BAB IV

KEAMANAN NASIONAL, PERKEMBANGAN CYBER ECONOMIC DAN PERLINDUNGAN DAN PENGEMBANGAN TEKNOLOGI

Setelah terjadi kesepakatan kerja sama antara AS-China, tentu menimbulkan banyak spekulasi mengenai mengapa AS sudi untuk menjalin kerja sama dengan rival terberatnya. Pada bab ini akan dipaparkan kemungkinan maksud terselubung AS. Diduga, kepentingan pribadi AS dibalik hubungan kerja samanya dengan China adalah demi keamanan nasionalnya, pengembangan cyber economic dan juga perlindungan dan pengembangan teknologi.

A. Keamanan Nasional

Di era sekarang ini, dimana semua aktivitas negara membutuhkan komputer dan terhubung dengan internet, perlindungan terhadap sistem jaringan sangat penting. Upaya yang dapat dilakukan oleh negara terkait dengan perlindungan institusi adalah dengan pembentukan badan cyber nasional. Sehingga keamanan nasional negara, yang didalamnya terdapat institusi keuangan, kesehatan dan institusi lain aman dari serangan cyber yang dapat merugikan negara.

Gambar 4.1 sektor dan infrastruktur penting AS

Sumber: Robert E. Kahn, dkk, " America's Cyber Future: Security And Prosperity In The Information Age", Kristin M Lord And Travis Sharp (Ed.), (United States:Center For American New Security, 2011)

Tabel diatas menjabarkan infrastruktur penting yang dimiliki AS. Memperkuat sistem jaringan pertahanan pada sektor industri menjadi hal penting. Data-data mengenai transaksi, aset perusahaan harus dilindungi. Perlindungan pada sektor perbankan dan keuangan merupakan sesuatu yang penting dilakukan.Tanpa adanya perlindungan, dapat dipastikan negara mengalami kerugian besar akibat data-data dari instansi bernilai milyaran USD yang dicuri para hacker.

Sektor energi juga merupakan sektor penting. Perusahaan listrik merupakan sektor yang rawan, apabila tidak diberi perlindungan karena dapat

menyebabkan jaringan listrik AS mati total akibat dari serangan hacker kesistem jaringan pada komputer di PLN.

Jaringan komunikasi juga penting. Tidak berfungsinya jaringan komunikasi akibat perbuatan hacker tentu akan membuat negara merugi dalam jumlah besar. Pun penyedia layanan kesehatan, yang akan kesulitan bila komputernya dijebol dan data-data didalamnya dihapus atau diubah. Hal ini akan membuat sistem penerimaan jaminan kesehatan menjadi salah sasaran atau malah pemerintah harus melakukan sensus lagi dari awal.

Supervisory Control and Data Acquisition (SCADA) yang menjalankan fungsi infrastruktur AS, seperti listrik, air dan komunikasi, juga memiliki hak kepemilikan dan mengoperasikan infrastruktur cyber, seperti kabel dan server juga sistem Fungsi kontrol SCADA ialah intranet atau biasanya internet.[184]

Berpegang pada yang ditetapkan pada tahun 1997 oleh Bill Clinton mengenai perlindungan pada infrastruktur penting AS dan mengidentifikasi sektor penting bernilai tinggi, seperti jaringan listrik, minyak dan gas, air, transportasi, bank dan finansial,telekomunikasi, pelayanan darurat dan kelanjutan program pemerintah. [185]

Lebih dari 80 persen dari penyedia layanan infrastruktur penting melaporkan mengalami penyerangan massal dalam skala besar, ada juga yang dalam skala kecil, seperti yang tercantum dalam survey yang diadakan pada

[184] Colonel Jayson M. Spade, "China's Cyber Power And America's National Security", U.S. Army War College, (United States: U.S. Army War College, 2012), hal. 25.
[185] Kenneth Geers, Op. Cit. hal. 125.

tahun 2011.[186] Tidak peduli dalam skala besar ataupun kecil, serangan terhadap sektor ini akan selalu menjadi ancaman yang serius.

Berdasarkan paparan diatas, AS sangat resah dengan ancaman yang diberikan oleh China, karena itu AS ingin bermain lebih "soft" sehingga kepentingan AS dapat tetap berjalan atau malah semakin terlaksana.

Kesepakatan damai dengan China bisa dibilang merupakan cara aman AS untuk menjaga keamanan nasionalnya. Aksi yang dilakukan China tidak hanya menyusup ke sistem keamanan mililter AS, juga melakukan transaksi hasil curian dari perusahaan swasta serta jaringan fungsional listrik.[187] Tindakan China termasuk dalam penyerangan infrastruktur penting dan spionase cyber. Hal tersebut sangat mengancam pada ekonomi, juga sektor energi. Spionase menggunakan teknologi sudah menjadi masalah terbesar bagi sektor energi seperti angin dan surya.

Beberapa langkah yang diambil China benar-benar memberikan ancaman bagi AS. Pertama, program China dalam memajukan negara melalui pengembangan teknologi tingkat tinggi dalam jangka pendek yang menghalalkan pencurian intelektual properti guna mengurangi ketergantungan teknologi barat, memaksa transfer teknologi, penggunaan praktek perdangan ilegal WTO.[188] Kedua, penyerangan terhadap infrastruktur penting memiliki resiko langsung dan tidak langsung pada daya saing

[186] Robert E. Kahn, dkk, Op. Cit. hal. 23.
[187] Melanie Hart, "Escalating Cybersecurity Threats Pose New Energy Challenges for the United States", dalam China and Cybersecurity: Political, Economic, and Strategic Dimensions. (San Diego: University of California.2012), hal. 26.
[188] Ibid, hal. 27.

ekonomi. Jaringan penggunaan listrik menggunakan sistem kontrol industri terpusat, biasa disebut sistem SCADA (Supervisory Control and Data Acquisition) yang kini tersembung dengan internet, meski tidak memiliki sistem keamanan karena tidak didesain untuk beradaptasi dengan lingkungan internet, dan kini menjadi rawan terhadap segala jenis kejahatan cyber.[189] Muncul dugaan Russia dan China telah menghack jaringan listrik AS dan menanamkan malware yang dapat diaktifkan dikemudian hari bila terjadi perselisihan diantara kedua negara, yang dapat mengakibatkan jaringan listrik AS mati total .[190]

Serangan cyber pada jaringan listrik dapat menyebabkan kota atau wilayah bagian mengalami pemadaman total, tidak adanya layanan telepon serta tidak berjalannya pelayanan darurat bagi warga. Sedang penyerangan terhadap sistem pengairan dapat menyebabkan persediaan air menjadi tidak layak minum serta membuka kanal sehingga tanggul dapat terbuka dan kota akan mengalami banjir.

Perusahaan dan sektor industri milik swasta sangatlah rawan terhadap segala macam kejahatan cyber. Sebabnya karena kedua sektor tersebut tidak dilengkapi dengan sistem keamanan cyber, tetapi lebih ke sistem yang dapat mencegah kejahatan cyber, terutama penyerangan yang disponsori oleh negara.[191] Hal ini dikarenakan perusahaan swasta menganggap bahwa

[189] Ibid.
[190] Ibid.
[191] Colonel Jayson M. Spade, Op. Cit., hal. 30.

pertahanan adalah tanggung jawab pemerintah, sedang keamanan adalah tanggung jawab masing-masing perusahaan.

Isu mengenai kerentanan perusahaan swasta, terutama penyedia layanan berbasis listrik sudah lama terjadi. Tepatnya ketika Department of Defense pada tahun 1997 melakukan simulasi penyerangan dengan NSA kepada AS menggunakan software hack yang tersedia di internet dan dalam jangka waktu dua minggu, NSA berhasil merusak jaringan listrik dan sistem respon darurat di sembilan kota.[192] Tidak hanya itu, 36 jarinngan DoD dijebol serta latihan Zenith star yang berhasil melakukan pengrusakan pada sistem SCADA yang mengendalikan jaringan listrik pada markas militer AS dengan Dos, denial of service attack.[193]

Pemerintah AS sedikit banyak telah belajar dari kasus Y2K atau virus year 2000 problem mengenai rentannya keamanan sektor-sektor penting negara yang kini semakin terintegrasi dengan internet dan menggunakan media komputer dalam prakteknya sehari-hari. Nantinya, sektor-sektor tersebut akan terhubung dengan e-commerce.[194]

Semenjak milenium baru, setiap pihak memiliki kemampuan untuk mengakses properti intelektual tanpa harus membayar. Spionase cyber yang disponsori negara biasanya menginginkan informasi berharga mengenai

---

[192] Ibid.

[193] Ibid.

[194] Helen Nissenbaum, "Where computer security meets national security", Journal Ethics and Information Technology, June 2005, Vol. 7, No.2, hal. 63.

ekonomi dan militer suatu negara.[195] Pencurian teknologi "sensitif" militer akan membuat negara mengalami keguncangan dikarenakan kerugian yang diderita amat banyak.

Spionase cyber dianggap oleh negara sebagai alternatif yang sangat murah untuk pengembangan teknologi, sehingga aksi spionase kini sudah dianggap sebagai sesuatu yang lumrah. Salah satu anggota intelijen AS mengatakan bahwa perusahaan perabotan AS di hack untuk kemudian dicuri properti intelektualnya hanya demi melihat design perabotan.[196] Cara seperti itu juga biasa digunakan untuk mencuri resep sereal, teknologi suku cadang mobil otomatis, desain sepatu, dll. Kerugian yang didapat perusahaan ditaksir berjumlah besar.

Mobil otomatis juga perlu mendapat perhatian dari pemerintah. Karena tersambung dengan beberapa perangkat, mobil otomatis menjadi rentan. Contoh kasus yang pernah terjadi adalah karena kecelakan sebagai akibat dari kejahatan cyber, serta pencurian informasi teknologi pada mobil yang didapat dari spionase cyber.[197]

Properti intelektual milik perusahaan yang menjadi korban masih dapat diakses dan masih dapat memproduksi barang. Dampak yang muncul adalah munculnya pesaing baru. Kerugian yang diderita akan semakin besar bila pesaing baru tersebut memiliki akses ke pemerintahan yang

---

[195] James Andrew Lewis dan Stewart Baker, "The Economic Impact Of Cybercrime And Cyber Espionage". Makalah disajikan dalam *Center for Strategic and International Studies*, (United States: Mc Afee, July 2013).
[196] Ibid.
[197] Ibid.

memberlakukan subsidi sehingga harga jual barang menjadi semakin rendah serta bila pemerintah tempat asal atau pihak lain melindungi pangsa pasar domestiknya.

Beberapa tahun ini, serangan cyber kepada sektor finansial kian menjadi. Operasi High Roller melenyapkan uang sebesar $2,5 juta dari bank-bank di Eropa, AS dan Amerika latin.[198]

B. Cyber Economic

Serangan Cyber kepada sebuah negara, terutama instansi keuangan negara, perusahaan atau jaringan pada kendaraan dapat membuat negara mengalami kerugian nyata yang besarnya dapat mencapai jutaan hingga milyaran USD. Rusaknya sistem jaringan membuat perusahaan atau negara harus mengeluarkan uang dalam jumlah banyak untuk melakukan perbaikan, dan juga sistem jaringan yang rusak tidak dapat diperbaiki dalam waktu cepat, yang dapat membuat hacker lain dapat melakukan tindak kejahatan. Para hacker yang membobol sistem jaringan bank dapat melakukan pencurian uang tanpa dapat dilacak, mengubah catatan transaksi hingga menghapus datad-data penting bank.

Salah satu contoh kasusnya adalah ketika virus ILOVEYOU pada tahun 2000 menyerang bank dan jaringan perusahaan. Virus ILOVEYOU sendiri telah mengakibatkan kerugian sangat besar, merusak ribuan file komputer yang senilai dengan $4 milyar lalu setelah dirinci oleh ahli IT yang bekerja diperusahaan keamanan, AS dapat mengalami kerugian sebesar $35

[198] Ibid.

milyar tiap harinya karena serangan cyber.[199] Virus ini menjadi sangat merugikan bila korban tidak memiliki file cadangan. Sebuah laporan dari U.S. Cyber Consequences Unit yang diterbitka pada tahun 2007 menyatakan bahwa serangan yang menyeluruh kepada infrastruktur AS dapat menyebabkan kerugian sebesar $700 milyar.[200]

Besarnya kerugian yang diakibatkan oleh kejahatan cyber pada kendaraan mobil otomatis pada tahun 2010 mencapai angka yang fantastis. The Center for Disease Control menyatakann jumlah kerugian akibat kecelakaan atau kerusakan mobil $99 milyar sedangkan The American Automobile Association memperkirakan kerugian yang diderita sebesar $168 milyar.[201]

Perusahaan memahami bahwa tingkat "pencurian" atau penyusutan simpanan merupakan resiko yang harus dialami bagi pelaku bisnis. Perusahaan di AS mengalaminya pada angka 1,5% hingga 2% tiap tahunnya, dan ditahun 2008 kerugian yang ditaksir dikisaran 1,7% atau sekitar $70 milyar hingga $280 milyar.[202] Dalam penelitian disimpulkan bahwa batas atas kerugian yang ditimbulkan oleh pencurian cyber berkisar antara 0,5% hingga 1% dari pemasukan nasional atau $70 milyar hingga $140 milyar.[203]

Kerugian sebesar $100 milyar setara dengan 508.000 pekerja yang kehilangan pekerjaannya atau jumlah pekerja berkurang sebesar 3 persen.[204]

---

[199] Colonel Jayson M. Spade, Op. Cit., hal. 26.
[200] Ibid.
[201] James Andrew Lewis dan Stewart Baker, Op. Cit., hal. 4.
[202] Ibid
[203] Ibid.
[204] Ibid.

Yang menjadi permasalahan adalah ketika para pekerja yang di PHK ini akan mendapatkan pekerjaan yang memberi gaji setara atau tidak. Jika begini, banyak pekerja yang harus merelakan diri mereka dibayar lebih rendah atau tetap menganggur. Jika banyak yang menganggur, tentu negara lah yang paling menderita.

Laporan yang dilansir UNODC memperkirakan biaya untuk mengidentifikasi pencurian cyber sebesar $780 juta dan diperkirakan tiap tahunnya AS mengeluarkan antara $300 juta hingga $500 juta.[205]

Untuk mengurangi kekhawatiran perusahaan mengenai reputasi mereka, ada beberapa cara yang dilakukan setelah mendapat komplain dari publik terkait dengan aktivitas hack. Yang dilakukan adalah mengurangi harga pasaran, berkisar antara 1% hingga 5%, yang mana total kerugiannnya tidak dapat dipandang sepele meski siklus ini tidaklah permanen.[206] Harga-harga biasanya kembali normal pada kuartal berikutnya.

The US Office of Management and Budget pada tahun 2012 melaporkan bahwa agen federal menghabiskan dana lebih dari $15 milyar pada proyek yang terkait dengan keamanan dan aktivitas cyber, atau sekitar 20%.[207] Hasil survey menyatakan bahwa rata-rata pengeluaran perusahaan besar untuk perbaikan setelah serangan cyber yang tergolong sukses sebesar $9 juta.[208]

---

[205] Ibid, hal. 10.
[206] Ibid, hal. 12.
[207] Ibid.
[208] Ibid.

Commerce Department's International Trade Administration menganalisis bahwa pada tahun 2011, ekspor senilai $1 milyar setara dengan 5080 pekerjaan, sedangkan jumlah pekerja di AS antara 135 juta sampai 145 juta dan kerugian sebesar itu dapat berpotensi menyebabkan berkurangnya jumlah pekerja sebanyak 3%.[209]

FBI mengklaim serangan pada tahun 2010 menyebabkan AS merugi sebesar $70 juta dan lagi, "flash crash" yang dialami Wall Street menyebabkan pasar mengalami volatilitas yang diperkirakan senilai $1 trilyun per menit ditambah stock yang mengalami kejatuhan nilai lebih dari 90%.[210] Meski keadaan berlangsung membaik, tapi sistem finansial yang menggunakan sistem perdagangan otomatis berfrekuensi tinggi sangat rentan dengan serangan cyber.[211]

Berdasarkan dokumen NSA yang dibocorkan Snowden, hacker asal China telah membuat Defense of Departmen merugi sebesar $100 juta, dengan rincian terjadi serangan sebanyak 30000 kali dan 16000 komputer mengalami kerusakan.[212]

Dengan diadakannya kerja sama dengan China, diharapkan bahwa resiko yang akan dialami ole AS mengenai cyber econnomic akan berkurang.

---

[209] Ibid, hal. 17
[210] Ibid.
[211] Robert E. Kahn, dkk, Op. Cit., hal. 25.
[212] Gito Yudha Pratomo, Peretas Tiongkok bikin AS rugi Rp.126 triliun, " http://www.cnnindonesia.com/teknologi/20150119103100-185-25583/peretas-tiongkok-bikin-as-rugi-rp-126-triliun", Diakses pada tanggal 7 Februari 2015.

C. Perlindungan dan Pengembangan Teknologi

Isu mengenai perlindungan teknologi juga merupakan isu yang sangat penting. Rentannya sistem pertahanan terhadap teknologi atau infrastruktur penting akan sangat merugikan negara. Pencurian terhadap data-data mengenai pengembangan sebuah teknologi, akan membuat negara kehilangan milyaran USD. Hal ini akan berakibat pada semakin lambatnya kemampuan negara untuk mengembangkan teknologi karena tidak mendapat dana dari teknologi yang semestinya dijual. Aksi pencurian dapat membuat sebuah negara mengembangkan teknologi tanpa perlu membeli hak cipta kepada negara pengembang. Aksi China menjadi perhatian serius karena selain mencuri, China juga memodifikasi lalu meluncurkan produk yang kemudian didaftarkan hak patennya. Hal seperti ini tidak bisa menjadi tuntutan kepada China karena teknologi yang diluncurkan China tidak 100% sama dengan teknologi curian.

Jurnal Wall Street pada 2009 mengumunkan bahwa mata-mata cyber yang berasal dari China dan Russia telah menjebol, memposisikan dan menanam software dijaringan listrik AS yang dapat menyebabkan kerusakan atau pencurian data dan pengendalian infrastruktur tersebut dari jarak jauh.[213] Operasi cyber "Aurora" mencoba mencuri source code dan intelektual properti dari perusahaan AS, seperti Apple dan ternyata berasal dari kumpulan hacker di beijing yang terikat dengan PLA.[214]

---

[213] Robert E. Kahn, dkk, Op. Cit., hal. 23.

[214] Hattie Jones, "China's 'Cyberwar' Against the US: Truth or Fiction?", 23 July 2013.

Aksi pencurian pada teknologi militer dapat membuat negara menjadi berkurang tingkat keamanannya dikarenakan semakin kuatnya musuh atau ancaman pasar ekspor cyber, produk tingkat tinggi atau materi yang lebih mumpuni.[215] Ada hubungan dari serangan cyber pada sektor finansial dengan sektor teknologi militer, karena biasanya merupakan aktor yang sama.

Besarnya kerugian yang dialami AS karena spionase cyber sulit untuk diperkirakan. Cara yang paling mudah adalah dengan melakukan perkiraan, perusahaan yang memiliki intelektual properti senilai $1 milyar menjadi korban kejahatan cyber dan mengalami kerugian secara total. Departemen energi AS mencurigai China terkait dengan tindakan menghack sistem komputer di Departemen energi yang terjadi ditahun 1999, yang didugai dilatar belakangi oleh motif mencuri data-data didalam laboratorium senjata nuklir AS.[216] Serangan cyber dapat membuat kacau sistem persenjataan, kapal, prajurit atau mengacak-acak informasi penting. Pada tahun 2009, kelompok militan AS mengakses gambar yang belum terenkripsi pada pesawat drone AS menggunakan software seharga $26.[217]

Berbekal informasi curian dari spionase cyber, aktor negara maupun non-negara dapat mengetahui seluk beluk mengenai rencana, operasi dan celah dari pasukan AS dan sekutunya. Mata-mata cyber mencuri data dari perusahaan yang bekerja di proyek pesawat tempur F-35 yang memerlukan jutaan kode yang berasal dari software dan program yang paling mahal

[215] James Andrew Lewis dan Stewart Baker, Op. Cit., hal. 4.
[216] Kenneth Geers, strategic cyber defense, Op. Cit., hal. 27.
[217] Robert E. Kahn, dkk, Op. Cit., hal. 13.

sepanjang sejarah AS, seharga $399 milyar.[218] Laptop milik militer AS terinfeksi dari flash disk yang membuat data dapat dipindah ke server yang berada dibawah kendali pihak asing, kode yang tersebar tidak mampu dilacak dan terprogram untuk mengirimkan rencana operasi ke tangan pihak yang tidak diketahui.[219]

Diketahui bahwa desain dan data elektronic Joint Strike Fighter (F-35) yang memiliki ukuran kurang lebih satu terabytes telah dicuri oleh sekumpulan hacker yang tidak diketahui identitasnya.[220] AS menuduh China berdasarkan IP addresses yang digunakan serta sidik jari digital yang telah dikenali dan menganggap ini adalah operasi intelijen tingkat tinggi yang sangat membahayakan negara.[221]

Berdasarkan dokumen NSA yang dibocorkan Snowden, China telah mencuri blueprint pesawat F-35 yang bahkan berukuran 50TB, juga mencuri rancangan senapanrel canggih, sistem pertahanan rudal Ballistik AEGIS dan rancangan kapal perang Litoral.[222]

Lebih lanjut lagi, pesawat buatan China, J-31 dan J-20 diduga kuat merupakan pesawat hasil modifikasi F-35 keluaran AS. Tidak hanya itu,

---

[218] Ibid, hal. 17.
[219] Ibid.
[220] Paolo Passeri, "After latest F-35 hack, Lockheed Martin, BAe Systems, Elbit under multiple cyber attacks....right now", dalam http://theaviationist.com/2012/03/14/f35-anonymous-attack/, diakses pada tanggal 12 Maret 2015.
[221] Ibid.
[222] Denny Armandhanu, "Dokumen NSA: Peretas Tiongkok Curi 50 TB Data Jet F-35", http://www.cnnindonesia.com/internasional/20150119221333-134-25808/dokumen-nsa-peretas-tiongkok-curi-50-tb-data-jet-f-35, diakses pada tanggal 7 Februari 2015.

China juga berhasil mendapatkan data mengenai pesawat siluman B-2, jet F-22, navigasi misil dan sistem lacak AS.[223]

Perlindungan kepada Drone juga harus semakin diperhatikan. Drone, kini marak digunakan untuk kegiatan meliput olahraga, dokumentasi hingga pengawasan area perbatasan. Drone sendiri tidak memiliki standar penerbangan atau manajemen lalu lintas yang diatur oleh dunia internasional, ditambah ketergantungan untuk terhubung dengan komputer.[224] Jika tidak diperhatikan, dapat menyebabkan kecelakaan dan kematian, meski kini desain Drone dan sistem navigasi telah mengurangi resiko kecelakaan. Namun, tanpa jaringan yang memadai, Drone dapat di hack dan membuatnya bergerak sesuai dengan keinginan hacker.

Langkah yang diambil AS dengan mengajak China bekerja sama merupakan jalan tengah. AS tentu ingin terus mengembangkan dan menjaga aset penting negaranya, namun kehadiran China sebagai negara yang kuat dalam dunia cyber sangat mengancam. Ketimbang terus bersaing dan berkonflik dengan China, kerja sama dipandang sebagai sesuatu yang menawarkan sesuatu lebih baik.

Rentannya sistem keamanan AS berimbas pada keamanan nasional, pengembangan cyber economic dan perlindungan dan pengembangan teknologi. Serangan yang bertubi-tubi ditujukan kepada ketiga sektor tersebut

---

[223] Franz-Stefan Gady, "New Snowden Documents Reveal Chinese Behind F-35 Hack", dalam http://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack, diakses pada tanggal 11 Maret 2015.

[224] Aditya Panji, "Drone dan Hacker Bisa Bunuh Penumpang Pesawat", dalam http://www.cnnindonesia.com/teknologi/20141205020730-185-15990/drone-dan-hacker-bisa-bunuh-penumpang-pesawat, diakses pada tanggal 7 Februari 2015.

sudah membuat AS merugi milyaran dollar. Baik dari sisi kerusakan pada infrastruktur penting akibat kejahatan cyber, tapi juga kerugian finansial karena data-data penting keuangan atau informasi pengembangan teknologi atau produk tingkat tinggi berhasil dicuri. Penggunaan spionase cyber tentu menjadi hal yang sangat menggiurkan bagi negara yang ingin mengembangkan teknologi dengan cara yang sangat murah. Tanpa harus membeli lisensi kepada AS. Pihak yang gemar menyerang dan merugikan AS salah satunya adalah China.

Oleh karena itu, AS ingin mengajak China bekerja sama untuk mengurangi potensi kriminal cyber dan kerugian yang disebabkan oleh China. Mengajak China bekerja sama sedikitnya membuat AS tenang, karena ancaman terbesarnya telah berhasil "dijinakkan". Meski, hal itu tidak menjadi jaminan bahwa China tidak akan menyerang AS lagi sewaktu-waktu, namun setidaknnya AS bisa sedikit rileks karena kepentingannya di dunia cyber dapat terus berjalan.