

## **BAB V**

### **KESIMPULAN**

AS yang merupakan negara super power dalam dunia cyber menganggap China sebagai rival utama, namun kemudian memilih untuk melakukan kerja sama. Hal ini dapat diteliti dari teori politik luar negeri dan kepentingan nasional serta aktor rasional. Dimana AS memiliki kepentingan dalam mempertahankan keamanan nasional, cyber economic dan pengembangan dan perlindungan teknologi. Serta dipilihnya China sebagai partner sudah dipikirkan masak-masak oleh AS mengenai untung-rugi jika menjalin kerja sama dengan China maupun tetap bermusuhan.

Selanjutnya dijelaskan juga mengenai definisi dan perkembangan Cyber, dari awal mula muncul hingga di era sekarang. Selain dapat bermanfaat dalam melindungi data, kemajuan cyber juga dapat menyebabkan kerugian dalam jumlah besar. Teknologi seperti Firewall bisa sangat berguna dalam membendung masuknya malware yang dapat merusak atau bahkan mencuri data korban. Seiring dengan berkembangnya teknologi, kemudahan dalam melakukan tindak kejahatan pun tak terelakkan. Hanya dengan bermodal software berharga beberapa sen, seorang hacker dapat menjebol, merusak bahkan mencuri data. Kejahatan cyber yang biasanya terjadi adalah kriminal cyber, terorisme cyber, spionase cyber dan perang cyber, yang sampai saat ini masih belum benar-benar terjadi.

Kemudian, isu-isu cyber mengakibatkan pembentukan organisasi cyber di AS maupun China. AS sebagai negara yang telah lama menjadi kekuatan "nomor 1" dunia telah memiliki organisasi cyber yang terpusat dan memiliki sistem yang baik dalam penjurangan bakat-bakat dalam diri anak SMP hingga Mahasiswa melalui lomba dan kurikulum cyber yang telah diimplementasikan pada kurikulum SMP hingga perguruan tinggi. Isu cyber yang kerap terjadi di AS sendiri merupakan akibat dari serangan yang dilakukan China.

Sedang China, memiliki organisasi cyber yang bersifat desentralisasi. Bermula dari negara yang mengimpor teknologi dari AS hingga dapat menjadi negara adidaya. Kini, China sendiri berusaha untuk terus memperbaiki sistem pengkaderan dalam organisasi cyber dengan cara mencontoh cara-cara yang dilakukan AS.

Persaingan antara AS-China berujung pada aksi saling serang dan menyebabkan konflik. Kehadiran dua raksasa dalam dunia cyber mengakibatkan persaingan sengit dalam hal pengembangan cyber dan pembuktian siapa paling hebat. Namun, setelah mengalami banyak gesekan, akhirnya kedua negara menjalin kerja sama setelah kehadiran John Kerry di China, pertemuan dua kepala negara di Sunnylands Summit dan dialog grup kerja sama cyber di Washington pada tanggal 8-12 Juli 2013 sebagai bagian dari diskusi S&ED.

AS yang sebelumnya merupakan musuh terbesar China, diduga memiliki kepentingan dalam kerja sama keamanan cyber dengan China.

Kepentingannya adalah demi perlindungan kepentingan nasional, cyber economic dan perlindungan dan pengembangan teknologi. Seluruh instansi pemerintah, perusahaan dan sektor publik telah terintegrasi ke sistem jaringan dan internet. Oleh karena itu, menjadi penting untuk melakukan perlindungan kepada instansi dan sektor penting negara. Jika tidak terproteksi maka akan terjadi kerusakan dan kerugian besar. Dengan terjalannya kerja sama dengan China, AS dapat sedikit bernapas lega karena ancaman utama terhadap keamanan nasional telah sedikit diminimalisir.

Instansi pemerintah dan bank serta perusahaan termasuk dalam cakupan cyber economic. Tanpa perlindungan software mutakhir pada sektor ini, atau kerusakan sistem jaringan akibat dijebol oleh hacker dapat menyebabkan kerusakan dan kerugian besar. File yang hilang atau rusak, catatan transaksi yang diubah, dicuri atau dimusnahkan, uang di bank yang dicuri oleh hacker dan kerusakan sistem jaringan memerlukan waktu lama dan biaya besar untuk perbaikan. Sistem jaringan yang kadung jebol dapat membuat hacker lain dapat masuk ke instansi atau bank atau perusahaan. Selain itu, jumlah kerusakan pada perusahaan atau bank dapat membuat perusahaan terpaksa memecat karyawannya karena telah merugi dalam hal perbaikan sistem jaringan.

Cara China untuk menciptakan teknologi sangatlah sederhana. Curi, modifikasi dan patenkan. Proyek pengembangan teknologi termahal AS, JF-35 merupakan contoh shahih. AS merugi milyaran dollar karena teknologinya telah dicuri dan China mendapat keuntungan karena menjual tanpa perlu

biaya dan waktu lama dalam pengembangan. Tidak hanya pesawat, teknologi yang dikembangkan oleh Apple maupun Microsoft pernah menjadi korban perampokkan China.

Oleh karena itu AS memilih cara aman dengan berdamai dengan China. Dengan harapan bahwa China menjadi semakin "jinak" dan meminimalisir kerugian yang didapat dimasa mendatang.

Sebelum melakukan penelitian ini, penulis telah mendapatkan ilmu mengenai kepentingan negara pada semester empat pada mata kuliah teori politik internasional. Disitu, dijelaskan secara gamblang mengenai kepentingan negara melalui kepentingan nasional. Juga karakteristik negara yang anarkis, berkompetisi, bertahan hidup melalui hubungan dengan negara lain. Selain itu juga dipaparkan bahwa militer dan ekonomi merupakan dua unit yang dapat mendukung tercapainya kepentingan negara dan upaya untuk mempertahankan diri.

Ke depannya, penulis berharap bahwa penelitian mengenai hubungan kerja sama antara AS dan China dapat terus berjalan. Terutama mengenai tentang komitmen keduanya untuk saling menjaga hubungan kerja sama diantara keduanya. Serta perundingan untuk menetapkan hukum dan norma cyber yang sampai saat ini masih nihil. Dengan ditetapkan dan diberlakukannya hukum dan norma cyber yang jelas, ini berarti hubungan kerja sama diantara kedua negara dapat berjalan dalam jangka waktu yang panjang