BAB II

TINJAUAN PUSTAKA

2.1 Literature Review

Penelitian yang juga meneliti terkait hubungan siber yang terjadi antara Amerika Serikat dan Tiongkok dan menjadi sumber penulusuran peneliti salah satunya ialah Dampak Pembangunan Cyber Power Tiongkok Terhadap Kepentingan Amerika Serikat yang dilakukan oleh Dewi Triwahyuni (D. Triwahyuni & Yani, 2018). Dalam penelitian ini dijelaskan bahwa keamanan nasional Tiongkok bertujuan untuk membangun kekuatan dunia maya dalam mempertahankan rezim komunis negaranya, Tiongkok menjaga kedaulatan nasional dan keutuhan wilayah dan Tiongkok mencoba memposisikan dirinya sebagai kekuatan regional dan kekuatan dunia. Semua tujuan ini dicapai dalam upaya Tiongkok untuk mencapai stabilitas dan kemajuan ekonomi, serta modernisasi militer Tiongkok. Dijelaskan bahwa Tiongkok memanfaatkan kemampuan ICT untuk menyusup ke pertahanan yang lebih lemah milik Amerika Serikat dan melakukan penyerangan yang mengancam keamanan infrastruktur sipil dan infrastruktur militer milik Amerika Serikat.

Dan dijelaskan pula bahwa kemampuan jaringan Tiongkok terus ditingkatkan, sehingga mampu menimbulkan kerusakan secara internasional. Persoalan yang terjadi antara Amerika Serikat dengan Tiongkok ini membuat situasi yang dilematis, sebab Karena hadirnya ketergantungan dalam hubungan antara Tiongkok dan Amerika Serikat dalam industri IT. Dilema ini tentu membuat Amerika Serikat terdorong untuk memajukan sistem pertahanan negaranya dengan cara meningkatkan sistem koordinasi yang diperlukan dalam rangka menjaga dan melindungi semua aspek negaranya dari serangan siber Tiongkok. Dalam kajian ini analisis permasalahan menggunakan metode kualitatif dengan kerangka teoritis yang lebih menekankan konsep *Cyber Power*.

Literatur lainnya hasil penelitian yang ditulis oleh Guntomo Raharjo berjudul "Srategi Amerika Serikat dalam Menghadapi Eskalasi *Cyber Power* Tiongkok Periode

2011-2015" (Guntomo, 2016) berpendapat bahwa hubungan antara Amerika Serikat dengan Tiongkok meningkatnya *cyber power* Tiongkok melahirkan sebuah situasi yang dilematis bagi Amerika Serikat dan menimbulkan konflik antara kedua negara dalam konteks dunia maya. Eskalasi *cyber power* Tiongkok telah dianggap menghambat dan mengganggu kepentingan nasional Amerika Serikat. Fakta yang ada menyebutkan bahwa Tiongkok melakukan praktek *cyber attack* kepada Amerika Serikat, sehingga kondisi tersebut mendesak Amerika serikat untuk segera meningkatkan kapabilitas negaranya dalam mengamankan keamanan siber negaranya melalui strategi defensif. Strategi ini dipilih Amerika Serikat dikarenakan *strategi ofensif* dianggap hanya mementingkan stabilitas jangka pendek, dan membuat *cyberwarfare* Amerika Serikat dan Tiongkok semakin hebat yang justru memperburuk keadaan.

Maka itu strategi defensif menjadi pilihan Amerika Serikat untuk merespon eskalasi *cyber power* Tiongkok terhadap negaranya. Strategi ini dianggap dapat meminimalisir ancaman siber yang dilakukan Tiongkok serta menjaga keamanan siber Amerika serikat dan tetap menjalin hubungan baik dengan Tiongkok. Kondisi sistem internasional yang anarki, menjadikan kerjasama sebagai pilihan alternatif yang logis dan strategis agar bisa keluar dari kondisi *security dilemma* yang terjadi pada kedua negara. Karena kerjasama dapat menciptakan keuntungan bagi kedua belah pihak, mengurangi dampak anarki yang terjadi, serta menciptakan situasi yang jauh lebih baik. Dalam fokus penelitian membahas mengenai langkah defensif Amerika Serikat dengan menggunakan konsep *security dilemma*, teori *offensive-deffensive* dan konsep *cyber power* dalam menganalisis strategi AS menghadapi eskalasi siber Tiongkok periode 2011-2015.

Literatur selanjutnya, buku berjudul "*Strategic Cyber Security"* oleh Kenneth Geers (Geers Kenneth, 2011) menuturkan bahwa ruang siber menjadi arena konflik baru yang menjadi dasar strategi pertahanan dan ancaman serangan yang masih belum jelas. Seperti halnya terorisme, para hacker telah menemukan h*ype* dalam dunia maya.

Sifat *cyberspace* yang *borderless* membuat *cyber warfare* berbeda dengan perang konvensional dan menjadi ancaman yang baru bagi negara.

Perang siber yang rentan terjadi, membuat meningkatnya upaya dan strategi yang diperlukan oleh para perencana keamanan nasional sebuah negara. Dalam buku ini membahas bahwa beberapa analis menganggap bahwa *cyber warfare* terlalu di lebih-lebihkan. Bagaimanapun juga keamanan nasional sebuah negara tidak bisa meremehkan potensi terjadinya *cyber warfare*. Ketergantungan negara-negara dengan aspek IT dan pertumbuhan internet, mendorong pemerintah agar membuat investasi dalam keamanan siber negaranya, respon terkait insiden siber, pelatihan teknis, dan juga kolaborasi internasional.

Munculnya dampak luar biasa dari kejahatan *cyber* dan spionase *cyber*, serta *hype* media, menjadikan perang siber berubah sebagai ancaman bagi sebuah negara. Dalam *cyber attack*, komputer bisa langsung diserang ketika ia terkoneksi dengan internet. Resiko *cyber* akan lebih tinggi jika sumber informasi telah terhubung dalam konektivitas global dan jika infrastruktur jaringan sifatnya lemah sehingga rentan terhadap eksploitasi informasi. Dalam memperoleh keseimbangan dan keberhasilan, *cyber defender* membutuhkan tingkat keamanan pada komponen *hardware* dan *software* yang jauh lebih canggih, serta turut meningkatkan kinerja dalam strategi pertahanan negara. Dalam buku ini digunakan konsep *Strategic Cyber Security* dalam mengahadapi ancaman dari ruang siber secara umum yang tidak ditujukan ke satu negara secara khusus.

2.2 Kerangka Teoritis

Dalam rangka mempermudah proses penelitian dan pembahasan, diperlukannya dasar-dasar pemikiran yang diperoleh dari teori-teori dan beberapa pendapat para ahli yang tentunya berkaitan objek penelitian. Teori dan konsep dari para ahli yang diperoleh akan dijadikan sebagai landasan penulis dalam mengemukan kerangka pemikiran. Masalah yang penulis merupakan suatu persoalan dalam menghadapai era globalisasi yang telah membuka era *borderless*, dimana komunikasi

antar aktor hubungan internasional kini bisa dilakukan melalui internet tanpa terhalang oleh batas wilayah dan perbedaan waktu.

Akibat perkembangan teknologi informasi tersebut, maka jalan yang harus ditempuh oleh setiap negara ialah dengan menerima perkembangan tersebut. Hal ini kemudian menyebabkan ketergantungan bagi setiap negara terhadap teknologi informatika, baik dalam rangka menjalankan suatu pemerintahan di suatu negara maupun sebagai bentuk pelayanan secara publik bagi masyarakat pun kini tergantung pada ketersediaan (*availability*), keutuhan (*integrity*) dan kerahasiaan (*confidentiality*) informasi di ruang siber. Oleh sebab itu, perlindungan terhadap sarana dan prasarana infrastruktur negara yang memanfaatkan teknologi informatika sangat penting. Dalam hal ini, ancaman keamanan siber tidak lagi dipandang pada masalah teknis keamanan komputer semata melainkan mencakup aspek ideologi, politik, ekonomi, sosial, budaya dan keamanan nasional (Chotimah, 2015).

Penggunaan teknologi tersebut ditujukan untuk memperkuat pertahanan suatu negara dan diarahkan untuk menghadapi berbagai ancaman atau gangguan terhadap keamanan nasional. Ancaman keamanan siber sendiri muncul seiring dengan meningkatnya pengetahuan terhadap penggunaan teknologi informasi termasuk jaringan komputer dan internet. Hal ini memunculkan serangan siber dalam bentuk *hacktivism*, *cyberterrorism* dan *cyberwarfare* yang melakukan serangan tanpa mengenal batas negara. Serangan siber terjadi karena adanya kelemahan pertahanan sistem yang menyebabkan sistem mengalami kerentanan keamanan sistem.

Saat ini keamanan internasional mengalami perkembangan dan perubahan secara signifikan. Konsep keamanan kini sudah tidak lagi dibatasi sebagai hubungan konflik atau kerjasama negara, melainkan juga berfokus pada keamanan masyarakat. Menurut Buzan: Keamanan adalah langkah yang dilakukan dengan melampaui aturan main secara umum dalam membingkai suatu isu apakah isu tersebut termasuk dalam ranah politik atau melampauinya (Buzan, 1998).

2.2.1 Teori Strategi

Menurut John P. Lovell strategi merupakan serangkaian tindakan maupun keputusan yang telah dirancang sebelumnya dalam situasi kompetitif dimana hasil akhirnya tidak semata mata bersifat untung-untungan (Mohtar, 1989). Strategi merupakan metode yang digunakan untuk meraih tujuan atau menggunakan *power* dalam rangka mencapai kepentingan tersebut, termasuk kekuatan militer. Dalam politik luar negeri suatu negara, strategi telah menjadi pola perencanaan yang digunakan oleh para pembuat keputusan untuk mewujudkan dan memajukan kepentingan-kepentingan nasional, sekaligus melakukan upaya pencegahan agar negara lain tidak menghalangi kepentingan tersebut (D. Triwahyuni & Yani, 2018).

Dalam penelitian Pengaruh *Cyber Security Strategy* Amerika Serikat Menghadapi Ancaman *Cyber Warfare*, oleh Moehammad Yuliansyah Saputera. Terdapat perspektif teori strategi. Strategi merupakan pendekatan secara keseluruhan yang berkaitan dengan pelaksanaan usul, perencanaan, dan eksekusi sebuah aktivitas dalam kurun waktu tertentu. Pada konsep *use of power*, strategi berupa sebuah kemampuan dalam menggunakan *power* sebagai sebuah alat ataupun sebuah ancaman. Teknologi Informasi dan Komunikasi (TIK) merupakan salah satu instrumen dalam bidang teknologi terkait konsep *use of power*. Penggunaan Teknologi informasi dan komunikasi ini merujuk pada sebuah istilah intelijen (Nugroho, 2018).

Dengan adanya modernisasi, makna strategi pun ikut mengalami perluasan makna, yakni dengan tidak selalu berkaitan dengan ranah militer. Termasuk didalamnya ancaman siber, karena meski bentuk ancaman tersebut berada dalam dunia maya (*cyber space*) namun *cyber power* memiliki kemampuan untuk menjadi salah satu penyebab terjadinya suatu peperangan.

(J.C. Wylie, dikutip dalam Frans Osinga 2005:9) Mengatakan bahwa: "*Strategy is a plan of action designed in order to achieve some end; a purpose together with a system of measures for its accomplishment"*. Menurut Wylie strategi adalah rencana

maupun tindakan yang dirancang untuk mencapai suatu tujuan tujuan bersama, dengan sistem pengukuran untuk mencapainya.

Strategi pada tingkatan yang tinggi disebut sebagai tingkatan strategis, sebagai contoh suatu pemerintahan negara mengambil keputusan dalam mengamankan keamanan siber negaranya, maka segala keputusan yang akan diambil tentu saja perlu mempertimbangan segala aspek yang mencakup wilayah negara tersebut. (Yudistira, 2017)

2.2.2 Keamanan Siber

Keamanan siber adalah tata kelola, pengembangan, pengelolaan, dan penggunaan keamanan informasi, keamanan operasional, serta alat dan teknik keamanan TI untuk mencapai kepatuhan terhadap peraturan, mempertahankan aset, dan membahayakan aset musuh. (A. Walls, Perkins E, 2013)

Keamanan siber mencakup berbagai praktik, alat, dan konsep yang berkaitan erat dengan keamanan teknologi informasi dan operasional. Istilah "keamanan siber" kini menjadi sinonim untuk keamanan informasi atau keamanan teknologi, dalam hal ini aspek keamanan harus menggunakan istilah "keamanan siber" untuk menunjuk praktik keamanan yang menggunakan tindakan defensif yang melibatkan atau mengandalkan teknologi informasi (Guberina, 2017).

Keamanan siber menjelaskan hubungan antara keamanan siber, keamanan informasi, keamanan operasional, keamanan IT, prakti dan disiplin ilmu terkait. Dalam pertahanan siber, penerapannya akan selaras dengan keamanan siber yang direncanakan atau yang sudah ada (Guberina, 2017). Hal ini mencakup strategi sebuah negara dalam mengamankan lingkungannya. Dalam contoh studi kasus, strategi keamanan siber Amerika Serikat, disertai dengan upaya dan strategi diuraikan. Tujuan utama strategi ini adalah untuk mengenali masalah/fenomena dan memperluas pemahaman tentang pentingnya masalah ini dalam memberikan dampaknya bagi sebuah negara.

Keamanan siber bertujuan untuk menyelesaikan masalah pada keamanan informasi milik pemerintah, organisasi-organisasi, dan data individu yang terkait dengan teknologi TIK (terutama yang terkait dengan Internet). Dalam hal ini, terdapat perbedaan antara keamanan informasi dan keamanan jaringan yang menjadi dua konsep yang berbeda. Dalam beberapa kasus, terdapat persamaan pemahaman jika melibatkan perlindungan aset atau perlawanan terhadap spionase dalam aspek ekonomi, industri, terorisme, kejahatan ekonomi, ataupun pencegahan berbagai macam konten terlarang (D. dan T. A. Triwahyuni, 2016).

Dalam kasus lain, kedua konsep tersebut tentu saja berbeda. Keamanan jaringan meliputi segala sesuatu yang berhubungan dengan dengan perlindungan komputer, *monitoring* hingga *controlling*. Pada saat yang sama, keamanan informasi melibatkan persoalan yang lebih luas, seperti kedaulatan nasional, keamanan nasional, perlindungan infrastruktur, keamanan aset berwujud dan tidak berwujud, dan perlindungan data pribadi (D. dan T. A. Triwahyuni, 2016).

2.2.3 Teori *Security Dilemma*

Teori *security dilemma* berasal dari konsep *security dilemma* milik Robert Jervis, ia memaparkan bahwa security dilemma dapat didefinisikan sebagai suatu fenomena aksi dan reaksi antara beberapa negara di mana tindakan suatu negara untuk meningkatkan keamanannya akan berakibat atau dianggap melemahkan keamanan negara lainnya. Prediksi dasar mengenai keseimbangan *offense-defense* adalah apabila *offense* mendominasi maka *security dilemma* akan meningkat, lalu diikuti oleh perlombaan senjata, dan pada akhirnya perang kemungkinan besar akan terjadi. Oleh karena itu, perang/*cyberwarfare* dapat dicegah apabila strategi defense dapat mengungguli dominansi strategi offense (Alghifari & Olga Letticia, 2016).

2.3 Hipotesis Penelitian

Ancaman siber Tiongkok terbukti beresiko menghambat dan mengancam stabilitas keamanan Amerika Serikat, maka Amerika Serikat mengagendakan pemberantasan kejahatan siber dengan membuat kebijakan-kebijakan baru terkait

siber, undang-undang siber, melakukan kerjasama antar lembaga siber, meningkatkan anggaran siber, serta menjalin kerjasama dengan negara-negara lain termasuk dengan Tiongkok dalam rangka meningkatan keamanan pada sistem keamanan siber serta menyusun strategi untuk mengamankan kepentingan nasional negaranya.

2.4 Verifikasi Variabel dan Indikator

Variabel dalam Hipotesis	Indikator	Verifikasi
Variabel bebas: Serangan siber yang dilakukan Tiongkok terhadap Amerika Serikat mempengaruhi kebijakan publik di Amerika Serikat dan telah merugikan Amerika Serikat.	1. Situs hosting GreatFire dan CN-NYTimes yang digunakan untuk mencegah penyensoran negara Tiongkok, mendapat serangan penolakan service. 2.Situs register.com merupakan situs yang digunakan untuk pendaftaran domain Internet, jaringannya diakses selama	1. Februari 2015, situs hosting GreatFire dan CN-NYTimes yang digunakan untuk mencegah penyensoran negara Tiongkok, mendapat serangan penolakan service, yang membanjiri Github dengan serangan DoS. Sumber: Walters, R. (2015). Cyber Attacks on U.S. Companies Since November 2014. 2. Maret 2015 Register.com (Online) jaringannya diakses selama sekitar satu tahun oleh para peretas (*hacker*) dengan kata sandi yang dicuri. Beberapa ahli telah menuding bahwa pelanggaran itu terkait dengan militer Tiongkok, pihak militer Tiongkok melakukan kegiatan tersebut dalam upaya mencuri rahasia dan informasi peradagangan. Sumber: Walters, R. (2015). Cyber Attacks on U.S. Companies Since November 2014. *ISSUE BRIEF*, *4487*, 3. 3. Data-data yang dicuri: rencana rudal anti-kapal supersonik yang akan dibawa di kapal selam AS, bagian dari proyek Sea Dragon. Peretasan ini juga

	sekitar satu tahun oleh para peretas. 3.Data-data yang dicuri adalah rencana rudal anti-kapal supersonik yang akan dibawa di kapal selam AS, bagian dari proyek Sea Dragon. 4. Adanya lonjakan spionase digital oleh Tiongkok yang menargetkan rahasia dagang dan kekayaan intelektual produsen. 5.National Security Agency (NSA) memperingatkan bahwa 25 Common Vulnerabilities and Exposures (CVEs) sedang	mengakibatkan pencurian data dari sinyal peralatan, sensor dan radio, serta sistem kriptografi. Sumber: Gechev, V. (2021). Political Shadows in the USA - China Trade Dispute. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3758750 4. Dari laporan oleh perusahaan keamanan siber Fire Eye, yang telah mengidentifikasi aktivitas dari grup berlabel 'APT41' yang menargetkan lebih dari 75 pelanggannya, dari produsen dan perusahaan media hingga organisasi layanan kesehatan dan organisasi nirlaba. Yang mejadi target adalah rahasia dagang dan kekayaan intelektual produsen. Sumber: Gechev, V. (2021). Political Shadows in the USA - China Trade Dispute. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3758750 5. Pada 20 Oktober 2020, National Security Agency (NSA) memperingatkan bahwa 25 Common Vulnerabilities and Exposures (CVEs) sedang digunakan atau ditargetkan oleh aktor siber yang disponsori negara Tiongkok telah melakukan operasi peretasan terhadap banyak korban. Jaringan yang dimaksud adalah milik Sistem Keamanan Nasional, Pangkalan Industri Pertahanan AS, dan sistem Departemen Pertahanan. NSA juga menyatakan bahwa jaringan-jaringan itu secara konsisten dipindai, ditargetkan, dan dieksploitasi oleh aktor yang disponsori Tiongkok.

	digunakan atau ditargetkan oleh aktor siber yang disponsori negara Tiongkok.	Sumber: Sumber: Gechev, V. (2021). Political Shadows in the USA - China Trade Dispute. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3758750
Variabel Terikat: Strategi kebijakan *cybersecurity* Amerika Serikat berupa kebijakan-kebijakan dan undang–undang terkait *cybersecurity*, kerjasama lembaga amerika serikat, serta kerjasama antar negara.	1.Diperbaharuinya kebijakan dan adanya UU yang mengatur keamanan siber. 2.Peningkatan anggaran cybersecurity AS meningkat setiap tahunnya. 3.Dibentuknya kerjasama dan diperkuatnya strategi Department of Defense, USSTRACOM, dan USCYBERCOM.	1. Pada 2011, dibuat kebijakan International Strategy for Cyberspace. Kebijakan Departement of Defense Strategy for Operating Cyberspace pada 2011, The Departement of Defense Cyber Strategy pada 2015, dan Departement of State International Cyberspace Policy Strategy pada 2016. dan UU Protecting Cyber Networks Act (PCNA), National Cybersecurity Protection Advancement Act (NCPAA, Cyber Threat Sharing Act 2015, Cybersecurity Intelligence Sharing and Protection Act (CISPA), Cybersecurity Information Sharing Act (CISA) dan Cybersecurity Act 2015. Sumber: Nugroho, K. A. (2018). Pengaruh Cyber Attack terhadap Kebijakan Cyber Security Amerika Serikat. Journal of International Relations, 4(3). 2. Kenaikan anggaran pada tahun 2018, pengeluaran global untuk keamanan siber diproyeksikan mencapai sekitar 66 miliar dolar AS. Sumber: https://www.statista.com/statistics/615450/cybersecurity-spending-in-the-us/

	4.Amerika Serikat menjalin kerjasama bersama negara-negara lain untuk membentuk lingkungan siber internasional dan menjalin kerjasama dengan Tiongkok	3. Kerjasama dan memperkuata kekuatan badan agensi: *Department of Defense*, US *Strategic Command* (USSTRACOM), dan US *Cyber Command* (USCYBERCOM). Sumber: Saputera, M. Y. (2015). Pengaruh Cyber Security Strategy Amerika Serikat Menghadapi Ancaman Cyber Warfare. Jurusan Hubungan Internasional, 2(2), 6–7. 4. Strategi *cyber security internasional* berupa langkah diplomatik AS untuk keamanan siber yang mengedepankan pada kerjasama antar negara dalam langkah membangun kepercayaan antar negara. Sumber: Nugroho, K. A. (2018). Pengaruh Cyber Attack terhadap Kebijakan Cyber Security Amerika Serikat. Journal of International Relations, 4(3). Dan Amerika menjalin kerjasama dengan Tiongkok sebagai strategi defensive guna meminimalisir ancaman siber yang dilakukan Tiongkok serta menjaga keamanan siber Amerika serikat dan tetap menjalin hubungan baik dengan Tiongkok. Sumber: Guntomo, R. (2016). Strategi Amerika S erikat Dalam Mengahadapi Eskalasi Cyber Power Tiongkok Periode 2011-2015.

2.5 Skema dan Alur Penelitian