DAMPAK PEMBANGUNAN *CYBERPOWER* TIONGKOK TERHADAP KEPENTINGAN AMERIKA SERIKAT

Dewi Triwahyuni
Program Studi Ilmu Hubungan Internasional, Universitas Komputer Indonesia, Bandung
Email : dewi.triwahyuni@email.unikom.ac.id

Yanyan Mochamad Yani
Program Studi Hubungan Internasional, Universitas Padjadjaran, Bandung
Email : yan2m@hotmail.com

Abstract

Chinese aggressiveness in the virtual world for the last 10 years is not an instantly made plan. The desire to modernize the military has been seen since 3 decades ago. Since 2006 China has released "The State Information Development Strategy" which contains the purpose of building the information of China until the year 2020 in the future. President Xi Jinping explicitly said that China should be a cyber-power country. The development of Chinese cyberpower led to the outrage of the United States following a number of Chinese behaviors in cyberspace that harmed the interests of the United States. This study aims to understand the purpose of China's cyber-power development and how it falls on the interests of the United States
.

Keywords: *Cyberpower, National Interest, China, United States of America*

Abstrak

Agresivitas Tiongkok dalam dunia maya kurang lebih 10 tahun terakhir ini bukan merupakan sebuah perencanan yang dibuat secara instan. Keinginan untuk melakukan modernisasi militer sudah terlihat sejak 3 dekade yang lalu. Sejak tahun 2006 Tiongkok telah merilis *"The State Information Development Strategy"* yang memuat tujuan pembangunan informasi Tiongkok sampai tahun 2020 kedepan. Presiden Xi Jinping secara tegas mengatakan bahwa Tiongkok harus menjadi negara *cyberpower*. Pembangunan *cyberpower* Tiongkok menimbulkan kegusaran Amerika Serikat menyusul sejumlah perilaku Tiongkok di dunia maya yang merugikan kepentingan Amerika Serikat. Studi ini bertujuan untuk memahami tujuan pembangunan *cyberpower* Tiongkok dan bagaimana hal tersebut berdampak pada kepentingan Amerika Serikat

Kata kunci: *Cyberpower, Kepentingan Nasional, Tiongkok, Amerika Serikat*

1. PENDAHULUAN

Perkembangan teknologi informasi dewasa ini mendorong pola-pola baru dalam interaksi hubungan internasional. Prilaku-perilaku internasional kini dilakukan tidak hanya secara aktual namun juga secara virtual. Dalam era teknologi informasi, khususnya perkembangan jaringan internet menambah luas sarana negara dalam mencapai kepentingan nasionalnya.

Kini interaksi yang dilakukan antar aktor hubungan internasional tidak hanya pada ruang darat, laut dan udara saja. Interaksi antar aktor juga memadati ruang maya (*cyberspace*) yang menjadi pilihan lain untuk mencapai kepentingan. Bertambahnya ruang interaksi ini sekaligus memperluas makna *power* dalam hubungan antar negara. Ukuran *power* dalam ruang darat, laut, udara lebih mudah untuk dicari standarisasinya, sebaliknya *cyberspace* mengaburkan standarisasi *power* tersebut. *Cyberspace* menjadi ruang sekaligus sarana baru dalam mencapai kepentingan yang kemudian dikenal dengan *cyberpower*.

Cybepower dapat dipahami sebagai seperangkat sumber daya yang dihubungkan dengan pembuatan, pengawasan, dan komunikasi elektronik, infrastruktur informasi berbasis komputer, jaringan, *software* dan kemampuan manusia. Jaringan yang dimaksud diatas tidak sebatas jaringan internet saja, tetapi juga Intranet, teknologi seluler, dan ruang berbasis komunikasi lainnya. (Nye, 2011 : 122-123).

Keamanan *cyberspace* semakin mendapat prioritas pemerintahan di dunia. Kekhawatiran terhadap dampak buruk yang dapat ditimbulkan oleh internet mendorong negara melakukan pengaturan yang lebih tepat terhadap penggunaan internet di negaranya. Dalam sebuah laporan disebutkan setidaknya ada 15 negara di dunia yang secara terang-terangan membatasi kebebasan penggunaan internet, yaitu: Tiongkok, Kuba, Korea Utara, Belarus, Myanmar, Mesir, Ethiopia, Iran, Arab Saudi, Suriah, Tunisia, Turkmenistan, Uzbeskistan dan Zimbabwe (Figliola et al, 2011: 4).

Prioritas terhadap permasalahan *cyber* ini sangat dibutuhkan oleh AS jika melihat maraknya serangan-serangan *cyber* yang dialamatkan kepada AS satu dekade terakhir. White House atau Gedung Putih tempat presiden AS bekerja dikabarkan mendapat serangan *cyber* hampir setiap hari. Dari hasil analisis AS menyimpulkan bahwa pelaku serangan tersebut ada yang berasal dari individual dan juga dari pemerintah yang diduga dilakukan oleh beberapa negara seperti: Rusia, Tiongkok, Korea Utara dan Iran (Jackson, dalam www.usatoday.com. Diakses 10 April 2015). Kenyataan ini tentu

saja membawa masalah baru dalam hubungan AS terhadap negara-negara yang diduga oleh AS melakukan serangan *cyber* terhadap institusi privat maupun institusi publik milik AS. Dalam catatan AS, negara Tiongkok merupakan negara yang paling sering melakukan serangan *cyber* kepada AS. Beberapa kasus *cyber* yang melibatkan AS dan Tiongkok bahkan sangat menyita perhatian dunia.

Salah satu peristiwa penting dalam sejarah hubungan *cyber* AS-Tiongkok adalah ketika New York Times (NYT) sebuah perusahaan media terbesar milik AS menjadi korban peretas yang berasal dari Tiongkok (Nicole, dalam www.nytimes.com diakses 5 Mei 2015). Untuk membuktikan hal tersebut, NYT mengontrak Mandiant sebuah perusahaan keamanan *cyber* pada tahun 2013 untuk menyelidiki masalah peretasan yang dialami perusahan media terbesar AS tersebut. Hasil investigasi forensik yang dilakukan Mandiant menunjukkan bahwa serangan-serangan terhadap New York Times yang berbentuk APT (*Advanced Persistent Thread*) dengan kode APT1 adalah berasal dan terpusat dari kota Sanghai, Tiongkok. Bahkan APT1 memiliki kesamaan digital forensik dengan Unit PLA 61398 yang merupakan kesatuan militer Tiongkok.

Unit 61398 adalah yang paling sering melakukan serangan kepada perusahaan-perusahaan dan agen-agen federal AS. Mandiant menyebut Unit 61398 sebagai salah satu tentaramaya (*cyber-army*) milik Cina. Unit 61398 ini tidak saja menyerang dokumen pemerintahan, tetapi juga *intelectual property* perusahaan-perusahan AS.

House Permanent Select Committee on Intelligence pada tahun 2012 merilis laporan yang menyimpulkan bahwa penggunaan perangkat telekomunikasi dari produk Huawei dan ZTE milik Tiongkok, membawa resiko pada ekonomi dan keamanan nasional AS. Laporan ini juga mengutip beberapa hasil riset yang mengatakan Tiongkok sebagai sumber terbesar serangan *cyber* (Scissors & Bucci, 2015). Selain itu, spionase dengan skala besar "*Titan Rain*" adalah serangan yang dilakukan para *hacker* (peretas) yang berbasis di Tiongkok. Mereka tidak hanya mendobrak sistem keamanan *software* perusahaan dan lembaga ekonomi AS saja, tetapi juga berhasil masuk dalam jaringan milik departemen pertahanan AS, Departemen energi AS, *Homeland Security* dan jaringan para kontraktor pertahanan AS. Data yang dicuri oleh para peretas ini diperkirakan tidak kurang dari 10 – 20 *terabytes* (Scissors & Bucci, 2015). Pencurian data yang dituduhkan AS terhadap agen peretas Tiongkok juga termasuk design helikopter, kapal, jet tempur dan beberapa sistem pertahanan misil AS lainnya (Holden, melalui

http://thediplomat.com/2014/07/breaking-through-chinas-great-firewall/)

AS merasa bahwa spionase ekonomi yang dilakukan oleh Tiongkok sudah sampai pada tahap yang tidak dapat ditoleran, kekhawatiran akan hal ini semakin mendalam karena saat ini AS dan Tiongkok berada pada posisi perang pasar yang cukup sengit (Roger dalam Mandiant, 2013: 1). Lebih lanjut Mandiant melaporkan bahwa kegiatan spionase dan pencurian data ini telah dilakukan Tiongkok sejak tahun 2006, tidak kurang dari 141 institusi dilaporkan sebagai korbannya (Mandiant, 2013: 2-6).

Tuduhan AS terhadap negara Tiongkok ini tentu saja mendapatkan reaksi. Pemerintah Tiongkok melalui juru bicara Departemen Pertahanannya menolak tuduhan laporan Mandiant yang menyimpulkan bahwa Tiongkok terkait dengan aksi *hacking* yang menimpa sejumlah perusahaan Amerika Serikat (detiknet dalam http://www.inet.detik diakses 27 April 2015).

Perseteruan di dunia maya antara AS dan Tiongkok juga didorong oleh kebijakan Tiongkok yang melakukan sensor ketat terhadap penggunaan internet di negaranya atau yang dikenal dengan *Great Firewall of China* (GFWoC). Ini adalah sebuah kebijakan yang digunakan pemerintah Tiongkok untuk melakukan sensor dan *blocking* atau pelarangan akses internet yang dianggap mengandung pornografi, perbedaan pandangan politik, pemberitaan negatif tentang negara Tiongkok baik yang beredar di situs-situs berita maupun media sosial. Metode yang digunakan Tiongkok diantaranya seperti *blocking IP address, blocking redirecting or specific domain, filtering/blocing any URL containing target keyword* (Mandiant, 2013:51).

Perseteruan AS-Tiongkok di dunia maya adalah situasi yang sangat dilematis. Ketergantungan dan keterhubungan AS dan Tiongkok dalam industri IT adalah fakta yang menciptakan situasi dilematis tersebut. Perusahan-perusahan IT milik AS seperti CISCO, Microsoft, Apple, Intel, IBM, Qualcomm, Oracle selain memiliki pasar yang besar di Tiongkok, merupakan bagian dan paket dari infrastruktur internet Tiongkok. Sementara itu perusahaan IT Tiongkok seperti Huwaei, ZTE, Lenovo telah masuk dalam pasar AS, mempekerjakan warga AS dan beroperasi dibawah peraturan dan hukum negara AS. Saham perusahaan Tiongkok lainnya seperti Baidu, Alibaba dan Tencent termasuk dalam daftar bursa saham elektronik pertama dan terbesar di AS: *National Association of Securities Dealers Automated Quotations* (NASDAQ), dimana sahamnya tidak saja dimiliki oleh warga negara Tiongkok, namun juga warga AS dan investor dari berbagai dunia lainnya

(Chuanying dalam http://www.chinausfocus.com diakses 24 April 2015).

Keseriusan Tiongkok dalam membangun *cyberpower* sesungguhnya telah menjadi perhatian AS. Meskipun bukan dalam rangka merespon secara langsung serangan *cyber* Tiongkok, pada tahun 2011, Presiden Barack Obama dan Mentri Luar Negeri AS Hillary Rodham Clinton telah mengidentifikasi isu *cyber* sebagai kunci prioritas dari Politik Luar Negeri Amerika Serikat (U.S. Departement of State, http://www.state.gov/documents/organization/168901.pdf.)

Dari pemaparan latar belakang diatas, peneliti menangkap adanya rivalitas yang intens terjadi dalam dunia maya antara AS dan Tiongkok. Kedua negara sama-sama menyadari bahwa persaingan dimasa mendatang akan sangat didominasi oleh kekuatan-kekuatan *cyber*.

Oleh karena itu peningkatan kapabilitas dan serangkaian strategi dibuat untuk menjawab tantangan tersebut. Peningkatan *Cyberpower* Tiongkok yang pesat ini sepertinya dilihat sebagai sebuah ancaman terhadap keamanan AS. Respon keberatan AS terhadap serangan *cyber* yang dilakukan Tiongkok juga semakin menegaskan hal tersebut. Berangkat dari latar belakang ini peneliti ini meneliti secara mendalam tentang bagaimana dunia maya menjadi prioritas dalam politik luar negeri AS dan mengapa AS melihat *cyberpower* Tiongkok sebagai ancaman terhadap kemanan nasionalnya.

2. TINJAUAN PUSTAKA

Berdasarkan penelusuran peneliti, ada beberapa hasil penelitian yang juga meneliti mengenai hubungan *cyber* antara Amerika Serikat dan Tiongkok. Yang pertama adalah penelitian dari Kolonel Jayson M. Spade, dari United States Army College, yang membuat sebuah penelitian dengan judul *China's Cyberpower and American National Security* (Spade, 2011). Penelitian Spade menelaah pertumbuhan cyberpower Tiongkok, pengetahuannya serta kemampuan ofensif, defensif serta ekploitif dari operasional jaringan komputer yang dimiliki Tiongkok dan memperbandingkan kemampuan Tiongkok tersebut dengan kapabilitas keamanan *cyber* yang dimiliki oleh AS. Dari perbandingan tersebut Spade kemudian mampu menggarisbawahi pada derajat *cyberpower* Tiongkok mana yang harus disikapi sebagai sebuah ancaman bagi keamanan nasional AS.

Penelitian-penelitian yang juga terkait dengan variabel penelitian ini seperti dari Robert O. Keohane dan Joseph S. Nye, Jr., yang mengulas konsep Power dan

perkembangan konsep tersebut saat ini. Keohane dan Nye mengemukakan pendapatnya mengenai *power* dan interdependensi pada era informasi dalam jurnal Foreign *Affairs* (1998: 81-94). Keohane dan Nye menggambarkan bagaimana revolusi informasi secara dramatis merubah pola hubungan internasional, yang mereka konsepkan sebelumnya[1] : "*complex interdependence*". Konsep ini merupakan gambaran dunia yang tidak lagi didominasi oleh hubungan keamanan dan militer. Negara terhubung satu sama lain melalui hubungan sosial dan politik. Revolusi informasi telah memperluas relasi transnasional secara cepat. Aktor non pemerintah memiliki kesempatan yang jauh lebih besar untuk mengatur dan mempropaganda pandangan-pandangannya. Akibatnya para pemimpin politik menjadi lebih sulit untuk memelihara kohesivitas dalam isu politik luar negeri.

Tantangan terhadap revolusi informasi tersebut berlanjut pada perdebatan ilmiah tentang bagaimana era informasi ini menciptakan difusi terhadap konsep *power* sehingga melahirkan konsep *cyberpower* . Penelitian mengenai *cyberpower* dikembangkan juga oleh lembaga-lembaga militer. Larry K. Wentz., Charles L. Barry, dan Stuart H. Starr (2009) menulis tentang perspektif militer dalam *cyberpower*. Sedangkan Joseph S. Nye, Jr (2011) menuliskan *cyberpower* sebagai kekuatan di masa depan. Sementara itu, penelitian mengenai *cyberpower* juga dlakukan oleh Tim L. Jordan (2002) dan David Betz (2012).

Cyberpower adalah kekuatan (*power)* berdasarkan sumber-sumber informasi. Ada banyak definisi tentang dunia maya (*cyberspace*) namun secara umum dihubungkan dengan kegiatan yang menggunakan komputer dan elektronik.

Pemahaman secara menyeluruh mengenai internet dan *cyberspace* (dunia maya) dari perspektif sosiologis, budaya, politik, dan ekonomi yang terintegrasi akan menjadi sumber kunci untuk memahami dan mengembangkan kehidupan virtual.

Sifat *cyberpower* tergantung pengaturan sumber-sumber yang berhubungan dengan pembuatan (*creation*), pengawasan (*control*), dan komunikasi (*communication*) alat elektronik dan komputer berbasis informasi, termasuk infrastruktur, *networks, software* serta *human skill*. Dilihat dari hal ini, *cyberpower* merupakan kemampuan untuk mencapai hasil yang diinginkan melalui penggunaan eloktronik yang terhubung

[1] Pada tahun 1977 Keohane dan Nye juga menulis bersama sebuah buku *Power and Interdependence*. Dalam buku tersebut mereka mengungkapkan bahwa perkembangan teknologi dan meningkatnya transaksi sosial ekonomi menuntun ke arah dunia yang baru dimana kontrol negara terhadap militer tidak lagi menjadi hal yang sangat penting.

dengan sumber informasi dalam dunia maya (Nye, 2010: 4).

Khuel dalam Kramer (2009: 38) mencoba mendefinisikan *cyberpower* sebagai berikut: "*cyberpower is the ability to create advantages and influence events in other operational environments and across the instruments of power*". *Power* adalah kemampuan untuk memperoleh pengaruh serta keuntungan dalam lingkungan operasional yang lain dan menyebrangi instrumen *power* yang ada.

Tim L. Jordan dalam (1999) menganalisa *cyberpower* dari sudut pandang yang berbeda. Ia mencoba mengartikulasikan secara teoritis, mengenai konsepsi tentang *power* dalam *cyberspace* (dunia maya). Jordan memberikan pemahaman tentang internet dan *cyberspace* melalui perspektif sosiologi, kultural, politik, dan ekonomi secara terintegrasi sehingga kita bisa melihat bagaimana sifat dasar *power* dalam kehidupan dunia maya. Jordan melihat *power* berkerja dalam tiga tingkatan (wilayah) : kehidupan individual, kehidupan sosial dan kehidupan imajiner (khayal).

Karya Jordan menekankan bahwa hal yang paling penting dari *cyberpower* adalah yang berasal dari individual dan masyarakat. Titik tekan analisis Jordan ini sekaligus menjadi kekurangan dalam buku ini. Karena Jordan tidak membahas bahwa negara pun dapat mempergunakan *cyberpower* untuk kepentingan nasionalnya.

Bertolak belakang dengan Tim Jordan , penelitian David Betz dalam *The Journal of Strategic Studies* (2012: 689-711) mencoba mengkaitkan *cyberpower* dengan hubungan strategis negara. Betz menegaskan bahwa keterhubungan yang terjadi dalam era digital memiliki implikasi penting terhadap praktik peperangan. Meskipun tidak merubah secara substantif sifat perang itu sendiri. Menurut Betz, *Cyberwar* sendiri tidak serta merta menggantikan bentuk perang dan membentuk ulang sistem internasional yang selama ini diwarnai pola "*balance of power*". Namun Betz mengingatkan bahwa akan ada perubahan dalam hubungan strategis negara yang terjadi seiring dengan berkembangnya dunia maya.

3. PEMBAHASAN

a. Arah Pembangunan CyberPower Tiongkok

Menurut para pengamat dan akademisi Barat, Tiongkok memiliki tiga tujuan utama yang berkaitan dengan keamanan nasional (Spade, 2011: 14). Pertama, Tiongkok membangun *cyberpower* untuk mempertahankan rezim Partai Komunis Tiongkok. Kedua, Tiongkok ingin mempertahankan kedaulatan nasional dan integritas teritorial. Ketiga, Tiongkok berusaha menempatkan diri sebagai kekuatan

regional dan kekuataan dunia. Dalam prakteknya, ketiga tujuan tersebut sangat bermanfaat untuk mempertahankan kestabilan kemajuan ekonomi dan sosial, modernisasi militer, serta mencegah kemerdekaan Taiwan.

Dokumen yang menjadi konfirmasi analisis di atas, diantaranya adalah *China's National Defense in 2008*. Dalam dokumen tersebut, pemerintah Tiongkok melihat dirinya yang selalu berhadapan dengan ancaman dan tantangan keamanan yang berlangsung dalam jangka waktu yang panjang dan kompleks. Ancaman dan tantangan keamanan tersebut muncul dalam bentuk superioritas negara-negara maju atas ekonomi, ilmu pengetahuan, teknologi, dan militer, manuver dan kepungan dari luar, gangguan dan sabotase dari gerakan-gerakan separatis, serta transisi ekonomi dan sosial yang memungkinkan munculnya situasi dan isu baru yang dapat mengganggu stabilitas sosial.

Namun sangat penting untuk mengetahui bagaimana Tiongkok memandang keamanan siber dari perspektif yang berbeda dari konsep yang dimiliki negara besar seperti Amerika Serikat. Dalam literatur-literatur Tiongkok, kata-kata seperti "cyber" dan "cybersecurity" jarang digunakan, meskipun pemerintah dan akademisi mengadaptasi penggunaannya dalam media berbahasa Inggris. Dibanding kata tersebut, Tiongkok menggunakan "information security" dan "network security" untuk menyebut konsep serupa.

Literatur pemerintah, akademisi, dan militer menggunakan kata "network" (*wangluo*) untuk kata yang berhubungan dengn "cyber", "network space" (*wangluo kongjian*) untuk kata yang terkait "cyberspace", dan "network warfare" (wangluo zhan) untuk mengganti kata "cyber operations". Literatur PLA memasukkan konsep "cyber" dalam wilayah "information operations" (*xinxi zuozhan*), meskipun istilah tersebut memiliki jangkauan yang lebih luas yang berkaitan dengan penghitungan, operasi psikologis, maupaun dalam spektrum elektromagnetik (Chang, 2014: 13).

b. Kapabilitas Cyberpower Tiongkok dan Dampaknya bagi Kepentingan Amerika Serikat

Tiongkok termasuk negara yang memiliki pengguna internet terbesar di dunia. Sampai bulan Juni 2016, Tiongkok memiliki 710 juta pengguna internet. Angka ini meningkat sebesar 21,32 juta dari angka di akhir 2015. Sementara itu, pengguna internet seluler mencapai 656 juta, bertambah 36,56 juta dari akhir 2015 (lihat gambar 4.2). Pengguna seluler terhitung sebesar 92,5 persen dari seluruh populasi pengguna internet. Pengguna internet di daerah pedesaan mencapai 26,9 persen dari total nasional, yang mencapai 191 juta pengguna. Meskipun demikian, penetrasi

internet di wilayah urban lebih tinggi 35,6 persen dari penetrasi di wilayah pedesaan. Hal tersebut memperlihatkan adanya gap yang cukup besar antara urban dan pedesaan. Data-data lain yang penting adalah proporsi pengguna telepon seluler yang menggunakan ponsel untuk mengakses internet sebesar 92,5 persen. Angka tersebut naik 2,4 persen dari angka pada akhir 2014. Sementara itu, pengguna yang mengakses menggunakan laptop untuk mengakses internet sejumlah 38,5 persen. Sampai bulan Juni 2016, seperti yang ditunjukkan pada gambar 4.3, Tiongkok memiliki total 4,54 juta situs, yang 2,12 juta diantaranya menggunakan domain ".CN" (China Internet Network Information Center, 2016: 1).

Dari segi ekonomi, sampai pertengahan tahun 2016, pemakaian internet untuk *online payment* dan *online banking* naik sebesar 9,3 persen dan 12,3 persen dari tahun sebelumnya. Dengan pengembangan ekonomi melalui aplikasi elektronik, skenario *online* tersebut diperkirakan akan terus meningkat. Percepatan yang berkelanjutan diperkirakan membantu pengguna mendapatkan pengalaman untuk mengembangkan kebiasaan *online banking*. Dari bidang pendidikan dan layanan pemerintah, jumlah pengguna yang menggunakan internet untuk program tersebut mencapai angka lebih dari 100 juta pemakai.

Data-data peningkatan dari tahun ke tahun yang ditunjukkan dalam gambar-gambar di atas dalam berbagai segi menunjukkan bahwa Tiongkok adalah *large internet country* seperti yang dikatakan Xi Jinping. Hal itu belum ditambah lagi menurut data yang tersedia pada awal tahun 1990-an di mana terdapat sekitar 37 juta orang Tiongkok yang tersebar di 136 negara. Menurut perkiraan, jumlah itu akan meningkat menjadi 96 juta pada tahun 2016. Data resmi menunjukkan bahwa 1,6 juta orang lahir di Tiongkok dan tinggal di Amerika Serikat. Di kawasan lain, pada tahun 2003, terdapat lebih dari 150.000 imigran di Uni Eropa yang lahir di Tiongkok (Magalhaes, et al., 2009: 140). Jumlah tersebut menunjukkan Tiongkok sebagai negara pengguna internet yang cukup besar.

Dari sisi kapabilitas militer, laporan Pentagon sejak tahun 2002 menunjukkan adanya laporan-laporan mengenai visi strategis dan implementasi taktikal mengenai perang informasi Tiongkok yang konstan (Magelhaes, et al., 2009: 141-142). Pertama, pada tahun 2002 dan 2003, laporan tersebut menunjukkan bahwa Tiongkok telah melakukan evolusi yang sistematis dalam kapabilitas C4I (*Command, Control, Communications, Computers, and Intelligence*). Evolusi tersebut diperkirakan akan terus berlanjut pada tahun-tahun ke

depan. Kedua, laporan tersebut menyatakan bahwa Tiongkok telah siap untuk mengembangkan apa yang disebut operasi informasi. Angkatan bersenjata Tiongkok mulai merekrut para ahli dan spesialis dalam teknologi informasi untuk memastikan kapabilitas serangan dan pertahanan. Ketiga, laporan tersebut menyatakan bahwa Tiongkok memiliki kapabilitas untuk melakukan penetrasi dalam jaringan komputer Amerika Serikat yang memiliki pertahanan lemah dan menggunakan jaringan komputer untuk menyerang infrastruktur sipil maupun militer milik Amerika Serikat. Keempat, penelitian dan pengembangan yang terus dilakukan Tiongkok menghasilkan peningkatan pengetahuan dalam perilaku dan penyebarluasan virus komputer. Secara tidak langsung, hal ini menunjukkan bahwa Tiongkok memiliki pengetahuan yang kuat mengenai penyerangan jaringan komputer melalui virus yang disebarluaskan lewat perangkat lunak. Kelima, yang tidak boleh diremehkan, ada kemungkinan Tiongkok menyalakan prinsip "perang rakyat" dalam hal perang di dunia maya.

Sementara itu, laporan Pentagon pada tahun 2004 dan 2005 menunjukkan adanya kapabilitas atau intensi Tiongkok untuk melakukan penyerangan ke Taiwan. Pada tahun-tahun tersebut, Tiongkok yang telah fokus pada evolusi peralatan C4I mulai meningkatkan investasi pada evolusi C4ISR (*Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance*). Laporan menunjukkan adanya strategi pemerintahan Tiongkok untuk memaksa perusahaan-perusahaan besar teknologi internasional untuk melakukan transfer teknologi, membagi pengetahuan, dan membuka pusat penelitian dan pengembangan di Tiongkok melalui regulasi akses terhadap pasar Tiongkok. Meski demikian, pada tahun 2004 dan 2005, Tiongkok masih tidak memiliki tenaga yang cukup ahli dalam manajemen teknologi dan kultur perusahaan yang tidak mendorong adanya inovasi dan kemajuan untuk meningkatkan kapabilitas dan program teknologi.

Pada tahun 2006, Pentagon melaporan bahwa Tiongkok telah memiliki unit khusus yang dibentuk untuk perang informasi. Unit khusus tersebut dibentuk untuk mendukung tindakan pasukan bersenjata Tiongkok dalam konflik melalui serangan siber. Pada tahun 2007, Tiongkok merupakan negara yang diduga melakukan sejumlah penyerangan jaringan di India (*National Informatics Center*), Jerman (*Chancellery*), Selandia Baru, dan Australia. Surat kabar juga mengeluarkan pemberitaan yang mengutip pegawai pemerintahan bahwa serangan pada sistem pemerintah Prancis dan Inggirs berasal dari Tiongkok. Pada tahun 2008, Pentagon

melaporan bahwa Tiongkok diduga melakukan gangguan pada jaringan departemen-departemen, agensi, dan perusahaan-perusahaan yang memiliki kontrak pengembangan militer dengan Amerika Serikat. Meskipun Tiongkok terus menyangkal adanya aktivitas *hacking* terhadap negara lain, dan bahkan menuduh Amerika Serikat dan negara lain lah yang mengeksplorasi dan melakukan aktivitas pengintaian, hal tersebut memperlihatkan bahwa kapabilitas Tiongkok dalam *cyberpower* terus meningkat dan mendapatkan dukungan dari regulasi pemerintah, serta mampu menimbulkan gangguan pada level internasional.

Bersamaan dengan peningkatan kapabilitas dalam bidang militer, Tiongkok juga fokus pada pengembangan kemampuan dan kapabilitas dalam sektor sipil. Program Jangka Menengah dan Jangka Panjang dalam Ilmu Pengetahuan dan Teknologi 2006-2020 mendorong Tiongkok untuk melakukan integrasi antara upaya-upaya sipil dan militer. Dalam domain siber, misalnya, PLA melakukan kerja sama pengembangan dengan universitas-universitas dan sektor telekomunikasi sipil. Sebagai contoh, ZTE dan Huawei merupakan dua perusahaan yang memiliki ikatan yang kuat dengan PLA. PLA juga memiliki relasi koloborasi penelitian dengan 46 universitas (Inkster, 2016: 58).

Dengan mengetahui ketergantungan dan kerentanan siber Amerika Serikat, pengamatan terhadap situasi siber Amerika Serikat harus dikaitkan dengan kepenitingan nasional Amerika Serikat. Jika pada bagian sebelumnya hal-hal tersebut berkaitan dengan akibat-akibat di dalam negeri seperti lambatnya penanganan panggilan darurat atau kerusakan sistem listrik di beberapa wilayah, bagian ini berusaha menunjukkan kepentingan nasional Amerika Serikat dan bagaimana kerentanan tersebut mempengaruhi kepentingan vital Amerika Serikat dalam konteks eksternal atau konteks internasional. Menurut Blackwill & Tellis (2015: 18-19), kepentingan nasional yang vital bagi Amerika Serikat dalam konteks hubungan internasional memiliki setidaknya empat poin utama. Keempat poin utama tersebut adalah sebagai berikut:

Pertama, Amerika Serikat memiliki kepentingan untuk mencegah, menghalangi, dan mengurangi ancaman serangan konvensional maupun tidak konvensional terhadap benua Amerika Serikat dan teritorial kepemilikan lainnya. Berbeda dari Tiongkok, dalam urusan *cyberspace*, Amerika Serikat lebih fokus pada penguatan kapabilitas pertahanan dan menguatkan jaringan tersebut dalam level "technological and human capital" (Chang, 2014: 14). Namun, hal ini masih menjadi masalah karena Amerika

Serikat memiliki kerentanan dalam hal pertahanan siber.

Kedua, Amerika Serikat ingin memelihara *balance of power* di Eropa dan Asia untuk mempromosikan perdamaian dan stabilitas melalui kontinuitas kepemimpinan peran Amerika Serikat dan aliansinya. Dalam hal ini, meskipun Amerika Serikat memiliki hubungan yang cukup kooperatif dengan Tiongkok terkait keamanan energi, ekonomi internasional dan isu-isu lainnya, pertumbuhan Tiongkok berpotensi untuk menganggu kepentingan vital nomor dua ini. Upaya sistematis Tiongkok yang mengarah pada hal itu adalah mengubah *balance of power* di Asia, mengurangi sistem aliansi Amerika Serikat dan negara-negara di Asia, untuk kemudian menggantikan Amerika Serikat dalam kepemimpinan di Asia. Dalam hal perdagangan bilateral, misalnya, nilai aliran perdagangan Tiongkok dengan beberapa negara telah melampaui relasi perdagangan bilateral Amerika Serikat dengan negara-negara tersebut.

4. KESIMPULAN

Tiongkok memiliki definisi yang berbeda dengan definisi Amerika Serikat mengenai *cyberpower* dan *cybersecurity*. Hal itulah yang memperlihatkan perbedaan kepentingan antara Tiongkok dan Amerika Serikat. Tiongkok memiliki strategi keamanan jaringan yang bukan hanya terkait dengan kontrol dan regulasi informasi dan aset-aset jaringan, melainkan juga usaha-usaha mereka untuk melayani kepentingan dan tujuan-tujuan nasional. Oleh karena itu, tujuan *cyberpower* Tiongkok bukan hanya untuk bidang militer, tapi juga meraih keuntungan dalam bidang ekonomi dan politik. Hal ini sedikit berbeda dengan Amerika Serikat yang sama-sama memiliki tujuan dalam militer, ekonomi, dan politik, namun menekankan pada tradisi kebebasan berekspresi dan berkumpul, sehingga Amerika Serikat mengkampanyekan tradisi liberal di internet.

Perkembangan kapabilitas Tiongkok, bersama dengan serangan siber Tiongkok, mengancam kepentingan nasional Amerika Serikat. Pertama, Amerika kesulitan untuk mencegah, menghalangi, dan mengurangi ancaman serangan konvensional maupun tidak konvensional, yang dalam hal ini serangan siber Tiongkok. Kedua, Amerika akan mendapatkan tantangan yang cukup kuat untuk memelihara *balance of power* di Eropa dan Asia dalam mempromosikan perdamaian dan stabilitas melalui kontinuitas kepemimpinan peran Amerika Serikat dan aliansinya. Ketiga, kepentingan Amerika mencegah penggunaan senjata nuklir dan senjata pemusnah massal lainnya berpotensi terancam karena serangan siber juga bisa memasuki area laboratorium senjata nuklir

Amerika Serikat. Keempat, kepentingan untuk mempromosikan stabilitas dan pertumbuhan ekonomi internasional menjadi semakin berat dengan adanya medan perang baru, yaitu medan perang siber di dunia maya.

Oleh karena itu, Amerika Serikat harus segera mengambil langkah-langkah di antara pilihan langkah-langkah yang tersedia. Dibandingkan strategi rivalitas atau mengakomodasi perkembangan Tiongkok dalam *cyberpower*, Amerika Serikat lebih baik menjalankan langkah internasional untuk mengikutsertakan Tiongkok dalam kerja sama global. Sementara Tiongkok memiliki banyak masalah dan sumber ketegangan di kawasan, Tiongkok cenderung asertif dalam lingkungan internasional. Untuk mempersiapkan hal tersebut, Amerika Serikat telah berupaya meningkatkan sistem pertahanan dalam negeri dan melakukan koordinasi yang diperlukan untuk melindungi semua sektor dari serangan siber Tiongkok. Amerika Serikat juga turut mendorong norma-norma berperilaku dalam *cyberspace* di tingkat internasional, seperti kebebasan berinternet dan perlawanan bersama untuk masalah *cybercrime*.

DAFTAR PUSTAKA

Austin, G. (2014). *Cyber Policy in China.* Cambridge: Polity Press.

_____(2016). *Mapping and Evaluating China's Cyber Power*. London: Lau China Institute Policy Paper Series.

Blackwill, R. D., & Tellis, A. J. (2015). *Revising U.S. Grand Strategy Toward China*. Council Special Report No. 72. U.S.: Council on Foreign Relations.

Chang, A. (2014). *Warring State: China's Cybersecurity Strategy*. Washington DC: Center for a New American Security.

Chang, F. K. (2012). *China's Naval Rise and the South China Sea: An Operational Assessment.* Foreign Policy Research Institute.

China Internet Network Information Center. (2016). *Statistical Report on Internet Development in China*. Beijing: Penulis.

Department of State International. (2016). *Cyber Policy Strategy: Public Law 114-113, Division N, Title IV, Section 402*.

Feakin, T. (2013). *Enter the Cyber Dragon: Understanding Chinese intelligence agencies' cyber capabilities.* Australian Strategic Policy Institute, Special Report, Issue 50.

Guojie, L. (ed.). (2011). *Information Science and Technology in China: A Roadmap to 2050.* Beijing: Chinese Academy of Social Sciences/ Science Press/ Springer.

Inkster, N. (2016). *China's Cyber Power*. London & New York: Routledge for The International Institute for Strategic Studies.

Jinping, Xi. (2014). *New Asian security concept for new progress in security cooperation.* Fourth Summit of the Conference on Interaction and Confidence Building Measures. Shanghai: Penulis.

Lanteigne, M. (2009). *Chinese Foreign Policy: An Introduction*. London & New York: Routledge.

Lewis, J. & Hansen, S. (2014). *China's cyberpower: International and domestic*

priorities. Astralian Strategic Policy Institute: International Cyber Policy Centre.

Li, X. (2015). Interpreting and Understanding "The Chinese Dream" in a Holistic Nexus. *Fudan Journal of the Humanities and Social Sciences, 8*(4), 505-520.

Magalhaes, S. T., et al. (2009). The People's Republic of China – The Emerging Cyberpower. Dalam H. Jahankhani, A.G. Hessami, and F. Hsu (Eds.), *Global Security, Safety, and Sustainibility: 5th International Conference* (h. 138–144). Springer-Verlag Berlin Heidelberg.

Medeiros, E. S. (2009). *China's International Behavior: Activism, Opportunism, and Diversification*. Santa Monica: RAND Corporation.

O'Rourke, R. (2015). *China Naval Modernization: Implications for U.S. Navy Capabilities ─ Background and Issues for Congress.* Congressional Research Service Report, 9-22.

Pernik, P., Wojtkowiak, J., & Verschoor-Kirss, A. (2016). *National Cyber Security Organisation: United States*. Tallian, Estonia: NATO Cooperative Cyber Defence Centre of Excellence.

Sharma, M. (2016). China's Emergence as a Cyber Power. *Journal of Defence Studies, 10*(1), January-March 2016, 43-68.

Spade, J. M. (2011). *China's Cyber Power and America's National Security* [Strategy Research Project]. Philadelphia: U.S. Army War College.

Swaine, M. D. (2012). China's Assertive Behavior Part Three: The Role of the Military in Foreign Policy. *China Leadership Monitor, 36*, 1-17.

The White House. (2003). *The National Strategy to Secure Cyberspace*. Washington: Penulis.

The White House. (2011). *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Washington: Penulis.

Yuxiao, L. (2012). Cyberspace Security and International Cooperation in China in *China and Cybersecurity: Political, Economic, and Strategic Dimensions* [Paper seminar]. San Diego: University of California.