BAB VI
PENUTUP

VI.1 Kesimpulan

Dalam penelitian ini, Cina memiliki sumber daya berupa perusahaan-perusahaan teknologi dan juga didukung oleh pengembangan ilmu pengetahuan teknologi yang sudah dijalankan sejak zaman pemerintahan Deng Xiaoping yang merupakan tokoh revolusi ekonomi Cina. Dengan segala sumber daya yang dimiliki dan proses panjang yang telah dilewati, Cina memilik ambisi untuk mencapai kepentingan nasionalnya dalam sektor teknologi yakni mencapai *high-tech global superpower* pada tahun 2025 atau *Made in China* 2025.

Cina menggabungkan sumber daya yang inovatif dengan diplomasi dan juga *power* yang dimiliki baik secara ekonomi maupun secara politik dan militer untuk mewujudkan *Made in China* 2020. Hal ini berkaitan dengan penelitian ini. Cina memiliki berbagai sumber daya yang inovatif dalam bidang teknologi, salah satunya yakni Huawei. Huawei adalah perusahaan swasta yang merupakan bagian dari Cina. Huawei juga merupakan salah satu perusahaan yang berkembang pada awal revolusi ekonomi Cina. Hingga saat ini, Huawei sudah memiliki jaringan hingga seluruh pelosok dunia dan sudah melayani sepertiga populasi dunia dengan teknologi yang dihasilkannya. Oleh karena itu, Huawei memiliki potensi untuk mewujudkan kepentingan nasional Cina dalam bidang teknologi yakni *Made in China* 2025. Selain mendukung Cina mencapai *Made in China* 2025, Huawei juga secara langsung dan tidak langsung mendukung Cina dalam menghadapi tantangan keamanan siber global. Huawei memiliki pusat peneltian keamanan siber dan sudah menghasilkan *Huawei Cyber Security White Paper*.

Tantangan keamanan siber global selalu dinamis dan berkembang secara pesat seiring perkembangan teknologi informasi dan komunikasi serta lingkungan siber itu sendiri. Tantangan keamanan siber global adalah ancaman siber yang bermacam-macama. Ancaman siber merupakan hasil evolusi dari ancaman tradisional ke ancaman non tradisional. Ancaman siber merupakan hasil inovasi

dari perkembangan kemajuan TIK. Contoh ancaman siber yang menjadi tantangan bagi keamanan siber global adalah seperti terorisme siber, hacktivist, malware, spionase siber, kejahatan siber dan perang siber. Perubahan juga dialami dalam dunia militer. Ancaman perang siber mengharuskan suatu negara untuk menerapkan konsep *revolution in military affairs* (RMA) untuk menanggapi ancaman aktual. Esesnsi perang pada masa sekarang bukan hanya terletak pada perang fisik melainkan sudah diterapkan dalam ruang siber. Pada masa damai seperti sekarang ini, negara-negara secara masif mengembangan kapabilitas keamanan siber dan kekuatan siber untuk menghadapi ancaman siber yang berskala besar seperti perang siber.

Keamanan siber global diterapkan oleh semua negara dan semua aktor selain negara. Dalam lingkungan internasional, keamanan siber global dinilai melalui *Global Cyber Security Index* (GCI). Negara-negara diharapkan untuk tetap berkomitmen dalam pengembangan keamanan siber. GCI melalui lima pilarnya secara tidak langsung memotivasi negara-negara untuk menguatkan sistem keamanan siber mulai dari hukum, organisasi, CERT, CBM dan hal lainnya. Untuk terciptanya keamanan global terkhusunya keamanan siber global, negara harus berusaha untuk meningkatkan kekuatan siber dengan *capacity building measures* dan mengembangkanan CERT/CIRT/CSIRT. Tujuannya adalah ketika ada insiden atau ancaman siber, negara telah siap untuk mengatasai dan menangani bahkan bisa mencegah ancaman siber sebelum terjadi insiden siber.

Akan tetapi, negara tidak dengan mudah membangunan keamanan siber global. Hal itu dikarenakan terus terjadi insiden siber dan serangan siber baik dalam skala nasional, regional maupun global. Berkaitan dengan fokus penelitian ini, Cina dalam skala nasional menghadapi tantangan keamanan siber global melalui lembaga CNCERT/CC yang bertugas untuk menganalisis ancaman siber, mencegah ancaman siber, menangani ancaman siber berdasarkan laporan yang masuk dan juga melakukan deteksi dan analisis terhadap insiden siber yang terjadi. Dalam lingkup nasional, ancaman siber juga dating dari internal atau domestic Cina seperti *phising, malware, vulneberalities* dan juga *backdoor*. Sasaran serangan siber ditujukan kepada masyarakat sipil, perusahaan dan organisasi yang disebut dalam laporan

sebagai daratan Cina. Selain itu, pemerintah Cina juga menjadi target serangan. Akan tetapi berdasarkan laporan mingguan yang dirangkum penulis dalam jangka waktu enam bulan yakni terhitung dari Desember 2019 sampai Mei 2020, Cina melalui CNCERT mampu mengatasi sebagian besar insiden siber yang terjadi.

Dalam penelitian ini secara khusus membahas tentang strategi keamanan Cina dalam menghadapi tantangan keamanan siber global. Stretegi keamanan nasional Cina adalah *Comprehensive National Power* (CNP) dan *Comprehensive National Security Outlook* (CNSO). CNP mengoptimalisasikan penggunaan kekuatan nasional untuk mewujudkan kepentingan nasional Cina. Hasil yang diharapkan dari CNP adalah kondisi damai, pembangunan perekonomian Cina tanpa gangguan dari konflik yang besar. Pengoptimalisasian kekuatan nasional oleh CNP sama seperti yang dikatakan oleh Morgenthau yakni kekuatan nasional adalah kekuatan atau faktor pendukung yang membantu negara untuk mencapai kepentingan nasional. Sedangkan CNSO meningkatkan keamanan nasional seperti keamanan tradisional dan keamanan non tradisional. Selain itu, CNSO juga memfokuskan pada keamanan internal dan keamanan eksternal. Dalam menghadapi tantangan siber global, Cina membentuk aliansi siber dengan Rusia dalam OEWG pada *Shanghai Corporation Organization.* OEWG menjadi arena atau wadah bagi Cina untuk perumusan *Intrenational Cyber Norms Behaviour.*

Peran Huawei dalam strategi keamanan Cina untuk menghadapi *global cyber security challenge* adalah sangat signifikan. Cina memanfaatkan kekuatan nasional berdasarkan pada CNP. Huawei menjadi salah satu instrument Cina dalam menanggapi tantangan keamanan siber global. Huawei selalu melakukan inovasi dalam pengembangan TIK. Kontribusi Huawei seperti membangun kerjasama dengan CNCERT/CC (China *Computer Emergency Response Technical Team*), CNNIC (*China Internet Network Information Centre*), dan APAC (*Anti-Phishing Alliance of China*). Dalam kerjasama tersebut, Huawei berfokus pada bidang keamanan siber seperti pemodelan ancaman, deteksi *malware* dan analisis perilaku serangan, untuk secara efektif membagikan kapabilitas keamanan. Kontribusi Huawei yang menjadi jawaban dalam penelitian ini adalah terkait kerjasama dengan lembaga-lembaga Cina. Huawei membantu CNCERT/CC dalam pemodelan

ancaman, deteksi malware, dan analisis perilaku ancaman. Seperti yang telah dibahas dalam pembahasan, CNCERT/CC juga bekerjasama dengan organiasi, perusahaan, lembaga pemerintahan Cina, masyarakat sipil dan akademisi terkait keamanan siber atau keamanan informasi. Pada pembahasan ini, telah terjadi relasi antara pemerintah dan MNC. Selain sebagai perusahaan global, Huawei juga merupakan perusahaan nasional yang berasal dari Cina. Relasi antara negara dan MNC ditunjukkan dengan kebijakan yang ditetapkan oleh Cina melalui strategi keamanan nasionalnya untuk melibatkan segala sumber daya yang dimiliki untuk mencapai kepentingan nasional.

Selain bekerjasama dengan CNCERT/CC, Huawei juga melakukan kerjasama dengan *Anti-Phishing Alliance of China* (APAC) dan *China Internet Network Informatioan Center* (CNNIC). Kedua lembaga ini bekerja di ranah yang berbeda tapi memiliki tujuan yang sama yakni keamanan infromasi di internet atau keamanan siber. Lembaga-lembaga ini saling bersinergi untuk tercapainya keamanan siber. Huawei turut melakukan afiliasi bersama dengan kedua badan tersebut. Kontribusi Huawei di sini adalah sebagai perusahaan teknologi yang memberikan deteksi ancaman dan analisis ancaman baik berupa *phishing* maupun ancaman siber lainnya. Berkaitan dengan CNNIC, Huawei memberikan kontribusi dalam keamanan jaringan internet dan inovasi jaringan yang selalu dilakukan oleh Huawei termasuk inovasi infrastruktur 5G. Inovasi infrastruktur 5G adalah salah satu produk teknologi yang bisa menghasilkan kecepatan dalam koneksi internet. Hal tersebut berhubungan dengan tujuan CNNIC untuk menciptakan jaringan internet yang baik, aman dan stabil. Tujuannya adalah untuk mendukung keamanan siber global. Huawei meyakini bahwa resolusi tantangan keamanan siber merupakan tantangan bersama. Oleh karena itu, setiap aktor harus secara bersama-sama, terbuka dan transparan untuk memberikan kontribusi positif, menerapkan hukum, standar, dan kebijakan internasional.

Untuk mewujudkan resolusi tantangan keamanan siber, Huawei melakukan penelitian dan pengembangan yang menghasilkan kajian dalam bentuk *white paper* keamanan siber dari tahu 2012 sampai dengan 2018. *Cyber Security White Paper* yang dihasilkan oleh Huawei membantu Cina dalam menghadapi *global cyber*

security challenge. Dalam dokumen yang dihasilkan oleh Huawei secara garis besar berisi anjuran dan solusi tentang keamanan siber bagi pengguna teknologi Huawei, kepada vendor, dan juga kepada seluruh pihak yang membangun kerjasama dengan Huawei. Segala hal yang dihasilkan oleh Huawei dalam bidang keamanan siber memiliki tujuan untuk resolusi tantangan keamanan siber.

VI.2 Saran

Dalam proses penelitian yang dilakukan, penulis menemukan banyak pengetahuan dan pembelajaran yang mendalam tentang keamanan siber. Hal itu dikarenakan banyak hal baru dan pengetahuan baru yang ditemukan oleh penulis yang berkaitan dengan keamanan siber global dan kaitannya dalam hubungan internasional. Ruang siber menjadi ruang peluang dan ruang tantangan dalam keamanan internasional. Berdasarkan objek penelitian yang diambil oleh penulis yakni Huawei, tantangan keamanan siber global dan strategi keamanan Cina, keamanan internasional sedang dalam kondisi tidak kondusif akibat adanya tantangan keamanan siber global. Oleh karena itu, penulis ingin memberikan saran terkait hasil penelitian yang ditemukan oleh penulis.

Pertama, setiap negara diharapkan untuk mengembangkan, memperkuat dan juga meningkatkan kapasitas keamanan siber negara. Hal itu dikarenakan keamanan internasional sedang tidak kondusif dengan terus terjadinya serangan siber baik melalui aktor individu, kelompok *hacker* baik secara mandiri maupun disponsori oleh negara, murni serangan siber dari negara, dan berbagai macam aktor lainnya yang tidak bisa dipastikan kapan dan siapa yang akan melakukan serangan siber.

Kedua, negara harusnya mengajak kerjasama atau berkolaborasi dengan sumber daya atau kekuatan nasionalnya untuk mendukung terciptanya keamanan siber dalam upaya menghadapi tantangan keamanan siber global. Perlu diketahui bahwa tantangan keamanan siber global selalu berkembang sehingga membuat ancaman siber global menjadi dinamis. Penulis mengambil Huawei sebagai contohnya.

Ketiga, penulis menyarankan kepada negara untuk meningkatkan sektor ilmu pengetahuan dan teknologi untuk perkembangan kemajuan negara dan sekaligus sebagai persiapan untuk menghadapi tantangan dan ancaman yang ada baik non tradisional maupun nasional. Potensi ancaman non tradisonal bisa menyebabkan potensi risiko lanjutan yang lebih besar dan dapat mennggganggu stabilitas keamanan internasional. Peningkatan ilmu pengetahuan dan teknologi juga harus diiringi dengan peningkatan anggaran untuk sektor ilmu pengetahuan dan teknologi. Selain, penelitian dan pengembangan juga wajib dilakukan terus oleh negara.

Keempat, negara harus memainkan peran dalam organisasi internsional untuk mencapai consensus bersama terkait norma siber yang sedang dibahas melalui UNGGE dan OEWG. Tatanan internasional membutuhkan norma yang mengatur prilaku dan batasan dalam ruang siber. Hal itu dikarenakan berdasarkan data yang ditemukan dalam penelitian, serangan siber mengakibatkan 'perang dingin siber' di mana negara saling balas serang dalam ruang siber.

Kelima, penulis menyarankan kepada negara untuk tetap komitmen dalam menerapkan lima pilar indikator yang ditetapkan dalam GCI. Menurut penulis, GCI adalah motivasi bagi negara untuk bagi negara untuk lebih maju dan lebih kuat dalam keamanan siber. Peningkatan kekuatan dan kapabilitas dalam keamanan siber pada organisasi atau lembaga yang bertanggung jawab terhadap keamanan siber sangat penting dan harus terus dikembangkan seperti penguatan CERT/CIRT/CSIRT. Libatkan semua pihak dalam usaha untuk mencegah dan menangani ancaman siber baik skala nasional, skala regional maupun skala global.

Keenam, penulis menyarankan negara untuk membangun diplomasi siber baik bilateral maupun multilateral dalam kaawasan maupun dalam lingkup internasional. Manfaat dan keuntungan dari adanya diplomasi yang dilakukan bisa bermacam-macam. Di satu sisi, negara bisa saling belajar dengan aktor diplomasi dan di sisi lain negara bisa mencegah terjadinya serangan siber yang berkelanjutan dan bahkan yang bisa menyebabkan perang siber.