China's Great Firewall: Cybersecurity as Strategy for Building World Cyberpower

JISPO
Jurnal Ilmu Sosial dan Ilmu Politik
2023, Vol. 13, No. 2: 193-232
https://journal.uinsgd.ac.id/index.php/jispo/index

Harvardry Gerald Abraham Wowor*
Universitas Padjadjaran, Indonesia

Arfin Sudirman
Universitas Padjadjaran, Indonesia

Falhan Hakiki
Sekolah Tinggi Ilmu Sosial dan Ilmu Politik (STISIP) Imam Bonjol Padang, Indonesia

Abstract
The information, communication, and technology (ICT) sector has grown significantly in China. One of the advancements they have seen is in the area of cybersecurity. China's growing cybersecurity competence enabled it to create the Great Firewall of China (GFW), a set of control and censorship regulations for internet communications in China. This article investigates the significance of cybersecurity in the development of China's authoritarian authority, with a focus on the GFW as a strategic component. The concepts of cybersecurity and cyberpower served as the article's theoretical foundation. Through interviews and literature reviews, this article employs qualitative methodologies. This article demonstrates how China employs GFW to protect its citizens from cyber-attacks by focusing on political risks. China's cyber power is likewise increasing.

Keywords
China, Great Firewall of China, cybersecurity, cyberpower

Abstrak
Tiongkok telah mengembangkan industri Informasi, Komunikasi, dan Teknologi (TIK) dalam beberapa tahun terakhir. Salah satu kemajuan yang mereka alami adalah di bidang keamanan siber. Keahlian baru Tiongkok dalam keamanan siber memungkinkannya membangun *Great Firewall of China* (GFW), yang merupakan kumpulan kebijakan pengendalian dan penyensoran untuk komunikasi internet di Tiongkok. Karena itu, artikel ini membahas peran keamanan siber dalam membangun kekuatan otoriter Tiongkok. Landasan teori yang digunakan dalam artikel ini adalah teori keamanan siber dan kekuatan

*Corresponding author:
Harvardry Gerald Abraham Wowor
Adress: Program Studi Hubungan Internasional, Universitas Padjadjaran, Indonesia
Email: harvardry17001@mail.unpad.ac.id

siber. Dengan menggunakan metode kualitatif melalui studi literatur dan wawancara, artikel ini menunjukkan bahwa Tiongkok menggunakan GFW untuk mengamankan negaranya dari ancaman dunia maya dengan fokus pada ancaman politik. Kekuatan siber Tiongkok juga semakin berkembang sebagai hasil dari berbagai kebijakan dan kemajuan yang diterapkan Tiongkok di bidang keamanan siber.

Kata-kata Kunci
Tiongkok, *Great Firewall of China*, keamanan siber, kekuatan siber

Pendahuluan

Teknologi Informasi dan Komunikasi (TIK) adalah segala jenis peralatan atau teknik yang digunakan untuk menyimpan, menerima, mengirimkan, dan memanipulasi data. Di zaman sekarang, istilah ini cenderung lebih identik dengan penggunaan peralatan elektronik dalam manajemen informasi. Karena itu, TIK meliputi berbagai jenis teknologi seperti telefon, televisi, dan media komunikasi lainnya (Dainith and Wright 2006). Sepanjang perkembangan teknologi informasi dan komunikasi, sudah banyak aspek dari kehidupan sehari-hari manusia yang terdampak atau berubah karena perkembangan tersebut.

Banyak studi yang meneliti mengenai TIK dari sudut pandang masing-masing ilmu. Salah satu bidang studi yang juga mengkaji mengenai TIK adalah ilmu hubungan internasional. Pembahasan TIK mulai masuk dalam pembahasan kajian hubungan internasional sejak abad ke-20 ketika para ahli hubungan internasional pada era tersebut mulai mengkaji hubungan kemajuan teknologi dan *power* suatu negara. Pada waktu itu, teknologi yang dikaji dalam pembahasan hubungan internasional adalah peran teknologi dalam mengembangkan kekuatan militer negara. Namun, seiring perkembangan zaman, pandangan ini berubah ketika sudah matangnya teknologi senjata nuklir. Setelah adanya senjata nuklir, teknologi informasi juga menjadi lebih canggih dan bergerak lebih cepat juga. Oleh karena itu, studi hubungan internasional juga mulai mengkaji peran kemajuan teknologi informasi terhadap kemampuan militer negara (Carr 2016).

Salah satu kemajuan yang muncul bersamaan dengan senjata nuklir adalah sistem jaringan komputer pertama yang diberi nama ARPANET (Lukasik 2011). Sistem ARPANET pertama mulai beroperasi pada 30 Agustus 1969 di University of California, Los Angeles. ARPANET sering kali disebut sebagai “nenek moyang internet” karena banyak teknologi

yang digunakan dalam internet yang modern pertama dikembangkan untuk mewujudkan ARPANET (Stewart 2007). Dengan suksesnya implementasi ARPANET, teknologi ini terbukti fungsional dan dapat dikembangkan lebih lanjut. Perkembangan selanjutnya adalah dibuatnya protokol-protokol yang dapat menghubungkan beberapa jaringan komputer. Kumpulan protokol-protokol ini lalu dikenal dengan istilah TCP/IP (*Transmission Control Protocol and Internet Protocol*) (Hauben 1998). Implementasi protokol TCP/IP ini menjadi penting dalam internet modern karena memungkinkan sistem yang berbeda untuk berkomunikasi. Di masa modern ini, semua sistem komputer yang menerapkan protokol TCP/IP dapat mengakses internet.

Dengan matangnya perkembangan internet, studi hubungan internasional mulai mengkaji TIK dengan pandangan baru. Menurut kajian hubungan internasional sekarang, TIK dipandang sebagai alat penting dalam pembentukan kebijakan luar negeri. Perkembangan TIK memberikan para pembuat kebijakan akses pada informasi yang terbaru dan terpercaya sehingga mereka dapat membentuk kebijakan yang sesuai dengan kondisi dunia pada waktu itu (Khumalo and Baloyi 2018).

Kemajuan TIK ini juga memunculkan aktor-aktor dan isu-isu baru ke dalam kajian hubungan internasional. Dengan mudahnya akses internet, individu dapat mempelajari apa yang terjadi di luar negaranya dan menyuarakan pendapat mereka mengenai suatu hal yang terjadi tersebut sambil juga mendengarkan opini lain yang disuarakan mengenai suatu kejadian tersebut. Suara yang diberikan kepada individu ini memberikan tekanan pada para pembuat keputusan mengenai apa saja yang perlu perhatian lebih dalam pembuatan keputusan (Weiss 2005). Aktor-aktor baru seperti perusahaan multinasional, agensi media, organisasi internasional, dan kelompok sosial juga membentuk opini publik secara lebih langsung karena mereka juga dapat menyampaikan kepentingan dan cara berpikir mereka dengan lebih bebas dan efisien (Radunovic 2010).

Selain itu, kemajuan TIK juga mengharuskan studi hubungan internasional untuk juga mengkaji ancaman-ancaman baru terhadap suatu negara. Serangan teroris 11 September dan pengeboman di Bali menunjukkan kepada dunia bahwa para jaringan teroris ini sudah memanfaatkan TIK untuk melancarkan rencana mereka. Ada pula perang jenis baru, yaitu perang informasi (*infowar*) dan perang dalam dunia maya (*cyberwar*), sehingga negara perlu memandang TIK secara lebih serius. Kejadian-kejadian tersebut mendorong studi hubungan internasional untuk juga mengkaji ancaman dari individu sambil mencari keseimbangan antara pengawasan

dan kebebasan individu (Derian 2003). Selain ancaman-ancaman dalam *cyberspace* tersebut, ancaman fisik terhadap suatu negara juga tetap menjadi fokus dalam hubungan internasional karena adanya kemajuan TIK yang dimanfaatkan oleh militer. Kemajuan dalam teknologi sensor, senjata terpandu, *cybersecurity*, sistem komunikasi militer, dan *mass surveillence* memunculkan potensi metode penyerangan dan pertahanan yang baru sehingga juga membuat studi hubungan internasional untuk mengkaji ulang ancaman-ancaman tersebut (Mallik 2016).

Proyek-proyek pengadaan jaringan yang akan menjadi internet di Tiongkok dimulai pada 1994. Walaupun cukup terlambat dibandingkan negara Barat yang sudah mulai dari tahun 80-an, Tiongkok tetap dapat mengembangkan teknologi-teknologi mereka sendiri. Pada 1995, Tiongkok sudah dapat memproduksi peralatan ATM-nya sendiri sehingga tidak lagi mengandalkan produk dari luar negeri. Pada 2006, Tiongkok juga sudah sukses mengadakan sistem komunikasi *fiber optic* dan menjadi salah satu eksportir teknologi fiber tersebut (Ping 2017) . Selain kemajuan dalam pembuatan produk, kecepatan internet di Tiongkok juga sudah menjadi salah satu yang tertinggi di dunia dan dengan pengguna yang cukup banyak juga. Pada 2014, 29% aktivitas internet berasal dari Tiongkok, sedangkan Amerika Serikat hanya menyumbang 13% (Hilbert 2016)

Dengan perkembangan yang pesat ini, Tiongkok sudah menjadi salah satu pemain besar dalam industri elektronik dan teknologi informatika. Pada tahun 2012-2016, perusahaan-perusahaan Tiongkok sudah dapat memproduksi dan menggunakan perlatan buatan dalam negeri saja. Perusahaan-perusahaan Tiongkok ternama dalam bidang ini yaitu Huawei dan ZTE mendapat keuntungan yang cukup besar. Walaupun mereka bermula dengan meniru produk buatan luar negeri, sekarang mereka sudah menjadi perusahaan produsen alat telekomunikasi terbesar di dunia dengan keuntungan hingga RMB283,1 miliar pada 2017 dan mengalahkan perusahaan seperti Nokia, Ericsson, dan ALE (Ping 2017).

Tiongkok juga mulai memfokuskan masa depannya dalam pengembangan ekonomi digital dengan integrasi terobosan-terobosan baru seperti *big data* dan AI dalam perekonomian mereka untuk mempermudah aliran modal dan tenaga kerja. Melalui integrasi internet dengan ekonomi ini, Tiongkok berharap mengembangkan pasar *e-commerce* mereka hingga mencapai luar negeri. Selain itu, Tiongkok juga terus merangsang perkembangan industri-industri baru seperti teknologi kendaraan pintar, layanan medis secara online, IoT (*Internet of Things*), AI, dan *Cloud Computing*. Untuk mencapai tujuan tersebut, pemerintah Tiongkok bekerja

sama dengan perusahaan-perusahaan lokal yang ada seperti Alibaba, Tencent, dan Huawei. Selain itu, perkembangan Belt & Road Initiative juga akan dijadikan salah satu alat untuk mengembangkan kerja sama dalam bidang ekonomi digital, terutama kerja sama dengan ASEAN dan EU melalui proyek *Tiongkok-ASEAN Information Harbor, Online Silk Road NIngxia Pivot Project*, dan *Tiongkok-EU Digital Silk Road Project* (Ping 2017).

Great Firewall of China (GFW) adalah sekumpulan peraturan-peraturan dan peralatan-peralatan yang digunakan oleh pemerintah Tiongkok untuk mengendalikan internet di Tiongkok. GFW berperan memblokir situs-situs asing tertentu, memperlambat koneksi lintas batas negara, dan menyensor konten-konten tertentu (Mozur 2015). Selain untuk menyensor konten-konten yang dianggap berbahaya, GFW ini juga digunakan untuk mendorong kemajuan perusahaan domestik dan mengurangi efektivitas produk asing yang masuk ke dalam negeri Tiongkok (Rauhala 2016).

Alasan terbentuknya GFW muncul dari sebutan Deng Xiaoping pada awal 1980-an yang mengatakan "Jika kamu membuka jendela, udara segar dan lalat akan masuk". Pokok pemikiran inilah yang menjadi dasar penyensoran media di Tiongkok untuk menghalangi masuknya "lalat" berupa ide-ide yang bertentangan dengan kepentingan pemerintah Tiongkok (MacKinnon 2008).

Sejak populernya internet di Tiongkok pada 1995, pemerintah Tiongkok sudah mulai merencanakan cara untuk mengendalikan internet. Pada awalnya, pemerintah Tiongkok dapat membatasi penggunaan internet melalui persyaratan dan peraturan yang rumit untuk dapat mengakses internet dan beberapa sistem pengawasan untuk memastikan pengguna internet tidak melanggar hukum yang ditetapkan. Pada 1996, pemerintah Tiongkok mengumumkan berlakunya Peraturan Administrasi Koneksi Informasi Komputer Internasional. Peraturan ini merupakan usaha nyata pertama dari pemerintah Tiongkok untuk membatasi akses internet. Tujuan peraturan ini adalah untuk memastikan bahwa penggunaan internet lintas batas negara hanya digunakan untuk "komunikasi informasi yang baik" (Shao 2012).

Pada tahun 1997, Tiongkok memberlakukan hukum kejahatan siber untuk pertama kalinya, dalam amandemen undang-undang kriminal mereka. Peraturan yang terkandung dalam amandemen ini secara umum mengatur mengenai kejahatan yang menargetkan jaringan komputer dan kejahatan yang dilakukan melalui jaringan komputer. Contoh kejahatan yang dilakukan melalui jaringan komputer adalah penyebaran konten

pornografi dan penyebaran rahasia negara (Keith and Lin 2006).

Pertama kali GFW digunakan untuk membatasi internet terjadi pada tahun 1998 ketika pemerintah Tiongkok mencegah mulai terbentuknya Partai Demokratis Tiongkok. Proyek GFW ini berlangsung hingga 2006 ketika sistem-sistem yang sudah ada dinilai sudah cukup memadai pada saat itu. Sistem yang digunakan dalam GFW sebenarnya buatan perusahaan Amerika, yaitu Cisco. Pada saat itu, Cisco ingin membuat sistem untuk memblokir situs-situs tertentu dalam perusahaan mereka agar karyawan mereka fokus bekerja. Setelah sukses membuat sistem tersebut, Cisco berniat menjual teknologi ini, salah satu yang berminat adalah pemerintah Tiongkok yang terpesona ketika melihat peragaan dari Cisco. Peralatan-peralatan dari Cisco ini segera dipasang di Tiongkok untuk memblokir situs-situs yang dianggap berbahaya oleh pemerintah Tiongkok (Goldsmith and Wu 2006).

Selain digunakan untuk mengendalikan komunikasi masyarakat, GFW juga digunakan sebagai bentuk proteksionisme perusahaan-perusahaan teknologi milik Tiongkok dari perusahaan luar. Sekarang, sudah tersedia alternatif Tiongkok dari berbagai situs dan layanan luar negeri. Tiga perusahaan terbesar yang terbantu pertumbuhannya dengan adanya GFW ini adalah Tencent, Alibaba, dan Baidu. Tencent merupakan situs media sosial yang menyediakan layanan video seperti YouTube dan juga layanan pesan pendek seperti Twitter, Baidu merupakan layanan mesin pencari seperti Google, dan Alibaba adalah situs belanja online yang serupa dengan Amazon (Dou 2015).

Namun, pemberlakuan GFW ini bertentangan dengan prinsip-prinsip demokrasi, yaitu transparansi dan akuntabilitas. Dengan adanya GFW, pemerintah Tiongkok memiliki kendali atas komunikasi dan penggunaan internet masyarakatnya sehingga pemerintah dapat membungkam kritik dari masyarakat dan membatasi kebebasan bersuara masyarakatnya. Dengan adanya GFW dan program serupa, Tiongkok sukses menjadi salah satu negara terkuat di dunia dan memiliki ekonomi yang berkembang pesat juga.

Dengan latar belakang di atas, artikel hendak membahas bagaimana GWF menjadi komponen strategis dalam mempertahankan otoritariansime Cina. Dalam metode penelitiannya, artikel ini menggunakan metode penelitian kualitatif. Metode ini bertujuan untuk menghasilkan suatu pemahaman yang mendalam mengenai dunia sosial partisipan penelitian dengan melakukan pengamatan sampel yang kecil namun dipilih karena menonjol, menggunakan metode pengumpulan data yang mendetail dan

lengkap, proses analisa yang terbuka pada konsep-konsep dan ide-ide baru, dan menggambarkan dunia sosial para partisipan penelitian (Snape and Spencer 2003). Lebih spesifik, artikel ini menggunakan pendekatan studi kasus, yakni penelitian yang mendalam terhadap suatu subjek, dokumen, atau fenomena yang spesifik (Bogdan and Biklen 2007) untuk mendeskripsikan dan menjelaskan fenomena tersebut dengan mengamatinya secara terfokus (Lune and Berg 2017).

Dalam konteks artikel ini, metode penelitian kualitatif ini dipilih karena ia dinilai paling cocok untuk membahas penerapan GFW yang memiliki dampak yang besar terhadap kehidupan masyarakat Tiongkok antara satu sama lain dan dengan masyarakat internasional. Pendekatan studi kasus dipilih karena ia memungkinkan kami menjelaskan GFW ini secara mendalam dan menghasilkan pandangan yang lebih lengkap tentang kasus ini.

Kajian Internet di Tiongkok

Penelitian mengenai penggunaan internet di Tiongkok dan penyensoran konten yang terjadi sudah banyak dilakukan dengan hasil dan fokus yang beragam. Salah satunya adalah "*Internet Censorship in China: Where Does the Filtering Occur?*" karya Xueyang Xu, Z. Morley Mao, dan J. Alex Halderman (2011). Penelitian mereka lebih mendalami sisi teknis penerapan GFW tersebut dengan menyelidiki metode-metode dan teknik-teknik apa saja yang diterapkan di Tiongkok untuk mengatur konten internet. Mereka menyimpulkan bahwa sebenarnya pemerintah Tiongkok mengandalkan perusahaan penyedia internet di Tiongkok untuk mengatur lalu lintas komunikasi internet dengan menggunakan peralatan pemblokir yang dipasang di daerah-daerah strategis (Xu *et* al. 2011).

Penelitian lainnya mengenai topik ini dilakukan oleh Crhistopher Stevenson (2007) dalam karyanya yang berjudul "*Breaching the Great China: China's Internet Censorship and the Quest for Freedom of Expression in a Connected World*". Dalam penelitian ini, Stevenson membandingkan kebijakan Tiongkok yang membatasi kebebasan di internet dan mengumpulkan data mengenai pengguna internet dengan kebijakan "*Global Online Freedom Act of 2006*" yang diajukan oleh Amerika Serikat yang mendukung keterbukaan dan kebebasan informasi di internet. Dalam kesimpulannya, Stevenson menyatakan bahwa internet harus bersifat terbuka agar dapat menjadi tempat bagi masyarakat untuk mengekspresikan diri dan mengakses informasi apa saja tanpa dibatasi oleh suatu pemerintahan tunggal. Stevenson juga menekankan pentingnya kerja

sama internasional untuk mewujudkan internet yang terbuka dan bebas (Stevenson 2007).

Penelitian serupa dilakukan oleh Steve Guo dan Guangchao Feng (2011) dalam artikel jurnal yang berjudul "*Understanding Support for Internet Censorship in China: An Elaboration of the Theory of Reasoned Action*". Dalam penelitian tersebut, mereka mengadakan survei pada beberapa pemuda di Tiongkok mengenai pendapat mereka tentang penyensoran internet yang terjadi. Hasil survei mereka menyatakan bahwa pendapat para pemuda Tiongkok cukup beragam berdasarkan pada komunitas yang ditanyakan. Namun, hasil survei ini menyatakan bahwa ada sentimen negatif terhadap penyensoran internet, bahkan jumlah suara yang menolak penyensoran ini juga cenderung meningkat dibanding tahun-tahun sebelumnya. Mereka juga mengakui dua kekurangan utama dalam survei mereka, yaitu kurangnya sampel yang digunakan dan adanya pemilihan kata yang kurang cocok berpotensi mengarahkan partisipan survei menyatakan bahwa mereka mendukung penyensoran (Guo and Feng 2011).

Penelitian yang mendalami mengenai mengapa terjadi krisis demokrasi di Tiongkok dilakukan oleh Trissia Wijaya (2015) dalam artikelnya yang berjudul "*Democracy Deficit in China: A Choice or Foreordained*". Penelitiannya ini mendalami faktor-faktor yang mempengaruhi suksesnya pemerintah Tiongkok menekan keinginan rakyatnya akan perubahan demokratis dan kebebasan. Dalam kesimpulannya, Wijaya menyimpulkan bahwa faktor utama fenomena ini adalah historis dan kebudayaan di Tiongkok yang belum pernah mengalami masa pemerintahan yang demokratis. Selain itu, pemerintah Tiongkok juga memiliki visi tersendiri dalam membangun Tiongkok menjadi salah satu negara besar di dunia sehingga mendapat dukungan juga dari masyarakatnya yang sebagian besar sudah merasa bahwa sistem demokrasi tidak cocok diterapkan di Tiongkok (Wijaya 2015).

Penelitian lain juga dilakukan oleh Bin Liang dan Hong Lu (2010) dalam artikelnya yang berjudul "*Internet Development, Censorship, and Cyber Crimes in China*". Dalam penelitian ini, mereka mendalami mengenai perkembangan penggunaan internet di Tiongkok dan dampaknya terhadap perkembangan Tiongkok secara keseluruhan. Mereka menyimpulkan bahwa strategi pemerintah Tiongkok telah sukses mengatur alur informasi yang beredar di Tiongkok dan terlihat berdampak positif bagi perkembangan Tiongkok. Namun, karena pemerintah Tiongkok terlalu terfokus mengendalikan diskusi politik yang terjadi, masalah kejahatan

siber, terutama pornografi dan perjudian, menjadi semakin muncul dalam masyarakat Tiongkok (Liang and Lu 2010).

Selain dari beberapa penelitian yang sudah disebutkan sebelumnya, masih ada beberapa penelitian lain mengenai penyensoran konten internet di Tiongkok. Namun, penelitian-penelitian ini sering membahas mengenai peran penyensoran yang menghalangi terjadinya revolusi demokrasi di Tiongkok, atau analisa mengenai teknik-teknik dan teknologi-teknologi yang digunakan untuk melakukan penyensoran tersebut. Karena itu, artikel ini membahas bagaimana GFW membentuk Tiongkok menjadi sebuah *maximalist state* yang kuat melalui penguasaan *cybersecurity*.

Dalam metode penelitiannya, artikel ini menggunakan metode penelitian kualitatif. Metode ini bertujuan untuk menghasilkan suatu pemahaman yang mendalam mengenai dunia sosial partisipan penelitian dengan melakukan pengamatan sampel yang kecil namun dipilih karena menonjol, menggunakan metode pengumpulan data yang mendetail dan lengkap, proses analisa yang terbuka pada konsep-konsep dan ide-ide baru, dan menggambarkan dunia sosial para partisipan penelitian (Snape and Spencer 2003). Lebih spesifik, artikel ini menggunakan pendekatan studi kasus, yakni penelitian yang mendalam terhadap suatu subjek, dokumen, atau fenomena yang spesifik (Bogdan and Biklen 2007) untuk mendeskripsikan dan menjelaskan fenomena tersebut dengan mengamatinya secara terfokus (Lune and Berg 2017).

Dalam konteks artikel ini, metode penelitian kualitatif ini dipilih karena ia dinilai paling cocok untuk membahas penerapan GFW yang memiliki dampak yang besar terhadap kehidupan masyarakat Tiongkok antara satu sama lain dan dengan masyarakat internasional. Pendekatan studi kasus dipilih karena ia memungkinkan kami menjelaskan GFW ini secara mendalam dan menghasilkan pandangan yang lebih lengkap tentang kasus ini.

***Cyberpower* dan *Cybersecurity* Sebagai Kerangka Analisis**

Power (kekuasaan) secara umum dapat dijelaskan sebagai hubungan antara suatu aktor dengan aktor yang lainnya. Dalam hubungan internasional, *power* merujuk pada bagaimana suatu negara dapat memanfaatkan sumber daya yang dimilikinya untuk mempengaruhi perilaku aktor lain (Anderson 2005). Dalam mengukur kuatnya suatu negara, ada beberapa cara yang dapat digunakan sebagai alat ukur. Salah satunya adalah GDP negara, karena GDP negara dapat memperhitungkan ukuran negara, tingkat kemajuan teknologi, dan kekayaan negara. Namun, menggunakan GDP

sebagai alat ukur kekuatan suatu negara tidak menghasilkan hasil yang akurat, karena kekuatan suatu negara juga dapat bersumber dari hal-hal yang bersifat non materialistis (Goldstein and Pevehouse 2014).

Oleh karena itu, perlu cara lain untuk menilai kekuatan suatu negara. Untuk itu, Hans Morgenthau (1948) menggagas menilai kekuatan suatu negara berdasarkan beberapa elemen yang membentuk negara kuat. Morgenthau menilai kekuatan berdasarkan delapan elemen, yaitu geografi yang mendukung, sumber daya yang berlimpah, kemampuan industri yang mampu memproses sumber daya negara, kemampuan militer yang mumpuni, jumlah populasi yang berkualitas, karakter negara yang positif, semangat juang yang kuat, dan diplomasi yang berkualitas. Dalam mengembangkan berbagai elemen kekuatan tersebut, teknologi yang maju juga merupakan pendukung yang memungkinkan suatu negara memaksimalkan elemen-elemen kekuatan tersebut. Dengan demikian, teknologi yang maju juga menandakan negara yang sudah kuat (Morgenthau 1948).

Namun, di era teknologi ini, negara-negara juga beraktivitas dalam dunia maya atau *cyberspace*. Joseph Nye mengagas istilah "*cyberpower*", yaitu sekumpulan sumber daya yang berhubungan dengan pembuatan, pengendalian, dan komunikasi elektronik dan infrastruktur, jaringan, *software* (perangkat lunak), serta sumber daya manusia yang mendukungnya. *Cyberpower* juga dapat dijelaskan sebagai kemampuan suatu negara mendapatkan suatu hasil dengan memanfaatkan keterhubungan informasi dalam *cyberspace* sehingga kekuatan suatu negara dalam *cyberspace* dapat dilihat dari *cyberpower*-nya (Nye 2011).

Dalam konteks *cyberspace*, suatu negara kuat harus dapat mengamankan dirinya dari serangan yang berada di dalam maupun di luar *cyberspace* tersebut. Untuk itu, suatu negara dapat memanfaatkan instrumen TIK maupun instrumen fisik. Dari dalam *cyberspace*, suatu negara dapat memanfaatkan instrumen TIK berupa serangan *denial of service* (DOS) yang bertujuan melumpuhkan suatu situs atau server tertentu sehingga tidak dapat diakses, atau memanfaatkan instrumen fisik berupa kendali pemerintah atas perusahaan-perusahaan dan aktor non negara yang terlibat dalam *cyberspace* tersebut. Sedangkan di luar *cyberspace*, instrumen TIK yang dapat dimanfaatkan negara adalah serangan terhadap sistem-sistem industri suatu negara, atau memanfaatkan instrumen fisiknya untuk menghancurkan server target mereka dan memutuskan kabel koneksi lawannya (Nye 2011).

Cyberpower suatu negara berasal dari beberapa faktor. Faktor pertama

berkaitan dengan kondisi negara tersebut, terutama geografi dan kebijakan. Karena pengadaan internet dan peralatan TIK lainnya tetap memerlukan peralatan fisik, pemerintah negara masih berdaulat atas geografi lokasi peralatan tersebut diadakan. Pemerintah negara juga dapat menerapkan kebijakan-kebijakan tertentu yang memudahkan akses ke *cyberspace* seperti pendidikan TIK, subsidi infrastruktur, dan perlindungan hak cipta. Pemerintah negara juga dapat menghambat akses informasi dengan menerapkan penyensoran, memblokir koneksi tertentu, dan pengawasan komunikasi jaringan.

Faktor yang kedua berkaitan dengan sumber daya yang dimiliki oleh suatu negara. Suatu negara yang memiliki ekonomi yang kuat dan pasar TIK yang besar akan lebih kuat dibandingkan dengan negara yang tidak memilikinya karena negara tersebut dapat lebih memaksa aktor-aktor lain untuk menyesuaikan diri dengan kebutuhan mereka. Suatu negara juga harus memiliki sumber daya manusia yang mumpuni untuk mempertahankan negaranya dari serangan-serangan ini dan juga melancarkan serangan jika dibutuhkan. Tentunya, sumber daya manusia ini juga harus didukung dengan peralatan yang baik juga, sehingga negara yang memberikan anggaran lebih pada sektor *cybersecurity*-nya juga akan semakin kuat (Nye, 2011).

Tim Jordan menjelaskan bahwa *cyberpower* terdiri dari tiga bagian yang saling berhubungan. Bagian pertama *cyberpower* berupa kekuatan yang dimiliki masing-masing individu. Kekuatan individu dalam *cyberspace* terjadi ketika mereka diberikan peralatan dan kesempatan untuk mengakses dan memanfaatkan informasi-informasi dari *cyberspace* dalam kehidupan mereka. Seiring berjalannya kehidupan mereka, informasi-informasi tersebut semakin bertambah jumlahnya sehingga menjadi semakin rumit untuk digunakan oleh masyarakat awam. Oleh karena itu, terbentuk bagian kedua dari *cyberpower* ketika beberapa individu yang lebih ahli dalam bidang teknologi ini membentuk kelompok sendiri yang bertujuan untuk membuat teknologi untuk memudahkan masyarakat untuk memproses informasi yang rumit tersebut sehingga mereka menjadi kelompok elite sendiri. Dalam bagian kedua *cyberpower* ini, kekuatan didominasi oleh kelompok elite ini karena mereka yang dapat memahami cara memproses informasi dari *cyberspace* tersebut dan mendorong teknologi tertentu untuk menjadi standar yang digunakan dalam kehidupan sehari-hari masyarakat umum. Namun, setiap kali kaum elite ini mengubah cyberspace dengan memberikan cara-cara baru untuk memproses informasi dari *cyberspace*, masyarakat umum yang menggunakan teknologi-teknologi tersebut menjadi paham cara memproses informasi dengan cara baru ini.

Ketika masyarakat umum sudah terbiasa dengan cara-cara baru ini, mereka akan mulai memanfaatkannya dalam kehidupan mereka sehari-hari lagi dan memunculkan informasi-informasi baru yang lebih rumit lagi. Akibatnya, kaum elite harus membentuk cara-cara baru lagi untuk memproses informasi-informasi baru ini, dan demikian siklus ini terus berulang (Jordan 2003).

Siklus tersebut menyebabkan adanya perubahan yang tidak dapat dihentikan dalam *cyberspace*. Perubahan yang terus menerus ini memicu imajinasi semua orang yang berada dalam *cyberspace* tersebut. Imajinasi ini merupakan bagian ketiga dari *cyberpower*. Karena *cyberspace* bersifat lebih luas dan menjangkau lebih banyak masyarakat, suatu imajinasi atau visi yang muncul dalam *cyberspace* dapat dengan cepat menjadi impian dan visi keseluruhan masyarakat dalam *cyberspace* tersebut. Impian bahwa inovasi selanjutnya berpotensi membawa peningkatan mendorong individu untuk mengadopsi teknologi baru dalam kehidupannya, kemudian mendorong para elite untuk segera membuat inovasi baru untuk membawa masyarakat lebih dekat kepada visi tersebut dan memicu terjadinya siklus yang membawa perubahan dalam *cyberspace* (Jordan 2003). Jika ada suatu negara yang ingin mengembangkan *cyberpower*, maka negara tersebut harus memberikan akses pada *cyberspace* yang mudah untuk masyarakatnya dan memberikan dukungan pada para ahli teknologi di negaranya untuk berinovasi dan berkreasi, sambil mengarahkan visi masyarakat agar sesuai dengan kepentingannya (Jordan 2003).

Selain itu, konsep penting lain yang bisa digunakan untuk menjelaskan masalah penelitian ini adalah *cybersecurity*. *Cybersecurity* dapat diartikan sebagai keamanan dan pengamanan sistem jaringan-jaringan komputer. *Cybersecurity* dapat dijelaskan dengan mengenali tujuan-tujuan adanya *cybersecurity*, yakni pencegahan, pendeteksian, respons (*prevent, detect, respond)*; orang, proses, teknologi (*people, process, technology*); dan kerahasiaan, integritas, ketersediaan (*confidentality, integrity, and availability*). Target-target ini menggambarkan tujuan keperluan adanya *cybersecurity* dan juga menjelaskan metode dan mekanisme yang diperlukan untuk mencapai *cybersecurity* (Bayuk et al. 2012).

Pencegahan, pendeteksian, dan respons mengacu pada target-target yang ada pada keamanan fisik dan *cybersecurity*. Untuk mewujudkan keamanan, kita harus dapat mencegah semua serangan yang datang. Namun, tidak semua serangan dapat kita cegah. Karena itu, serangan harus dapat dideteksi dengan cepat sebelum dapat menyebabkan kerusakan yang substansial. Setelah suatu serangan dideteksi, perlu ada respons yang menghentikan serangan tersebut. Dalam konteks keamanan fisik, tahap

respons ini biasanya ditangani oleh orang-orang dengan profesi tertentu (seperti polisi atau tenaga medis) yang menghentikan serangan, menangani korban, dan mengamankan aset yang dirusak. Dalam konteks *cybersecurity*, tahap respons ini digantikan dengan tahap perbaikan. Tahap perbaikan ini bertujuan untuk mengidentifikasi kelemahan dalam sistem tersebut dan memperbaikinya agar sistem tersebut lebih kuat menangkal serangan lain dan juga untuk memulihkan sistem yang sempat dirusak. Tahap pencegahan, pendeteksian, dan respons/perbaikan ini membentuk suatu siklus yang lama kelamaan akan membentuk sistem *cybersecurity* yang lebih kuat (Bayuk et al. 2012).

Orang, proses, dan teknologi merujuk pada metode-metode yang digunakan dalam ilmu manajemen dan *cybersecurity*. Kombinasi ini mengamati orang-orang yang mengoperasikan sistem, dan para operator ini perlu mengikuti prosedur yang sudah ada untuk melaksanakan suatu tugas. Dalam konteks keamanan, kombinasi ini menyatakan bahwa keamanan tidak terwujud hanya oleh ahli keamanan saja. Sedangkan dalam konteks *cybersecurity*, keamanan tidak terwujud hanya dengan teknologi saja. Dalam usaha mengamankan suatu sistem, perlu adanya faktor manusia yang mengoperasikan sistem tersebut dan tidak semua individu yang menggunakan sistem tersebut memahami bagaimana cara menerapkan kombinasi pencegahan, pendeteksian, dan respons/perbaikan seperti yang dijelaskan sebelumnya. Karena itu, para ahli *cybersecurity* diharapkan dapat menyematkan program dan prosedur *cybersecurity* ke dalam proses operasional suatu sistem dan menggunakan teknologi yang ada secara strategis untuk mendukung tujuan-tujuan *cybersecurity* (Bayuk et al. 2012).

Kerahasiaan, integritas, dan ketersediaan secara spesifik mengarah pada peran *cybersecurity* yang berhubungan dengan informasi. Kerahasiaan merujuk pada kemampuan suatu sistem untuk membatasi persebaran informasi tertentu. Integritas merujuk pada kemampuan suatu sistem untuk memastikan keaslian, akurasi, dan sumber dari suatu informasi yang dimasukkan. Ketersediaan merujuk pada seberapa tepat waktu suatu sistem dapat menyampaikan suatu informasi. Target-target keamanan ini sudah diterapkan sejak sebelum diciptakannya komputer, namun metode yang digunakan dan masalah yang muncul dalam konteks *cybersecurity* berbeda dari pemahaman yang sebelumnya. Dalam konteks *cybersecurity*, sering kali kombinasi dari tiga target ini saling berlawanan. Misalnya, dalam usaha meningkatkan ketersediaan informasi, perlu ada kompromi dalam kerahasiaan. Salah satu tugas bagi para ahli *cybersecurity* adalah menentukan keseimbangan dari kerahasiaan, integritas, dan ketersediaan informasi ini (Bayuk et al. 2012).

Setelah melihat penjelasan dari ketiga kombinasi target yang menjadi tujuan utama penerapan *cybersecurity*, dapat disimpulkan definisi *cybersecurity* adalah sekumpulan metode memanfaatkan orang, proses, dan teknologi untuk mencegah, mendeteksi, dan memperbaiki kerusakan kerahasiaan, integritas, dan ketersediaan informasi dalam *cyberspace*. Choucri (2012) menjelaskan *cybersecurity* sebagai salah satu dimensi dari keamanan nasional. Keamanan nasional terbagi dalam empat dimensi, yaitu keamanan eksternal, keamanan internal, keamanan lingkungan, dan *cybersecurity*. Konsep keamanan empat dimensi ini muncul dari pemikiran bahwa ancaman yang dihadapi negara sudah lebih dari hanya ancaman militer dari negara lain saja, melainkan ada juga aktor-aktor lain yang perlu diperhatikan. Menurutnya, sebuah negara baru dapat disebut aman ketika sudah memenuhi keempat dimensi ini (Choucri 2012).

Cybersecurity adalah kemampuan suatu negara melindungi dirinya dan institusi-institusi di dalamnya dari ancaman spionase, sabotase, kejahatan, penipuan, pencurian identitas, dan interaksi digital lainnya yang bertujuan merusak. Karena setiap orang yang memiliki akses kepada *cyberspace* ini dapat menyuarakan suatu pesan dengan bebas, suatu negara perlu perhatian lebih dalam menghadapi ancaman *cybersecurity* sebab jumlah ancaman yang mungkin terjadi lebih banyak dibandingkan dimensi keamanan lainnya. *Cybersecurity* juga bersifat meliputi keseluruhan lapisan sosial masyarakat sehingga agar suatu negara dapat mengamankan *cybersecurity* secara total, negara tersebut harus dapat mengendalikan keseluruhan akses masyarakatnya terhadap *cyberspace* ini (Choucri 2012).

Seperti yang sudah disebutkan sebelumnya, aktor yang dapat mengancam *cybersecurity* sangat beragam dan dapat berasal dari mana saja. Namun, ancaman-ancaman *cybersecurity* dapat dikelompokkan menjadi empat kategori berdasarkan potensi merusaknya, yaitu *hacking*, kejahatan terorganisasi, ekstremisme politik dan ideologi, dan agresi *cyber* yang disponsori negara.

Pertama, *hacking*. *Hacking* merupakan aktivitas yang dilakukan seorang ahli untuk menyusupi suatu sistem jaringan komputer. Kategori hacking ini biasanya dilakukan oleh seorang individu atau kelompok kecil dan merupakan kategori yang paling tidak mengancam dari keempat kategori ini. Beberapa ahli dalam bidang *cybersecurity* berargumen bahwa *hacking* perlu ada sebagai penguji ketahanan suatu sistem. Selain itu, sering kali juga aktivitas *hacking* ini dilakukan bukan dengan tujuan untuk merusak, tapi untuk mempelajari suatu sistem atau untuk menguji keahlian pelakunya. Walaupun memang ada beberapa pelaku *hacking* yang

bertujuan untuk merusak, biasanya kerusakan yang disebabkan oleh seorang individu tidak terlalu signifikan sehingga tidak menimbulkan kerugian yang besar.

Kedua, kejahatan terorganisasi. Sejak internet mulai digunakan untuk melakukan transaksi finansial dan properti intelektual, mulai muncul juga para kriminal yang ingin mencuri dari transaksi tersebut. Sebagian besar aksi kejahatan dalam kategori bertujuan untuk mendapatkan keuntungan finansial. Kategori ini biasanya dilakukan oleh organisasi kejahatan yang sudah bersifat transnasional dan dapat berada dimana-mana. Contoh kejahatan yang termasuk dalam kategori ini adalah penipuan kartu kredit, pencurian data perbankan, pembajakan film, dan lain-lain.

Ketiga, ancaman ekstremisme politik dan ideologi. Karena internet dapat diakses oleh siapa saja dan dapat digunakan untuk menyebarkan segala jenis pesan, tidak heran jika muncul kaum ekstremis yang menyampaikan pesan mereka. Karena internet memiliki latar belakang sebagai alat militer, kaum ekstremis ini juga dapat memanfaatkan fitur-fitur militeristis yang dimiliki internet yaitu anonimitas dan keandalan. Selain dengan banyaknya situs yang menawarkan layanan media sosial, semakin mudah juga bagi para kaum ekstremis ini untuk merekrut semakin banyak pengikut. Selain menjadikan alat untuk merekrut anggota, internet dan cyberspace juga dijadikan arena perang virtual bagi para ekstremis ini, seperti kasus Imam Samudra yang sudah disinggung sebelumnya. Kaum ekstremis dapat menargetkan serangan terhadap suatu negara atau badan lainnya yang mereka anggap sebagai musuh mereka.

Keempat, agresi *cyber* yang disponsori negara. Ancaman dalam kategori ini termasuk yang paling berbahaya karena sumber daya yang dimiliki suatu negara akan lebih besar dibandingkan dengan yang dimiliki individu atau organisasi yang relatif kecil. Karena semua negara semakin mengandalkan internet dalam aktivitas sehari-harinya, serangan skala besar terhadap suatu negara berpotensi melumpuhkan negara tersebut secara signifikan. Salah satu negara yang sangat pesat mengembangkan kemampuan serangan *cyber* mereka adalah Tiongkok. Bahkan menurut laporan dari rapat kongres di Amerika Serikat menilai bahwa Tiongkok merupakan negara yang sudah siap melakukan *cyber war* (Cornish 2009).

Selain menghadapi ancaman-ancaman tersebut, dalam rangka mengamankan *cyberspace*, suatu negara juga menghadapi kritik dari segi hak asasi manusia. Sebagaimana tertulis dalam Pernyataan Umum tentang Hak-Hak Asasi Manusia tahun 1948, salah satu hak asasi manusia adalah hak untuk mencari, mendapatkan, dan menyebarkan informasi melalui

segala jenis media. Namun, hak ini terkadang bertentangan dengan upaya-upaya suatu negara dalam mencapai *cybersecurity*.

Negara-negara yang sudah kuat dalam bidang *cybersecurity* seperti Amerika Serikat atau Tiongkok sering mengalami kritik bahwa kebijakan mereka dalam mencapai *cybersecurity* menghalangi hak asasi masyarakatnya. Amerika Serikat dikritik karena melakukan pengawasan yang berlebihan pada rakyatnya, sedangkan Tiongkok dikritik karena memiliki kebijakan penyensoran yang sangat ketat sehingga membatasi arus informasi di masyarakatnya.

Namun, penerapan kebebasan berpendapat tersebut juga berbeda tergantung kebudayaan setiap negara. Dalam beberapa kebudayaan, mengkritik pemerintah mungkin merupakan suatu hal yang normal, tapi menjadi tabu dalam kebudayaan lain. Setiap negara harus menentukan kebijakan yang sesuai dengan kebudayaan negara mereka. Dalam rezim pemerintahan yang lebih ketat, wajar saja jika kebebasan internet dipandang sebagai sesuatu yang berpotensi merendahkan pemerintahan yang sedang berkuasa. Akibatnya, kebijakan seperti penyensoran atau pengawasan yang lebih ketat pada masyarakat dipandang perlu untuk memastikan pemerintah tetap memegang kuasa atas masyarakat (Singer and Friedman 2014).

Dengan konsep *cyberpower* dan *cybersecurity*, artikel ini mencoba memahami bagaimana GFW diterapkan dan apa dampaknya kekuasaan negara Tiongkok atas masyarakatnya dan terhadap komunitas internasional. Konsep *cybersecurity* ini dipilih karena GFW merupakan program yang diberlakukan untuk mengatur aktivitas internet di Tiongkok. Selain itu, diskusi mengenai kebebasan berinternet yang dibatasi oleh GFW juga merupakan salah satu topik dalam *cybersecurity*.

Dengan konsep *cybersecurity*, artikel ini menjelaskan aktor-aktor yang terlibat dan penerapan GFW, apa tujuan dibentuknya GFW tersebut, apa saja yang dianggap berbahaya oleh pemerintah Tiongkok, dampak GFW terhadap aktivitas internet di Tiongkok, dan bagaimana GFW dapat melindungi dan memperkuat kekuasaan pemerintah Tiongkok.

GFW, *Cybersecurity* dan *Cyberpower*

Sebagaimana pendapat Choucri (2012), dunia *cyber* merupakan salah satu dari empat dimensi keamanan sehingga suatu negara tidak dapat hanya mengandalkan dimensi-dimensi kekuatan tradisional saja. Oleh karena itu, Tiongkok juga merasa perlu memperkuat sisi *cyber* dari negara mereka untuk menyamai *cyberpower* Amerika Serikat. Dalam usahanya untuk

menjadi negara kuat dalam cyberspace, Republik Rakyat Tiongkok telah berusaha untuk memicu inovasi dan kemajuan teknologi di negaranya.

Instrumen Cyberpower Tiongkok

Tiongkok telah menerapkan sebuah strategi yang dinamakan "*China Broadband Strategy*" yang bertujuan untuk menyediakan internet yang lebih cepat dengan harga terjangkau ke seluruh penjuru negaranya. Salah satu buah dari strategi tersebut adalah peningkatan jaringan menjadi jaringan 5G dan peralihan dari koneksi tembaga ke koneksi fiber. Peningkatan kecepatan jaringan ini terus berkembang drastis dengan peningkatan hingga 50% per tahun. Tidak hanya kecepatan, luasnya jaringan internet di Tiongkok juga sudah mencapai 97,4% negaranya, termasuk daerah pedesaan terpencil. Dengan luasnya cakupan jaringan ini, pada tahun 2018, Tiongkok menjadi negara dengan pengguna internet terbanyak kedua di dunia dengan total 338 juta komputer yang aktif terhubung ke internet (Chinese Academy of Cyberspace Studies 2018).

Selain meningkatkan teknologi yang sudah ada, Tiongkok juga aktif mengembangkan teknologi-teknologi baru. Pada tahun 2017, Tiongkok mengajukan sebanyak 3,7 juta hak paten dalam bidang TIK, membuatnya sebagai negara dengan pengajuan hak paten terbanyak kedua di dunia dan ditetapkan sebagai negara terinovatif ke-17 oleh WIPO. Pada 2018, Tiongkok juga menyelesaikan proyek pembangunan superkomputernya[1] yang bernama Tianhe 3. Kemajuan ini memungkinkan perusahaan-perusahaan TIK di Tiongkok memanfaatkan komputer tersebut untuk melakukan riset dalam berbagai bidang seperti AI, big data, dan *cloud computing*. Sistem-sistem buatan Baidu, Alibaba, dan Tencent juga sudah diterapkan dalam berbagai aplikasi seperti teknologi *smart city* dan layanan kesehatan (Chinese Academy of Cyberspace Studies 2018).

Dalam laporan yang dibuat pada tahun 2018, Tiongkok menyatakan bahwa kecemasan utamanya pada masa ini adalah serangan DOS, virus komputer, dan celah keamanan yang baru ditemukan dalam sistem-sistem komputer yang sedang beroperasi. Untuk menghalau ancaman-ancaman tersebut, Tiongkok melakukan beberapa hal. Salah satunya adalah menyempurnakan pertahanan *cybersecurity* mereka dari sisi administrasi dengan hukum *cybersecurity* yang lebih jelas, melakukan reformasi komite keamanan *cyber*, mengkaji dan menetapkan standar keamanan *cyber* pada perusahaan-perusahaan Tiongkok, dan menetapkan protokol-protokol darurat untuk menanggulangi kejadian serangan *cyber* dan kebocoran data. Selain itu, Tiongkok juga mendukung kemajuan perusahaan-perusahaan *cybersecurity* dan menggunakan layanan perusahaan-perusahaan tersebut

[1] Superkomputer adalah komputer yang performanya jauh lebih tinggi dibandingkan komputer biasa, biasanya digunakan untuk penelitian saintifik.

untuk meningkatkan *cybersecurity* di Tiongkok. Pada tahun 2017, perusahaan-perusahaan *cybersecurity* ini mendapatkan keuntungan rata-rata hingga 256 juta Yuan, sedangkan total keuntungan diperkirakan mencapai 2 miliar Yuan. Jumlah keuntungan terbesar dipegang oleh Venustech, Weston, Bluedon, Lanxum, dan Sangfor. Perusahaan-perusahaan ini juga menerima bantuan dari pemerintah pusat berupa insentif, sehingga memungkinkan mereka untuk meningkatkan pengeluaran untuk riset. Teknologi-teknologi yang menjadi fokus mereka pada saat ini adalah penggunaan AI untuk membantu pengamanan, pengamanan data yang lebih ketat, dan transisi ke sistem *cloud computing*. Pemerintah Tiongkok juga mengajak rakyatnya untuk berpartisipasi dalam membangun *cybersecurity* yang lebih kuat melalui berbagai program seperti penghargaan khusus bagi peneliti *cybersecurity* yang berbakat, melakukan publisitas mengenai pentingnya *cybersecurity*, memudahkan akses pelajaran mengenai *cybersecurity* dan hukum *cyber*, dan mengadakan konferensi dan kompetisi *hacking* untuk memicu inovasi dan mencari talenta-talenta baru (Chinese Academy of Cyberspace Studies 2018).

Dalam usaha mengimbangi kemampuan militer Amerika Serikat, Tiongkok sangat banyak menuangkan sumber daya dalam memperkuat *cybersecurity* dan mempersiapkan dirinya menghadapi perang dalam *cyberspace*. Tiongkok sudah memiliki 12 kelompok tentara *cyber* untuk melakukan serangan *cyber* kepada Amerika Serikat dengan mengumpulkan informasi-informasi penting dari pemerintah dan berbagai perusahaan Amerika. Bahkan, Tiongkok sudah menyiapkan badan khusus untuk mengamankan *cyberspace* negaranya sekaligus untuk melaksanakan serangan jika dibutuhkan, yaitu *Technical Reconnaissance Bureau* (TRB) yang bermarkas di Chengdu. Dengan mempertimbangkan berbagai kemajuan ini, para ahli *cybersecurity* menyatakan bahwa Tiongkok adalah negara yang paling maju dalam bidang *cybersecurity* (Andress and Winterfeld 2014).

Kebijakan dan Aturan yang Membentuk GFW

Sejak masuknya layanan internet di Tiongkok pada tahun 1994, pemerintah Tiongkok sudah menetapkan beberapa batasan dan aturan yang bertujuan untuk mengatur kemudahan berinternet, menjaga hak dan keamanan rakyat Tiongkok, dan mengatur informasi yang beredar melalui internet tersebut. Untuk itu, Tiongkok telah membentuk hukum-hukum yang mengatur berbagai kegiatan di internet.

Pada tahun 1996, pemerintah pusat Tiongkok menetapkan hukum *Provisional Regulations for the Administration of International Connection*

of Computer Information Network, yang merupakan hukum pertama dari pemerintah Tiongkok untuk mengatur informasi di internet. Hukum ini bertujuan untuk mengatur arus informasi yang berhubungan dengan jaringan luar negeri. Hukum ini juga bertujuan untuk mendukung perkembangan transaksi informasi (Shao 2012). Kemudian, pada tahun 1997, Tiongkok pertama kali mendefinisikan jenis-jenis kejahatan cyber dalam hukum yang dikenal dengan *Criminal Law* 1997 (CL97). Kejahatan yang dijelaskan dalam CL97 terbagi menjadi dua kategori, yaitu penyebaran konten pornografi dan penyebaran rahasia negara. Pada waktu itu, CL97 dikritik oleh para ahli hukum di Tiongkok yang mengatakan bahwa CL97 tidak efektif dan tidak dapat ditegakkan. Namun, pemerintah Tiongkok mengatakan bahwa CL97 sengaja dibuat fleksibel agar dapat bebas diinterpretasikan sesuai dengan perkembangan jaman. CL97 inilah yang menjadi dasar berbagai pemblokiran konten di internet dan menjadi hukum yang biasanya digunakan dalam kasus yang melibatkan GFW. Fleksibilitas yang diterapkan dalam pembuatan CL97 juga telah memunculkan interpretasi baru hukum ini. Karena itu, CL97 di masa modern juga sering dikaitkan dengan kasus apa pun yang dianggap menyebarkan "pengaruh negatif" bagi masyarakat (Keith and Lin 2006).

Hukum mengenai kontrol di internet kemudian diperbarui pada September 2000 dengan hukum *Telecommunications Regulations* dan *Adminstrative Measures for Internet Information Services* yang menetapkan internet sebagai alat telekomunikasi, sehingga aktivitas di internet dapat diawasi sebagaimana alat telekomunikasi lainnya. Hukum ini juga mengatur secara lebih spesifik mengenai syarat-syarat administrasi bagi orang yang ingin mengakses internet, mendirikan badan publikasi *online*, aturan mengenai penerbitan konten *online*, dan mengenai proses pendaftaran situs web di Tiongkok. Pemberlakuan hukum ini memberikan pemerintah Tiongkok yurisdiksi atas aktivitas internet di Tiongkok. Akibatnya, berbagai badan pengawas yang mengawasi konten dalam media tradisional juga mulai berhak mengatur konten yang beredar di internet (Shao 2012).

Lalu, kumpulan hukum-hukum yang sudah ada tersebut digabungkan dan diperbarui menjadi *Decision on Safeguarding Internet Security*. Secara umum, hukum ini melarang masyarakat Tiongkok untuk menyerang sistem komputer milik pemerintah dengan virus maupun serangan fisik, mengadakan atau memutuskan hubungan internet tanpa izin pemerintah, menggunakan internet untuk menyebarkan rumor atau memfitnah dengan tujuan menggulingkan pemerintah yang sedang menjabat, menyebarkan informasi rahasia, memicu perpecahan antar kelompok, menjalankan bisnis

ilegal, menyebarkan pornografi, dan menyebarkan rahasia pribadi orang lain tanpa persetujuan. Hukum ini ditegakkan melalui proses yang sama dengan proses hukum pidana. Tujuan utama penerapan hukum ini adalah untuk menjaga keamanan nasional, menjaga keteraturan sosial, dan menjaga hak setiap individu maupun perusahaan (Shao 2012).

Pada November 2016, Republik Rakyat Tiongkok memperbarui lagi hukum *cybersecurity* mereka. Hukum baru ini lebih menekankan pada kedaulatan Tiongkok dalam dunia *cyber*. Dengan hukum ini, pemerintah Tiongkok ingin menerapkan hukum yang menjadi dasar hukum mereka untuk menjaga kedaulatan mereka sambil juga melindungi hak dan kewajiban masyarakatnya. Hukum yang terbaru ini lebih banyak mengatur mengenai bagaimana untuk mengelola data-data yang beredar dalam *cyberspace*.

Bagian pertama hukum tersebut mengatur peran penyedia layanan internet. Pihak yang dimaksud penyedia layanan internet adalah penyedia internet dan juga semua perusahaan yang menyediakan layanan *online*. Hukum ini mengharuskan para penyedia layanan untuk mematuhi hierarki pertahanan *cyber* yang berlaku sehingga setiap perusahaan berkewajiban untuk berpartisipasi dan membantu melindungi kedaulatan Republik Rakyat Tiongkok. Selain itu, para penyedia layanan juga harus membuka produk yang mereka sediakan untuk diaudit oleh pemerintah dalam rangka memastikan bahwa produk yang mereka sediakan tetap memenuhi standar *cybersecurity* Tiongkok. Hukum ini juga mengharuskan bahwa para penyedia layanan menyimpan identitas asli para penggunanya dan menjaga keamanan data tersebut (Qi *et al*. 2018).

Hukum yang baru ini juga membahas mengenai perlindungan data pribadi para pengguna internet di Tiongkok. Karena para pengguna internet di Tiongkok diharuskan untuk memberikan identitas asli mereka untuk menggunakan berbagai layanan internet, keamanan data pribadi mereka harus terjamin. Hukum ini mengharuskan para penyedia layanan untuk menjelaskan dengan baik tujuan pengumpulan data, data apa saja yang dikumpulkan, dan perlu ada izin secara eksplisit dari penggunanya. Para penyedia layanan juga tidak diperbolehkan memberikan data pengguna ke perusahaan lain tanpa sepengetahuan penggunanya. Jika suatu penyedia layanan memberikan data pengguna ke pihak lain atau jika mereka mengalami kebocoran data, maka penyedia layanan tersebut akan diproses secara hukum dan dapat didenda hingga 4% dari keuntungan perusahaan. Selain itu, hukum ini juga mengharuskan para penyedia layanan untuk memberikan kesempatan bagi pengguna untuk merevisi atau menghapus data yang sudah berikan (Qi *et al*. 2018).

Aktor yang Terlibat dalam Pembentukan GFW

Proyek GFW dan penyensoran media secara umum di Tiongkok merupakan gagasan dari pemerintah pusat yang sedang menjabat di Tiongkok, yaitu dari Partai Komunis Tiongkok. Lebih spesifik lagi, ada beberapa badan pemerintah Tiongkok yang terlibat dalam penerapan GFW ini, yaitu Departemen Propaganda, yang bertugas untuk menentukan konten apa saja yang perlu disensor dari masyarakat dan konten mana yang perlu disebarkan; Kantor Informasi Negara dan Administrasi Pers dan Publikasi, yang bertugas untuk mengatur publikasi media massa, termasuk publikasi melalui internet; Kementerian Budaya dan Kementerian Edukasi, yang bertugas mengatur konten edukasi yang disediakan kepada masyarakat; Kementerian Industri dan TIK, yang bertugas untuk mengatur informasi yang beredar di internet; Kementerian Keamanan Publik yang bertugas untuk menegakkan hukum-hukum yang berlaku, termasuk hukum yang berkaitan dengan GFW; Kementerian Keamanan Nasional yang bertugas untuk mengumpulkan informasi mengenai konten yang berpotensi mengancam keamanan negara; Administrasi *Cyberspace* Tiongkok dan Pusat *Cybersecurity* dan Informasi yang juga bertugas untuk menentukan konten mana yang perlu disensor dan menegakkan hukum penyensoran. Badan ini diketuai secara langsung oleh Xi Jinping (Roberts 2018).

Selain badan-badan pemerintah tersebut, penerapan GFW ini juga dilakukan oleh aktor lain. Kontribusi terbesar pada GFW dari luar pemerintah datang dari perusahaan-perusahaan penyedia internet di Tiongkok yang bertugas mengadakan dan merawat peralatan pemblokir jaringan. Penyedia peralatan pemblokir terbesar adalah TIONGKOKNET yang menangani 80% pemblokiran, terutama di daerah-daerah pinggiran Tiongkok, sedangkan perusahaan CNCGROUP juga berkontribusi dalam pemblokiran pada jaringan yang terletak di pusat Tiongkok (Xu *et al*. 2011). Dalam pengadaan peralatan pemblokiran, Tiongkok mendapat bantuan dari perusahaan Cisco. Cisco sudah membuat perangkat untuk memblokir akses situs-situs web tertentu pada awal 1990-an, pemerintah Tiongkok kemudian melihat potensi teknologi ini dan kemudian mengontrak Cisco untuk membantu mereka menyediakan peralatan untuk proyek GFW ini (Goldsmith and Wu 2006).

Selain itu, dalam perkembangan GFW, ada juga seseorang yang dikenal sebagai "Bapak Penyensoran Tiongkok", yaitu Fang Binxing. Dia menjadi identik dengan GFW dan usaha penyensoran lainnya di Tiongkok karena dia adalah seorang ahli cybersecurity di BUPT (*Beijing University of Post and Telecommunications*) yang banyak meneliti mengenai teknologi penyensoran. Banyak hasil penelitiannya yang menjadi dasar

penerapan GFW (Bu 2013).

Kontribusi GFW bagi Cybersecurity Tiongkok

Kontribusi proyek GFW ini terhadap *cybersecurity* Tiongkok adalah kemampuannya untuk mengawasi berbagai data yang beredar internet. GFW dapat memonitor berbagai konten yang beredar di internet Tiongkok mulai dari publikasi berita yang bersifat publik hingga email pribadi yang dikirim dari dan keluar Tiongkok. Hasil dari pemantauan GFW ini kemudian diteruskan ke Kepolisian Tiongkok yang dapat segera menindaklanjuti pihak yang dinilai mengancam keamanan publik (Qinglian 2008). Selain itu, GFW juga menyaring koneksi ke dan dari luar negeri Tiongkok, sehingga hanya koneksi yang terpercaya yang boleh diteruskan ke jaringan Tiongkok. Penyaringan ini memungkinkan pemerintah Tiongkok untuk lebih fokus pada ancaman yang berasal dari dalam negeri karena ancaman dari luar negeri sudah tersaring (Denyer 2016).

Penyaringan dan pengamanan arus informasi di internet ini juga memungkinkan pemerintah Tiongkok untuk menerapkan *cyber governance* yang memerlukan jaringan yang aman, tertutup, dan menyeluruh. GFW memenuhi seluruh kebutuhan tersebut sehingga *cyber governance* dapat diterapkan di Tiongkok untuk mempermudah proses birokrasi dan pertukaran informasi bagi masyarakat Tiongkok. Keamanan ini dibuat sesuai dengan pandangan Xi Jinping mengenai peran internet di Tiongkok sebagai "rumah kedua" bagi masyarakatnya (Chinese Academy of Cyberspace Studies 2018).

GFW juga berperan dalam membantu dalam *cybersecurity* Tiongkok dengan cara mendorong dan memajukan teknologi buatan dalam negeri. Dengan membatasi akses ke jaringan luar negeri, GFW memberi insentif ekonomi bagi para perusahaan internet dan akademisi TIK di Tiongkok untuk berinovasi secara mandiri. Salah satu contohnya adalah penerapan sistem enkripsi miliki Tiongkok sendiri yang bernama sistem "*Skeleton Key*" ketimbang menggunakan sistem RSA yang merupakan standar internasional untuk enkripsi. Sistem *Skeleton Key* ini digunakan untuk mengamankan data-data penting, terutama data-data yang harus melalui pemerintah pusat (Balke 2018).

Selain digunakan untuk menyensor dan memonitor konten yang beredar di internet, GFW juga dapat digunakan sebagai sistem pengalihan. Dalam menjaga *cybersecurity* Tiongkok, GFW ini dapat juga digunakan untuk mengalihkan koneksi. Jika sistem GFW mendeteksi ada koneksi yang berasal dari luar negeri dan diduga bersifat mengancam, maka

koneksi tersebut dapat dialihkan ke server yang tidak berhubungan sehingga menggagalkan koneksi tersebut atau mengalihkan potensi serangan. Informasi dari koneksi ini dapat digunakan untuk melakukan serangan balik dengan cara memicu program yang merusak pada komputer luar negeri tersebut (Kalathil 2017).

Efektivitas GFW

Sejak tahun 2001, kemampuan *cybersecurity* Tiongkok sudah berkembang pesat, hingga Pemerintah AS mengakui bahwa Tiongkok merupakan saingan utamanya dalam kecanggihan *cybersecurity*. Tiongkok sendiri sudah memiliki unit khusus yang berlatih menyerang jaringan-jaringan AS, dan sudah melakukan beberapa serangan yang cukup sukses (Pollpeter 2015). Menurut laporan yang dibuat oleh FireEye, sebuah perusahaan konsultan *cybersecurity* di Amerika, Tiongkok melancarkan serangan *cyber* menjelang pemilu AS. Laporan ini juga menyatakan bahwa kekuatan *cybersecurity* Tiongkok lebih tinggi dari yang sebelumnya diperkirakan sehingga Tiongkok diperkirakan dapat menyamai bahkan melampaui AS pada tahun 2021. Oleh karena itu, negara-negara perlu bersiap menghadapi Tiongkok karena Tiongkok cenderung tetap melakukan serangan *cyber* walaupun dengan adanya perjanjian internasional atau gerakan diplomasi sebelumnya (FireEye 2020).

Selain itu, GFW juga berdampak pada masyarakat Tiongkok itu sendiri. Karena masyarakat Tiongkok sudah terbiasa dengan GFW dan belum pernah melihat sisi lain dari pemikiran yang disensor oleh pemerintahnya, mereka cenderung mendukung dan mengikuti cara berpikir yang diajarkan kepada mereka melalui GFW tersebut (CBC Radio 2019). GFW telah cukup sukses dalam membatasi akses ke luar negeri bagi masyarakat Tiongkok. Situs-situs seperti YouTube, Twitter, dan Facebook telah sukses diblokir oleh penerapan GFW ini. Selain itu, GFW juga sudah sukses memantau komunikasi orang-orang yang dianggap berbahaya dan menyensor konten-konten tertentu.

Namun, ada beberapa kelemahan dalam GFW. Walaupun GFW memang dapat memblokir situs-situs dari luar Tiongkok, sebagian masyarakat Tiongkok sendiri tampak sudah dapat melewati pemblokiran ini dengan bantuan alat-alat anti pemblokir yang tersedia. Walaupun secara hukum situs-situs tertentu tidak boleh diakses oleh masyarakat Tiongkok, dengan sedikit usaha, mereka tetap dapat mengaksesnya (MacKinnon 2012). Namun, menurut pengamat di Tiongkok, kelemahan ini merupakan sesuatu yang disengaja karena dua hal. Pertama, kelemahan ini memungkinkan turis dan pendatang lainnya yang berada di Tiongkok untuk

tetap menjalankan kebutuhan mereka selama di Tiongkok. Kedua, pemerintah Tiongkok tidak berniat untuk mengisolasi Tiongkok dari dunia luar, tapi hanya mengendalikan narasi mengenai pemerintah yang beredar. Selama tidak digunakan untuk mengancam keamanan masyarakat Tiongkok, situs-situs tersebut dapat diakses dengan cara-cara tertentu (Denyer 2016).

Selain memblokir situs, penyensoran konten berlaku meskipun ternyata tidak terlalu ketat. GFW memonitor konten yang beredar di internet dengan cara membaca konten dan mencocokkannya dengan daftar kata kunci yang sudah dibuat. Salah satu studi menunjukkan bahwa konten yang mengkritik pemerintah masih diperbolehkan untuk beredar di masyarakat Tiongkok. Namun, jika konten tersebut mengandung ajakan untuk "mengubah" pemerintah yang sedang menjabat, maka barulah konten tersebut akan disensor oleh pemerintah. Sedangkan konten-konten yang kontroversial bagi Tiongkok seperti protes Tianamen, Dalai Lama, kemerdekaan Tibet, dan lain-lain akan melalui proses pengulasan sebelum dapat dimunculkan untuk publik. Untuk konten di situs-situs kecil, biasanya konten yang mengandung topik-topik tersebut dapat langsung dipublikasikan tanpa melalui proses pengulasan ini. Jika terbukti bahwa konten ini mengancam keamanan masyarakat, maka konten tersebut akan dihapus dan pembuatnya berkemungkinan diproses secara hukum. Konten di situs-situs dengan audiensi yang lebih besar akan melalui proses pengulasan yang lebih teliti (King et al. 2013).

GFW Sebagai Cybersecurity

GFW dimanfaatkan untuk mengamankan Tiongkok dari ancaman. Tiongkok melakukan pembangunan *cybersecurity* disebabkan karena Tiongkok memandang komunikasi digital bukan sekedar alat komunikasi, melainkan juga diterapkan dalam banyak hal. Xi Jinping menilai bahwa *cybersecurity* merupakan bagian penting dari keamanan nasional dan jika ada kekurangan dalam pertahanan *cybersecurity*, maka kelemahan tersebut juga akan mempengaruhi aspek-aspek lain dalam kehidupan bernegara mereka. Dia menyebut internet sebagai "rumah bersama" untuk semua orang di dunia, sehingga dibutuhkan keamanan.

Selain itu, *cybersecurity* ini menjadi penting bagi Tiongkok karena mereka sudah mulai menerapkan digitalisasi dalam berbagai keseharian mereka (Chinese Academy of Cyberspace Studies, 2018). Pemikiran studi keamanan yang populer di Tiongkok adalah konsep CNP. Jika mengikuti pandangan CNP, Tiongkok masih belum setara dengan negara-negara Barat. Karena itu, muncul keinginan dalam masyarakat Tiongkok untuk

menyusul negara-negara Barat dalam berbagai hal, salah satunya adalah *cybersecurity*.

Tiongkok sudah cukup memenuhi kebutuhan *cybersecurity* mereka dengan adanya GFW. Bagian pertama dari definisi *cybersecurity* tersebut adalah pencegahan, pendeteksian, dan respons. Sesuai dengan hukum *Provisional Regulations for the Administration of International Connection of Computer Information Network* tahun 1996, GFW berfungsi untuk membatasi koneksi dari luar negara. Dengan ini, GFW dapat menyaring aktivitas yang dianggap mencurigakan. GFW juga berfungsi untuk mengawasi konten yang beredar di internet, tidak hanya konten yang dipublikasikan, namun juga sampai mengawasi komunikasi yang tidak publik. Dengan adanya GFW, pemerintah Tiongkok dapat mengawasi dan mendeteksi ancaman yang mungkin muncul dari dalam maupun dari luar negara mereka.

Walaupun GFW tidak dapat merespons langsung terhadap suatu ancaman, salah satu bagian dari fungsi GFW adalah untuk meneruskan aktivitas yang diduga sebagai ancaman kepada orang-orang yang bertugas untuk mengulas dan memutuskan tindakan yang cocok untuk ancaman tersebut. Hal ini dilaksanakan berdasarkan hukum *Telecommunications Regulations dan Adminstrative Measures for Internet Information Services* yang diberlakukan pada tahun 2000. Dengan adanya GFW, para pengulas tersebut tidak harus mengulas seluruh aktivitas yang terjadi dalam *cyberspace* Tiongkok sehingga mereka dapat lebih fokus kepada ancaman yang benar-benar serius. Tipe konten yang diulas juga ditandai oleh beberapa faktor, seperti apakah konten tersebut mengandung kata-kata kunci yang sudah ditetapkan, apakah tema konten tersebut termasuk topik yang kontroversial, data-data mengenai pembuat konten tersebut, dan kapan dan dari mana konten tersebut dibuat.

Kebijakan menyerahkan proses tindakan kepada manusia ini memastikan bahwa suatu ancaman dapat dianalisis dengan secara lebih organik untuk menghasilkan penilaian ancaman yang lebih akurat dibandingkan jika hanya mengandalkan algoritma mesin. Sistem pemeriksaan manual ini dapat dilihat sebagai kelemahan GFW itu sendiri yang terkadang masih memperbolehkan orang-orang yang berada Tiongkok untuk mengakses situs-situs luar negeri. Selain itu, masih adanya diskusi politik yang terjadi di Tiongkok menandakan bahwa GFW tidak langsung memblokir konten politik, tapi menyaringnya dan menyerahkannya kepada pihak berwajib.

Bagian kedua *cybersecurity* adalah orang, proses, dan teknologi. Dalam bagian ini, GFW adalah teknologi canggih yang sudah dapat

mengawasi dan menyaring konten yang beredar di internet. Ditambah lagi, berbagai teknologi pengamanan yang dimilikinya GFW sangat sulit untuk dilewati oleh orang dari luar dan dalam negeri. Teknologi yang canggih ini kemudian didukung juga oleh hukum *cybersecurity* yang cukup ketat dan ditambah dengan berbagai badan pemerintah yang bertugas untuk menegakkan hukum tersebut. Hukum *cybersecurity* yang diterpakan dalam GFW sudah menjelaskan hak dan kewajiban seluruh masyarakat Tiongkok yang berkaitan dengan akses mereka dengan internet.

Dapat dilihat bahwa Tiongkok juga mengharapkan bahwa isu *cybersecurity* ini menjadi kepentingan seluruh masyarakat negaranya. Hal ini terlihat dari hukum *cybersecurity* terbaru Tiongkok yang diberlakukan pada tahun 2016 lalu. Hukum ini menjelaskan bahwa setiap masyarakat Tiongkok ikut bertanggungjawab akan *cybersecurity* dengan cara hanya menggunakan layanan yang sudah diverifikasi keamanannya oleh pihak pemerintah.

Selain itu, dengan mengharuskan setiap orang melalui proses verifikasi data ketika mendaftar untuk suatu layanan online, setiap orang akan lebih berhati-hati ketika menggunakan internet. Pemerintah Tiongkok juga aktif melakukan pendidikan mengenai pentingnya *cybersecurity*, bagaimana cara menjamin keamanan privasi dalam *cyberspace*, dan secara aktif mengajak para pemudanya untuk mempelajari TIK, khususnya dalam bidang *cybersecurity*. Para penyedia layanan pun diharuskan menjamin keamanan data para penggunanya sambil terus bekerja sama dengan pemerintah dalam proses validasi data dan audit keamanan berkala. Dengan adanya hukum yang terperinci, setiap masyarakat Tiongkok juga mengambil bagian dalam mengamankan keamanan *cyberspace* negaranya jika mereka mematuhi hukum-hukum yang berlaku tersebut.

Bagian ketiga *cybersecurity* adalah kerahasiaan, integritas, dan ketersediaan informasi. Bagian ketiga *cybersecurity* ini adalah fokus utama dari penerapan GFW. Sistem GFW memang dirancang dari awal untuk memastikan bahwa informasi-informasi yang bersifat rahasia tetap menjadi rahasia dan tidak dapat diakses oleh pihak yang tidak berwenang dengan cara membatasi peredarannya dan menyensor informasi tersebut jika tidak sengaja tersebarkan kepada publik. Sistem ini menjamin bahwa informasi yang sudah beredar ke masyarakat adalah informasi yang benar-benar sudah diulas oleh petugas pemerintah dan dinyatakan pantas untuk konsumsi masyarakat umum. Dengan demikian, GFW memastikan bahwa masyarakat Tiongkok tetap dapat dengan mudah mengakses informasi yang mereka inginkan sambil tetap mengendalikan dan membatasi informasi apa saja yang dapat diakses oleh masyarakatnya.

Tiongkok sudah melakukan beberapa upaya untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi ini. Dalam rangka memastikan kerahasiaan, Tiongkok telah mengembangkan sistem enkripsinya sendiri bernama sistem "*Skeleton Key*" yang digunakan untuk mengenkripsi informasi-informasi rahasia negara. Karena sistem *Skeleton Key* ini unik milik Tiongkok, sistem ini menjamin informasi rahasia negara hanya dapat dilihat oleh pihak yang berwenang. Dalam menjaga integritas, Tiongkok memiliki berbagai Kementerian Budaya, Kementerian Edukasi, Kementerian Industri dan TIK, Kementerian Keamanan Nasional, dan Pusat *Cybersecurity* dan Informasi yang bertugas memonitor informasi yang beredar melalui internet, sehingga informasi sesat yang tidak benar dapat dicegat dalam proses penyaringan konten yang dilakukan badan-badan pemerintah ini. Dalam memastikan ketersediaan informasi, perusahaan-perusahaan penyedia internet di Tiongkok sudah cukup sukses mencakup hingga 97% negaranya, sehingga memungkinkan semua masyarakatnya di seluruh penjuru negara mengakses internet dengan mudah.

Pertahanan GFW memang bukan untuk melindungi dari hacking yang biasanya dilakukan oleh individu. Namun, GFW masih dapat menyaring koneksi yang berbahaya sehingga masih dapat memperlambat atau mencegah ancaman *hacking* dalam skala kecil. Perlu diingat juga bahwa dalam dunia *cybersecurity*, *hacking* merupakan suatu proses yang harus dijalani dalam rangka mengetahui kelemahan suatu sistem agar sistem tersebut dapat ditingkatkan kekuatannya. Karena itu, upaya-upaya individu yang berusaha untuk menembus GFW dapat dipandang secara positif oleh pemerintah Tiongkok sebab aktivitas *hacking* tersebut akan menunjukkan bagaimana GFW dapat ditingkatkan.

Kategori lain ancaman *cyberspace* adalah kejahatan terorganisasi. Terlihat dari hukum-hukum *cyberspace* yang berlaku di Tiongkok bahwa pemerintah Tiongkok cukup serius dalam melindungi masyarakatnya dari kejahatan *cyber*. Hukum *cyberspace* terbaru mereka yang diberlakukan pada tahun 2016 juga menambahkan perlindungan mengenai penyimpanan data pengguna dan audit produk-produk jasa *online* yang disediakan bagi masyarakatnya. Dengan kontrol dan pengawasan yang dilakukan dengan adanya GFW, pemerintah Tiongkok dapat menjaga keamanan ini dengan lebih mudah.

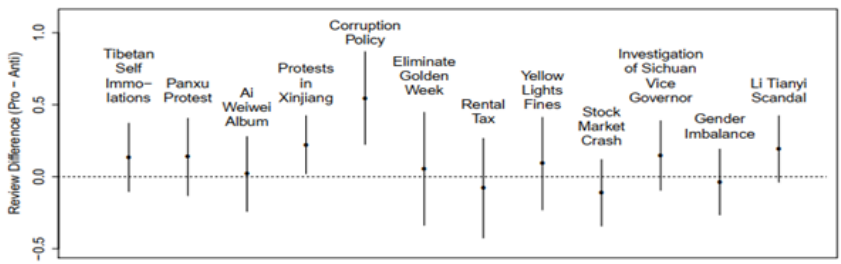
Ancaman ini juga sangat penting bagi Tiongkok karena mereka mengharuskan masyarakatnya untuk menggunakan identitas asli ketika beraktivitas di internet. Selain itu, menurut hukum *cyberspace* yang berlaku, tindakan mengajak aktivitas revolusi, menyebarkan informasi

rahasia, dan menyebarkan informasi sesat diklasifikasikan sebagai kejahatan *cyber*. Dengan hukum yang menjadi dasar GFW ini, pemerintah Tiongkok tetap dapat melancarkan kontrol masyarakat dengan memperluas definisi kejahatan *cyber* yang berlaku di negara mereka. Tiongkok sudah pernah melakukan ini ketika mereka merevisi hukum *cybersecurity* yang berlaku dari tahun ke tahun. Hukum CL97 menambahkan bahwa penyebaran informasi negara merupakan kejahatan. Lalu dengan hukum *Decision on Safeguarding Internet Security*, definisi kejahatan *cyber* ditambahkan lagi dengan melarang masyarakat Tiongkok untuk menyerang sistem-sistem komputer milik negara, memicu perpecahan, dan menyebarkan informasi yang tidak benar. Kemudian dengan hukum *cybersecurity* tahun 2016, definisi ini kembali diperinci dengan melarang penyebaran informasi pribadi seseorang baik oleh individu dan perusahaan.

Kategori selanjutnya dari ancaman *cyberspace* adalah ancaman politik dan ideologi. Ancaman kategori ketiga ini adalah pusat fokus utama dari GFW. Sejak awal, GFW memang dimaksudkan untuk mengamankan posisi politik pemerintah pusatnya dengan cara menyembunyikan topik-topik yang dinilai berpotensi memicu keresahan masyarakatnya. Terlihat dari topik-topik yang diblokir oleh GFW ini seperti topik kemerdekaan Tibet, Protes Tianamen Square, Dalai Lama, dan topik lainnya, semuanya bersifat politik seperti kemerdekaan Tibet atau protes di Xinjiang akan cenderung lebih diawasi oleh pemerintah seperti yang dapat dilihat dalam Grafik 1. Selain itu, GFW juga fokus memblokir konten yang bersifat ajakan untuk mengubah pemerintahan sekarang. Dengan menyensor konten-konten politik ini, GFW telah membantu mencegah terjadinya protes dari masyarakat Tiongkok karena terbatasnya informasi yang menunjukkan pandangan yang berbeda dari pandangan pemerintah pusat. Selain itu, dengan keharusan menggunakan identitas asli di internet, pemerintah Tiongkok dapat dengan mudah melacak individu yang berpotensi mengancam kedaulatan negara mereka sehingga mempersulit munculnya gerakan reformasi melalui media internet.

Tiongkok membentuk GFW merupakan cara bagi Tiongkok untuk menjaga kesatuan nasionalnya dan menjaga tingkat kemajuan ekonomi. Menurutnya, karena Tiongkok merupakan negara komunis yang sangat terpusat, mereka cenderung lebih rawan mengalami perpecahan. Jika masyarakat merasa bahwa kebutuhan mereka tidak terpenuhi, maka mereka akan melakukan protes yang berpotensi memicu perpecahan dalam negara. Sehingga, GFW merupakan cara pemerintah Tiongkok untuk mengendalikan konten media sosial yang bersifat provokatif agar tidak menginspirasi gerakan politik yang berpotensi menyebabkan perpecahan.

Dalam hal ini, GFW juga digunakan untuk mengontrol narasi mengenai pemerintah yang beredar dalam masyarakat Tiongkok secara sedemikian rupa sehingga masyarakat tidak merasa perlu ada perubahan yang signifikan.



Gambar 1 Topik-Topik yang Diulas oleh Pemerintah Tiongkok
Sumber: King *et al.* 2013.

Kategori terakhir adalah agresi *cyber* yang disponsori negara. Walaupun ancaman ini memang dialami Tiongkok, GFW bukan merupakan salah satu alat untuk mengatasi ancaman ini. Namun, GFW tetap berkontribusi dalam membantu Tiongkok menangani ancaman ini. Karena GFW membatasi akses kepada layanan luar negeri, hal ini memicu para ahli TIK di Tiongkok untuk semakin kreatif dalam mengembangkan sistem-sistem mereka sendiri. Selain itu, dengan adanya dorongan dari pemerintah untuk mengajak pemuda-pemudi Tiongkok untuk mempelajari dan berpartisipasi dalam perkembangan TIK, Tiongkok sekarang memiliki keahlian yang cukup baik untuk mengatasi bahkan melakukan agresi *cyber* ini. Hal ini dapat dilihat dari adanya laporan yang dipublikasikan oleh perusahaan auditor *cybersecurity* FireEye dan dari seorang peneliti, Kevin Pollpeter, bahwa Amerika Serikat mengalami serangan-serangan ini yang diduga berasal dari Tiongkok.

GFW Sebagai Cyberpower Tiongkok

Dengan pengembangan kemampuan *cybersecurity* ini, *cyberpower* Tiongkok pun berkembang. Tiongkok berupaya menjamin *cybersecurity* tersebut tetap berkelanjutan agar dapat mempertahankan statusnya sebagai salah satu pemimpin dalam bidang ini. Prioritas Tiongkok membangun *cybersecurity* yang kuat terlihat dari pesatnya perkembangan industri TIK yang terjadi di Tiongkok. Kemajuan-kemajuan ini memungkinkan

Tiongkok untuk menjadi salah satu aktor yang memiliki *cyberpower* yang signifikan. Tiongkok sudah dapat mengamankan dirinya dari serangan-serangan terhadap peralatan fisik jaringannya dengan memanfaatkan militer yang kuat dan hukum *cyber* yang cukup kuat. Tiongkok juga sudah mampu mempertahankan jaringannya dari serangan *cyber* oleh aktor lain bahkan sudah sampai dapat melakukan serangan terhadap negara lain. Selain itu, tingkat pengadopsian internet yang tinggi dan didukung dengan program-program pendidikan seperti beasiswa untuk individu yang berbakat dan berbagai konferensi seperti *China Annual Cybersecurity Conference* dan inkubasi perusahaan *start-up cybersecurity* seperti yang sudah diberikan kepada Weston, Bluedon, Lanxum, dan lainnya.

Jika kita menilai *cyberpower* Tiongkok menurut yang didefinisikan oleh Tim Jordan, dapat dilihat bahwa Tiongkok juga sudah menguasai ketiga bagian dalam *cyberpower*. Bagian pertama *cyberpower* adalah kekuatan yang dimiliki individu, dalam hal ini kita melihat bahwa masyarakat Tiongkok telah mendapat banyak kesempatan dalam berpartisipasi dan memanfaatkan *cyberspace*. Hal ini dapat kita lihat dari banyaknya jumlah pengguna internet di Tiongkok yang membuat Tiongkok menjadi salah satu negara teraktif di internet. Program-program pendidikan TIK yang dilakukan oleh pemerintah juga memastikan bahwa masyarakat tidak hanya bisa, tetapi juga mahir dalam memanfaatkan berbagai fasilitas yang dimungkinkan oleh kemajuan TIK ini. Selain itu, dari aspek politik, GFW memungkinkan Tiongkok untuk mulai menerapkan *cyber governance* dengan tujuan untuk mempersingkat birokrasi, mempermudah pertukaran informasi, dan transparansi bagi masyarakatnya. Sehingga *cybersecurity* akan sangat diperlukan karena informasi-informasi yang dibahas dalam *cyber-governance* tersebut dapat mengandung informasi rahasia.

Selain itu, Tiongkok juga memanfaatkan *cyberspace* untuk memajukan kepentingan politik mereka dengan cara memperbanyak konten yang menunjukkan sisi positif Tiongkok, Xi Jinping, dan kesuksesan pemikiran sosialisme mereka (Chinese Academy of Cyberspace Studies, 2018). Untuk keperluan ini, pemerintah Tiongkok sudah memiliki *platform* tersendiri untuk menyebarkan informasi-informasi mengenai kemajuan mereka. Pemerintah pusat Tiongkok memberikan situs web untuk dikelola oleh pemerintah daerah, sehingga setiap pemerintah daerah dapat mempublikasikan kemajuan mereka melalui situs tersebut. Kemudahan akses terhadap layanan-layanan TIK ini juga memupuk kemampuan TIK masyarakat Tiongkok karena mereka terus-menerus menggunakan layanan-layanan tersebut.

Namun, karena GFW memblokir akses layanan-layanan internet yang berasal dari luar negeri, masyarakat Tiongkok harus menggunakan produk-produk dan layanan-layanan buatan Tiongkok sendiri. Akibatnya, secara ekonomi GFW dapat juga sebagai proteksionisme ekonomi yang memicu perusahaan-perusahaan Tiongkok untuk menjadi lebih baik. Hal ini dapat terlihat dari kemajuan Tiongkok di bidang TIK yang sangat pesat dan kualitas layanan alternatif Tiongkok seperti WeChat sebagai aplikasi *chatting* alternatif, Youku sebagai alternatif YouTube, Baidu sebagai alternatif Google yang sudah cukup memuaskan bagi masyarakat Tiongkok. Layanan-layanan alternatif tersebut dirasa perlu oleh Tiongkok tidak hanya untuk mengurangi ketergantungan mereka pada produk luar negeri, tapi juga sebagai wujud kontrol sosial dan juga untuk memudahkan pemerintah Tiongkok melacak masyarakatnya karena layanan-layanan tersebut mengharuskan penggunanya untuk menggunakan identitas asli.

Selain itu, penggunaan aplikasi-aplikasi tersebut membantu Tiongkok menetapkan kontrol sosial karena menurut hukum *cybersecurity* tahun 2016, pemilik aplikasi-aplikasi tersebut diharuskan memberikan akses terhadap data-data yang sudah mereka kumpulkan kepada pemerintah pusat pemerintah Tiongkok untuk pengawasan keamanan dan juga audit keamanan yang rutin dilakukan oleh pemerintah. Dengan hukum tersebut, pemerintah Tiongkok tetap dapat mengendalikan dan dengan bebas memeriksa operasi perusahaan-perusahaan tersebut walaupun status mereka sebagai perusahaan swasta. Adapun cara pemerintah Tiongkok memastikan bahwa perusahaan-perusahaan tersebut menyensor konten adalah melalui perusahaan penyedia internet yang merupakan badan usaha milik negara. Karena perusahaan-perusahaan ini bergantung pada penyedia internet yang merupakan badan usaha milik negara ini, mereka harus mematuhi kebijakan-kebijakan yang berlaku jika ingin tetap beroperasi di Tiongkok (Xu *et al*. 2011).

Namun, proteksionisme ekonomi ini juga memupuk sumber daya manusia yang berkualitas karena juga didukung program pendidikan TIK dari pemerintah pusat. Dengan sumber daya manusia yang baik, industri TIK Tiongkok dapat tetap berinovasi dan berkembang walaupun tanpa akses layanan luar negeri. SDM ini juga diperkerjakan dalam bidang pertahanan nasional dengan adanya unit khusus *cybersecurity* maupun dalam berbagai perusahaan penyedia layanan *cybersecurity* yang ada di Tiongkok.

Bagian kedua *cyberpower* adalah adanya kaum elite yang ahli dalam memahami *cybersapce*. Di Tiongkok, ada kelompok tertentu yang lebih mahir dalam bidang ini dibandingkan masyarakat umum. Adapun yang

dimaksud dengan kelompok elite ini terdiri dari beberapa badan pemerintah seperti Kementerian Industri dan TIK, Administrasi *Cyberspace* Tiongkok dan Pusat *Cybersecurity* dan Informasi, dan perusahaan-perusahaan dalam bidang TIK. Dalam laporan kemajuan *cybersecurity* tahun 2018, disebutkan tiga perusahaan terbesar dalam bidang *cybersecurity* ini yaitu Venustech, Weston, dan Bluedon. Dampak dari kelompok elite tersebut pada kehidupan masyarakat Tiongkok dan dunia dapat dilihat dengan jelas. Perusahaan-perusahaan TIK Tiongkok sudah sangat berkembang pesat sehingga dapat menyaingi perusahaan-perusahaan Barat dan bahkan menjadi inovator dan mendahului perusahaan barat dalam beberapa bidang. Pemerintah Tiongkok, terutama Kementerian Industri dan TIK, senantiasa membantu mempopulerkan hasil karya perusahaan-perusahaan tersebut. Salah satu contoh kemajuan Tiongkok adalah dalam bidang pengembangan 5G. Dalam implementasi 5G, Tiongkok sudah memasang peralatan 5G di 12 kota mereka dengan kerja sama dari perusahaan produsen peralatan 5G seperti Huawei dan ZTE dengan perusahaan penyedia internet China Telecom. Pemerintah Tiongkok pun juga mendukung kemajuan 5G ini dengan cara membawakan standar 5G milik Tiongkok kepada forum *International Telecommunication Union* (ITU).

Sedangkan peran pemerintah Tiongkok dapat dilihat dari berbagai laporan yang menyatakan bahwa mereka mengalami serangan cyber yang diduga berasal dari Tiongkok. Kejadian tersebut menunjukkan bahwa pemerintah Tiongkok sudah memiliki pengetahuan yang cukup signifikan sehingga dapat melakukan serangan *cyber* yang berhasil mengganggu target mereka. Selain itu, Tiongkok juga mulai membangun kerja sama dengan beberapa negara untuk menjual teknologi penyensoran yang digunakan dalam GFW. Rusia dan Iran sudah menunjukkan ketertarikan dan mulai bekerja sama dengan Tiongkok untuk secara perlahan menerapkan sistem yang serupa dengan GFW di negara mereka (Esfandiari 2020). Tiongkok juga dengan aktif berusaha mempromosikan teknologi Tiongkok untuk dijadikan standar di internet. Salah satu topik yang mereka junjung adalah untuk mempromosikan kontrol pemerintah terhadap internet. Gagasan ini sudah mereka bawakan sebagai topik diskusi dalam forum ICANN (*Internet Corporation for Assigned Names and Numbers*) dan W3C (*World Wide Web Consortium*) (Griffiths 2019). Perilaku-perilaku tersebut menunjukkan bahwa masyarakat Tiongkok sudah memiliki keahlian yang cukup sehingga membuat masyarakat internasional berminat menggunakan teknologi mereka.

Bagian ketiga dalam *cyberpower* adalah adanya imajinasi untuk membuat inovasi yang akan membuat *cyberspace* menjadi lebih baik.

Tiongkok juga sudah cukup memenuhi bagian ketiga ini. Pada tahun 2017, ada 3,7 juta hak paten dan Tiongkok dinobatkan sebagai negara terinovatif ke-17 oleh WIPO. Hal ini menunjukkan bahwa masyarakat Tiongkok memiliki imajinasi yang aktif dalam berusaha membentuk *cyberspace* yang lebih baik. Dedikasi para perusahaan TIK Tiongkok yang lebih banyak melakukan riset pada topik-topik baru seperti AI, *cloud computing*, dan big data. Jika melihat bagaimana perusahaan Tiongkok mengimplementasikan inovasi-inovasi tersebut, dapat dilihat bahwa Tiongkok berharap inovasi-inovasi tersebut akan mempermudah dan mempersingkat berbagai proses. Misalnya, AI buatan Tencent yang dapat mendiagnosis pasien dan meresepkan obat, sistem *cloud computing* Baidu yang membantu dalam penyimpanan *database*, atau teknologi Alibaba ET Brain yang dapat memproses *big data* untuk meningkatkan efisiensi pabrik.

Selain itu, pemerintah Tiongkok juga sukses menumbuhkan gagasan bahwa adanya kontrol pemerintah dalam *cyberspace* merupakan hal yang baik. Secara umum, penerapan GFW ini diterima secara positif oleh masyarakat Tiongkok. Walaupun akses mereka terhadap media internasional dibatasi, dengan adanya alternatif dalam negeri yang berkualitas, masyarakat Tiongkok tetap dapat menikmati gaya hidup yang serupa dengan yang terjadi di luar Tiongkok namun dengan mengandalkan produk buatan Tiongkok sendiri. Selain itu, kestabilan politik dan kemajuan ekonomi yang pesat juga membuat masyarakat Tiongkok enggan untuk mengubah kondisi mereka saat ini. GFW ini juga memupuk rasa nasionalisme masyarakat Tiongkok karena pembatasan yang dilakukan GFW dijadikan bukti bahwa Tiongkok sudah dapat membuat produk-produk yang setara atau melampaui yang dapat dihasilkan oleh negara-negara lainnya. Salah satu contohnya adalah popularitas ponsel buatan Tiongkok yang banyak digunakan tidak hanya di Tiongkok, melainkan juga di seluruh dunia. Pada tahun 2020, 80% ponsel yang aktif di Tiongkok adalah produk buatan dalam negeri oleh Huawei, Xiaomi, Oppo, dan Vivo. Sedangkan dalam skala global, 26% dari seluruh ponsel yang aktif pada tahun 2020 merupakan ponsel buatan Tiongkok. Hal ini menunjukkan bahwa produk-produk Tiongkok sudah dapat menyamai produk-produk luar dan bahwa produk-produk dari Tiongkok ini lebih disukai oleh masyarakat Tiongkok dan internasional (StatCounter 2021).

Penggunaan GFW ini memungkinkan pemerintah Tiongkok untuk mengontrol perusahaan asing yang ingin memasarkan produknya bagi masyarakat Tiongkok. Perusahaan asing juga diharuskan menyensor konten-konten dan mengikuti peraturan ketat yang ditentukan oleh pemerintah Tiongkok jika ingin produknya dapat diakses oleh masyarakat

Tiongkok. Karena tidak semua perusahaan merasa nyaman mengikuti peraturan-peraturan ini, tidak semua perusahaan dapat memberikan layanan mereka di Tiongkok. Akibatnya, masyarakat Tiongkok diharuskan menggunakan alternatif dalam negeri yang sudah dikontrol oleh pemerintah. Contoh kasus yang terjadi adalah perusahaan-perusahaan seperti Google dan Yahoo yang menyediakan jasa pencarian *online* terpaksa menyensor beberapa konten yang dianggap ilegal menurut definisi GFW, bahkan pada tahun 2010, Google secara resmi menghentikan layanan mereka di Tiongkok.

Namun, ada juga yang mengkritik sistem penyensoran GFW ini. Amerika Serikat mengkritik GFW karena sering kali menyulitkan perusahaan-perusahaan Amerika yang ingin berbisnis di Tiongkok. Pada tahun 2016, 79% perusahaan di AS merasa bahwa bisnis mereka terdampak negatif oleh adanya GFW (Carsten and Martina 2016). Menurut mereka, kebijakan GFW ini dianggap terlalu ketat dalam membatasi konten sehingga mereka perlu perhatian lebih ketika berkomunikasi dengan rekan bisnis mereka di Tiongkok. Selain itu, tidak mudahnya mengakses layanan-layanan komunikasi yang populer di negara barat seperti Facebook, Whatsapp, Twitter, dan lain-lain, menyebabkan komunikasi yang kurang ideal dengan, terutama untuk perusahaan kecil yang masih hanya mengandalkan komunikasi secara *online.* Ada juga kritik dari advokat hak asasi manusia bahwa GFW ini membatasi demokrasi dan hak menyuarakan pendapat masyarakat Tiongkok dan jika GFW menjadi populer sehingga diterapkan oleh negara-negara lain, maka kejadian ini akan menghambat atau bahkan menghentikan kebebasan pertukaran informasi global yang sedang terjadi sekarang (Chan 2018). Namun, dalam menghadapi kritik-kritik tersebut, Tiongkok tetap menekankan bahwa demokrasi dan kebebasan tetap ada di Tiongkok dengan menganut gaya yang lebih cocok dengan masyarakat Tiongkok. Tiongkok juga tetap dapat mempertahankan pandangannya karena posisinya sebagai salah satu negara yang penting dalam perekonomian global sehingga Tiongkok dapat dengan mudah menolak hubungan dengan negara yang berbeda pandangan dengan Tiongkok.

Dari penjelasan di atas, dapat dikatakan bahwa Tiongkok adalah negara yang memiliki *cyberpower* yang cukup signifikan karena Tiongkok sudah dapat berkontribusi pada kemajuan dalam bidang TIK dan *cybersecurity*, memberi akses TIK yang mudah kepada masyarakatnya, dan melindungi dirinya dari ancaman-ancaman yang berkaitan dengan ranah *cyberspace* negaranya. *Cyberpower* yang dimiliki Tiongkok ini juga memungkinkan Tiongkok untuk memanfaatkan kecakapannya dan

kendalinya dalam bidang TIK untuk mempengaruhi aktor-aktor lain seperti mengusir perusahaan yang tidak menyesuaikan produk mereka untuk masyarakat Tiongkok seperti yang terjadi pada Google dan Yahoo yang terpaksa mundur dari Tiongkok, mengajak negara lain seperti Rusia, Iran dan Pakistan untuk membangun sistem seperti GFW di negara mereka, dan menormalkan gagasan kontrol pemerintah di internet melalui diskusi-diskusi dalam berbagai forum internasional seperti yang sedang mereka lakukan dalam forum ICANN dan W3C.

Kesimpulan

Artikel ini sudah mendeskripsikan penerapan GFW dan peran-perannya dalam membentuk Tiongkok sebagai negara yang kuat. Pertama, Tiongkok memanfaatkan GFW untuk menjamin cybersecurity-nya untuk mencegah, mendeteksi, dan merespons ancaman dengan mengawasi internet, sehingga dapat mencegah dan mendeteksi ancaman, kemudian menyerahkan hasil pendeteksian ke pihak yang berwajib. GFW dilengkapi dengan teknologi yang canggih, didukung oleh berbagai badan pemerintah yang mengawasi, dan didasari hukum kriminal yang jelas sehingga GFW juga dapat menjamin kerahasiaan, integritas, dan ketersediaan informasi dengan memanfaatkan teknologi yang canggih, jangkauan jaringan yang luas, dan proses penyaringan konten yang berlapis. Dalam melindungi Tiongkok dari ancaman politik dalam dunia *cyber*, GFW menerapkan sistem penyaringan pada konten yang bertopik politik sehingga konten-konten politik yang berpotensi mengandung diskusi kontroversial dapat diulas oleh petugas yang berwenang sebelum dipublikasikan ke masyarakat luas atau dihapus.

GFW telah berperan membentuk Tiongkok sebagai negara kuat sesuai dengan definisi negara kuat dalam teori *cyberpower*. GFW memastikan seluruh masyarakat Tiongkok dapat tetap dengan mudah mengakses dan menggunakan berbagai fasilitas internet sambil tetap memastikan kontrol sosial. GFW berkontribusi dengan cara memupuk kemajuan kualitas SDM dan kualitas produk-produk TIK milik Tiongkok dengan cara membatasi peran produk luar negeri dalam kehidupan masyarakat Tiongkok. GFW telah sukses membentuk pandangan dalam masyarakat Tiongkok bahwa kontrol pemerintah dalam berinternet adalah suatu hal yang baik. Selain itu, Tiongkok juga sudah sukses meyakinkan beberapa negara bahwa GFW merupakan sistem yang baik sehingga sudah ada beberapa negara yang tertarik juga menerapkan sistem serupa GFW di negara mereka. Dengan memanfaatkan GFW sebagai alat pengaman *cybersecuirty*, terutama dari ancaman politik dari *cyberspace*, Tiongkok juga membangun *cyberpower*

yang memungkinkannya mempengaruhi aktor-aktor lain yang berelasi dengannya baik dari dalam negeri maupun luar negeri.

GFW juga berperan dalam membentuk Tiongkok sebagai negara yang kuat melalui kontrol atas konten dengan penyaringan dan penyensoran untuk menjamin bahwa seluruh konten yang beredar di internet tidak akan memicu konflik dan menciptakan kestabilan politik dalam *cyberspace* Tiongkok. Selain itu, karena GFW membatasi penggunaan produk-produk dari luar Tiongkok, masyarakat Tiongkok didorong untuk semakin berinovasi untuk mengembangkan berbagai pengganti dari produk-produk yang sama bagusnya bahkan melampaui produk-produk yang berasal dari luar negeri, sehingga masyarakat Tiongkok tidak tergantung dengan produk-produk luar negeri bahkan dapat memasarkan hasil karya mereka sebagai alternatif yang kompetitif. Dengan demikian, bagi Tiongkok, kontrol dan penyaringan melalui GFW membentuk kestabilan, keamanan, dan mendorong inovasi yang membentuk Tiongkok menjadi negara yang kuat.

Referensi

Anderson, P. 2005. *The Global Politics of Power, Justice and Death.* New York: Routledge.

Andress, J., and S. Winterfeld. 2014. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners.* Waltham: Elsevier.

Bajwa, J. S. 2008. "Defining Elements of Comprehensive National Power." *CLAWS Journal,* 151-162.

Balke, L. 2018. "China's New Cybersecurity Law and U.S-China Cybersecurity Issues." *Santa Clara Law Review,*137-163.

Bayuk, J.L., J. Healey, P. Rohmeyer, M.H. Sachs, J. Schmidt, and J. Weiss. 2012. *Cyber Security Policy Guidebook.* New York: John Wiley and Sons.

Bogdan, R., and S.K. Biklen. 2007. *Qualitative Research for Education: An Introduction to Theories and Methods.* Boston: Pearson A & B.

Bu, R. 2013. *The Great Firewall of China.* Murray: Murray State University.

Carr, M. 2016. *US Power and the Internet in International Relations.* New York: Palgrave Macmillan.

Carsten, P., and M, Martina. 2016. "U.S. Says China Internet Censorship A Burden for Businesses." *Reuters,* https://www.reuters.com/article/us-usa-china-trade-internet/u-s-says-china-internet-censorship-a-burden-for-businesses-idUSKCN0X50RD

CBC Radio. 2019. "Counter-Protests Against Pro-Hong Kong Demonstrators May Reflect Chinese State Influence." *CBC,* https://www.cbc.ca/radio/day6/hong-kong-counter-protests-vasek-pospisil-cosplaying-while-black-ao3-gets-a-hugo-how-to-free-dive-and-more-1.5256258/counter-protests-against-pro-hong-kong-demonstrators-may-reflect-chinese-state-influence-1.5256272

Chan, E. 2018. "The Great Firewall of China." *Bloomberg*, https://www.bloomberg.com/quicktake/great-firewall-of-china

Chan, G. 1999. *Chinese Perspectives on International Relations: A Framework for Analysis.* London: Macmillan Press.

Chinese Academy of Cyberspace Studies, 2018. *China Internet Development Report 2018: Blue Book of World Internet Conference,* Beijing: Springer.

Choucri, N. 2012. *Cyberpolitics in International Relations.* Cambridge: Massachusetts Institute of Technology University Press.

Cornish, P. 2009. *Cyber Security and Politically, Socially, and Religiously Motivated Cyber Attacks,* Brussels: European Parliament.

Dainith, J., and E. Wright. 2006. *The Facts on File Dictionary of Computer Science.* New York: Facts On File.

Denyer, S. 2016. "China's Scary Lesson to the World: Censoring the Internet Works." *Washington Post,* https://www.washingtonpost.com/world/asia_pacific/chinas-scary-lesson-to-the-world-censoring-the-internet-works/2016/05/23/413afe78-fff3-11e5-8bb1-f124a43f84dc_story.html

Derian, J. D. 2003. "The Question of Information Technology in International Relations." *Millennium: Journal of International Studies,* 441-456.

Dou, E. 2015. "China's Great Firewall Gets Taller." *WSJ,* https://www.wsj.com/articles/chinas-great-firewall-gets-taller-1422607143

Esfandiari, G. 2020. "Iran To Work with China to Create National Internet System." *RFERL,* https://www.rferl.org/amp/iran-china-national-internet-system-censorship/30820857.html [Accessed 6 April 2021].

FireEye. 2020. *A Global Reset: Cyber Security Predictions 2021,* Milpitas: FireEye.

Goldsmith, J., and T. Wu. 2006. *Who Controls the Internet? Illusions of Borderless World.* New York: Oxford University Press.

Goldsmith, J., and T. Wu. 2006. *Who Controls the Internet? lllusions of Borderless World.* New york: Oxford.

Goldstein, J. S., and J.C. Pevehouse. 2014. *International Relations.* New Jersey: Pearson.

Griffiths, J. 2019 . *The Great Firewall of China; How To Build and Control an Alternative Version of the Internet.* London: Zed Books.

Guo, S., and Feng, G. 2011. "Understanding Support for Internet Censorship in China: An Elaboration of the Theory of Reasoned Action." *Journal of Chinese Political Science* 17 (1): 34-52. https://doi.org/10.1007/s1136601191778.

Haixia, Q., 2017. *From Comprehensive National Power to Soft Power: A Study of the Chinese Scholars' Perception of Power.* Brisbane: Griffith University.

Hauben, R. 1998. *From the ARPANET to the Internet: A Study of the ARPANET TCP/IP Digest and of the Role of Online Communication in the Transition from the ARPANET to the Internet.* http://www.columbia.edu/~rh120/other/tcpdigest_paper.txt

Hilbert, M. 2016. "The Bad News is that the Digital Access Divide is Here to Stay: Domestically Installed Bandwidths Among 172 Countries for 1986 – 2014." *Telecommunications Policy* 40 (6): 567-581. https://doi.org/10.1016/j.telpol.2016.01.006.

Jordan, T. 2003. *Cyberpower: The Culture and Politics of Cyberspace and the Internet.* London: Routledge.

Kalathil, S. 2017. *Beyond the Great Firewall: How China Became a Global Information Power,* Washington: CIMA.

Keith, R. C., and Z. Lin. 2006. *New Crime in China: Public Order and Human Rights.* Oxon: Routledge.

Keith, R. C., and Z. Lin. 2006. *New Crime in China: Public Order and Human Rights.* New York: Routledge.

Khumalo, N. B., and M. Baloyi. 2018. "The Importance of Information in International." *Library Philosophy and Practice.*

King, G., J. Pan, and M.E. Roberts. 2013. "A Randomized Experimental Study of Censorship in China." *APSA 2013 Annual Meeting Paper,* pp. 1-25.

Liang, B., and H. Lu. 2010. "Development, Censorship, and Cyber Crimes in China." *Journal of Contemporary Criminal Justice* 26 (1): 103-120. https://doi.org/10.1177/1043986209350437.

Lukasik, S. J. 2011. "Why the Arpanet Was Built." *IEEE Annals of the History of Computing* 33 (3): 4-21. https://doi.org/10.1109/MAHC.2010.11.

Lune, H., and B.L. Berg. 2017. *Qualitative Research Methods for the Social Sciences.* Essex: Pearson.

MacKinnon, R. 2008. "Flatter World and Thicker Walls? Blogs, Censorship and Civic Discourse in China." *Public Choice* 134(1): 31-46. https://doi.org/10.1007/s11127-007-9199-0.

MacKinnon, R. 2012. *Consent of the Networked.* Philadelphia: Basic Books.

Mallik, A. 2016. *Role of Technology in International Affairs.* New Delhi: Pentagon Press.

Morgenthau, H. J. 1948. *Politics among Nations: The Struggle for Power and Peace.* A. A. Knopf.

Mozur, P. 2015. "Partnership Boosts Users Over China's Great Firewall." *New York Times*, 14 September.

Nye, J. S. 2011. *The Future of Power.* New York: Public Affairs.

Ping, P. 2017. *China Internet Development Report 2017.* Beijing: Springer.

Pollpeter, K. 2015. "China's Modernization Efforts and Activities in Outer Space, Cyberspace and the Arctic." Pp. 113-135 in *Assessing China's Power.* Hampshire: Palgrave Macmillan.

Qi, A., G. Shao, and W. Zheng. 2018. "Assessing China's Cybersecurity Law." *The International Journal of Technology Law and Practice* 34 (6):1-13. https://doi.org/10.1016/j.clsr.2018.08.007.

Qinglian, H. 2008. *The Fog of Censorship: Media Control in China.* New York: Human Rights in China.

Radunovic, V. 2010. *Diplo.* https://www.diplomacy.edu/resources/general/role-information-and-communication-technologies-diplomacy

Rauhala, E. 2016. "America Wants to Believe China Can't Innovate. Tech Tells A Different Story." https://www.washingtonpost.com/world/asia_pacific/america-wants-to-believe-china-cant-innovate-tech-tells-a-different-story/2016/07/19/c17cbea9-6ee6-479c-81fa-54051df598c5_story.html

Roberts, M. E. 2018. *Censored: Distraction and Diversion Inside China's Great Firewall.* New Jersey: Princeton University Press.

Shao, G. 2012. *Internet Law in China.* Cambridge: Chandos Publishing.

Shao, G. 2012. *Internet Law in China.* Oxford: Chandos Publishing.

Singer, P. W. and A. Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford: Oxford University Press.

Sipress, A. 2004. "An Indonesian's Prison Memoir Takes Holy War into Cyberspace." https://www.washingtonpost.com/archive/politics/2004/12/14/an-indonesians-prison-memoir-takes-holy-war-into-cyberspace/71edfe6f-5231-479f-8bab-2a3ce9944ccf/

Snape, D., and L. Spencer. 2003. "The Foundations of Qualitative Research." Pp. 3-5 in *Qualitative Research Practice: A Guide for Social Science Students and Researchers.* London: SAGE.

StatCounter. 2021. "Mobile Vendor Market Share Worldwide*."* https://gs.statcounter.com/vendor-market-share/mobile# [Accessed 16 April 2021].

Stevenson, C. 2007. "Breaching the Great Firewall: China's Internet Censorship and the Quest for Freedom of Expression in a Connected World." *Boston College International and Comparative Law Review* 30(2): 531-558. http://lawdigitalcommons.bc.edu/iclr/vol30/iss2/8.

Stewart, B. 2007. "ARPANET – The First Internet*."* https://www.livinginternet.com/i/ii_arpanet.htm

The United Nations. 2007. "Universal Declaration of Human Rights". http://www.un.org/events/humanrights/2007/hrphotos/declaration%20_eng.pdf (Accessed 12 February 2009).

Weiss, C. 2005. "Science, Technology and International Relations." *Science, Technology and International Relations* 27(3): 295-313. https://doi.org/10.1016/j.techsoc.2005.04.004.

Wijaya, T. 2015. "Democracy Deficit in China: A Choice or Foreordained?" *Jurnal Ilmiah Hubungan Internasional* 11 (2): 191-217. https://doi.org/10.26593/jihi.v11i2.1617.%25p.

Xu, X., Z.M. Mao, Z. M., and J.A. Halderman. 2011. *Internet Censorship in China: Where Does the Filtering Occur?* Atlanta: Springer.