tahun 2013 tersebut.

1.8.2 Batasan Penelitian

Batasan dalam penelitian in bertujuan untuk membatasi pembahasan pokok terkait permasalahan dalam penelitian, sehingga tidak terjadi kebingungan dalam memaparkan hasil penelitian secara keseluruhan. Batasan waktu yang digunakan penulis untuk penelitian yang berjudul "Faktor Pendorong Tiongkok Melakukan Kerja sama Keamanan Siber dengan Amerika Serikat" ini yakni dari tahun 2011 hingga 2015. Tahun 2011-2013 merupakan periode yang mencakup kejadian-kejadian penting yang mendahului kesepakatan kerja sama keamanan siber antara Tiongkok dan Amerika Serikat. Tahun 2015 merupakan periode Tiongkok melakukan kesepakatan dengan Amerika Serikat mengenai keamanan siber.

1.8.3 Unit dan Level Analisis

Berdasarkan pernyataan Mochtar Mas'oed bahwa unit analisis merupakan variable dependen di mana terdapat objek yang akan dianalisis, dijelaskan serta dideskripsikan oleh peneliti.[33] Maka unit Analisa dari penelitian ini yakni Tiongkok, yang berfokus pada faktor pendorong Tiongkok. Sedangkan, unit eksplanasi merupakan variabel yang mempengaruhi perilaku unit Analisa yang akan diteliti.[34] Dengan demikian, unit eksplanasi dalam penelitian ini adalah keamanan siber

[33] Mochtar Mas'oed," Ilmu Hubungan Internasional: Disiplin dan Metodologi," (Yogyakarta: Pusat Antar Universitas-Studi Sosial Universitas Gadjah Mada, LP3E, 1990): 35.
[34] Mochtar Mas'oed, Ilmu Hubungan Internasional: Disiplin dan Metodologi, 43.

Amerika Serikat. Level analisis terdiri dari tingkatan individu, kelompok, negara, kelompok negara atau kawasan, serta sistem internasional.[35] Penelitian ini berada pada tingkat negara karena penelitian ini melihat dari faktor pendorong Tiongkok melakukan kerja sama keamanan siber dengan Amerika Serikat.

1.8.4 Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan dalam penelitian ini yaitu *library research* (studi kepustakaan) yang menjadi sumber data sekunder. Data sekunder diperoleh peneliti dari sumber-sumber bahan bacaaan seperti buku, jurnal, arsip, artikel berita terkait subjek untuk menemukan semua data tentang penelitian yang akan diteliti. Data yang digunakan dalam penelitian ini berasal dari laman resmi Tiongkok dan Amerika Serikat, yaitu *The State Council The People's Republic of China, China Education And Research Network* dan *U.S. Department of State*.

Dalam melengkapi penelitian ini, terdapat sumber artikel jurnal dan buku yang berkaitan dengan fenomena keamanan siber Tiongkok dan Amerika Serikat beserta kasusnya yang diperoleh melalui JSTOR, *Emerald, Scopus, Researchgate*. Data sekunder terkait berita serta informasi lainnya diperoleh dari laman *website* seperti *Washington Post, Reuters, China Daily, The Economic Times, People's Net* dan lainnya.

[35] Carmen Gebhard, "Student Feature, Level of Analysis," *E-International Relations*, 2018, diakses melalui https://e-ir.info/2018/02/25/student-feature-levels-of-analysis/.

1.8.5 Teknik Analisis Data

Berdasarkan Teknik analisa dilakukan dengan tujuan untuk membuat penjelasan yang lebih sistematis.[36] Menurut Miles dan Huberman dalam bukunya yang berjudul *Qualitative Data Analysis: An Expanded Sourcebook* pada tahun 1994, terdapat tiga tahapan dalam menganalisis data dalam penelitian kualitatif adalah sebagai berikut.[37]

a. Reduksi data

Merupakan tahapan dalam mengelompokkan data yang telah peneliti bagi ke dalam beberapa kategori yakni *cyber warfare* antara Tiongkok dan Amerika Serikat, dinamika kerja sama keamanan siber Tiongkok dan Amerika Serikat yang juga berisikan kebijakan tiongkok, serta dampak *cyber warfare* terhadap Tiongkok. Data yang peneliti kumpulkan sesuai dengan Batasan penelitian yakni tahun 2011-2015. Pengelompokkan data dalam penelitian ini didukung dengan dokumen atau sumber informasi lainnya terkait kebijakan Tiongkok mengenai keamanan siber, dengan tujuan agar dapat menjawab faktor pendorong Tiongkok melakukan kerja sama keamanan siber dengan Amerika Serikat.

b. Penyajian data

Merupakan tahapan pengolahan data setelah mengumpulkan informasi-informasi penting yang berkaitan dengan pembahasan yang diteliti kemudian memparafrase kalimat sesuai dengan gaya bahasa penulis dalam penelitian tanpa mengubah arti dari ide yang ditulis oleh peneliti sebelumnya.

---

[36] Barbara D. Kawulich, "Data Analysis Technique in Qualitative Research," Georgia: State University of Georgia, (2005): 97.
[37] Matthew B. Miles and Michael Huberman, "Qualitative Data Analysis: An Expanded Sourcebook," *Sage*, (1994): 10-11.

Peneliti menganalisis faktor pendorong Tiongkok melakukan kerja sama keamanan siber dengan Amerika Serikat tahun 2015.

c. Kesimpulan dan verifikasi

Merupakan tahapan setelah melakukan proses penyajian data berupa hasil dari analisis peneliti dengan menggunakan kerangka konseptual, peneliti kemudian menyimpulkan dan memverifikasi penelitian untuk memastikan kerangka konseptual yang digunakan dapat menjawab pertanyaan penelitian.

1.9 Sistematika Penulisan

Sistematika penulisan dalam penelitian ini terbagi dalam 5 (lima) bab, dalam masing-masing bab memiliki kaitan satu sama lain. Berikut merupakan sistematika penulisan dalam penelitian ini:

BAB I Pendahuluan

Bab ini berisikan latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, tinjauan pustaka, kerangka teori dan konseptual, metodologi penelitian, dan sistematika penulisan.

BAB II *Cyber Warfare* Antara Amerika Serikat Dan Tiongkok Serta Dampaknya Terhadap Tiongkok

Bab ini berisikan tentang penjelasan terkait penyadapan yang dilakukan Amerika Serikat terhadap Tiongkok ataupun sebaliknya serta dampak yang ditimbulkan akibat penyadapan tersebut. Bab ini juga berisi tentang hukum internasional yang mengatur tentang aksi penyadapan atau spionase.

BAB III Kebijakan Keamanan Siber Tiongkok

Bab ini menguraikan terkait kebijakan keamanan siber Tiongkok serta perubahan yang terjadi dalam kebijakan keamanan siber yang mana pada awalnya hanya berfokus pada kepentingan pemerintahan. Bab ini juga akan menjelaskan bentuk perubahan kebijakan tersebut hingga munculnya perjanjian keamanan siber antara Tiongkok dengan Amerika Serikat.

BAB IV Faktor Pendorong Tiongkok Melakukan Kerja Sama Dengan Amerika Serikat

Bab ini memberikan analisis dan penjelasan terkait faktor pendorong Tiongkok melakukan kembali kerja sama keamanan siber dengan Amerika Serikat dengan menggunakan konsep *cyber security* yang nantinya mampu menjelaskan hal-hal yang menjadi sorotan Tiongkok dalam melakukan kerja sama terkait keamanan siber khususnya dengan Amerika Serikat.

BAB V Penutup

Pada bab ini berisikan rangkuman yang mencakup keseluruhan dalam penelitian serta saran.