Vol 10, No 1 (2024)
Journal Of Government : Manajemen Pemerintahan dan Otonomi Daerah

HWAWEI DALAM RIVALITAS TIONGKOK-AMERIKA

Dejehave Al Jannah[1], Fita Nofiana[2]

[1]Universitas 17 Agustus 1945 Jakarta

[1]email: dejehavealj@gmail.com

Abstrak

Studi ini mendiskusikan pemboikotan Huawei oleh Amerika Serikat karena diduga digunakan sebagai alat spionase Pemerintah Tiongkok. Fokus kajian akan memaparkan klaim Amerika Serikat akan terjadinya perang siber yang dimotori oleh Tiongkok melalui Huawei. Oleh karena itu, penelitian ini dikerangkai melalui dua konsep besar, yaitu keamanan dan perang siber di mana kajian literatur digunakan sebagai metode penelitian ini. Hasil analisis menunjukkan, bahwa ketakutan Amerika atas ancaman serangan siber cukup beralasan mengingat Tiongkok berhasil mengembangkan teknologi Artificial Intelligance (AI) dan telah terbukti melakukan beberapa kejahatan siber pada perusahaan-perusahaan, lembaga, hingga bank Amerika dan Eropa. Meskipun demikian, fakta tersebut hanyalah sedikit permasalahan antara Amerika dan Tiongkok. Perang siber hanyalah sebagian kecil dari potongan kue yang lebih besar, yaitu rivalitas antar negara.

Kata Kunci: Huawei, Amerika, Tiongkok, Perang Siber, Keamanan, Artificial Intelligence.

Abstract

This study examines the boycott of Huawei by the United States because it was allegedly used as a Chinese Government's espionage tool. This research will focus on explaining the United States claims that there will be a cyber war led by China through Huawei. Therefore, this research is structured through two major concepts, security study and cyber warfare . Literature studies are used as this research method. The results of the analysis show that America's fear of cyber attack threats is quite reasonable, considering that China has succeeded in developing Artificial Intelligence (AI) technology and has been proven to do some cyber crimes in companies, institutions, and American and European banks. Nevertheless, this fact is only a slight problem between America and China. Cyber war is only a small part of a larger piece of cake, rivalry between countries.

Key Words: Huawei, America, China, Cyber war, Security, Artificial Intelligence.

A. Pendahuluan

Kajian ini mendiskusikan tentang pemboikotan Huawei oleh Amerika Serikat pada 2019, karena diduga digunakan sebagai alat spionase Pemerintah Tiongkok. Fokus kajian akan memaparkan tentang klaim Amerika Serikat akan terjadinya *cyber war* akibat tindakan spionase dan peretasan. Kekhawatiran ini didukung dengan kemajuan teknologi *artificial intelligent* Tiongkok yang telah mampu mengawasi seluruh warganya dan diekspor di beberapa negara. Sementara itu, Tiongkok mengklaim bahwa kekhawatiran Amerika hanyalah soal persaingan ekonomi karena Huawei berhasil menjadi promotor teknologi 5G pertama di dunia. Teknologi generasi kelima atau 5G ini belum mampu dikembangkan oleh perusahaan dari negara manapun, termasuk Amerika Serikat.

Pemboikotan ini merupakan keputusan Presiden Donald J. Trump pada 23 Mei 2019 dengan memasukkan Huawei dalam The US Entity List nomor 4 bagian 744. Perusahaan Amerika Serikat dilarang menjual produk apapun ke Huawei dan dilarang membeli apapun dari Huawei. Sebagai contoh, tiga per empat chipset yang dibeli Huawei dari Qualcom, harus dihentikan. Semua aplikasi yang dimiliki Google juga memutuskan kerjasama dengan Huawei. Dampaknya, produk *smartphone* yang rilis pasca pemboikotan tidak lagi berbasis android dan tidak dilengkapi dengan produk dari Google. Secara terpisah, Departemen Keamanan dalam Negeri AS mengatakan bahwa pesawat nirawak militer Tiongkok dengan teknologi Huawei dikhawatirkan dapat menjadi sarana mata-mata Tiongkok. Data yang diperoleh dari pesawat nirawak tersebut diduga dapat memberikan informasi tak terbatas bagi Tiongkok. Nyatanya, pemboikotan ini tidak dianggap sebagai ancaman besar bagi Tiongkok mengingat mereka mengklaim sudah menerapkan chipset pengganti keluaran Qualcom. Tiongkok menunjukkan bahwa mereka mampu menjadi sejajar dengan Amerika, terutama dalam perkembangan teknologi informasi.

Berdasarkan pemaparan sebelumnya, terdapat dua klaim yang berbeda. Amerika mengklaim bahwa tindakan pemboikotan Huawei terkait dengan persoalan ancaman perang siber. Sementara Tiongkok hanya menganggap pemboikotan tersebut sebagai bentuk strategi perang dagang akibat kecanggihan perkembangan teknologi Huawei. Oleh karena itu, menarik untuk menganalisis lebih jauh apakah pemboikotan Amerika terhadap Huawei benar-benar dilatarbelakangi ketakutan akan adanya spionase dan peristiwa perang siber.

Guna menganalisis lebih dalam mengenai ancaman perang siber, penulis menggunakan beberapa konsep yang dianggap sesuai, yakni konsep keamanan dan perang siber. Konsep kemanan digunakan untuk mengkerangkai kekhawatiran Amerika terhadap munculnya berbagai ancaman terkait keamanan nasional terutama keamanan siber. Sedangkan konsep perang siber digunakan untuk mengkerangkai bentuk kecurigaan Amerika dan tindakan Tiongkok dalam melakukan berbagai tindakan spionase yang dituduhkan.

Pada masa perang dingin, kajian keamanan berfokus pada negara melalui militer karena tekanan atas perlombaan senjata nuklir. Pendekatan mengenai kemanan pada masa ini disebut dengan pendekatan tradisionalis atau realis. Kemanan versi tradisionalis menitikberatkan kemanan sebagai kebebasan dari segala mancam ancaman militer terhadap kelangsungngan hidup negara. Nyatanya, ancaman tidak hanya menyasar negara melainkan juga masyarakat dan lingkungan secara umum. Masalah kemanan tidak monolitik dan global, melainkan beragam dan muncul juga di ranah lokal. Pada tahun 1980-an pandangan tentang keamanan mulai berkembang. Pandangan baru ini dipelopori oleh The Compenhagen School of Framework dengan Barry Buzzan sebagai salah satu tokoh utama. Konsep ini dikenal juga dengan istilah *widening security*. Buzan dalam jurnalnya Rethinking Security after the Cold War (1997) menjelaskan pendekatan

widening berusaha memperluas dan memperdalam apa yang dimaksud dengan kemanan dengan memperluas domain mengenai ancaman.

Dalam mengkritisi keamanan model tradisional mereka menilai bahwa *core* utama studi kemanan tidak dapat dibatasi hanya pada masalah perang, kekerasan, militer, serta isu apa saja yang terkait dengan hal-hal tersebut. Pendekatan *widening* berangkat dari pandangan bahwa kebenaran tentang realitas merupakan intrepretasi yang dibangun secara sosial, begitupun dengan apa yang dianggap sebagai ancaman dan keamanan. Ancaman kemanan sebenarnya adalah hasil dari konstruksi sosial, ancaman tidak secara objektif ada dengan sendirinya. Oleh karenanya model ini tidak hanya melihat isu yang nyata-nyata sebagai ancaman, melainkan juga isu yang dirasa sebagai ancaman. Jika sebelumnya kelompok tradisional mendefinisikan kemanan sebagai kebebasan dari ancaman militer, maka kelompok ini mendefinisikan kemanan adalah tentang keberlangsungan hidup (*survival*).

Apakah semua masalah atau isu publik dapat dikategorikan sebagai ancaman keamanan? Sebuah masalah publik hanya dapat dimasukkan dalam kategori ancaman kemanan ketika pemimpin mulai membicarakannya, *".....when leaders (whether political, societal, or intellectual) begin to talk about them...*" (Buzzan, 1997: 14). Tidak hanya berhenti di situ, isu tersebut harus dapat diterima oleh masyarakat atau objek sasaran ancaman bahwa hal tersebut memang mengancam keberlangsungan hidup mereka. Singkatnya isu harus mampu menghadirkan kepanikan, Buzzan menyebutnya dengan istilah 'politik panik'. Biaya kepanikan menjadi daya pikat objek dan digunakan untuk untuk melegitimasi tindakan tindakan di luar aturan formal yang mengikat.

Buzzan menambahkan bahwa tidak adanya definisi khusus mengenai kemanan juga dikarenakan tiap sektor memiliki jenis ancaman dan objek sasaran yang berbeda. Sektor yang dimaksud Buzzan adalah militer, politik, ekonomi, sosial, dan lingkungan. Pada sektor politik, jika sebelumnya ancaman adalah tentang hal-hal yang berusaha mengganti prinsip negara, maka dalam pendekatan *widening* ancaman juga terkait hal-hal yang dapat merusak aturan, norma, dan institusi. Misalnya kegiatan korupsi, kolusi, dan nepotisme. Ancaman di sektor ekonomi dapat berupa bangkrutnya perusahaan-perusahaan akibat krisis moneter atau persaingan tidak sehat. Di sektor sosial, identitas kolektif berskala besar bisa menjadi ancaman bagi identitas-identitas kecil jika mereka yang termasuk dalam anggota kelompok identitas besar cenderung *close minded* terhadap pluralitas. Ancaman pada sektor lingkungan lebih bervariasi, mulai dari ancaman kepunahan spesis tertentu, habitat, hingga keberlangsungan planet akibat *global warming*. Lenturnya persepsi mengenai apa yang dianggap sebagai ancaman menjadikan ancaman memiliki tingkat subjetivitas yang tinggi dan tak jarang masing-masing kelompok masyarakat mendefinisikan ancaman yang berbeda. Tiap negara biasanya memiliki perbedaan dalam pendefinisian ancaman. Sebut saja Amerika Serikat yang memandang terrorisme sebagai salah satu ancaman paling berbahaya, atau Inggris yang sangat terusik dengan banyaknya jumlah imigran.

Guna mendefiniskan apa itu perang siber, perlu dilihat terlebih dahulu tentang apa yang dimaksud sebagai 'perang'. Jason Andress dan Steve Winterfeld (2014) menjelaskan bahwa perang dapat dipahami melalui dua perspektif, yakni *on war* dan *art of war*. Ketika perang dipahami melalui perspektif *on war* maka akan mengarah pada perang langsung berupa duel, adu fisik, atau serangan bersenjata yang memaksa satu pihak tunduk pada pihak lain. Namun ketika perang diartikan sebagai *art of war* maka itu mencakup segala hal yang dapat menyebabkan hidup dan mati, yakni mengenai keselamatan atau kehancuran. Sehingga perang tidak hanya di definisikan sebagai bentuk serangan langsung melainkan juga segala hal yang mengancam keberlangsungan kehidupan. *Art of war* juga mencakup hukum moral, komando, dan metode. Kita akan lebih leluasa melihat perang siber dengan menggunakan konsep dari *art of war*.

Perang siber sendiri merupakan salah satu bentuk perang modern. Apabila perang tradisional berfokus pada upaya pengendalian sumber daya yang terbatas di mana kemampuan bertarung ditentukan oleh jumlah pasukan, senjata, dan logistik, pada perang modern fokus utama adalah memperluas jumlah simpul jaringan agar mampu mengendalikan informasi dan memperluas pengaruh. Sementara kemampuan bertarung ditentukan oleh sistem dan jaringan komputasi (*hardware dan software*) serta kemampuan pencegahan. Perang siber menjadi salah satu ancaman paling berbahaya saat ini mengingat internet telah digunakan dalam berbagai objek vital, seperti jaringan komunikasi, transportasi, pertahanan dan kemanan, serta berbagai fasilitas publik lainnya. Apabila negara lain ingin mengetahui sistem persenjataan baru sebuah negara, mereka hanya perlu menyusup pada *server* informasi atau *mainframe* Departemen Pertahanan. Mereka tidak perlu lagi mencoba menyusupkan mata-mata atau bekerjasama dengan pihak dalam layaknya pada perang tradisional. Dalam operasi dunia maya, ruang pertempuran mencakup hal-hal, seperti jaringan, komputer, perangkat keras, perangkat lunak, aplikasi, protokol, perangkat seluler, dan orang-orang yang menjalankannya.

Perang siber dapat ditimbulkan oleh berbagai pihak, diantaranya adalah oleh orang dalam (*insider*) dan negara. *Insider* dapat menyebabkan 80% kerusakan karena mereka lebih memahami apa yang berharga dalam sistem mereka sendiri dan sering memiliki akses yang sah ke dalamnya. Selanjutnya *Advanced Presistent Threat* atau APT merupakan jenis seragan yang biasanya dipandu oleh negara. APT merupakan ancaman dengan dampak kerusakan paling tinggi, baik fisik maupun finansial. Inilah yang dikhawatirkan oleh Amerika serikat akan dilakukan oleh Tiongkok melalui produk-produk Huawei apabila mereka tidak melakukan pembatasan.

B. Metode Penelitian

Kajian ini merupakan penelitian kualitatif yang bertujuan untuk mengetahui dan memahami tentang pemboikotan Huawei oleh Amerika Serikat pada 2019 yang dilakukan lantaran adanya dugaan Huawei sebagai alat spionase Pemerintah Tiongkok. Fokus kajian akan memaparkan tentang klaim Amerika Serikat akan terjadinya cyber war akibat tindakan spionase dan peretasan. Untuk mengetahui dan memahami topik penelitian,

maka kajian ini menggunakan metode studi pustaka (library research). Metode ini menitiberatkan pada pengumpulan data melalui berbagai literature yang berkaitan dengan penelitian (Zed, 2004). Pengumpulan data dilakukan dengan mengumpulkan dan menganalisis berbagai sumber mulai dari buku, jurnal, artikel, hingga media. Sumber-sumber tersebut kemudian dianalisis secara kritis dan mandalam untuk memetakan cyber war dalam konteks pemboikotan Huawei oleh Amerika Serikat pada 2019. Peneliti juga menggunakan pendekatan studi kasus dalam mendalami peristiwa pemboikotan Huawei oleh Amerika Serikat pada 2019 dan keterkaitannya dengan cyber war dalam dugaan upaya spionase oleh pemerintahan Tiongkok.

C. Hasil dan pembahasan

Sebagai negara komunis, Tiongkok memegang teguh institusi dan ideologi mereka, sehingga prioritas utama negara tersebut adalah stabilitas nasional. Hal ini yang membuat Tiongkok memberikan hukuman tegas pada para penentang dan pelanggar ketertiban nasional. Sikap ideologis garis keras yang diterapkan dalam bentuk hukum dan ketertiban dianggap sudah ada sejak abad ketiga sebelum masehi. Pemikir dan penasihat elit Han Fei pada masa itu menguraikan filosofi legalisme yang kemudian dianggap melengkapi kekurangan etika Konfusianisme dan Taois Tiongkok. Pada filosofi tersebut menyatakan, bahwa kebajikan, kebenaran, cinta, dan kemurahan hati tidak ada gunanya, tetapi hukuman berat dan mengerikan bisa menjaga keadaan tetap teratur (Hough & Malik, 2015). Hal ini berpengaruh pada pandangan keamanan Tiongkok sendiri yang berpusat pada negara dengan hukum-hukum yang cukup mengikat. Tak mengherankan jika di Tiongkok muncul keganasan pembantaian para demonstran di Lapangan Tiananmen pada 1989 dan intoleransi pada pandangan-pandangan yang dianggap menyimpang.

Ambisi Tiongkok dalam menciptakan stabilitas nasional kini membuat Tiongkok melakukan pengawasan pada warganya sendiri. Menggunakan perangkat lunak melalui kamera pengintai, pemerintah Tiongkok mengawasi kegiatan warganya di setiap wilayah. Menurut laporan SCMP per Juli 2018, Tiongkok sudah memasang sekitar 200 juta kamera pengintai di seluruh negeri (Jiaquan, 2018). Kamera-kamera ini diapasang di berbagai fasilias umum, jalan besar, maupun kecil, dan lain sebagainya.

Selain kamera yang terpasang, belum lama ini Tiongkok mulai mengembangkan perangkat pengenalan wajah (*face recognition*) yang terintegrasi dengan database warga. Perangkat ini disematkan di berbagai alat aparat dan pejabat, termasuk kacamata yang digunakan polisi dan tentara. Perangkat lunak pengenal wajah itu disebut dengan "*Gait Recognition*" di mana tak hanya mampu mendeteksi wajah, perangkat ini juga bisa mendeteksi seseorang hanya dengan bentuk tubuh dan cara berjalan dengan jarak maksimal 50 meter (Debora, 2018). Perangkat juga bahkan bisa memindai data meski hanya tampak punggung atau dengan wajah tertutup dengan kecepatan mencapai 3 detik dan keabsahan data hingga 90 persen.

Sistem pengintai tersebut digunakan untuk tujuan keamanan dan pemerintahan. Untuk birokrasi sendiri, perangkat ini digunakan sebagai pusat administrasi publik dan

memudahkan berbagai urusan lain, seperti mengurus imigrasi hingga simpan pinjam di bank. Sedangkan dalam konteks keamanan, perangkat ini digunakan untuk melacak buronan, mengawasi gerak-gerik warga, ketertiban lalu lintas, sekolah, hingga rumah sakit. Pada beberapa wilayah di Tiongkok, tentara-tentara juga menerbangkan drone berbentuk merpati (*dove drone*). Drone ini sangat menyerupai burung merpati asli yang diterbangkan untuk mengintai kegiatan warga.

Teknologi pengenalan wajah sendiri sebelumnya telah digunakan di berbagai aspek, selain pemerintah dan keamanan. Outlet KFC di Hangzhou telah meluncurkan sistem *"Smile to Pay"* di mana pembayaran dilakukan melalui scan wajah. Universitas juga menggunakan perangkat ini untuk menyaring staf dan mahasiswa, sekolah-sekolah menggunakannya untuk mengawasi perhatian siswa, hingga beberapa toilet di Beijing menyediakan pemindai wajah ini untuk membatasi jumlah tisu di toilet umum. Tak hanya pemindai wajah, pabrik-pabrik di Tiongkok bahkan memasang alat pendeteksi emosi pekerja dalam helm keamanan pekerja.

Sekilas, teknologi ini memang terlihat membantu di berbagai aspek karena membuat kerja menjadi lebih efektif. Namun, teknologi seperti ini mendapatkan banyak perhatian karena dianggap melanggar privasi warganya. Pengawasan warga paling mencolok di Tiongkok dilakukan di Xinjiang, daerah dengan minoritas Uighur (minoritas muslim Tiongkok). Wilayah ini mendapatkan pengamanan paling ketat di Tiongkok dengan dalih memerangi ektremisme yang mungkin datang dari komunitas muslim. Laporan Human Rights Watch menggambarkan aplikasi seluler yang digunakan polisi dan pejabat pemerintah di Xianjiang memiliki basis data yang sangat luas, bahkan bisa melacak informasi pribadi sedetail warna mobil orang.

Menurut laporan Human Right Watch, di Xianjang ada pengembangan Platform Operasi Gabungan Terpadu (IJOP) untuk melakukan pengawasan lebih pada warga. Platform ini merekayasa aplikasi seluler warga yang terhubung ke sistem, sehingga bisa melacak pergerakan setiap orang dengan memantu lintasan dan data lokasi ponsel. Selain melacak pergerakan, IJOP ini bahkan bisa melacak identitas, kendaraan, hingga penggunaan listrik dan gas. Ketika sistem IJOP mendeteksi penyimpangan, seperti menggunakan telefon dengan nomor yang tidak terdaftar atas nama mereka, menggunakan lebih banyak listrik, hingga meninggalkan rumah, sistem akan mengajukan pengaduan dan polisi akan melakukan investigasi.

Polisi memeriksa ponsel warganya untuk melihat apakah ponsel mereka mengandung salah satu dari 51 alat jaringan yang dianggap mencurigakan, seperti jaringan pribadi *virtual* dan program komunikasi seperti WhatsApp. Polisi menilai apakah seseorang cocok dengan salah satu dari 36 "tipe orang" yang pantas mendapatkan perhatian khusus, termasuk orang yang telah bepergian ke luar negeri, memiliki lebih banyak anak daripada yang diizinkan, atau menyebarkan nilai-nilai Islam tanpa izin. Semua data dikirim kembali ke sistem pusat IJOP melalui aplikasi, di mana data tersebut disimpan dalam *database* yang juga berisi gambar wajah dan banyak data lainnya.

Human Rights Watch bahkan menunjukkan bahwa sistem pengawasan serupa nyataya diterapkan di seluruh Tiongkok. Seperti yang telah dijelaskan sebelumnya, bahwa setidaknya ada sekitar 200 juta kamera pengintai warga yang dioperasikan di seluruh negeri. Tak hanya itu, aplikasi perpesanan dan pencarian pun sudah terintegrasi dengan sistem yang bisa diawasi oleh pemerintah. Aplikasi perpesanan terpopuler di Tiongkok, WeChat tidak menyediakan enkripsi ujung ke ujung, yang berarti bisa menghadirkan pihak ketiga. Dalam hal ini, peretas, pemerintah, dan operator internet memiliki saluran untuk mengakses pesan dan data pengguna (Watch, 2019).

Pengawasan Tiongkok terhadap warganya ini mirip dengan konsep *panopticon* yang mulanya dirancang sebagai sebuah arsitektur bangunan oleh Jeremy Bentham. *Panopticon* sendiri merupakan sebuah bangunan melingkar berisi kamar-kamar atau sel-sel di mana di tengah ada menara pengawas. Kamar-kamar tersebut berdinding kaca, sehingga menara utama yang berada di tengah bisa mengawasi setiap pergerakan orang di tiap-tiap kamar atau sel (Suryono, 2002). Bangunan ala Bentam ini yang kemudian dianggap Foucault sebagai konsep paling pas dalam menggambarkan pendisiplinan warga. Dalam bukunya Dicipline and Punish, Foucault menggunakan *panopticon* sebagai cara untuk menggambarkan kecenderungan pendisiplinan masyarakat yang menundukkan warganya. Dia menggambarkan tahanan dari sebuah *panopticon* berada di ujung pengawasan asimetris di mana tahanan tidak melihat pengawas, tapi tahu sedang diawasi.

Sebagai akibatnya, narapidana mengawasi dirinya sendiri karena takut akan hukuman. Prinsip dari *panopticon* yang muncul dari Bentham sendiri berawal dari gagasan, bahwa seseorang akan melakukan hal yang lebih baik jika berada dalam pengawasan (Suryono, 2002). Konsep *panopticon* sendiri mirip dengan pengawasan pemerintah Tiongkok pada wargaya di masa kini, yaitu dengan kamera-kamera pengawas. Dalam banyak hal, menara pengawal di tengah *panopticon* sama dengan pusat pengawasan CCTV di mana kamera tersebar luas di daratan Tiongkok. Sama halnya pada *panopticon*, warga dalam pengawasan kamera tidak melihat secara langsung pengawas, namun mengetahui jika mereka sedang dalam pengawasan. Tujuan *panopticon* sendiri adalah untuk mengendalikan perilaku masyarakat, sama halnya Tiongkok yang mengendalikan masyarakat demi stabilitas nasional.

Pengawasan Tiongkok nyatanya bukan hanya terhadap warga sendiri, Tiongkok juga disebut mengekspor perangkat-perangkat pengawas warga dan melakukan spionase di negara-negara lain. Tiongkok telah dipercaya Afrika untuk mengembangkan teknologi pengawas warga. Begitupun Venezuela tahun 2018 lalu juga meluncurkan Homeland Card, yang diproduksi oleh ZTE Corp, yang bisa melacak, memberi penghargaan, dan menghukum warga negara tergantung pada tindakan. Beberapa negara lain, seperti Singapura, Thailand, Filipina, Pakistan, Zimbabwe, dan Ekuador juga telah membeli produk Tiongkok mulai dari kamera polisi hingga jaringan CCTV "Safety City".

Saat ini, lebih dari 30.000 perusahaan pengawasan Tiongkok memiliki lebih dari 1,6 juta karyawan. Perusahaan-perusahaan ini dipimpin oleh Perusahaan Huawei, Zhejiang

Dahua, dan Hikvision. Mereka bekerja untuk menyempurnakan dan mengekspor sistem pengawasan massal Tiongkok. Produk mereka seperti kamera Hikvision banyak dijual di Amerika Serikat. Beberapa dari mereka, seperti Alibaba, menggunakan pasar bebas Amerika untuk mengakses modal dan teknologi untuk mengembangkan produk pengawasan (Thayer & Han, 2019).

Pada konteks spionase, beberapa tahun terakhir Tiongkok telah disibukkan dengan ambisinya untuk berada setidaknya tepat di belakang Amerika Serikat (AS) dalam hal teknologi informasi. Tiongkok diduga telah berada di garis depan dalam berbagai kegiatan perang dunia maya pada beberapa tahun terakhir. Mereka melakukan peretasan dan merusak situs web bisnis Barat untuk keperluan spionase industri dan kompetisi keunggulan di berbagai bidang. Pada 2014, Pengadilan AS mengeluarkan surat perintah penangkapan pertama untuk personel militer Tiongkok yang diduga terlibat dalam kegiatan tersebut. Bukti terus meningkat bahwa Tiongkok berada di garis depan dalam memata-matai perusahaan Barat, politisi, dan aset strategis lainnya (Hough & Malik, 2015).

Pada bulan April 2014, sebuah laporan pemerintah AS menyarankan kontrol yang lebih ketat pada teknologi luar angkasa karena takut bahwa Tiongkok berusaha mencurinya. Demikian pula, pada 2013, para diplomat Eropa mengetahui upaya Tiongkok untuk memata-matai mereka. Tetapi Tiongkok merespon dengan penolakan, diikuti tuduhan balasan yang ditujukan kepada AS dan Eropa (Hough & Malik, 2015). Menurut Jeffrey Carr, penulis Inside Cyber Warfare: Mapping the Cyber Underworld, banyak negara, seperti India dan Rusia, mencuri kekayaan intelektual Barat (terutama AS). Meskipun begitu, Tiongkok tetap dipilih oleh banyak agen keamanan serta perusahaan sebagai pihak yang paling bertanggung jawab hingga 80% atas semua peretasan dan spionase dari perusahaan AS. Amerika juga khawatir apabila data yang Huawei peroleh dimanfaatkan oleh pemerintah Tiongkok terlebih melihat adanya peraturan dalam Tiongkok's Cyber Security Act, yang mulai diberlakukan pada 2017, yang mewajibkan perusahaan untuk menyimpan data pada server berbasis lokal sehingga memungkinkan akses data penuh oleh pemerintah.

Melalui kecanggihan dan ambisi Tiongkok, tak mengherankan jika Amerika cukup geram dan mengambil langkah tegas. Amerika telah membokir beberapa perusahaan yang diduga bekerjasama dengan pemerintah Tiongkok dalam melakukan spionase, termasuk Huawei. Tak hanya itu, Amerika juga memberikan hukuman terkait tarif perdagangan antar kedua negara tersebut. Menurut National Counterintelligence and Security Center (NCSC) Amerika dalam laporan soal spionase *cyberspace,* manyatakan bahwa Tiongkok sering kali melakukan spionase terhadap Amerika. Bagi Amerika, Tiongkok berupaya keras dalam memperoleh informasi teknologi Amerika untuk mengintervensi rahasia perdagangan dan teknologi. Tiongkok dianggap terus menggunakan spionase dunia maya untuk mendukung sasaran pengembangan strategisnya dalam konteks kemajuan sains dan teknologi, modernisasi militer, dan sasaran kebijakan ekonomi. Operasi dunia maya

Tiongkok adalah bagian dari strategi pengembangan teknologi multi-kompleksitas yang menggunakan metode legal dan ilegal untuk mencapai tujuannya (Center, 2018).

Mengenai pelanggaran HAM di Tiongkok, Amerika melalui Trump Administration mulai mempertimbangkan sanksi-sanki yang akan dilakukan pada Tiongkok, terutama dalam kasus Xianjiang. Kongres Amerika mendesak agar pemerintah Trump mempertimbangkan sanksi yang menargetkan perusahaan dan pejabat yang terkait dengan tindakan keras Tiongkok, termasuk Sekretaris Partai Xinjiang, Chen Quanguo, sebagai anggota politbiro yang kuat, berada di eselon atas kepemimpinan Tiongkok. Sementara itu, Tiongkok mengatakan bahwa dalam persoalan HAM, Amerika seharusnya mengurusi pelanggaran di negaranya sendiri sebelum ikut campur urusan HAM negara lain. Faktanya, Amerika juga melakukan pelanggaran privasi melalui pengawasan terhadap warganya oleh National Security Agency (NSA). Fakta ini muncul melalui pengungkapan seorang mantan anggota NSA pada 2013.

Berdasarkan pemaparan mengenai kemajuan artificial intellegent yang dikembangkan oleh Tiongkok sebelumnya, tak heran apabila Amerika menjadi ‘paranoid’ dan terkesan menghalalkan berbagai cara untuk mengatasi ketakutan akan upaya perang siber serta spionase. Namun satu hal yang perlu ditekankan, bahwa kenyatannya Amerika Serikat telah melakukan hal serupa, jauh sebelum Tiongkok memberlakukan pengawasan cukup ketat melalui ribuan mata kamera. Amerika juga telah melakukan spionase serupa kepada beberapa negara dan pemimpin dunia.

Pada tahun 2013, publik Amerika dan dunia digegerkan dengan pernyataan Edward Snowden, mantan pekerja Central Intelligence Agency (CIA) dan National Security Agency (NSA), yang membocorkan program mata-mata NSA kepada pers. Ia mengungkapkan fakta bahwa ternyata upaya perlindungan yang dilakukan oleh Pemerintah Amerika Serikat dalam menangkal adanya perang siber, justru berakibat pada hilangnya privasi dan kebebasan individu. Pemerintah Amerika telah melakukan spionase kepada berbagai negara seperti Tiongkok, Rusia, dan Iran. Tak berhenti di situ, spionase juga dilakukan pada negara-negara sekutunya termasuk Jepang. Melalui pembangunan Epic Shelter, mereka menyusupkan penyadapan pada sistem komunikasi, infrastruktur fisik, pembangkit listrik, bendungan air, hingga rumah sakit di Jepang. Pemerintah Amerika berdalih bahwa ini merupakan upaya *jaga-jaga* apabila suatu hari Jepang tidak lagi menjadi sekutu Amerika. Pemerintah AS juga memata-matai para pemimpin dunia guna mempertahankan daya tawarnya dalam G20. Bahkan mereka tak segan memata-matai warga negaranya sendiri.

Pemerintah Amerika memiliki akses data pada 3,1 miliar lalu lintas komunikasi email warga negara Amerika, sementara di Rusia mereka hanya mengakses 1,5 miliar lalu lintas komunikasi. Artinya negara justru lebih banyak memata-matai warganya sendiri. Pemerintah berdalih bahwa tindakan pengawasan sejak awal ditujukan untuk mencegah ancaman *cyberspace* yang mungkin di timbulkan akibat keterlibatan warganya dengan pemerintah atau pihak asing. Tindakan pengawasan tidak secara langsung dimaksudkan untuk memata-matai warga negaranya. Kehadiran The Foreign Intelligence Surveillance

Act (FISA) semakin melegitimasi upaya pemerintah melakukan spionase tersebut. Selanjutnya Pemerintah Amerika juga memiliki *search engine* bernama XkeyScore, semacam mesin pencari Google, namun memiliki jangkauan yang lebih luas. XkeyScore dapat membaca email, melacak *hardware*, media sosial yang digunakan, *website* yang dikunjungi, serta metadata pengguna. Bahkan analis NSA juga dapat menggunakan XKeyscore yang dikolaborasikan dengan sistem lain untuk mencegat aktivitas seseorang di internet secara *real-time.* Corbin O'Brian, atasan Snowden berdalih bahwa cara yang diambil Pemerintah Amerika ditujukan untuk mewujudkan kebaikan dunia, mencegah kemunculan perang dunia ketiga, menciptakan kekayaan, dan keamanan. Bahwa tanpa adanya kerja keras intelijen sepanjang waktu, kita tidak akan bertahan dari perang nuklir, serangan teroris, dan serangan siber. Ia juga mengklaim bahwa sebagian besar orang Amerika lebih mengingkinkan rasa aman ketimbang kebebasan. Mereka rela menukar kebebasan dengan jaminan rasa aman dari negara.

Berdasarkan ketakutan akan kemungkinan serangan siber oleh Tiongkok terhadap Amerika, menarik untuk melihat apakah pernah terjadi perang siber antar negara sebelumnya. Andress dan Winterfeld (2014) menjelaskan bahwa untuk menjawab pertanyaan tersebut, jawabannya tergantung pada definisi mengenai apa yang kita sebut sebagai 'perang'. Sampai saat ini tidak ada negara yang menyatakan perang siber, dan meskipun banyak negara telah berbicara tentang kegiatan cyber, tidak ada yang menyatakan mereka menderita kerugian akibat perang tersebut. Selama ini yang ada hanyalah serangan siber. Mengutip pernyataan Thomas Rid (2011) dalam Andress dan Winterfeld (2014) berpendapat bahwa kemungkinan terjadinya perang siber adalah sangat kecil bahkan cenderung tidak mungkin terjadi. Apa yang selama ini disebut sebagai serangan-serangan siber nyatanya hanyalah upaya subversi, spionase, dan sabotase yang dilakukan antar negara.

D. Kesimpulan

Melalui analisis yang telah dipaparkan kami menyimpulkan, bahwa pemboikotan Huawei, lebih merupakan sebuah rivalitas kedua negara besar dalam bentuk saling mengawasi kemajuan teknologi dan ancaman yang mengikutinya. Ketakutan Amerika akan kemajuan teknologi *artificial intelligence* dan aktivisme spionase Tiongkok memang cukup berdasar, sebab beberapa peretasan terbukti didalangi oleh Tiongkok baik melalui perusahaan maupun langsung oleh negara. Apalagi, Amerika sama halnya dengan Tiongkok yang melakukan pengawasan terhadap warganya sendiri sepanjang waktu. Amerika memiliki data yang sangat banyak terkait lalu lintas komunikasi maupun perekonomian dari hasil penyadapan NSA. Apabila data-data ini terinfeksi oleh teknologi peretas Tiongkok−yang diduga berasal dari Huawei−maka, Tiongkok akan sangat mudah membaca strategi keamanan negara dan rencana strategis di sektor lain.

Meskipun begitu, fakta tersebut hanyalah sedikit permasalahan antara Amerika dan Tiongkok. Perang siber hanyalah sebagian kecil dari potongan kue yang lebih besar, yaitu rivalitas itu sendiri. Oleh karena itu, kami menyimpulkan, bahwa di luar persoalan

ancaman perang siber, nyatanya ini merupakan sebuah upaya pengendalian ekonomi dan sosial untuk mempertahankan atau bahkan memperkuat supremasi pemerintahan masing-masing. Kami juga berasumsi, bahwa tindakan spionase yang dilakukan antar negara sebenarnya merupakan bentuk terselubung perang dagang terutama perdagangan teknologi dan informasi. Mengingat perkembangan masyarakat yang sangat bergantung pada jaringan komputasi, maka siapa yang paling menguasai data dan informasi, dia lah yang menguasai dunia. Tak heran negara begitu sensitif terhadap ancaman pencurian informasi melalui jaringan siber dan berbagai tindakan pencegahan terus dilakukan termasuk spionase dan pemboikotan.

Daftar Pustaka

Andress, J., & Winterfeld, S. (2014). *Cyber Warfare: Techniques, Tactics, and Tools for Security Practitioners.* Elsevier Inc.: United State of America.

Buzan, B. (1997). Rethinking Security after the Cold War. SAGE, 5-28.

Center, N. C. (2018). *Foreign Economic Espionage in Cyberspace.* Office of The Director of National Intelligent.

Debora, Y. (2018, November 6). *Tiongkok Kini Dapat Mendeteksi Warga Hanya Melalui Cara Jalan.* Retrieved from Tirto.id: https://tirto.id/Tiongkok-kini-dapat-mendeteksi-warga-hanya-melalui-cara-jalan-c9ob.

Holland, T. (2019, Mei 25). *Don't ask why US acted against China's Huawei. Ask: why now? Retrieved from scmp.com:* https://www.scmp.com/week-asia/opinion/article/2176891/dont-ask-why-us-acted-against-chinas-huawei-ask-why-now

Hough, P., & Malik, S. (2015). *Tiongkok: Security and Threat Preceptions.* In P. Hough, S. Malik, A. Moran, & B. Pilbeam, International Security Studies: Theory and Practice. New York: Routledge.

Iskan, D. (2019, Mei 22). *Long-March Huawei.* Retrieved from Disway.id: https://www.disway.id/r/458/long-h-march

Jiaquan, Z. (2018, Agustus 4). *Drones, facial recognition and a social credit system: 10 ways Tiongkok watches its citizens.* Retrieved from South Tiongkok Morning Post: https://www.scmp.com/news/Tiongkok/society/article/2157883/drones-facial-recognition-and-social-credit-system-10-ways-Tiongkok

Suryono, S. J. (2002). *Tubuh yang Rasis.* Yogyakarta: Pustaka Pelajar.

Thayer, B. A., & Han, L. (2019, 5 29). *Tiongkok's weapon of mass surveillance is a human rights abuse.* Retrieved from The Hill: https://thehill.com/technology/445726-Tiongkoks-weapon-of-mass-surveillance-is-a-human-rights-abuse.

Watch, H. R. (2019, Mei 1). *Tiongkok's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App.* Retrieved from hrw.org:

https://www.hrw.org/report/2019/05/01/Tiongkoks-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance#page.

Wei, C. (2018, Mei 17). Chinese school uses facial recognition to monitor student attention in class. Retrieved from telegraph.co.uk: https://www.telegraph.co.uk/news/2018/05/17/chinese-school-uses-facial-recognition-monitor-student-attention/.

Zed, Mastika. (2008). *Metode Penelitian Kepustakaan.* Jakarta: Yayasan Obor Indonesia.