BAB I

PENDAHULUAN

1.1. Latar Belakang

Selama hampir dua dekade, perkembangan internet di Amerika Serikat telah semakin berkembang dengan pesat ditandai dengan pengguna internet yang melonjak setiap tahun. Berdasarkan data yang didapat dari *American Community Survey* dan *Current Population Survey*, mengindikasikan bahwa persentase pengguna internet di Amerika Serikat sejak tahun 1997 hingga 2015 meningkat hingga 77%.[1] Hal ini mengindikasikan bahwa tingginya ketergantungan Pemerintahan Amerika Serikat beserta warga negaranya terhadap dunia siber serta internet.

Amerika Serikat mulai berusaha untuk memberantas ancaman potensial yang berkaitan dengan siber yang menyerang baik negara, industri dan individu. Tujuan pencegahan kejahatan siber oleh Pemerintah Amerika Serikat melibatkan penggabungan kepentingan publik dan pribadi, serta peningkatan dalam hal berbagi informasi antara pemerintah federal, lokal dan perusahaan–perusahaan swasta.[2] Pada tahun 2003, Amerika Serikat mengeluarkan *National Strategy to Secure Cyberspace*, dan arahan kebijakan terkait yang menspesifikkan elemen kunci

[1] Camille Ryan dan Jamie M. Lewis, "Computer and Internet Use in the United States : 2015", *American Community Survey Reports*, 2017, diakses di https://www.census.gov/content/dam/Census/library /publications/2017/acs/acs-37.pdf, 18 Desember 2018

[2] The White House, "The National Strategy to Secure Cyberspace", Washington, 2003, diakses di https://georgewbush-whitehouse.archives.gov/pcipb/, 18 Desember 2018: 5

tentang bagaimana mengamankan sistem utama berbasis komputer, termasuk sistem pemerintah dan mendukung infrastruktur penting yang dimiliki dan dioperasikan oleh sektor swasta.[3]

Strategi dan kebijakan terkait juga membentuk Departemen Keamanan Dalam Negeri (Department of Homeland Security) yang selanjutnya akan disingkat DHS sebagai lembaga untuk perlindungan infrastruktur penting (*Critical Infrastructure Protection*) yang mana selanjutnya akan disingkat CIP dalam dunia maya.[4] Selain itu, peran dan tanggung jawab dari lembaga ini adalah untuk membangun rencana nasional yang komprehensif terkait CIP termasuk keamanan siber, membangun dan meningkatkan analisis siber nasional dan kapabilitas siaga terhadap ancaman, menyediakan dan mengkoordinasikan tanggapan insiden dan rancangan perbaikan, mengidentifikasi, menilai dan mendukung usaha dalam mengurangi ancaman siber dan menguatkan keamanan siber internasional.[5]

Kebijakan keamanan siber di Amerika Serikat kemudian menjadi pekerjaan rumah bagi Presiden Obama sebagai pengganti Presiden Bush. Pada tahun 2009, Pemerintahan Presiden Obama melakukan ulasan mengenai kebijakan siber sebelumnya yang kemudian dinamakan *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*.[6] Dalam

[3] The White House: 5
[4] David Powner, "National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture",*United States Government Accountability Office* (2009): 3
[5] David Powner: 3-4
[6] The White House, "Cyberspace Policy Review : Assuring a Trusted and Resilient Information and Communication Infrastructure", 2010 diakses di http://www.whitehouse.gov/assets/documents /Cyberspace_Policy_Review_final.pdf: 5

ulasan dibentuk *action plan* yang berfokus kepada perlindungan infrastruktur informasi dan komunikasi, perlindungan terhadap privasi warga negara, perusahaan, dan negara, pembangunan posisi Amerika Serikat untuk kerangka kebijakan keamanan siber internasional dan memperkuat kerjasama internasional terkait keamanan siber, serta persiapan rancangan strategi dalam menghadapi ancaman dan serangan siber.[7]

Pada tahun 2011, Amerika Serikat mengeluarkan *International Strategy for Cyberspace* yang berisikan strategi Amerika Serikat dalam memperkuat kerjasama internasional melalui diplomasi dan juga mengenai pertahanan keamanan siber dari ancaman siber secara internasional. Selain itu, terdapat beberapa prioritas kebijakan seperti; mempromosikan pasar internasional yang terbuka, melindungi dan meningkatkan keamanan, mempromosikan tata kelola global dalam keamanan siber juga mendukung adanya kebebasan internet dan perlindungan privasi. Dalam hal ini, Amerika Serikat dan Tiongkok untuk pertama kalinya sepakat memasukkan isu siber sebagai agenda yang penting dalam hubungan bilateral.[8]

Namun Amerika Serikat menuduh Tiongkok melakukan serangkaian kegiatan mata–mata, bahkan sebelum kedua negara melakukan kerjasama siber, Amerika Serikat dan Tiongkok terlibat dalam konflik siber dalam Operasi Titan Rain dan Shady RAT sejak tahun 2003. Operasi Titan Rain dan Shady RAT itu sendiri merupakan operasi serangan spionase yang dilakukan oleh Tiongkok

[7] The White House: 6
[8] Ting Xu, "China and The United States : Hacking Away at Cyber Warfare", *Asia Pacific Bulletin,* No. 135, (2011): 1

terhadap instansi milik pemerintah maupun swasta Amerika Serikat.[9] Institusi yang sering menjadi target dalam serangan spionase tersebut adalah, Departemen Keamanan Dalam Negeri Amerika Serikat dan Departemen Pertahanan Amerika Serikat.

Selain itu, tercatat dari tahun 2011 hingga 2013 setelah adanya kerjasama diantara kedua negara, Tiongkok melakukan kegiatan spionase terhadap Departemen Pertahanan Amerika Serikat yang dinamakan dengan Operasi Beebus. Amerika Serikat pun juga melakukan kegiatan spionase terhadap salah satu perusahaan Tiongkok yakni Huawei yang dinamakan dengan Operasi Shotgiant dari tahun 2010 hingga 2014 .[10]

Hubungan keduanya semakin memburuk dikarenakan pernyataan Edward Snowden yang merupakan mantan agen Central Intelligence Agency (CIA) dan juga mantan agen National Security Agency (NSA) Amerika Serikat mengenai adanya program pengawasan internet masal oleh Amerika Serikat dan menjelaskan kampanye spionase siber Amerika Serikat melawan Tiongkok serta adanya pernyataan bahwa Amerika Serikat telah memata-matai teknologi informasi Tiongkok, bank dan Pemimpin Partai Komunis Tiongkok.[11] Akibat dari saling tuduh antara kedua negara ini, hubungan kedua negara ini semakin buruk dan

[9] James A. Lewis,"Computer Espionage, Titan Rain and China",Center for Strategic and International Studies-Technology and Public Policy Program, http://cybercampaigns.net/wp-content/uploads/2013/05/Titan-Rain-Moonlight-Maze.pdf (diakses 6 Maret 2019)
[10] Robert Bebber, "China's Cyber Economic Warfare Threatens U.S", *US Naval Institute,* Vol.143, No. 7 (2017): 2
[11] Marie Baezner,"Cybersecurity in Sino-American Relations", *CSS Analyses in Security Policy,* No.224 (2018): 2

ketidakpercayaan pun mendominasi hubungan bilateral antara Amerika Serikat dan Tiongkok.

Kemudian pada tahun 2015, Amerika Serikat secara eksplisit melakukan pendekatan dengan Tiongkok. Presiden Obama dan Presiden Xi Jinping mengumumkan *common understanding* yang merupakan nota kesepahaman dan kesepakatan kedua negara untuk tidak melakukan kegiatan spionase khususnya spionase komersil dan ekonomi termasuk pencurian data informasi rahasia dagang dan informasi penting lainnya. Hasil dari nota kesepahaman bersama tersebut adalah berupa perjanjian yang dinamakan *US-China Agreement* 2015.[12]

Dalam hal ini, berangkat dari adanya konflik antara Amerika Serikat dengan Tiongkok kemudian kedua negara sepakat untuk melakukan kerjasama. Namun kemudian terjadi konflik hingga pada akhirnya kedua negara sepakat untuk menandatangani perjanjian terkait siber, tulisan ini akan menganalisis motivasi Amerika Serikat melakukan kerjasama keamanan siber dengan Tiongkok

1.2 Rumusan Masalah

Melalui *International Strategy for Cyberspace,* Amerika Serikat pun lalu kemudian memilih Tiongkok sebagai salah satu mitra kerjasama keamanan siber yang ditandai dengan adanya kesepakatan dalam hal memasukkan isu siber sebagai agenda yang penting dalam hubungan bilateral pada tahun 2011. Namun kerjasama tersebut tidak berjalan sebagaimana yang diharapkan. Tercatat dari tahun 2011

[12] Marie Baezner: 3

hingga 2013 setelah adanya kerjasama diantara kedua negara, Tiongkok melakukan kegiatan spionase terhadap Departemen Pertahanan Amerika Serikat, yang dinamakan dengan Operasi Beebus. Amerika Serikat pun juga melakukan kegiatan spionase terhadap salah satu perusahaan Tiongkok yakni Huawei yang dinamakan dengan Operasi Shotgiant dari tahun 2010 hingga 2014. Kemudian pada tahun 2015, Amerika Serikat secara eksplisit melakukan pendekatan dengan Tiongkok. Presiden Obama dan Presiden Xi Jinping mengumumkan *common understanding* yang merupakan nota kesepahaman dan kesepakatan kedua negara untuk tidak melakukan kegiatan spionase khususnya spionase komersil dan ekonomi termasuk pencurian data informasi rahasia dagang dan informasi penting lainnya dan hasil dari kesepahaman bersama tersebut ialah berupa perjanjian yang dinamakan *US-China Agreement* 2015. Oleh karena itu, penelitian ini menganalisis motivasi Amerika Serikat melakukan kerjasama keamanan siber dengan Tiongkok.

1.2.Pertanyaan Penelitian

Berdasarkan penjelasan latar belakang serta rumusan masalah, maka penelitian ini akan menjawab pertanyaan penelitian yakni;

"Mengapa Amerika Serikat Melakukan Kerjasama Keamanan Siber dengan Tiongkok?"

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk menganalisis motivasi Amerika Serikat melakukan kerjasama keamanan siber dengan Tiongkok.

1.5 Manfaat Penelitian

1. Sebagai acuan dan rekomendasi bagi aktor baik negara maupun organisasi internasional dalam mempertimbangkan kerjasama keamanan siber sebagai bentuk keamanan siber.
2. Selain itu, manfaat dari penelitian ini adalah dapat memberikan informasi dan data bagi Ilmu Hubungan Internasional terkait konsep *cybersecurity* dalam hubungan internasional

1.6 Studi Pustaka

Untuk menganalisis motivasi Amerika Serikat melakukan kerjasama keamanan siber dengan Tiongkok diperlukan informasi–informasi yang relevan dan bisa dijadikan acuan dalam menyelesaikan penelitian ini. Tidak banyak penelitian yang mengangkat topik yang serupa, namun ada beberapa karya ilmiah, buku, dan jurnal relevan yang bisa dijadikan pijakan bagi peneliti.

Studi pustaka yang pertama ialah tulisan yang berjudul *Great Power Politics in Cyberspace: U.S. and China are Drawing the Lines Between Confrontation and Cooperation* oleh Andrew Liarpoulos dalam jurnal Panorama of Global Security Environtment.[13] Dalam tulisan ini menjelaskan mengenai politik dalam dunia siber antara dua negara yang notabenenya merupakan negara *great power* yakni Amerika Serikat dan Tiongkok. Selain itu, dalam tulisan ini juga

[13] 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): 155-166

menjelaskan mengenai hubungan kedua negara yang berada diantara konfrontasi dan kerjasama.

Dalam hal untuk mengurangi ketegangan antara Amerika Serikat dan Tiongkok dan membangun jaringan komunikasi merupakan tugas yang tergolong sulit, menurut Andrew Liarpoulos, hal tersebut disebabkan oleh dua alasan; yang pertama adalah mencapai kemajuan dalam kebijakan *cyber détente* (perubahan kebijakan dari konfrontasi kepada kerjasama) adalah tugas yang sulit karena sifat dunia maya yang kompleks.[14] Maksudnya adalah, membangun hubungan kemunikasi berupa dialog antara sektor bisnis, masyarakat sipil, dan pemerintah mengenai ketidaksesuian kerangka hukum internasional yang telah ada sebelumnya, mencapai tujuan kebebasan warga negara dan perlindungan privasi warga negara didunia maya merupakan hal yang cukup sulit dilakukan kedua negara yang mempunyai pandangan berbeda.[15] Alasan yang kedua ialah kedua negara (Amerika Serikat dan Tiongkok) masih melihat masing– masing sebagai musuh dan masih ada ketidakpercayaan diantara keduanya. Terkait hal tersebut, penulis menyatakan bahwa *cyber diplomacy* harus bekerja keras dalam hal untuk menurunkan saling curiga diantara keduanya dengan membangun norma-norma dan mengkoodinasikan mekanisme.[16]

Studi pustaka selanjutnya yakni artikel yang berjudul *National Cybersecurity Strategy of the US and Its Constructive Implications for China* oleh

[14] Andrew Liaropoulos: 156
[15] Andrew Liaropoulos: 162
[16] Andrew Liaropoulos: 164

Bowei Shi dalam jurnal Sociology Study.[17] Dalam tulisan ini menjelaskan fokus utama Amerika Serikat dalam mempertahankan keamanan siber nya dengan beberapa strategi–strategi yang secara eksplisit dimulai sejak pemerintahan Presiden George W Bush. Konsep yang digunakan penulis terkait dengan tulisan tersebut ialah konsep strategi. Komponen – komponen strategi dalam strategi keamanan siber nasional Amerika Serikat ialah; (1) membangun organisasi pemerintah yang relevan, (2) Undang – undang hukum domestik terkait dunia maya, (3) kolaborasi antara pemerintah dengan perusahaan internet swasta, (4) memfasilitasi penelitian dan pembangunan jaringan teknologi yang mumpuni dan pelatihan komputer profesional, (5) melakukan kerjasama dengan komunitas internasional.[18]

Dalam tulisan ini juga menjelaskan mengenai dinamika hubungan antara Amerika Serikat dan Tiongkok dalam hal keamanan siber. Terkait dengan dinamika hubungan antara kedua negara tersebut maka penulis menjelaskan mengenai *The Constructive Implications* yang ditujukan untuk Tiongkok. Penulis memberikan beberapa opini terkait kerjasama keamanan siber antara Amerika Serikat dan Tiongkok serta saran untuk kapabilitas siber Tiongkok antara lain; dalam membangun *internet hard power*, Tiongkok harus mempercepat perencanaan secara keseluruhan dan mendirikan lembaga pemerintah terkait untuk memperkuat dan memperbaharui organisasi yang ada sebelumnya baik secara kuantitas maupun

[17] Bowei Shi, "National Cybersecurity Strategy of the US and Its Constructive Implications for China*", Sociology Study,* Vol.5, No.11 (2015): 825
[18] Bowei Shi: 827

kualitas. Yang kedua, untuk membangun *internet soft power*, Tiongkok harus meningkatkan pengawasan untuk meningkatkan citra nasional agar tidak ada tuduhan bahwa Tiongkok merupakan aktor utama dalam melakukan serangan siber. Yang ketiga, dalam aspek hukum internasional, karena dunia maya merupakan area baru dalam manajemen global, dan komunitas internasional belum membentuk regulasi yang jelas sehingga dalam praktiknya hukum dalam dunia maya masih tergolong "hukum rimba" yang mana artinya adalah kapabilitas suatu negara terhadap dunia menentukan hak dan kekuatan mereka.[19]

Studi pustaka berikutnya adalah artikel yang berjudul *Cyberwar : The United States and China Prepare for the Next Generation of Conflict* oleh George Patterson Manson III dalam jurnal Comparative Strategy.[20] Dalam beberapa tahun terakhir, Tiongkok telah menarik perhatian internasional karena kemampuan siber yang agresif dan canggih. Dalam banyak kasus dan fakta, target operasi siber Tiongkok adalah Amerika Serikat baik pemerintahan maupun swasta. Hal tersebut membuat hubungan antara Amerika Serikat dan Tiongkok mengalami konflik terutama dalam hal keamanan siber. Dalam tulisan ini dengan menggunakan konsep 'perbandingan' penulis membandingkan kapabilitas siber Amerika Serikat dan Tiongkok dalam dua aspek yakni; *Offensive Capabilities* dan *Defensive Capabilities.*

[19] Bowei Shi: 829

[20] George Patterson Manson III, "Cyberwar : The United States and China Prepare for the Next Generation of Conflict", Comparative Strategy, Vol.30, No.2, DOI:10.1080/01495933. 2011.561730: 120

Partai Komunis Tiongkok yang berkuasa telah mengembangkan kapabilitas *cyber-offensive* nya melalui sejumlah upaya termasuk rekrutmen kelompok *hackers*, penciptaan dan pelatihan unit militer khusus bidang siber, distribusi jaringan perangkat keras ke pasar dunia, serta penempatan titik eksploitasi diseluruh jaringan asing. Sedangkan Amerika Serikat telah lama mempertahankan dominansi ofensif melalui pembentukkan jaringan *packet-switching* yang merupakan salah satu komponen yang menjadi prekursor utama dalam internet modern dan baru – baru ini mulai mengoperasikan pentagon "cyber range", yang merupakan sebuah sistem internet tertutup dengan kapasitas yang memadai untuk memungkinkan pengujian senjata siber dalam hal untuk mempertahankan keunggulan ofensif Amerika Serikat.[21]

Sedangkan dalam hal *Defensive Capabilities*, bentuk defensif siber dari Tiongkok adalah mengamankan dan mengisolasi seluruh jaringan yang berasal dari luar negara. Hal ini dilakukan untuk menjaga kontrol atas situs dan informasi mana yang boleh diakses oleh masyarakat Tiongkok di dalam negeri.[22] Pemerintah Tiongkok memblokir dan menutup gerbang internet dari seluruh dunia. Sedangkan bentuk defensif dari Amerika Serikat adalah membagi jaringan Amerika Serikat menjadi tiga kategori yakni; jaringan rahasia, jaringan pemerintah, dan jaringan swasta. Jaringan rahasia termasuk yang dioperasikan oleh Komunitas Intelijen dan Departemen Pertahanan Amerika Serikat.

[21] George Patterson Manson III: 124
[22] George Patterson Manson III: 125

Studi pustaka yang keempat adalah artikel yang berjudul *Cybersecurity in Sino-American Relations* oleh Marie Baezner dalam CSS Analyses in Security Policy.[23] Tulisan ini menjabarkan mengenai faktor–faktor yang membuat kedua negara saling tidak percaya sehingga melakukan spionase. Selama beberapa tahun terakhir, ketegangan antara kedua negara ini secara khusus meningkat terkait masalah keamanan siber. Tiongkok dan Amerika Serikat telah melakukan spionase siber satu sama lain. Hal yang mempengaruhi tindakan saling tidak percaya diantara kedua negara ini ialah Tiongkok tidak setuju dengan model tata kelola global internet yang diajukan oleh Amerika Serikat dan peningkatan kapabilitas militer siber Tiongkok yang digunakan dalam pembentukkan Zona Anti-Akses.

Dalam tersebut dijabarkan ada dua faktor yang menjadi penyebab kedua negara saling melakukan spionase. Yang pertama adalah masalah tata kelola global internet. Hal ini disebabkan Amerika Serikat yang mana merupakan negara yang menginisiasi pembentukkan tata kelola global dalam hal siber. Internet dikelola oleh organisasi non profit yang bernama Internet Cooperation for Assigned Names and Numbers (ICANN).[24] Namun, negara seperti Tiongkok dan Rusia mencurigai bahwa pembentukkan tata kelola global dalam hal siber tersebut hanya untuk mencapai kepentingan nasional Amerika Serikat dan juga memudahkan akses untuk mengetahui rahasia negara lain melalui siber. Faktor yang kedua adalah zona anti akses di bangun oleh Tiongkok di kawasan Laut Tiongkok Selatan. Zona anti

[23] Marie Baezner,"Cybersecurity in Sino-American Relations", *CSS Analyses in Security Policy*, No.224, (2018): 1
[24] Marie Baezner: 3

akses merupakan pendekatan pertahanan asimetris yang digunakan untuk mencegah dan menghalangi musuh memasuki zona tersebut dengan meningkatkan kemampuan siber untuk mengendalikan ruang informasi jika terjadi konflik. Tujuannya adalah menganggu sistem komunikasi dan GPS musuh.[25]

Studi pustaka yang terakhir adalah artikel yang berjudul *An Analysis of Cyberspace Rule-Making in China-US Relations* oleh Zhao Geng dalam jurnal International Relations and Diplomacy.[26] Artikel ini menjelaskan mengenai analisis pembuatan peraturan terkait dunia siber dalam hubungan Tiongkok dan Amerika Serikat. Kedua negara tersebut saling bernegosiasi untuk menciptakan peraturan terkait dunia siber agar terciptanya keamanan dan kestabilan dunia siber secara global. Kedua negara mempunyai kepentingan nasional nya masing–masing dalam pembuatan peraturan siber ini. Dengan adanya landasan norma dalam tata kelola dunia siber ditujukan untuk membatasi perilaku setiap aktor internasional dengan norma – norma yang efektif.[27]

Dalam tulisan ini dijelaskan bahwa pembuatan peraturan terkait dunia maya memiliki implikasi yang penting bagi Amerika Serikat dan Tiongkok. Hal ini dilakukan untuk mengurangi adanya serangan siber baik itu dalam bentuk pencurian data, menyerang dengan menggunakan *malware* dan melakukan kegiatan spionase. Kedua negara mempromosikan norma dan membuat peraturan

[25] Marie Baezner: 4
[26] Zhao Geng, "An Analysis of Cyberspace Rule-Making in China-US Relations*", International Relations and Diplomacy,* Vol. 6, No.1 (2018): 16
[27]Zhao Geng: 18

terkait dunia siber dengan menggunakan *soft power* yang ditempuh melalui negosiasi dan diplomasi. Dengan demikian, disamping kepentingan kedua negara terpenuhi, keamanan dan kestabilan pun juga terpenuhi.

Keseluruhan dari studi pustaka tersebut secara umum menjelaskan mengenai dinamika hubungan antara Amerika Serikat dengan Tiongkok dalam hal siber. Pada studi pustaka terakhir menjelaskan mengenai kerjasama diantara kedua negara tersebut dengan menggunakan konsep *cybernorms*. Dalam penelitian ini, penulis akan meneliti motivasi Amerika Serikat melakukan kerjasama keamanan siber dengan Tiongkok salah satunya dengan menggunakan konsep *cybernorms* namun juga konsep–konsep lain yang untuk lebih menganalisis secara detail mengenai motif Amerika Serikat dengan menggunakan konsep *cybersecurity*

1.7 Kerangka Konseptual

Dalam menganalisis Motivasi Amerika Serikat dalam Melakukan Kerjasama Keamanan Siber dengan Tiongkok, maka penulis akan menggunakan konsep *Cyber Security*.

1.7.1 Cyber Security

Konsep keamanan oleh Nazri Choucri didalam bukunya yang berjudul *Cyber Politics in International Relations* membagi keamanan nasional dalam empat dimensi yakni; *External Security, Internal Security, Environtmental Security,*dan *Cyber Security*. Keamanan siber merupakan dimensi keempat dalam

konsep keamanan nasional kontemporer.[28] Hal ini mengacu kepada kemampuan negara dalam melindungi keamanan nasional mereka sendiri dari adanya ancaman siber seperti spionase, sabotase, kejahatan penipuan, pencurian, dan lain sebagainya. Isu siber merupakan isu yang sangat krusial dalam hubungan internasional sehingga dalam konteks hubungan internasional itu sendiri mengidentifikasi *Cyber Security* kedalam *cyber conflict* dan *cyber cooperation. Cyber Conflict* merupakan istilah yang mendeskripsikan bentuk kejahatan siber dalam interaksi hubungan internasional.

Cyber conflict adalah penggunaan teknologi komputasi untuk merusak, mengubah, dan memodifikasi informasi rahasia dan infrastruktur penting yang dimiliki oleh suatu negara sehingga hal tersebut berdampak terhadap hubungan diplomatik dan militer kedua negara yang berkonflik.[29] Sedangkan *cyber cooperation* merupakan penggunaan teknologi sebagai arena untuk kerjasama diantara dua negara atau lebih dengan tujuan untuk mengejar beberapa tujuan dan kepentingan mereka yang mungkin tidak dapat dicapai secara individual. Selain itu, kerjasama dilakukan dikarenakan negara menghadapi kondisi buruk yang membutuhkan tindakan yang terkoordinasi.[30]

[28] Nazli Choucri, *Cyberpolitics in International Relations,* (Cambridge : MIT Press, 2012): 43
[29] Brandon Valeriano dan Ryan C Maness, The Dynamics of Cyber Conflict between Rival Antagonist, *Journal of Peace Research,* Vol.51, No.3 (2011): 347
[30] Nazli Choucri, *Cyberpolitics in International Relations,* (Cambridge : MIT Press, 2012): 170

Menurut Myriam Dunn Cavelty dalam *Cyber Security,* masalah umum dalam ancaman-ancaman siber adalah menyerang jaminan informasi yang mengenai keamanan dasar informasi dan sistem infomasi.[31] Oleh sebab itu, jaminan informasi (*information assurance*) merupakan konsep proteksi utama dalam keamanan siber.

1.7.1.1. Jaminan Informasi

Jaminan Informasi *(Information Assurance)* merupakan konsep utama dalam *cyber Security*. Jaminan keamanan informasi merupakan praktik standar untuk memanajemen resiko yang berkaitan dengan penggunaan, proses, penyimpanan dan transmisi informasi atau data serta sistem dan proses yang digunakan untuk tujuan tersebut.[32] Perlindungan terhadap informasi merupakan hal yang paling mendasar dan penting yang harus dilakukan oleh negara dalam hal untuk mempertahankan keamanan siber. Hal ini dikarenakan informasi dasar seperti informasi finansial, militer, strategi pemerintahan, bahkan jaringan informasi dalam komputer sewaktu-waktu dapat diserang dan hal tersebut menimbulkan kerentanan dalam sistem informasi dan komputasi sehingga mengganggu kestabilan keamanan siber.[33]

[31] Myriam Dunn Cavelty, *Cyber Security,* (Oxford:Oxford University Press,2012): 17
[32] Corey D. Schou, dan Kenneth J. Trimmer, "Information Assurance and Security", *Journal of Organizational and End User Computing on Information Security* (2005), https://www.researchgate.net/publication/220349069_Information_Assurance_and_Security: 1
[33] Erbu Yeniman Yildirim, "The Importance of Risk Management in Information Security", IIER International Conference, ISBN: 978-93-86083-34-0 (2016): 5

Jaminan informasi berakar dari analisis resiko yang mana hasil dari analisis resiko tersebut digunakan untuk menyediakan panduan dalam area yang mengalami atau memiliki resiko tertinggi, dan berdasarkan hal tersebut maka disusunlah rencana dan kebijakan untuk memastikan bahwa sistem tersebut terlindungi sepenuhnya.

Model dari jaminan keamanan ini memiliki tiga tujuan utama. Ketiga tujuan tersebut adalah; *Confidentiality*, mengacu kepada perlindungan informasi dari pengungkapan pihak yang tidak berwenang. *Integrity*, mengacu kepada perlindungan informasi agar tidak diubah oleh pihak yang tidak berwenang. Dan yang ketiga *Availability* yang mana maksudnya adalah informasi harus selalu tersedia apabila pihak yang berwenang membutuhkan informasi tersebut.[34] Dalam jaminan informasi, tujuan dasarnya adalah pencegahan terhadap adanya serangan-serangan siber dengan membentuk strategi-strategi terkait jaminan informasi yang dibagi kedalam dua tingkatan; yakni tingkat nasional dan tingkat internasional yang mana masing-masing tingkatan tersebut juga terdiri dari beberapa bentuk strategi.[35]

1. Tingkat Nasional

Tindakan penanggulangan serangan siber untuk menjamin keamanan informasi dalam keamanan siber ditingkat nasional terdiri dari;

[34] Corey D. Schou, dan Kenneth J. Trimmer, "Information Assurance and Security", *Journal of Organizational and End User Computing on Information Security* (2005), https://www.researchgate.net/publication/220349069_Information_Assurance_and_Security: 1
[35] Myriam Dunn Cavelty, *Cyber Security*, (Oxford:Oxford University Press,2012): 17

cyber deterrence, cyber offense, cyber defence, dan perlindungan infrastruktur penting

a. ***Cyber Deterrence***

Cyber deterrence mengacu kepada usaha negara untuk memberikan kekhawatiran kepada musuh dengan cara memperlihatkan kapabilitas siber yang dimiliki oleh negara tersebut. Tidak hanya memberikan kekhawatiran kepada musuh, namun juga menunjukkan kepada aktor–aktor dalam sistem internasional mengenai kapabilitas dan kapasitas teknologi informasi dan komunikasi yang dimiliki oleh negara tersebut.

Konsep *Deterrence* ini berlandaskan kepada ide–ide mencegah musuh untuk mengambil tindakan sebelum perang dimulai, yang mana dalam konteks ini negara tidak harus berada dalam situasi konflik, namun bisa juga bekerjasama. Karakteristik utama dari konsep ini adalah; kejelasan konsekuensi dan resiko, kapabilitas dan kapasitas dari teknologi, serta kesiapsiagaan pemerintah dalam merespon.[36]

Menurut W. Goodman, *cyber deterrence* adalah menghalangi para penyerang mengambil tindakan agresif di dunia siber.[37] Dua komponen strategis yang diimplementasikan oleh negara bangsa dalam hal untuk

[36] Myriam Dunn Cavelty, *Cyber Security*, (Oxford:Oxford University Press,2012): 18
[37] T. Stevens, A cyberwar of ideas?: Deterrence and norms in cyberspace. Contemporary Security Policy, Vol. 33, No.1, (2012): 151. doi:10.1080/13523260.2012.659597

menghalangi musuh ialah; *deterrence by denial* dan *deterrence by punishment or retaliation.*

deterrence by denial merupakan mencegah para penyerang untuk mendapatkan keuntungan atau manfaat yang diperoleh dari serangan siber yang dilancarkan. *Deterrence by denial* bertujuan untuk menurunkan keuntungan yang dicari oleh penyerang dengan meningkatkan pertahanan untuk melindungi sistem dan jaringan komputer.[38]

Deterrence by punnishment atau *retaliation* merupakan strategi *deterrence* yang berbentuk tindakan ofensif, dan mengarah kepada penggunaan ancaman terhadap penyerang dengan memberikan sanksi atau penalti berupa sanksi ekonomi dan serangan kembali atau segala sesuatu yang mengakibatkan para penyerang akan mendapatkan kerugian yang lebih besar dibandingkan dengan keuntungan yang mereka peroleh dari serangan.[39]

b. ***Cyber Offense***

Cyber offense berisikan serangkaian strategi nasional yang digunakan untuk menyerang musuh seperti melancarkan serang DoDs, *Malware*, sabotase dan lain sebagainya untuk menyerang *critical infrastructure* dan melemahkan sistem komputer dan jaringan musuh serta

[38] T. Stevens, A cyberwar of ideas?: Deterrence and norms in cyberspace. Contemporary Security Policy, Vol. 33, No.1, (2012): 151-152. doi:10.1080/13523260.2012.659597
[39] T.Stevens: 152

mendapatkan informasi dengan cara melakukan kegiatan spionase. Selain itu *cyber offense* dilakukan bertujuan untuk melindungi sistem komputer dan jaringan dari serangan musuh.

Cyber offense yang lazim dilakukan dalam militer dan juga dalam strategi keamanan nasional negara ialah dengan peningkatan kapabilitas offense. OCC itu sendiri diartikan sebagai kapablitas yang dirancang untuk mendapatkan beberapa capaian atau tujuan terkait tindakan ofensif sebuah negara terhadap targetnya.[40] Selain itu bentuk tindakan offensif lainnya ialah berupa *cyber deterrence by punnishment* seperti yang telah dijelaskan sebelumnya.

c. ***Cyber Defense***

Cyber Defense mengacu kepada usaha negara untuk meningkatkan pertahanan negaranya dengan meningkatkan sistem pertahanan siber dengan cara meningkatkan sistem perangkat lunak dan menemukan kerusakan dan memperbaiki kerusakan dari sistem tersebut.

Tindakan defensif siber berfokus kepada pencegahan, pendeteksian, dan respon yang cepat serta tanggap terhadap serangan atau ancaman sehingga infrastruktur penting dan jaminan informasi dapat dilindungi sepenuhnya. Bentuk-bentuk defensif siber secara umum ada dua, secara teknis bentuknya ialah dengan menerapkan operasi siber dan meningkatkan

[40] Max Smeets dan Herbert S. Lin, "Offensive Cyber Capabilities: To What End" NATO CCDCOE (2018): 57

sistem resiliensi agar stabilitas pertahanan siber dapat terjaga dan yang kedua ialah defensif siber dengan adanya pertukaran informasi dan memperkuat hubungan kerjasama baik itu dengan sektor privat, negara maupun organisasi internasional.[41]

d. **Perlindungan Infrastruktur Penting**

Sejak tahun 1990an, infrastruktur penting menjadi objek referensi utama dalam perdebatan keamanan siber. Menurut *Presidential Policy Directive 21* (PPD-21) 16 sektor Infrastruktur penting Negara yang harus dilindungi ialah Sektor Kimia, Sektor Komunikasi, Sektor Bendungan, Sektor Layanan Darurat, Sektor Layanan Keuangan, Sektor Fasilitas Pemerintahan, Sektor Teknologi Informasi, Sektor Sistem Transportasi, Sektor Sistem Air dan Limbah, Sektor Reaktor dan Material Nuklir, Sektor Layanan Kesehatan, Sektor Makanan dan Agrikultur, Sektor Energi, Sektor *Defense Industrial Base*, Sektor Pabrik, dan Sektor Fasilitas Komersial.[42]

Tantangan utama dalam usaha melindungi infrastruktur penting berangkat dari privatisasi dan deregulasi sebagian besar sektor publik pada tahun 1980an dan proses globalisasi pada tahun 1990an yang mana banyak pengalihan infrastruktur penting ke tangan swasta. Oleh sebab itu, prinsip–

[41] Diego Fernandez Vazquez,dkk, "Conceptual Framework for Cyber Defense Information Sharing within Trust Relationships", 4th International Conference on Cyber Conflicts, (2012)
[42] Department of Homeland Security, "Critical Infrastructure Sectors", CISA, https://www.dhs.gov /cisa/critical-infrastructure-sectors, diakses 1 Januari 2019

prinsip dalam hal perlindungan infrastruktur penting ialah dengan adanya *Public Private Partnerships and Information Sharing.*[43]

Public Private Partnerships (kemudian disingkat PPP) merupakan bentuk kerjasama antara negara dengan sektor swasta dalam hal untuk melindungi infrastruktur penting. Bentuk kerjasama yang dilakukan adalah memfasilitasi pertukaran informasi antara perusahaan dengan pemerintah khusus keamanan. Adanya saling menguntungkan antara pertukaran informasi itu tercermin dari keuntungan sektor swasta dalam mendapatkan informasi oleh layanan intelijen negara dan dari sektor negara memperoleh pengetahuan teknologi yang lebih maju.

2. Tingkat International

Tindakan penanggulangan serangan siber atau strategi untuk menjamin keamanan informasi dalam keamanan siber ditingkat internasional adalah dengan Konstruksi norma siber.

a. Konstruksi Norma Siber

Keamanan dunia siber saat ini menjadi masalah dan prioritas utama bagi negara dalam hal untuk meningkatkan keamanan nasionalnya. Didalam teorinya, efektivitas *cyber detterence* mewajibkan adanya skema yang luas dari kapabilitas siber suatu negara baik dalam hal ofensif maupun

[43] Myriam Dunn Cavelty: 19

defensif yang didukung oleh kerangka hukum internasional yang kuat serta kemampuan untuk menyerang penyerang tanpa adanya keraguan. Desain kapabilitas defensif dan desain undang–undang merupakan hal yang tidak terbantahkan.[44] Banyak negara–negara, organisasi internasional dan komunitas internasional lainnya meningkatkan kewaspadaan dengan melakukan kerjasama internasional dan menyetujui aturan dan norma yang disepakati bersama.

Setelah adanya kasus Stuxnet, negara–negara telah mulai untuk berupaya mengendalikan penggunaan eksploitasi sistem komputer yang digunakan untuk tujuan militer melalui kontrol senjata atau pembentukkan norma multilateral serta perjanjian internasional.[45]

Pembentukkan norma dimaksudkan untuk melindungi hak asasi manusia dan kedaulatan negara sehingga dengan adanya norma tersebut negara akan sadar bahwa negara harus mempunyai batasan dalam melakukan kegiatan didalam dunia maya.

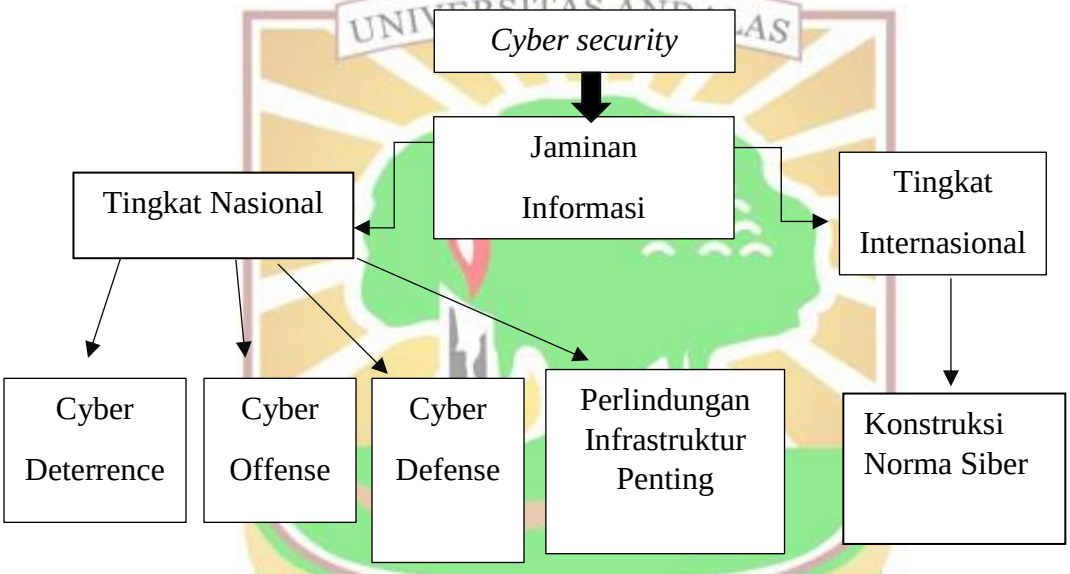
Menurut Finnemore, jika proses norma yang kuat, sebagaimana dilakukan dengan mengkonstruksi, mempromosikan, dan diinstitusionalkan merupakan bagian integral dari norma siber yang baik, maka pendukung norma siber harus mencurahkan sebanyak mungkin perhatian pada proses

[44] Myriam Dunn Cavelty: 19
[45] Myriam Dunn Cavelty: 17

tersebut layaknya mereka harus melakukan negosiasi dalam hal untuk mencapai tujuan yang diinginkan.[46]

Berdasarkan penjelasan tersebut, maka konsep *cyber security* dirangkum kedalam bagan 1.1 berikut

Bagan 1.1. Bagan konsep keamanan siber



Sumber: Myriam Dunn Cavelty, 2015

1.8. Metode Penelitian

1.8.1. Pendekatan dan Jenis Penelitian

Dalam penelitian ini, penulis akan menggunakan metode kualitatif. Penelitian kualitatif merupakan jenis penelitian yang bersifat eksplanatif dan menggunakan logika berpikir dalam memecahkan masalah penelitian.[47] Metode dalam penelitian

[46] Martha Finnermore, dan Duncan B. Hollis, "Constructing Norms for Global Cybersecurity", *The American Journal of International Law*, Vol.110, No.3 (2016): 460
[47] Husaini Usman dan Purnomo Setiady Akbar,*Metodologi Penelitian Sosial* (Jakarta: PT Bumi Aksara, 2011): 108

jenis kualitatif ini adalah dengan mengumpulkan beberapa data berupa jurnal ilmiah yang berisikan penelitian – penelitian terdahulu terkait kerjasama keamanan keamanan siber Amerika Serikat dengan Tiongkok, dan tinjauan pustaka lainnya yang dirasa dapat membantu dalam penelitian ini.[48] Data–data tersebut digunakan sebagai alat untuk menganalisis langkah–langkah, strategi serta motif yang menjadi landasan Amerika Serikat melakukan kerjasama keamanan siber dengan Tiongkok.[49]

Jenis penelitian yang akan digunakan dalam menganalisis motivasi Amerika Serikat melakukan kerjasama keamanan siber dengan Tiongkok adalah eksplanatif. Dalam melakukan penelitian peneliti akan melihat keterkaitan antara teori atau konsep, dan hipotesis dengan fenomena serta menjawab pertanyaan terkait fenomena tersebut untuk menjawab anomali dalam penelitian.

1.8.2. Batasan Penelitian

Batasan waktu yang digunakan penulis untuk penelitian yang bertajuk "Motivasi Amerika Serikat Melakukan Kerjasama Keamanan Siber dengan Tiongkok" ini adalah dari tahun 2011 hingga 2015 dimulai dari kerjasama keamanan siber pertama diantara kedua negara tersebut namun terjadi kegagalan kerjasama siber pada tahun 2013 akibat adanya saling ketidakpercayaan yang berujung kepada kegiatan spionase dan kemudian adanya normalisasi hubungan pada tahun 2015.

[48] Husaini Usman dan Purnomo Setiady Akbar: 108
[49] Husaini Usman dan Purnomo Setiady Akbar: 109

1.8.3. Unit Analisa

Unit analisa atau biasa disebut sebagai variabel dependen merupakan objek yang akan dijelaskan atau dianalisis dalam sebuah penelitian.[50] Sedangkan unit eksplanasi atau biasa disebut sebagai variabel independen merupakan unit penjelas dari unit yang akan dianalisa[51]. Berdasarkan penelitian yang berjudul "Motivasi Amerika Serikat Melakukan Kerjasama Keamanan Siber dengan Tiongkok" maka unit analisa nya adalah Kebijakan Amerika Serikat sedangkan unit eksplanasi dalam penelitian ini adalah *cyber security* Tiongkok.

1.8.4. Tingkat Analisa

Tingkat analisa merupakan tingkatan dalam penelitian yang digunakan sebagai acuan dalam menganalisis.[52] Tingkat analisa secara umum ada 3 yakni; individu, negara, dan sistem internasional.[53] Terkait penelitian yang berjudul "Motivasi Amerika Serikat Melakukan Kerjasama Keamanan Siber dengan Tiongkok", tingkat analisa adalah Sistem Internasional.

1.8.5. Teknik Pengumpulan Data

Penelitian ini dilakukan dengan salah satu teknik pengumpulan data yakni studi kepustakaan dengan mempelajari, serta membandingkan beberapa data berupa

[50] Mohtar Mas'oed, *Ilmu Hubungan Internasional: Disiplin dan Metodologi,* (Yogyakarta: Pusat Antar Universitas-Studi Sosial Universitas Gadjah Mada, LP3E, 1990): 108
[51] Mohtar Mas'oed: 108
[52] Mohtar Mas'oed: 35
[53] Mohtar Mas'oed: 35

buku, jurnal, atau karya ilmiah lainnya yang didapat dari beberapa tempat. Data yang diperoleh sebagai rujukan dalam penelitian ialah data sekunder.

Data sekunder didapatkan dari berbagai laporan dari *website* resmi Pemerintah Amerika Serikat (http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf), dokumen dari DoD (Department of Defense) Amerika Serikat, untuk mengetahui kebijakan keamanan siber Amerika Serikat. Data lainnya juga didapatkan dari beberapa tulisan berupa buku, jurnal, laporan – laporan penelitian sebelumnya, situs berita internasional dan tulisan ilmiah lainnya yang diperlukan dalam penelitian.

1.8.6. Teknik Analisa

Teknik analisa dilakukan dengan tujuan untuk membuat penjelasan yang lebih sistematis.[54] Menurut tulisan *Data Analysis Technique in Qualitative Research* oleh Barbara D. Kawulich, ada 5 tahapan dalam teknik analisa. 5 tahapan tersebut ialah;

a. Narasi

   Merupakan teknik yang digunakan untuk mengidentifikasi permasalahan penelitian dalam kerjasama keamanan siber antara Amerika Serikat dengan Tiongkok dengan menggunakan pendekatan narasi sesuai dengan data–data terkait hubungan konflik dan kerjasama siber antara Amerika Serikat dan Tiongkok.

[54] Barbara D. Kawulich, *Data Analysis Technique in Qualitative Research,* (Georgia: State University of Georgia),2005: 97

b. Koding

Merupakan teknik dalam menorganisasi data–data yang dapat dilihat dalam studi pustaka dengan tujuan untuk membantu penulis dalam menentukan data mana yang sesuai dengan topik penelitian yakni mengenai motivasi Amerika Serikat melakukan kerjasama keamanan siber dengan Tiongkok dan mana yang tidak.

c. Interpretasi

Merupakan teknik yang membantu penulis memahami masalah berdasarkan data yang didapatkan dengan menggunakan kerangka konseptual yakni *cyber security.*

d. Konfirmasi

Merupakan tahapan bagi penulis menemukan bukti–bukti termasuk didalamnya konflik siber antara Amerika Serikat dan Tiongkok serta kebijakan Amerika Serikat sehingga menghasilkan kerjasama dengan Tiongkok dan kerangka konseptual yang digunakan sehingga menghasilkan klaim

e. Presentasi

Tahapan ini merupakan tahap yang mana penulis akan melakukan presentasi atas penemuan yang didapatkan terkait motivasi Amerika Serikat melakukan kerjasama keamanan siber dengan Tiongkok.

1.9. Sistematika Penulisan

BAB I **Pendahuluan**

Merupakan pengantar yang berisikan latar belakang masalah, rumusan masalah, pertanyaan penelitian, tujuan penelitian, manfaat penelitian, tinjauan pustaka sebagai bahan rujukan dan pembanding, kerangka konseptual yang digunakan dalam menganalisis, metode penelitian, unit analisa, tingkat analisa, teknik pengumpulan data, dan teknik analisa.

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

Bab ini mendeskripsikan konflik antara Amerika Serikat dan Tiongkok terkait keamanan siber, yang mana dimulai dari kegiatan spionase hingga kegiatan *hacking* yang dilakukan oleh kedua negara satu sama lain. Selain pada bab ini juga dijelaskan dampak konflik tersebut terhadap ekonomi, politik dan keamanan Amerika Serikat

BAB III **Kebijakan Keamanan Siber Amerika Serikat**

Bab ini akan menjelaskan mengenai kebijakan keamanan siber Amerika Serikat dan kebijakan keamanan nasional siber Amerika Serikat serta menjelaskan perubahan kebijakan keamanan siber yang mana awalnya hanya berfokus terhadap keamanan nasional.

Pada bab ini juga akan menjelaskan bentuk perubahan kebijakan tersebut yakni merupakan perjanjian keamanan siber antara Amerika Serikat dengan Tiongkok

BAB IV **Analisis Motivasi Amerika Serikat Melakukan Kerjasama Siber dengan Tiongkok**

Bab ini menjelaskan Motivasi Amerika Serikat Melakukan Kerjasama Siber dengan Tiongkok dengan menggunakan konsep *Cyber Security* sesuai dengan data–data yang dijabarkan dari Bab II dan Bab III. Hal yang disoroti disini ialah motivasi dari Amerika Serikat dalam melakukan kerjasama dalam bidang keamanan siber khususnya dengan Tiongkok.

BAB V **Penutup**

Bab ini berisikan kesimpulan dan saran sebagai hasil dari penelitian.