ANALISA PERLOMBAAN SENJATA SIBER ANTARA AMERIKA DAN CHINA 2014-2018 MENGGUNAKAN *RICHARDSON MODEL OF ARMS RACE*

ANALYSIS OF CYBER ARMS RACE BETWEEN UNITED STATES AND CHINA 2014-2018 USING RICHARDSON MODEL OF ARMS RACE

Rangga Setiawan[1], Agus H.S. Reksoprodjo[2], Suhirwan[3]

UNIVERSITAS PERTAHANAN
(Ranggasetiawan13@gmail.com, Yonorex@gmail.com, Suhirwan32@gmail.com)

Abstrak – Perang siber, dimana ranah teknologi informasi, pertahanan, diplomasi, dan politik domestik diracik pada barisan-barisan skrip komputer, tidak hanya stabilitas keamanan internasional, namun, stabilitas keamanan nasional pun menjadi sasaran utama dalam perkembangan teknologi ini. Bukan menjadi fenomena baru di dalam ilmu pertahanan maupun ilmu hubungan internasional mengenai dinamika dan sinergi dari teknologi, pertahanan, diplomasi, dan politik dalam negeri yang sering disebut Revolution in Military Affairs, namun, siber-lah yang memberikan ruang baru untuk sinergi tersebut dapat berkembang lebih pesat, dan leluasa. Terdapat sebuah pola perlombaan senjata di setiap era hubungan teknoloi, pertahanan, diplomasi, dan politik domestik, pertanyaan mengenai apakah pola ini juga terjadi dalam ruang siber dan senjata-senjatanya yang tidak kasat mata atau tidak, dan bagaimana Indoensia menghadapi perang siber yang tidak kunjung surut? Dengan menggunakan metode Kualitatif, dengan desain Studi Kasus, kasus perlombaan senjata yang diteliti antara Amerika dan China. Hasil penelitian yang dihitung mealalui Richardson Model of Arms Race menunjukkan bahwa terdapat perlombaan senjata siber yang tengah terjadi diantara Amerika dan China.

Kata Kunci: Perang Siber, *Logical Weapon*, Perlombaan Senjata, Perlombaan Senjata Siber, Senjata siber

Abstract *– Cyber war, where the realm of information technology, defense, diplomacy, and domestic politics blended on a computer script. The stability of global security and also the stability of domestic security become the prime target of the sophistication of cyber technology. This is not a new phenomenon in the defense science nor international relations science, the dynamics and synergy between technology, defense, diplomacy, and domestic politics, which often called by Revolution in Military Affairs, yet, cyber is the one which provides a new frontier for those synergy to grows faster and more flexible. There are always a patterns of arms race in each era of relations between technology, defense, diplomacy, and domestic politics. Questions about is this patterns applicable in cyber space and its invisible weapons or not? By using Qualitative methods, and Case Study as design, the cyber arms race between United States and China serve as the first researched case. The research result that counted using Richardson Model of Arms Race shows there is a cyber-arms race that is happening between US and China.*

Key words: *Cyber war, Logical weapon, Arms Race, Cyber Arms Race, Cyber Weapon*

[1] Program Studi Peperangan Asimetris, Fakultas Strategi Pertahanan, Universitas Pertahanan
[2] Program Studi Peperangan Asimetris, Fakultas Strategi Pertahanan, Universitas Pertahanan
[3] Lembaga Pengembangan Pendidikan dan Penjaminan Mutu, Universitas Pertahanan

Pendahuluan

Perang siber atau yang sering dikenal dengan *Cyberwar*, memberikan corak khas pada perkembangan ilmu pertahanan dengan memperlihatkan pentingnya peran informasi sebagai dasar pembentukan sebuah kebijakan luar dan dalam negeri, serta strategi perang; hal ini menjadi perihal yang mendesak saat negara dan seluruh komponennya mulai tergantung pada ruang siber.

Pertahanan negara dalam kondisi perang siber akan dihadapkan pada ancaman dari penggunaan senjata yang tak berwujud *(intangible)* yang disebut sebagai senjata siber *(cyber weapon)*. Definisi dari senjata siber ini masih menjadi perdebatan diantara para pakar siber. Beberapa pakar menggunakan pendekatan legal [4], beberapa pakar menggunakan pendekatan dampak[5], dan lainnya menggunakan pendekatan bentuk [6], maupun prilaku [7] dari senjata siber. Artikel ini mencoba melihat senjata siber dari fungsinya sebagai alat yang dapat membentuk *arms race* yang unik, dimana perlombaan senjata sering kali memberikan "anggapan" kepada musuh secara asimetris.

Pada umumnya, teknik perang asimetris dipandang sebagai sebuah teknik atau perang di luar mainstream, jenis perang ini sering kali di implementasikan oleh aktor non-negara karena jenis perang ini tidak diatur seperti halnya perang konvensional, serta memiliki tujuan utama untuk memelihara *"the effect of shock"* [8]. Sama seperti teknik serangan-serangan asimetris yang selalu baru, serangan siber juga tidak dapat diulang[9] karena pihak lawan akan selalu membuat 'anti' untuk menghadapi teknik serangan yang sama.

Setiap pemangku kepentingan *(stakeholder)* di dalam dunia siber memiliki peran sebagai produsen dan konsumen atau sebagai pihak penyerang dan pihak yang diserang. Penelitian ini berfokus pada aktor negara yang berada di dalam kondisi security dilemma dengan melihat kebijakan-kebijakan yang mengarah pada pola struggle for survival

[4] Robert S. Dewar, *Cyberweapons: Capability, Intent, and Context in Cyberdefense*, (Zurich: Center for Security Studies, 2017)

[5] Thomas Rid & Peter McBurney, "Cyber Weapons", *The RUSI Journal*, vol. 157, no. 1, 2012, hlm 6-13

[6] Lucas Kello, *The Virtual Weapon and International Order*, (New Haven: Yale University Press, 2017)

[7] Martin C. Libicki, *Cyberdetterence and Cyberwar*, (California: RAND Corporation, 2009)

[8] Rod Thornton, *Asymmetric Warfare: Threat and Response in the Twenty First Century*, (Cambridge: Polity Press, 2007)

[9] Lich J. Janczewski, & Andrew M. Colarik, *Cyber Warfare and Cyber Terrorism*, (Pennsylvania & London: IGI Global, 2008)

melalui pengakumulasian senjata siber, dengan tujuan membentuk poros kekuatan baru pada tatanan politik global[10]. Pentingnya poros-poros baru ini berdasar pada hipotesis: "saat sebuah negara mememiliki peran utama pada sebuah tatanan politikan global, maka negara tersebut memiliki modal yang lebih besar dalam prsoes negosiasi kepentingan nasional".

Pembentukan pola poros di atas tidak terlepas dari dominasi jenis kekuatan baru. Seperti halnya yang terjadi pada sejarah dunia yang dimasanya telah membentuk pola-pola hegemoni yang serupa; pada pra-Perang Dunia I terdapat perlombaan akumulasi alutsista[11]; pra-Perang Dunia II terdapat akumulasi industri dan angkatan laut[12]; selanjutnya terdapat perlombaan akumulasi senjata nuklir pada masa Perang Dingin[13]; dan terdapat pola perlombaan akumulasi aliansi pada pasca-Perang Dingin[14].

Setiap masa memiliki pola akumulasi yang dilakukan oleh aktor negara untuk menghadapi ancaman di masanya, sekarang, adalah masa dimana akumulasi kekuatan ada pada ranah siber. Tidak terlepas dari akumulasi senjata di masa lampau, perpindahan akumulasi dari senjata tangible ke senjata intangible didasarkan pada fakta bahwa perkembangan senjata yang sering kali dikenal dengan Revolutionary in Military Affairs (RMA)[15] telah masuk pada ranah teknologi informasi dan komunikasi (TIK).

Perkembangan RMA selanjutnya dapat diaplikasikan pada masa yang disebut dengan era perang siber. Beberapa pakar telah memperingatkan mengenai bahaya senjata siber yang dapat memiliki dampak kerusakan seluas senjata nuklir meski tidak memiliki daya penghancur seperti senjata nuklir[16,17,18]; terlebih lagi potensi ancaman senjata nuklir yang terkontrol melalui teknologi komputer dalam menentukan target[19]

[10] Hans J. Morgenthau, & Kenneth W. Thompson, *Politics Among Nations: The Struggle for Power and Peace*, Terj: S. Maimoen, A. M. Fatwan, & C. Sudrajat, (Jakarta: Yayasan Pustaka Obor Indonesia, 2010)

[11] Vannevar Bush, *Modern Arms and Free Men*, (New York: Simon and Schuster, Inc., 1949)

[12] Joseph Maiolo, Cry Havoc: How the Arms Race Drove the World to War, 1931-1941, (New York: Basic Book, 2010)

[13] David E. Hoffman, *The Dead Hand: The Untold Story of the Cold War Arms Race and Its Dangerous Legacy*, (New York: Anchor Books, 2009)

[14] Kjell Goldmann, Ulf Hannerz, & Charles Westin, *Nationalism and Internationalism in the Post-Cold War Era*, (London: Routledge, 2000)

[15] *Op. Cit.*, Thornton (2007)

[16] *Op. Cit.*, Janczewski & Colarik (2008)

[17] *Op.Cit.,* Dewar (2017)

[18] *Op.Cit.,* Libicki (2009)

[19] Henry D. Sokolski (*Ed.*), *The Next Arms Race*, (Pennsylvania: Strategic Studies Institute Book, 2012)

serta proses peluncuruannya[20]. Potensi-potensi ancaman ini telah perlahan namun memungkinkan untuk menggeser agenda pengamanan senjata nuklir kepada agenda pengamanan sistem komputer yang menaungi senjata-senjata tangible dari ancaman-ancaman senjata siber.

Dengan adanya pola yang terulang di masa-masa konflik sejarah dunia, maka, menggunakan pola-pola konflik dan perlombaan senjata terdahulu yang diterapkan pada konflik masa kini adalah sebuah pendekatan yang tepat untuk mencari titik yang dapat dimanfaatkan oleh aktor negara.

Fokus penelitian ini ada pada perlombaan senjata siber, yang terbatas pada jenis *logical weapon* yang sedang terjadi diantara Amerika dan China antara tahun 2013-2018. Penelitian ini mencoba menggambarkan istilah *cyber arms-race* yang sudah banyak digaungkan, namun belum ada yang menggambarkan pola dinamika dan aksi-reaksi pada perlombaan senjata siber.

Pemilihan negara Amerika dan China pada artikel ini berdasar pada fakta bahwa kedua negara yang seing disorot oleh media, yang selanjutnya menjadi sumber dokumentasi dari artikel ini.

Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah metode kualitatif yang dijelaskan oleh sugiyono sebagai metode yang artistik, karena proses penelitian lebih bersifat seni (kurang terpola), dan disebut sebagai metode yang menggunakan pendekatan interprestasi terhadap data yang ditemukan pada proses penelitian[21].

Metode kualitatif disampaikan oleh Creswell bahwa penelitian kualitatif adalah sebuah proses eksplorasi dan memahami arti dari seorang individual atau kelompok yang menunjukkan atau memperlihatkan sebuah pola persoalaan yang dihadapi masyarakat luas[22].

Penelitian pada tesis ini menggunakan metode kualitatif karena penulis meneliti pola aksi reaksi, saling menyerang antara negara-negara adikuasa (superpower) pada bidang siber. yang selanjutnya mengkerucut pada pembuktian bahwa terdapat ancaman ditengah aks-reaksi antara negara-negara yang saling bertikai pada

[20] *Op. Cit.,* Janczewski & Colarik (2008)
[21] Sugiyono, *Metode Penelitian & Pengembangan: Research and Development*, (Bandung: Alfabeta, 2015)
[22] *Ibid.*

ranah siber, dalam hal ini terbatas pada hubungan aksi-reaksi antara Amerika Serikat dan China.

Langkah-langkah yang dilakukan pada penelitian ini adalah mengumpulkan data serangan siber diantara kedua negara berbentuk data sekunder dari berbagai sumber tertulis buku, koleksi e-book, maupun data-data daring yang mendasari penelitian ini sebagai studi pustaka. Data-data yang dikumpulkan berdasar pada faktor-faktor yang digunakan dalam rumus dasar *Richardson Basic Model of Arms Race*[23], yaitu Waktu (t), Sektor (k), Hubungan Internasional (y), Anggaran Militer (a), Hutang Nasional (x), Akumulasi Senjata (h), yang faktor-faktor ini dirumuskan dalam sebuah formula:

X(t) = yk-ax+h

Hasil dari analisa setiap faktor akan menghasilkan sebuah nilai yang selanjutnya dibentuk dalam sebuah grafik, kartesius. Peneltian ini terbatas pada aplikasi teori *Richardson model,* dalam menganalisa perlombaan senjata siber Amerika dan China, dengan batasan waktu 2014-2018.

Selanjutnya, data yang telah dikumpulkan akan melalui tiga tahapan proses analisa, pertama, Reduksi Data, yang berguna untuk merangkum hal-hal pokok, memfokuskan pada hal-hal yang penting, dicari tema, dan polanya, dengan demikian data yang telah direduksi akan memberikan gambaran yang lebih jelas dan mempermudah peneliti untuk melakukan pengumpulan data selanjutnya, dan mencarinya bila diperlukan. Kedua, Penyajian Data, yang dapat dilakukan dalam bentuk tabel, grafik, *pie chart, pictogram*, dan sejenisnya. Melalui penyajian data tersebut, maka data terorganisasikan, tersususn dalam pola hubungan, sehingga akan semakin mudah dipahami. Ketiga, Pengambilan Kesimpulan dalam penelitian kualitatif mungkin dapat menjawab rumusan masalah maupun tidak dapat menjawab rumusan masalah, dalam penelitian ini, rumusan masalah dapat dijawab dan dibentuk sesuai dengan langkah-langkah penelitian yang telah ditentukan oleh peneliti.

Hasil dan Pembahasan

Data Senjata Siber Amerika dan China

[23] Craig Etcheson, *Arms Race Theory: Strategy and Structure of Behavior*, (Connecticut: Greenwood Press, 1989)

Aksi-reaksi serangan siber yang dikumpulan dalam penelitian ini dibatasi pada serangan siber yang dilakukan oleh dua instansi siber di dua negara, yaitu USCYBERCOM Amerika Serikat, dan Unit 61398 milik militer China.

Selanjutnya, dijelaskan gambaran umum USCYBERCOM dan Unit 61398. Pertama, Instansi Siber di Amerika secara garis besar dapat digambarkan seperti pada gambar 1 Instansi siber dalam ruang lingkup militer berada dibawah komando *United States Strategic Command* (USSTRATCOM) yang berada tepat dibawah Menteri Pertahanan Amerika Serikat *(Secretary of Defense)*[24].

USCYBERCOM memberikan perintah kepada empat kekuatan siber di empat matra; *Army Cyber Command* (ARCYBER), *Fleet Cyber Command* (FLTCYBER), *Marine Corps Forces Cyberspace Command* (MARFORCYBER), dan *Air Force Cyber* (AFCYBER)[25]. Fungsi dari USCYBERCOM juga memberikan dukungan terhadap tiga badan lainnya, yaitu *United States Army Intelligence and Security Command* (INSCOM), *Naval Network Warfare Command* (NNWC) ketiga badan tersebut dijelaskan lebih lanjut didalam *United States Code: Title 50 War and National Defense* [26,27].

Kedua, Adapun instansi siber di china secara garis besar dapat digambarkan pada Gambar 2, yang menjadi fokus dari bagan tersebut ada pada Unit 61398, yang menjadi ujung tombak (yang sering disebutkan dan dianalisa oleh media massa maupun pusat penelitian siber Amerika Serikat). Unit 61398 diberi istilah *Advance Presistance Threat 1* (APT 1) oleh Fire Eye, sebuah perusahaan keamaan siber asal Amerika Serikat, yang juga membongkar bagan organisasi Unit 61398 yang bersumber dari berbagai sumber pustaka. Hasil dari laporan analisa Fire Eye mengenai APT 1[28] menunjukkan bahwa Unit 61398 berada dibawah Pusat Komisi Militer *(Central Militer Commission).*

Sebelum pembahasan mengenai hubungan dinamika perkembangan logical weapon di dua negara, sebagai

[24] Noah Shachtman, "Dot-Mil Cyber Security Spending: Now Extra FUBAR", dalam https://www.wired.com/2011/04/dot-mil-cyber-security-spending-now-extra-fubar/, 04 Januari 2011, diakses pada 2019

[25] U.S. Cyber Command, "U.S. Cyber Command History", dalam https://www.cybercom.mil/About/History/, 2019, diakses pada 2019

[26] *Op. Cit.,* N. Shachtman (2011)

[27] United States Code, "Title 50-War and National Defense", dalam https://uscode.house.gov/, 2015, diakses pada 2019

[28] Mediant Report, *APT 1: Exposing One of China's Cyber Espionage Units,* (Fire Eye, 2014)

gambaran umum kekuatan siber di masing-masing negara, Peneliti mengadopsi gambaran umum kekuatan siber yang dinilai melalui Global Cybersecurity Index 2018 (GCI) [29] dan pada buku Cyber War[30] mengenai cyber power yang dianalisa oleh Richard A. Clarke. Kedua sumber dapat memberikan memberikan gambaran umum dan perkembangan kekuatan siber China dan Amerika Serikat dari dua metodelogi, kualitatif yang digambarkan pada buku Cyber War, dan kuantitatif yang disebutkan pada GCI 2018.

Pertama, Amerika Serikat, Kekuatan Siber Amerika Serikat, diproyeksi oleh GCI dengan nilai 0.926, yang menduduki peringkat 1 pada regional, dan peringkat kedua pada peringkat internasional [31] . Nilai yang diberikan oleh GCI berdasar pada lima pendekatan, Legal, Technical, Organizational, Capacity Building, dan Cooperation, dengan nilai maksimal 1. Nilai tersebut meningkat 0.007 berbanding dengan tahun 2017 [32] . Terdapat peningkatan dan penurunan pada setiap sektor yang diteliti oleh GCI, pada tahun 2017 Amerika Serikat memiliki nilai sempurna pada perihal legal dan capacity building pada tahun 2018, Amerika serikat memiliki nilai sempurna pada legal dan Organizational. Disini dapat terlihat bagaimana Amerika Serikat "memupuk" kekuatan siber, dengan berfokus pada capacity building terlebih dahulu sebelum membentuk hubungan antar instansi domestik pada ranah siber. Hal ini berkorelasi dengan proyeksi "kekurangan" kekuatan siber yang digambarkan oleh Clarke.

Bentuk yang lebih spesifik dari Cyber Power disebutkan oleh Clarke sebagai Cyber war strength yang dapat dilihat dari tiga kempuan; Cyber Offense, Cyber Defense, dan Cyber Dependence. Cyber Offense dapat diartikan sebagai kemampuan dalam menyerang negara lain [33] , Cyber Defense diartikan sebagai kemampuan sebuah negara dalam melakukan penanggulangan saat negara berada ditengah serangan [34] . Cyber Dependence dapat diartikan sebagai tingkat ketergantungan dan koneksi

[29] International Telecommunication Union, *Global Cybersecurity Index (GCI) 2018.* (Geneva: Place des Nations, 2019)

[30] Richard A. Clarke & Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About it?* (New York: Harper Collins Publisher, 2012)

[31] *Op. Cit.,* International Telecommunication Union (2018)

[32] International Telecommunication Union, *Global Cybersecurity Index (GCI) 2017.* (Geneva: Place des Nations, 2017)

[33] *Op. Cit., Richard A. Clarke (2012)*

[34] *Ibid.*

(wired) pada sebuah negara teruma pemerintah[35]

Penilaian yang diberikan kepada Amerika Serikat dalam penilaian Cyber war strength adalah 11 – nilai terendah diantara Rusia, China, Iran, dan Korea Utara, dengan nilai pada Cyber Offense tertinggi diantara negara-negara yang disebutkan, yaitu 8. Cyber Dependence Amerika Serikat adalah 2, dengan argumen bahwa infrastruktur publik dan swasta telah sangat tergantung dengan internet, dengan demikian, nilainya semakin kecil, karena membuka peluang untuk menjadi cyber vulnerability. Cyber Defense Amerika Serikat dinilai 1 yang disertai dengan argumen bahwa Amerika Serikat tidak memiliki rencana maupun kapisatas untuk dapat memutuskan *(disconnected)* koneksi internet bersekala nasional secara sepihak, hal ini dikarenakan koneksi internet di Amerika Serikat dimiliki dan dijalankan oleh pihak-pihak swasta[36].

Kedua, cyber power China jika dilihat melalui laporan CGI oleh International Telecommunication Union (ITU) pada tahun 2019 memiliki nilai 0.828, yang cukup jauh dibandingkan dengan Amerika Serikat. China ditetapkan pada peringkat ke-6 pada ranah regional Asia-Pasifik, dan peringkat ke-27 pada tatanan global [37], dengan peningkatan 0.204, berbanding dengan nilai pada tahun 2017 0.624 [38]. Pada laporan CGI 2017 maupun 2018, tidak dijabarkan mengenai nilai sertiap sektor, seperti Amerika Serikat, namun, pada CGI 2017, disebutkan bahwa China berada pada status *"Maturing"* mengenai Cyber Security, yang tentu tidak dapat langsung mengambarkan bagaimana posisi China pada perihal kemampuan dan kebijkan mengenai *Computer Network Operation*.

Selanjutnya, dari segi *Cyber war strength*, China mendapatkan nilai akhir yang lebih tinggi dari Amerika Serikat, yaitu 15, dengan nilai Cyber Offense yang lebih rendah dibandingkan dengan Amerika Serikat, yaitu 5, nilai Cyber Dependence 4 yaitu 2 skor lebih tinggi dibanding Amerika Serikat, hal ini dikarenakan penggunaan internet masih belum merata di China, dan pemerintah yang memiliki sistem yang berbeda dari sistem pada umumnya, seperti yang

[35] *Ibid.*
[36] *Ibid.*
[37] *Op. Cit.,* International Telecommunication Union (2018)
[38] *Op. Cit.,* International Telecommunication Union (2017)

dinamakan dengan Kylin[39]. Nilai untuk *Cyber Defense* China adalah 6 – nilai tertinggi kedua setelah Korea Utara, dengan argumen bahwa tingginya *Cyber Defense* China adalah kemampuan dan rencananya untuk dapat memutuskan koneksi internet berskala nasional dari internet global. Amerika dan China adalah dua negara yang dibandingkan secara konstan dalam pembahasan tiga faktor *Cyber Offense, Cyber Dependence*, dan *Cyber Defense*[40].

Penjelasan dua negara diatas yang dipandang melalui dua perspektif – GCI dan *Cyber War Strength*, menghasilkan dua hasil yang berbeda antara hubungan maupun peringkat, hal ini tentu memberikan perspektif lain terhadap hipotesis yang telah ditetapkan pada tesis ini untuk menggambarkan perbedaan antara hasil CGI dan *Cyber War Stregth*, dengan pandangan Peneliti yang melihat Amerika dan China memiliki kekuatan siber terutama logical weapon yang tengah berkembang secara dinamis, namun, terdapat faktor yang harus digaris bawah pada nilai yang diberikan oleh GCI, dimana nilai tersebut berdasar dari lima faktor yang telah disebutkan sebelumnya, dengan tidak mewakili senjata siber yang telah digunakan oleh kedua negara hingga terbentuk perlombaan senjata yang selanjutnya akan dibahas.

Penelitian ini mencoba untuk memberikan independent perspective, dengan melihat dinamika aksi-reaksi penggunaan *logical weapon* diantara Amerika dan China dari tahun 2014-2018 yang diolah melalui *Richardson Basic Model of Arms Race* ditambahkan dengan pembahasan mengenai catatan-catatan mengenai hubungan kedua negara dengan negara lain, maupun politik dalam negeri yang dapat mempengaruhi perkembangan kekuatan siber kedua negara pada tesis ini, dengan tetap mempertimbangkan pandangan GCI 2017-2018 dan Clarke dalam menentukan hasil akhir.

Penelitian ini mencoba untuk memberikan *independent perspective*, dengan melihat dinamika aksi-reaksi penggunaan logical weapon diantara Amerika dan China dari tahun 2014-2018 yang diolah melalui *Richardson Basic Model of Arms Race* ditambahkan dengan pembahasan mengenai catatan-catatan mengenai hubungan kedua negara dengan negara lain, maupun politik dalam

[39] *Op. Cit., Richard A. Clarke (2012)*

[40] *Ibid.*

negeri yang dapat mempengaruhi perkembangan kekuatan siber kedua negara pada penelitian ini.

Seperti yang telah disebutkan sebelumnya, bahwa pencarian data terbatas pada lima faktor (y, k, a, x, h), yang terbatas pada tahun (t). Simbol (y) mewakili prilaku (attitudes) pada ranah siber antara Amerika kepada China dan juga sebaliknya, dengan melihat serangan besar (major attak) yang dikurangi dengan nilai hubungan internasional e.g. perjanjian internasional mengenai kerjasama dibidang siber. Simbol (k) mewakili jumlah sektor yang menjadi serangan siber pada satu serangan, klasifikasi sektor terbagi menjadi 9 sektor yaitu: Pemerintah, Infrastruktur, Sistem Militer, Obyek Fisik, Gedung, Masyarakat, Perumahan, Kendaraan, dan Robot. Simbol (a) mewakili anggaran militer negara pada kurun waktu tertentu yang dibagi menjadi nilai satuan dengan membagi setiap anggaran militer per-seratus miliar (10^{11}). Simbol (x) mewakili hutang internasional yang dimiliki oleh setiap negara pada kurun waktu tertentu, yang diambil persentase (%) berbanding dengan Gross Domestic Product (GDP). Simbol (h) mewakili jenis senjata dan nama senjata siber yang digunakan dalam penyerangan yang membentuk nilai (y)[41].

Secara berurutan, dimulai pada tahun 2014-2018, diolah dengan membagi hasil studi pustaka kepada tabel perhitungan per-tahun, maka, didapatkan nilai perlombaan senjata Amerika (Lihat Tabel 2) dan China (Lihat Tabel 3) yang mana nilai dari setiap tahun di kedua negara didapatkan menggunakan rumus $X(t) = yk-ax+h$**.** Data mengenai Anggaran Militer Amerika dan China didapatkan melalui website world bank [42] . Data mengenai Growth Domestic Product Amerika dan China didapatkan melalui website world bank [43]. Sedangkan, nilai hutang luar negeri Amerika [44] dan China [45] didaptkan melalui website Statistia. Data mengenai kerjasama siber diantara kedua negara diambil dari

[41] *Op. Cit.,* Craig Etcheson (1989)

[42] World Bank Group, "Military expenditure (current USD) - China, United States", dalam https://data.worldbank.org/indicator/MS.MIL.XPND.CD?end=2018&locations=CN-US&start=2014, 2019, diakses pada 2019

[43] World Bank Group, "GDP (current US$) - China, United States", dalam https://data.worldbank.org/indicator/NY.GDP.MKTP.CD, 2019, diakses pada 2019

[44] Erin Duffin, "Public debt of the United States from 1990 to 2019 (in Billion Dollars)", dalam https://www.statista.com/statistics/187867/public-debt-of-the-united-states-since-1990/, November 8 2019, diakses pada 2019

[45] H. Plecher, "China: National debt from 2014 to 2024 (in billion U.S. dollars)", dalam https://www.statista.com/statistics/531423/national-debt-of-china/, 3 Desember 2019, diakses pada 2019

website resmi pemerintah Amerika Serikat, kerja sama siber di antara kedua negara terjadi dua kali pada tahun 2015, dan 2017 yang dinamakan sebagai *Cyber Agreement*[46] & *Cybersecurity Dialogue*[47].

Data-data serangan siber dengan masing-masing nama senjata siber, dapat menunjukkan jumlah senjata siber minimum di masing-masing negara, data-data tersebut dirangkum pada Tabel 1 yang terbagi pada kolom Nomor, Tahun, Bulan, *Attack* (Negara yang menyerang)/ *Target* (Negara yang diserang), Nama Malware, dan Sektor Serangan.

Tabel 1. Logical Weapon yang digunakan dalam Proyeksi Perlombaan Senjata Siber Amerika dan China Tahun 2014-2018

#	Thn.	Bln.	*Atk/Trg*	Malware	Sek.
1	2014	01	CH/US	POSRAM	Keu.
2	2014	01	US/CH	Preemptive Cyber Strike	Gov.
3	2014	02	US/CH	Massive Crash	DNS
4	2014	02	CH /US	China OS	Gov.
5	2014	03	US/ CH	Huawei Infiltration	Tek.
6	2014	04	US/ CH	Panda Burning	Pub.
7	2014	04	CH /US	Internet Power	Gov.
8	2014	04	CH /US	Flash Exploit IE 9~11	Pub.
9	2014	05	US/CH	Netizen Spy	Gov.
10	2014	05	CH /US	Cyber Espionage	Pub.
11	2014	06	US/ CH	Plan X	Keu.
12	2014	06	US/ CH	Flame Boost, Flask, Jimmy, Munch, Snack, Spotter, Transport,	Gov.

[46] The White House, "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference", dalam https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint, 25 September 2015, diakses pada 2019

[47] Department of Justice Office of Public Affairs, "First U.S.-China Law Enforcement and Cybersecurity Dialogue", dalam https://www.justice.gov/opa/pr/first-us-china-law-enforcement-and-cybersecurity-dialogue, 6 Oktober 2017, diakses pada 2019

				Euphoria, Headache	
13	2014	09	CH /US	Threebyte	Gov.
14	2014	11	CH /US	Operation Double Tap	Gov.
15	2015	01	CH /US	Cyber Hacking	Mil.
16	2015	02	CH /US	Anthem cybersecurity breach	Kes.
17	2015	02	US/ CH	Lizard Squad	Tek.
18	2015	02	US/ CH	Intelligence Integration Center	Mil.
19	2015	04	CH /US	APT 30	Tek.
20	2015	04	CH /US	The Great Cannon	Tek.
21	2015	04	US/ CH	Quantum	Tek.
22	2015	04	US/ CH	Chinese Consulate data bank	Gov.
23	2015	04	US/ CH	freeze assets and bar other financial transactions	Keu.
24	2015	04	US/ CH	DoD 2nd Cybersecurity Strategy	Mil.
25	2015	04	US/ CH	Western Hostile Forces	Pub.
26	2015	05	CH /US	Avago/ Skyworks	Keu.
27	2015	05	CH /US	Blackcoffee	Gov.
28	2015	06	CH /US	Adobe Flash Zero Day	Gov.
29	2015	06	US/ CH	US-Nato Cyber Centre	Gov.
30	2015	07	CH /US	Office of Personnel Management Breach (SF 86)	Gov.
31	2015	07	CH /US	Ghost RAT (Remote Access Trojan)	Gov.
32	2015	09	US/ CH	Xcode (iOS) Weakness abuse	Tek.

33	2016	08	US/ CH	Straider (RemSec)	Gov.
34	2016	05	CH /US	US Presidential Campaigns Attack	Gov.
35	2016	04	US/ CH	CTB-Locker	Pub.
36	2016	04	CH /US	Sogu	Gov.
37	2016	10	CH /US	Dyn Attack	Tek.
38	2017	03	US/ CH	Vault7	Gov.
39	2017	05	US/ CH	Wannacry	Pub.
40	2017	04	CH /US	Operation Cloud Hopper	Tek.
41	2017	04	CH /US	Haymaker	Gov.
42	2017	04	CH /US	Bug Juice	Gov.
43	2017	04	CH /US	Snugride	Gov.
44	2017	04	CH /US	Quasar RAT	Gov.
45	2017	06	US/ CH	Eternal blue	Pub.
46	2017	06	US/ CH	Eternal Romance	Pub.
47	2017	12	CH /US	Fake LinkedIn	Gov.
48	2018	01	CH /US	Mimic DNS	Gov.
49	2018	04	CH /US	Report 301	Keu.
50	2018	05	CH /US	Cross Walk (APT 41)	Pub.
51	2018	09	CH /US	APT10 / Stone Panda / Red Apollo	Pub.
52	2018	11	CH /US	Marriot Hacking	Pub.

Sumber: Diolah oleh Peneliti (2019)

Aplikasi *Richardson Model of Arms Race*

Pada tahun 2014 – yang berlaku sebagai nilai (t), Amerika memiliki nilai 35.80, dan China 27.28. Amerika mendapatkan nilai (y) 7, berdasar pada 7 *major cyber-attack* terhadap China, dan 0 kerjasama siber diantara Amerika dan China. Nilai (k) adalah 5, dengan 7 serangan yang ditujukan kepada 5 sektor. Total anggaran militer Amerika pada tahun 2014 (a) adalah 6.09914. Selanjutnya, nilai (x) mencapai 101.72%, dengan setiap serangan menggunakan 7 *logical weapon* (h) berbeda. Sedangan pada sisi China, mendapatkan nilai (y) 7, dengan 7 *major cyber-attack* terhadap Amerika, dan 0 kerjasama siber pada tahun 2014. Nilai (k) adalah 3, dengan 7

serangan yang ditujukan kepada 3 sektor. Total anggaran militer China pada tahun 2014 (a) adalah 2.00772. Dikalikan dengan nilai (x) 35.85%. didukung dengan 7 logical weapon berbeda disetiap serangannya.

Pada tahun 2015, Amerika memiliki nilai 43.06, dan China 48.19. Amerika mendapatkan nilai (y) 8, berdasar pada 9 *major cyber-attack* terhadap China, dan 1 kerjasama siber diantara Amerika dan China. Nilai (k) adalah 5, dengan 7 serangan yang ditujukan kepada 5 sektor. Total anggaran militer Amerika pada tahun ini (a) adalah 5.96105. Selanjutnya, nilai (x) mencapai 99.62%, dengan setiap serangan menggunakan 9 *logical weapon* (h). Sedangan pada sisi China, mendapatkan nilai (y) 8, dengan 9 *major cyber-attack* terhadap Amerika, dan 1 kerjasama siber pada tahun 2015. Nilai (k) adalah 5, dengan 7 serangan yang ditujukan kepada 5 sektor. Total anggaran militer China pada tahun 2015 (a) adalah 2.14093. Dikalikan dengan nilai (x) 37.75%. didukung dengan 9 logical weapon (h) berbeda disetiap serangannya.

Pada tahun 2016, Amerika memiliki nilai -0.28, dan China 8.07. Amerika mendapatkan nilai (y) 2, berdasar pada 2 *major cyber-attack* terhadap China, dan 0 kerjasama siber diantara Amerika dan China. Nilai (k) adalah 2, dengan 2 serangan yang ditujukan kepada 2 sektor. Total anggaran militer Amerika pada tahun ini (a) adalah 6.00106. Selanjutnya, nilai (x) mencapai 104.63%, dengan setiap serangan menggunakan 2 *logical weapon* (h). China, mendapatkan nilai (y) 3, dengan 3 *major cyber-attack* terhadap Amerika, dan 0 kerjasama siber pada tahun 2016. Nilai (k) adalah 2, dengan 3 serangan yang ditujukan kepada 2 sektor. Total anggaran militer China pada tahun 2016 (a) adalah 2.16031. Dikalikan dengan nilai (x) 42.84%. didukung dengan 3 logical weapon (h) berbeda disetiap serangannya.

Pada tahun 2017, Amerika memiliki nilai 3.71, dan China 14.96. Amerika mendapatkan nilai (y) 3, berdasar pada 4 *major cyber-attack* terhadap China, dan 1 kerjasama siber diantara Amerika dan China. Nilai (k) adalah 2, dengan 4 serangan yang ditujukan kepada 2 sektor. Total anggaran militer Amerika pada tahun ini (a) adalah 6.05803. Selanjutnya, nilai (x) mencapai 103.90%, dengan setiap serangan menggunakan 4 *logical weapon* (h). Sedangan China, mendapatkan nilai (y) 5, dengan 6 *major cyber-attack* terhadap Amerika, dan 1 kerjasama siber pada tahun 2017. Nilai (k) adalah 2, dengan 6 serangan yang ditujukan

kepada 2 sektor. Total anggaran militer China pada tahun 2015 (a) adalah 2.27829, dikalikan dengan nilai (x) 45.50%. didukung dengan 6 logical weapon (h) berbeda disetiap serangannya.

Khusus pada tahun 2018, Peneliti menemui keterbatasan data pada serangan siber yang dilakukan oleh Amerika terhadap China, namun mendapat data serangan siber yang dilakukan China terhadap Amerika. Pada Gambar 4.3 di tahun 2018, Peneliti memberi simbol segitiga pada nilai Amerika yang menandakan keterbatasan Peneliti dalam mendapatkan data serangan pada tahun tersebut. Namun, Peneliti memutuskan untuk tetap memasukkan data yang telah dikumpulkan selama penelitian data sekunder sebagai gambaran proyeksi pergerakan nilai perlombaan *logical weapon,* terutama pada sisi China. Pada tahun 2018, Amerika memiliki nilai (tanpa serangan siber) -6.81, dan China 18.81. Amerika mendapatkan nilai (y, k, dan h) 0, berdasar pada keterbatasan Peneliti. Total anggaran militer Amerika pada tahun ini (a) adalah 6.48798. Selanjutnya, nilai (x) mencapai 104.99%, dengan setiap. Sedangan China, mendapatkan nilai (y) 5, dengan 5 *major cyber-attack* terhadap Amerika, dan 0 kerjasama siber pada tahun 2018. Nilai (k) adalah 3, dengan 5 serangan yang ditujukan kepada 3 sektor. Total anggaran militer China pada tahun 2018 (a) adalah 2.49997, dikalikan dengan nilai (x) 47.65%, dengan menggunakan 5 *logical weapon* (h) berbeda disetiap serangannya.

Istilah perlombaan senjata siber telah didengungkan secara konsep pada tahun 2012 [48] dan selanjutnya "potensi" perlombaan senjata siber Amerika dan China disebutkan pada thun 2013[49] Kedua pendekatan tersebut menggunakan pendekatan historis, dan pendekatan pola, yang menggambarkan *arms race*.

Tabel 2 Hasil Hitung Nilai Amerika dalam Perlombaan Senjata Melalui Rumus *Richardson Basic Model of Arms Race*

t	y	k	a	x	h	X(t)
2014	7	5	6.09	101.72%	7	35.80
2015	8	5	5.96	99.62%	9	43.06
2016	2	2	6.00	104.63%	2	-0.28
2017	3	2	6.05	103.90%	4	3.71
2018	n/a	n/a	6.48	104.99%	n/a	-6.81

Sumber: Diolah oleh Peneliti (2019)

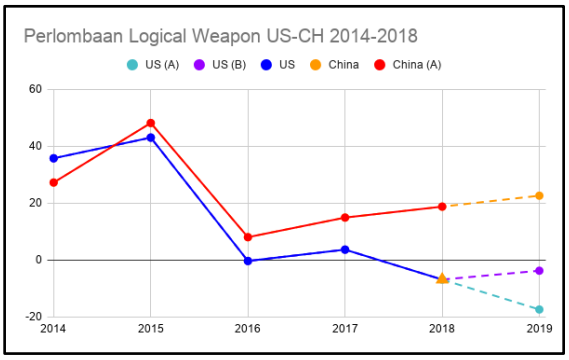
Tabel 3 Hasil Hitung Nilai China dalam Perlombaan Senjata Melalui Rumus *Richardson Basic Model of Arms Race*

[48] *Op. Cit.,* Sokolski (2012)

[49] Frank C. Zagare, *The Dynamics of Deterrence*, (Chicago: The University of Chicago Press, 1987)

t	y	k	a	x	h	X(t)
2014	7	3	2.01	35.85%	7	27.28
2015	8	5	2.14	37.75%	9	48.19
2016	3	2	2.16	42.84%	3	8.07
2017	5	2	2.27	45.50%	6	14.96
2018	5	3	2.49	47.65%	5	18.81

Sumber: Diolah oleh Peneliti (2019)



Gambar 3. Perlombaan *Logical Weapon* US-CH 2014-2018 dan Proyeksi Tahun 2019
Sumber: Diolah oleh Peneliti (2019)

Berawal dari hipotesa yang terdapat di beberapa sumber, penggunaan teori perlombaan senjata telah terbukti mampu memberikan gambaran umum mengenai kondisi perlombaan senjata siber, yang pada penelitian ini terbatas pada logical weapon.

Dengan berdasar pada tahun pembentukan teori Richardson Basic Model of Arms Race pada tahun 1922 dan kondisi dari bentuk perang yang tidak lagi membentuk poros seperti konflik-konflik internasional yang terjadi saat terbentuknya teori perlombaan senjata tersebut, maka, Peneliti memutuskan untuk menjelaskan lebih lanjut, mengenai faktor-faktor yang membentuk dan memicu perlombaan senjata yang terjadi antara Amerika dan China. Perlombaan senjata siber tidak dapat terjadi jika perkembangan teknologi tidak memberikan "fasilitas" untuk senjata-senjata siber dapat berkembang, dan hubungan dengan negara-negara lain pun memiliki pengaruh terhadap terjadinya perlombaan siber.

Perkembangan dinamika aksi-reaksi dan industri senjata pada ranah hubungan internasional dapat membentuk sebuah kondisi perang, pada penelitian ini, istilah perang siber adalah interaksi aksi-reaksi antara dua aktor dalam menggunakan Logical Weapon untuk mendapatkan kepentingan pada ranah siber, maupun mempertahankan sistem informasi dan komunikasi dari serangan siber. Clarke menekankan kepada seluruh negara untuk melihat cyber war lebih dalam lagi, pada tahun 2010, ia menyebutkan bahwa "*Cyber war is real. Cyber war happens at the speed of light. Cyber war is global. Cyber war skips the battlefield. Cyber war has begun*"[50].

[50] *Op. Cit.* Richard A. Clarke (2010)

Kesadaran atas kondisi ini diharapkan ada di tiap-tiap negara yang secara langsung maupun tidak terhubung dengan cyber war. Kondisi pada perang siber pada penelitian ini, digambarkan melalui hubungan Amerika dan China dalam berperan dalam perang siber.

Mengenai perang siber antara Amerika dan China telah terbentuk dari awal operasi Desert Storm Amerika serikat pada tahun 1990-1991[51]. Berawal pada pada penggunaan *Senior Shutter*, penggunaan teknologi navigasi terbaharukan, dan *smart bomb*, pada penyerangangan ke Basra, selanjutnya, perang teluk *(Gulf War)* memberikan "inspirasi" kepada para pemerintah dan perwira tinggi di China untuk menyebutya sebagai *Zhongda Biange (the great transformation)*, yang diikuti dengan penurunan investasi senjata militer yang disebut dengan *wangluohua atau networkization* yang memiliki tujuan untuk mencapai taraf *zhixinxiquan (information dominance)*. Proses perpindahan arah kebijakan militer memancing terbentuknya *Integrated Network Electronic Warfare* milik China untuk bersaing dengan *Netcentric Warfare* milik Amerika Serikat[52].

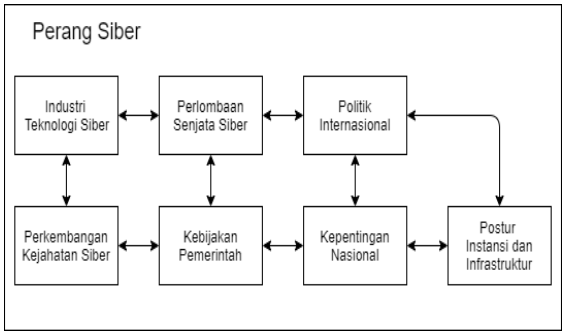
Dapat ditarik kesimpulan sementara bahwa perang siber terbentuk dan mempengaruhi tujuh sektor; industri teknologi siber, perlombaan senjata siber, kebijakan pemerintah, perkembangan kejahatan siber pada ranah domestik maupun global, kepentingan nasional, dinamika politik internasional, dan postur instansi dan badan pemerintah yang dapat digambarkan pada Gambar 4. Industri teknologi siber adalah "jantung" dari perkembangan teknologi senjata siber, yang mana dapat berupa industri legal maupun illegal, berbentuk perusahaan maupun perorangan. Perlombaan senjata siber terbentuk dengan adanya supply yang disediakan oleh industri teknologi siber yang juga dipengaruhi oleh pola kebijakan pemerintah.

Kebijakan Pemerintah mengenai teknologi siber dipengaruhi oleh perkembangan kejahatan siber yang terjadi pada ranah domestik dan global. Kepentingan Nasional yang ditentukan oleh Kebijakan Pemerintah secara langsung mempengaruhi pola pergerakan negara dalam politik internasional, yang dapat pila mempengaruhi bentuk postur instansi

[51] *Ibid.*

[52] *Ibid.*

dan infrastruktur nasional. Dinamika hubungan diantara kerujuh sektor dapat membentuk perang siber, dan kondisi dari perang siber dapat mempengaruhi ketujuh sektor.



Gambar 4. Hubungan Faktor-Faktor yang mempengaruhi dan yang dipengaruhi oleh Perang Siber
Sumber: Diolah oleh Peneliti (2019)

Kesinambungan antara beberapa sektor yang telah disebutkan dapat dilihat dari perkembangan Industri senjata dan keamanan siber yang terbukti meningkatkan supply dengan tingginya demands dari pengguna internet pada sebuah negara[53]. Industri-industri siber di beberapa negara meningkatkan kemampuan badan-badan negara untuk memberikan tingkat keamanan siber yang lebih tinggi, e.g. China yang membatasi supply produk TIK yang berasal dari luar negeri [54] , dimana peningkatan keamanan berdasar pada kondisi keamanan siber pada ranah domestik dan internasional yang dirasa pada tingkat tertentu (memburuk maupun membaik)[55]. Begitu juga kondisi keamanan internasional dan global yang memberikan input kepada pembentukan kepentingan nasional (pola maupun arah kebijakan) e.g. program Kementerian Pertahanan (*Department of Defense*) Amerika Serikat yang diberi nama "*Hack The Pentagon*" [56], maupun penyesuaian strategi siber China [57], yang selanjutnya dibawa ke ranah internasional dan domestik.

[53] Simons Kemp, "DIGITAL 2019: Essential Insights Into How People Around the World Use The Internet, Mobile Device, Social Media and E-Commerce", dalam https://www.slideshare.net/DataReportal/digital-2019-global-digital-overview-january-2019-v01?from_action=save, diakses pada 2019

[54] Han Qi, "Procurement list adjusted for security reasons", dalam: http://www.chinadaily.com.cn/cndy/2015-03/04/content_19711098.htm, 4 Maret 2015, diakses pada 2019

[55] B. Kendall, "Hybrid warfare: The new conflict between East and West", dalam https://www.bbc.com/news/world-europe-29903395, November 6 2014, diakses pada 2019

[56] U.S. Department of Defense, "Department of Defense Expands 'Hack the Pentagon' Crowdsourced Digital Defense Program", dalam https://www.defense.gov/Newsroom/Releases/Release/Article/1671231/department-of-defense-expands-hack-the-pentagon-crowdsourced-digital-defense-pr/, 24 Oktober 2018, diakses pada 2019

[57] Xin Hua, "China releases first strategy on cyberspace cooperation", dalam http://www.chinadaily.com.cn/china/2017-03/02/content_28403019.htm, 2 Maret 2017, diakses pada 2019

Kesimpulan dan Rekomendasi

Berdasar pada hasil penelitian ini, dapat ditarik sebuah kesimpulan bahwa pola perlombaan senjata konvensional dengan menggunakan rumus *Richardson Basic Model of Arms Race* dapat digunakan sebagai alat atau rumus dasar dalam menggambarkan dinamika perlombaan senjata yang tengah terjadi di era perang siber.

Teori *Richardson Model of Arms Race* yang selama ini digunakan dalam melihat pola perlombaan senjata pada perang-perang dunia pada masa lampau, kini terbukti dapat digunakan dalam menggambarkan pola perlombaan senjata siber yang bersifat *intangible.*

Pengaruh perlombaan senjata siber sangat dipengaruhi oleh perjanjian internasional antara kedua negara, yang mana mempengaruhi perkembangan industri teknologi, yang selanjutnya memberikan tekanan pada proses *RMA* di negara lain, dan pada akhirnya mempengaruhi stabilitas keamanan siber internasional.

Adapun rekomendasi kepada pemerintah Indonesia, terutama instansi siber nasional di Indonesia, harus dapat memperhatikan dan memberikan perhatian dengan melakukan persiapan lebih terhadap fakta-fakta perlombaan senjata siber yang mana perlombaan senjata sering kali berujung pada perang berskala besar.

Terhadap peneliti selanjutnya yang membahas mengenai perlombaan senjata siber, rekomendasi penelitian membahas mengenai Perlombaan Senjata Siber selain antara Amerika dan China, ditengah proses penelitian, penulis menemukan fakta-fakta bahwa Russia dan Israel dapat menjadi penelitian yang lebih menarik.

Daftar Pustaka

Buku

Bush, Vannevar, *Modern Arms and Free Men*, (New York: Simon and Schuster, Inc., 1949)

Clarke, Richard A. & Knake, Robert K., *Cyber War: The Next Threat to National Security and What to Do About it?,* (New York: Harper Collins Publisher, 2012)

Dewar, Robert S., *Cyberweapons: Capability, Intent, and Context in Cyberdefense*, (Zurich: Center for Security Studies, 2017)

Etcheson, Craig, *Arms Race Theory: Strategy and Structure of Behavior*, (Connecticut: Greenwood Press, 1989)

Goldmann, Kjell, Hannerz, Ulf, & Westin, Charles, *Nationalism and Internationalism in the Post-Cold War Era*, (London: Routledge, 2000)

Hoffman, David E., *The Dead Hand: The Untold Story of the Cold War Arms*

Race and Its Dangerous Legacy, (New York: Anchor Books, 2009)

International Telecommunication Union, *Global Cybersecurity Index (GCI) 2018*, (Geneva: Place des Nations, 2019)

International Telecommunication Union, *Global Cybersecurity Index (GCI) 2017*, (Geneva: Place des Nations, 2017)

Janczewski, Lech J., & Colarik, Andrew M., *Cyber Warfare and Cyber Terrorism*, (Pennsylvania & London: IGI Global, 2008)

Kello, Lucas, *The Virtual Weapon and International Order*, (New Haven: Yale University Press, 2017)

Libicki, Martin C., *Cyberdetterence and Cyberwar*, (California: RAND Corporation, 2009)

Maiolo, Joseph, *Cry Havoc: How the Arms Race Drove the World to War*, 1931-1941, (New York: Basic Book, 2010)

Mediant Report, *APT 1: Exposing One of China's Cyber Espionage Units*, (Fire Eye, 2014)

Morgenthau, Hans J. & Thompson, Kenneth W., *Politics Among Nations: The Struggle for Power and Peace*, Terj: S. Maimoen, A. M. Fatwan, & C. Sudrajat, (Jakarta: Yayasan Pustaka Obor Indonesia, 2010)

Sokolski, Harry H., *The Next Arms Race*, (Pennsylvania: Strategic Studies Institute Book, 2012)

Thornton, Rod, *Asymmetric Warfare: Threat and Response in the Twenty First Century*, (Cambridge: Polity Press, 2007)

Zagare, Frank C., *The Dynamics of Deterrence*, (Chicago: The University of Chicago Press, 1987)

Jurnal

Rid, Thomas & McBurney, Peter, "Cyber Weapons", *The RUSI Journal*, vol. 157, no. 1, 2012, hlm. 6-13

Website

Department of Justice Office of Public Affairs, "First U.S.-China Law Enforcement and Cybersecurity Dialogue", dalam: https://www.justice.gov/opa/pr/first-us-china-law-enforcement-and-cybersecurity-dialogue, 6 Oktober 2017, Diakses pada 2019

Duffin, Erin, "Public debt of the United States from 1990 to 2019 (in Billion Dollars)", dalam https://www.statista.com/statistics/187867/public-debt-of-the-united-states-since-1990/, November 8 2019, Diakses pada 2019

Kemp, Simons, "DIGITAL 2019: Essential Insights Into How People Around the World Use The Internet, Mobile Device, Social Media and E-Commerce", Kepios Pte.; We Are Social Ltd.; Hootsuite Inc, dalam https://www.slideshare.net/DataReportal/digital-2019-global-digital-overview-january-2019-v01?from_action=save, diakses pada 2019

Hua, Xin, "China releases first strategy on cyberspace cooperation", dalam http://www.chinadaily.com.cn/china/2017-03/02/content_28403019.htm, 2 Maret 2017, diakses pada 2019

Kendall, Bridget, "Hybrid warfare: The new conflict between East and West", dalam https://www.bbc.com/news/world-europe-29903395 November 6 2014, Diakses pada 2019

Plecher H., "China: National debt from 2014 to 2024 (in billion U.S. dollars)", dalam https://www.statista.com/statistics/531423/national-debt-of-china/, 3 Desember 2019, Diakses pada 2019

Qi, Han, "Procurement list adjusted for security reasons", dalam http://www.chinadaily.com.cn/cndy/2015-03/04/content_19711098.htm (4 Maret 2015) Diakses pada 2019

Shachtman N., "Dot-Mil Cyber Security Spending: Now Extra FUBAR" dalam https://www.wired.com/2011/04/dot-mil-cyber-security-spending-now-extra-fubar/, 04 Januari 2011, diakses pada 2019

The White House, "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference", dalam https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint, 25 September 2015, diakses pada 2019

U.S. Cyber Command, "U.S. Cyber Command History", dalam https://www.cybercom.mil/About/History/, 2019, diakses pada 2019

U.S. Department of Defense, "Department of Defense Expands 'Hack the Pentagon' Crowdsourced Digital Defense Program", dalam https://www.defense.gov/Newsroom/Releases/Release/Article/1671231/department-of-defense-expands-hack-the-pentagon-crowdsourced-digital-defense-pr/, 24 Oktober 2018, diakses pada 2019

United States Code, "Title 50-War and National Defense", dalam https://uscode.house.gov/, 2015, diakses pada 2019

World Bank Group, "Military expenditure (current USD) - China, United States", dalam https://data.worldbank.org/indicator/MS.MIL.XPND.CD?end=2018&locations=CN-US&start=2014, 2019, diakses pada 2019

World Bank Group, "GDP (current US$) - China, United States", dalam https://data.worldbank.org/indicator/NY.GDP.MKTP.CD, 2019, diakses pada 2019