BAB II
PENCURIAN KEKAYAAN INTELEKTUAL MELALUI MEDIA SIBER OLEH TIONGKOK SERTA RESPON PEMERINTAHAN BARACK OBAMA DAN DONALD TRUMP

Pencurian kekayaan intelektual milik AS oleh Tiongkok telah berlangsung selama bertahun-tahun. Selain agresifitas Tiongkok di Laut Cina Selatan dan Korea Utara, kasus pencurian kekayaan intelektual kerap menjadi pengganggu hubungan kedua negara. Meskipun berkali-kali pemerintah Tiongkok mengelak, namun tetap saja serangan-serangan terhadap jaringan komputer AS terdeteksi oleh perusahaan-perusahaan keamanan siber AS.

Bab ini membahas mengenai pencurian, tren pencurian dan respon pemerintahan Obama dan Trump terkait serangan peretasan Tiongkok. Pembahasan akan diawali dengan pencurian kekayaan intelektual milik AS oleh Tiongkok. Bagian ini menjelaskan mengenai pencurian kekayaan intelektual sebagai usaha Tiongkok mengejar ketertinggalannya dari Barat. Pembahasan dilanjutkan dengan menjelaskan aktor-aktor peretas Tiongkok yang kerap melancarkan operasi pencurian data-data penting yang dapat memberikan keuntungan ekonomis kepada perusahaan Tiongkok ataupun militer Tiongkok. Pembahasan dilanjutkan dengan tren pencurian kekayaan intelektual Tiongkok dan respon AS pada masa pemerintahan Obama dan Trump. Bagian ini membahas operasi-operasi serangan oleh Tiongkok yang terjadi selama pemerintahan Obama sampai awal periode pemerintahan Trump serta bagaimana kedua pemerintah tersebut merespon kasus itu.

II.1 Kasus Pencurian Kekayaan Intelektual AS oleh Tiongkok

Tiongkok adalah negara dengan peradaban berumur lebih dari 5.000 tahun yang kini berambisi mengembalikan kejayaannya. Kalah dalam kedua Perang Candu, dijajah oleh Eropa, dan diinvasi Jepang membuat Tiongkok berada dalam masa-masa tersulitnya. Masa-masa yang disebut sebagai “abad penghinaan” ini dijadikan pelecut semangat oleh Tiongkok untuk bangkit dan memastikan abad

tersebut tidak datang lagi di masa depan dengan mengembalikan kejayaan (Allison, 2017, p. 94).

Untuk mengembalikan kejayaannya, Tiongkok merasa perlu untuk berpengaruh dalam bidang ekonomi, politik dan budaya. Untuk mendapatkan pengaruh dalam bidang politik dan budaya, Tiongkok sadar bahwa kekuatan dalam bidang ekonomi sangat penting. Dalam bidang ekonomi, Tiongkok berusaha meningkatkan pengaruhnya dalam rantai nilai global. Setelah lebih dari 30 tahun hanya menjadi pusat perakitan barang-barang dari negara-negara besar, pemerintah Tiongkok merasa sudah saatnya bagi Tiongkok untuk mengerjakan produknya dan mengembangkan teknologi sendiri.

Sejak 1978, di bawah kepemimpinan Deng Xiaoping Tiongkok menerapkan serangkaian kebijakan untuk meningkatkan kemampuan industrinya agar meraih kembali kejayaannya(Hannas, et al., 2013, p. 450). Untuk meningkatkan kemampuan industri, pemerintah Tiongkok sadar pentingnya memiliki teknologi yang maju. Dengan bekal tenaga kerja murah dan akses pasar yang luas, Tiongkok berusaha mendapatkan teknologi yang dimiliki perusahaan-perusahaan yang beroperasi di negaranya dengan menerapkan kebijakan agar perusahaan tersebut memberikan teknologinya kepada Tiongkok.

Namun, usaha Tiongkok untuk mendapatkan kekuatan ekonomi sebagai usaha mengembalikan kejayaannya kerap menimbulkan gesekan dengan negara yang sedang menikmati posisinya sebagai kekuatan dominan. Pasca Perang Dingin AS menikmati posisinya sebagai satu-satunya kekuatan dominan dalam hubungan internasional. Bubarnya Uni Soviet meninggalkan AS tidak hanya dominan dalam bidang politik saja, melainkan juga teknologi, budaya dan ekonomi. Menurut AS, Tiongkok kerap melakukan praktik curang yang dapat memberikan keuntungan ekonomis bagi perusahaan-perusahaan Tiongkok seperti kebijakan proteksi bagi produk AS, transfer teknologi yang dipaksakan hingga pencurian hak kekayaan intelektual milik perusahaan AS melalui jaringan internet sehingga Tiongkok tidak perlu melakukan riset yang mahal dan meningkatkan posisi pada saat bernegosiasi dengan AS dalam hal perdagangan (White House Office of Trade and Manufacturing Policy, 2018, p. 2).

Tuduhan AS kepada Tiongkok atas peretasan dan pencurian Kekayaan Intelektual (KI) cukup mengejutkan. Hal ini dikarenakan AS merupakan negara

terdepan dalam bidang teknologi informasi dan merupakan negara tempat internet dilahirkan namun tidak berhasil menjamin keamanan siber milik pemerintah maupun perusahaan-perusahaannya. Tetapi pada kenyataannya, Tiongkok berhasil mencuri jutaan data dari jaringan komputer perusahaan AS yang berisi kekayaan intelektual. Begitu besarnya dampak dari peretasan Tiongkok, Jendral Keith Alexander, Direktur dari NSA pada 2012 mengatakan bahwa spionase ekonomi Tiongkok melalui media siber dimana pencurian KI termasuk di dalamnya, merupakan transfer kekayaan terbesar dalam sejarah (Hannas, et al., 2013, p. 349). Sedangkan untuk jumlah serangan Tiongkok, mantan Direktur FBI James Comey dalam sebuah *talkshow* yang diadakan oleh stasiun televisi CBS mengatakan bahwa jumlah serangan Tiongkok terhadap jaringan perusahaan AS besar sekali sampai-sampai ada perusahaan yang tidak menyadari jaringannya diretas (Red Team Cyber Security, 2014). Meskipun media telah ramai membicarakan adanya intrusi besar-besaran Tiongkok dalam jaringan komputer perusahaan AS, pejabat resmi AS baru mengakui adanya pencurian data pada 2006 ketika Pentagon menyatakan telah terjadi serangan terhadap NIPRNET yang berasal dari suatu daerah di Tiongkok. Serangan tersebut telah mengunduh data sebanyak 20 terabyte (Onlely & Wait, 2006).

Kasus serangan siber Tiongkok muncul ke publik pertama kali pada 2004 ketika Shawn Carpenter, seorang analis keamanan siber dari Sandia National Laboratories mendeteksi aktifitas serangan siber oleh Tiongkok yang kemudian oleh FBI diberi kode “Titan Rain”. Serangan tersebut terlacak dilakukan oleh komputer yang berlokasi di Provinsi Guangdong, Tiongkok. Menurut Carpenter, serangan ini telah menyasar NASA, Bank Dunia, Kontraktor Senjata dan Departemen di AS (Pearson, 2005). Carpenter sebenarnya telah mendeteksi serangan ini sejak 2003 ketika sedang bekerja dengan tim keamanan siber di kantor Lockheed Martin di Orlando, Florida. Carpenter mendapati jejak peretasan sampai ke Tiongkok dengan menelusuri file-file dan *malware* yang terdapat pada komputer. Carpenter awalnya mengusulkan peretasan balasan untuk melihat apa yang telah dicuri oleh si peretas, namun usulannya ditolak karena pejabat di Sandia merasa hal tersebut melawan hukum dan tidak baik secara ekonomis. Akhirnya, Carpenter melakukannya sendiri di rumahnya dan menghubungi FBI untuk melaporkan apa yang terjadi. Carpenter akhirnya diberhentikan dari pekerjaannya

karena dianggap melanggar hukum dan bertindak di luar wewenangnya. Namun setelahnya dia memenangkan gugatan melawan Sandia dan mendapatkan hadiah sebesar US$ 4,7 juta (Schmidle, 2018).

Penggunaan media internet sebagai sarana mencuri kekayaan intelektual setidaknya menguntungkan Tiongkok dalam dua hal, yaitu logistik dan kemungkinan menyangkal (Hannas, et al., 2013, p. 353). Dengan internet Tiongkok hanya butuh membayar seorang peretas profesional dan menyediakan komputer yang cukup tangguh dan layanan internet yang cepat untuk mencuri formula dari suatu barang yang diproduksi oleh perusahaan AS tanpa perlu membeli barang tersebut terlebih dahulu dan kemudian diteliti mengenai unsur apa yang ada di dalam barang tersebut atau bagaimana barang tersebut dibuat. Selain itu, penggunaan media siber menguntungkan Tiongkok untuk menyangkal jika ada tuduhan mengenai pencurian KI yang ditujukan kepadanya. Hal ini dikarenakan aktifitas pencurian melalui siber tidak meninggalkan jejak dan kalaupun ada jejak sangat sulit untuk dilacak dan dibuktikan.

Pencurian KI melalui media siber berdasarkan asal pelakunya dibagi menjadi dua, yaitu internal dan eksternal. Serangan eksternal adalah serangan yang dilakukan oleh seseorang atau kelompok yang bukan pegawai atau tidak memiliki kaitan apapun dengan perusahaan yang menjadi korban peretasan. Contoh kasus dari serangan jenis ini adalah serangan Tiongkok yang dilaporkan oleh Google. Serangan ini diungkap oleh Google ketika menyelidiki kasus pencurian data milik aktifis HAM Tiongkok yang berada dalam jaringannya. Serangan tersebut juga mengungkapkan bahwa serangan pencurian informasi juga diarahkan kepada perusahaan besar lainnya yang bergerak dalam bidang media, keuangan, teknologi dan kimia (Drummond, 2010). Sedangkan serangan internal dilakukan oleh orang yang memiliki kaitan dengan perusahaan yang menjadi korban peretasan ini. Contoh dari kasus ini adalah kasus pencurian formula mengenai teknologi OLED oleh Meng Hong pada 2009. Hong Meng adalah seorang ilmuwan di Pusat Riset Dupont yang mengunduh formula teknologi OLED dan memberikannya melalui *email* kepada Universitas Peking. Meng Hong juga mendorong pemerintah Tiongkok untuk membantu komersialisasi formula OLED tersebut (Hannas, et al., 2013, p. 355). Namun pada penelitian ini yang menjadi fokus adalah serangan eksternal Tiongkok

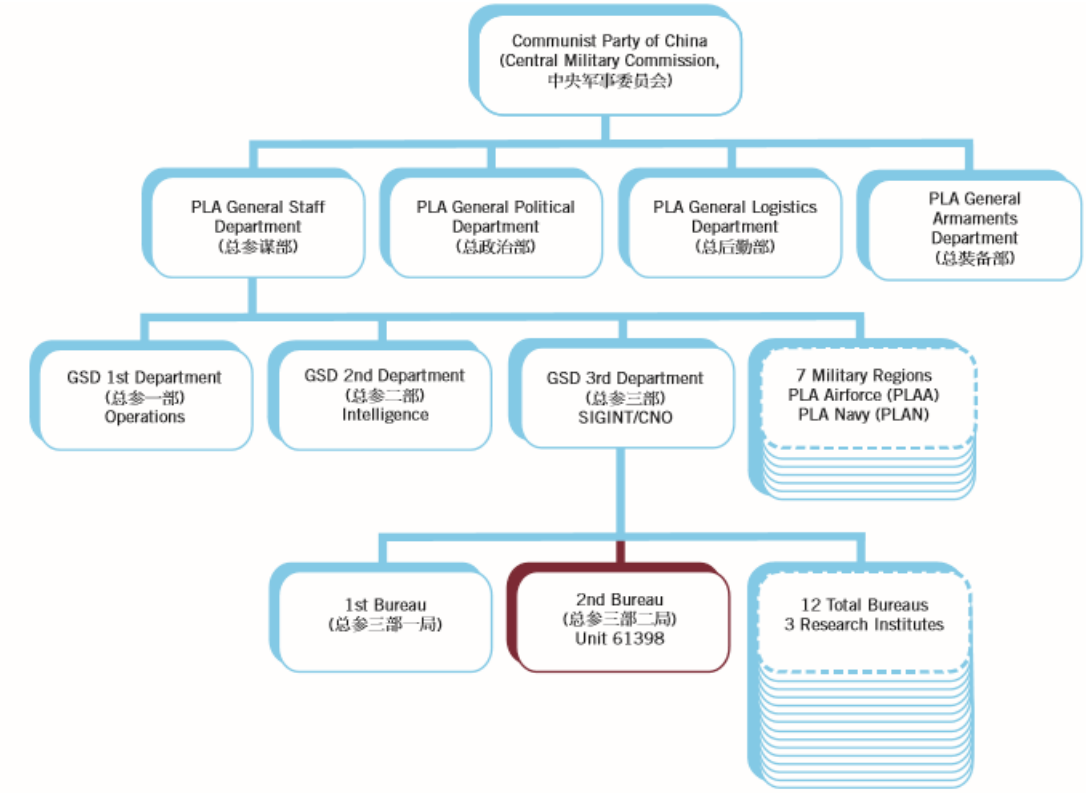
II.2 Tentara Siber Tiongkok

Tiongkok memiliki "tentara" siber yang dikerahkan untuk berbagai tujuan, seperti untuk keperluan intelijen, keamanan dan bahkan pencurian KI. Selain peretasan yang dilakukan perorangan, Tiongkok memiliki kelompok-kelompok peretas yang bekerja untuk melayani negaranya. Perusahaan yang bergerak dalam bidang keamanan siber, Fireeye, mengidentifikasi kelompok-kelompok penyerang yang dinamakan sebagai *Advance Persistent Threat* (APT) (Fireeye, n.d.). APT adalah kelompok peretas profesional dan memiliki motif politik atau ekonomi (Rouse, n.d.). APT diasosiasikan sebagai aktor yang didukung oleh negara dan diarahkan untuk mencuri rahasia pemerintah ataupun industri (Grimes, 2019). Pada subbab ini akan dibahas kelompok-kelompok APT yang berasal dari Tiongkok. Tiongkok memiliki puluhan APT, namun pada tulisan ini akan dibahas beberapa dari seluruh APT yang berasal dari Tiongkok.

Kelompok pertama adalah APT 1 atau juga disebut Unit 61398 atau Comment Crew. Sejak 2004, Mandiant, Perusahaan Keamanan Siber yang telah diakusisi oleh Fireeye telah melakukan serangkaian investigasi mengenai dugaan peretasan terhadap jaringan komputer yang ditujukan kepada pemerintah AS ataupun perusahaan AS. Menurut laporan Mandiant tahun 2014, APT 1 telah melakukan serangan setidaknya sejak 2006 (Mandiant, 2014, p. 2). Masih menurut laporan yang sama, besarnya dampak dari serangan kelompok ini menarik Mandiant untuk menulis laporan khusus mengenai kelompok ini.

APT 1 dipercaya sebagai bagian dari Departemen Ketiga dari Departemen Staff Umum Tentara Pembebasan Rakyat atau Tentara Nasional Tiongkok. Mandiant mengklaim kesamaan keduanya berdasarkan lokasi jaringan dan kesamaan tindakan APT dan misi unit 61398. Unit ini bertugas melakukan spionase dan pencurian data pada beragam organisasi di dunia (Mandiant, 2014, p. 2). Secara khusus Unit 61398 ini berfokus pada operasi intelijen yang berhubungan dengan politik, ekonomi dan militer yang sasarannya adalah AS dan Kanada. Untuk memudahkan operasi, perusahaan milik pemerintah Tiongkok, China Telecom,

menyediakan infrastruktur bagi kelompok ini demi keamanan nasional. Mandiant berhasil menemukan Memo yang berisi perintah dari eksekutif China Telecom untuk membangun jaringan komputer dan penyediaan kabel fiber. Unit 61398 berada di bawah komando Departemen Ketiga angkatan bersenjata Tiongkok. Departemen Ketiga tersebut diperkirakan memiliki 130.000 personel dalam 12 Biro, tiga institut riset dan 16 Biro Fungsional dan Regional (Mandiant, 2014, p. 8). Secara khusus, APT 1 diperkirakan adalah Biro Kedua dari Kedua belas Biro milik Departemen Ketiga Angkatan Bersenjata Tiongkok.

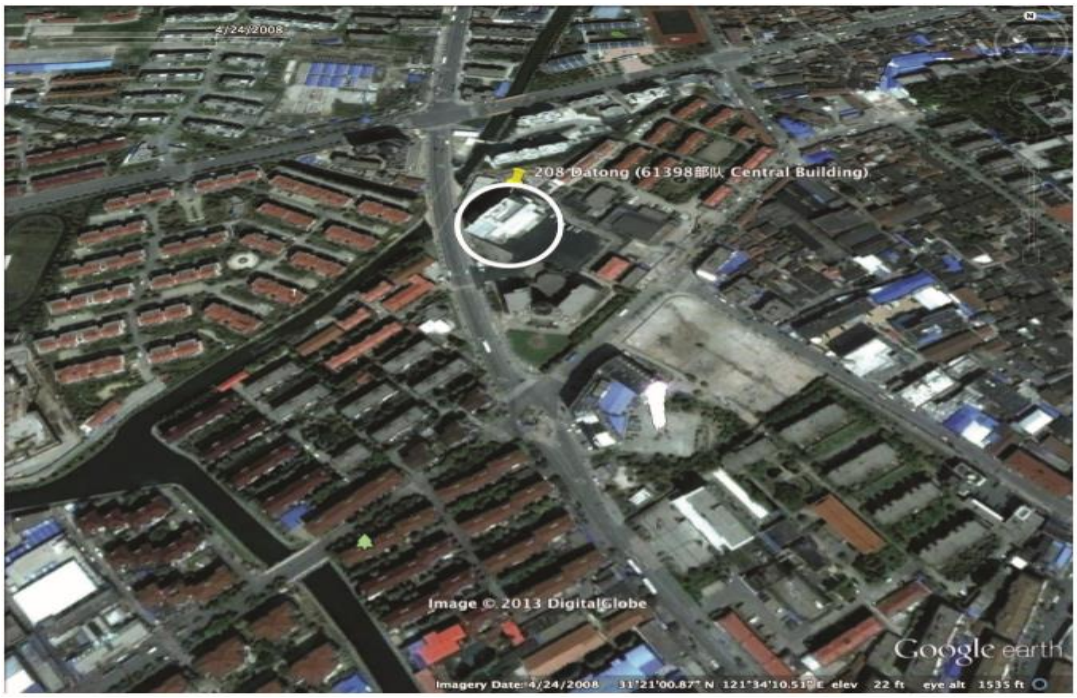


Gambar 2.1 Unit 61398 dalam Struktur Tentara Pembebasan Rakyat (Mandiant, 2014, p. 8)

Ketika melacak jejak Unit 61398, Mandiant berhasil menemukan beberapa bangunan yang dicurigai sebagai tempat unit tersebut beroperasi. Dengan mempelajari operasi dan hasil investigasi selama bertahun-tahun terhadap kelompok ini, Mandiant berhasil menemukan lokasi serta gambar dari bangunan yang diduga sebagai tempat operasi APT 1. Sebagai contoh, Mandiant mencurigai bangunan yang dibangun pada 2007 oleh Jiangsu Longhai Construction

Engineering Group sebagai salah satu markas dari APT 1. Bangunan yang terletak di Shanghai tersebut memiliki 12 lantai dan luas 130 ribu lebih meter persegi, yang diperkirakan dapat menampung 2000 orang (Mandiant, 2014, p. 11).

APT 1 adalah kelompok dalam militer Tiongkok yang cukup terampil dalam meretas dan menghapus jejak aktifitasnya, sehingga Mandiant mengalami kesulitan dalam menelusuri aktifitas dan mengetahui jumlah data yang telah dicuri oleh kelompok tersebut secara terperinci. Kesulitan yang dihadapi Mandiant yaitu APT menghapus data terkompresi yang telah mereka curi, sehingga bukti-bukti yang ada tercampur dengan bekas-bekas penggunaan sehari-hari. Selain APT 1 yang menghapus bukti, seringkali jarak antara waktu pencurian dengan investigasi terlalu jauh. Faktor-faktor teknis seperti tidak mamadainya perangkat lunak yang ada untuk memonitor pencurian yang terjadi juga berpengaruh pada keadaan ini (Mandiant, 2014, p. 25).

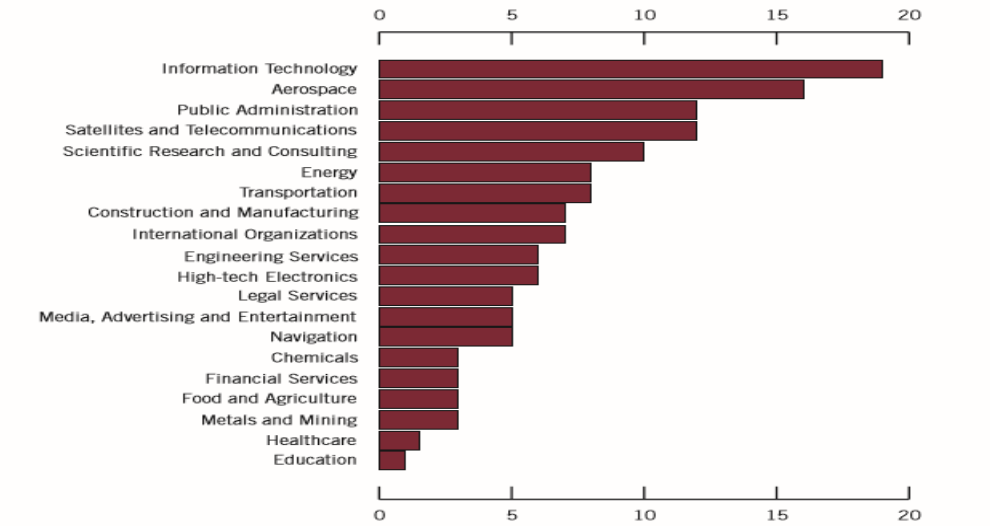


Gambar 2.2 Posisi Markas APT 1 dari Satelit (Mandiant, 2014, p. 13)

Menurut Mandiant, kelompok ini telah berkontribusi sebesar ratusan terabyte (1 terabyte = 1000 GB) data dari 141 organisasi industri sejak 2006. Hebatnya, kelompok ini dapat meretas ratusan dokumen penting dari organisasi-organisasi yang menjadi korbannya secara bersamaan. Ketika berhasil masuk ke

dalam jaringan komputer yang menjadi korbannya, kelompok ini secara berkala mencuri berbagai kekayaan intelektual milik organisasi tersebut seperti cetak biru teknologi, hak milik proses pembuatan, hasil tes, rencana bisnis, dokumen kalkulasi harga, perjanjian kerjasama, dan kontak serta email dari pemimpin organisasi tersebut (Mandiant, 2014, p. 20).

APT 1 atau Unit 61398 mengincar perusahaan yang memiliki kantor pusat di negara-negara berbahasa Inggris. Menurut Mandiant, mayoritas dari 141 korban yang teridentifikasi berasal dari negara berbahasa Inggris, yaitu 115 berasal dari AS sedangkan korban yang berasal dari Kanada dan Inggris masing-masing 7 (Mandiant, 2014, p. 21). Selain perusahaan, kelompok ini mengincar agensi kerjasama dan pembangunan internasional serta pemerintah asing dimana Bahasa Inggris menjadi salah satu bahasa yang dipakai. Untuk bidang industri yang menjadi incaran, APT 1 mengincar perusahaan yang dapat memberi keuntungan strategis bagi pemerintah Tiongkok atau perusahaan yang dimiliki oleh pemerintah, oleh karena itu bidang-bidang seperti teknologi informasi dan dirgantara menjadi bidang teratas yang menjadi incaran.



Tabel 2.1 Bidang industri yang menjadi target penyerangan APT1 (Mandiant, 2014, p. 24)

Selain APT 1, Tiongkok masih memiliki kelompok-kelompok lainnya seperti APT 18. APT 18 adalah kelompok penyerang yang dipercaya berasal dari Tiongkok. APT 18 dipercaya mulai beroperasi dari tahun 2009 (ATT&K, 2016). Kelompok ini dipercaya mengincar kontraktor senjata, jaringan komputer pemerintah, dan berbagai perusahaan yang bergerak dalam bidang medis serta

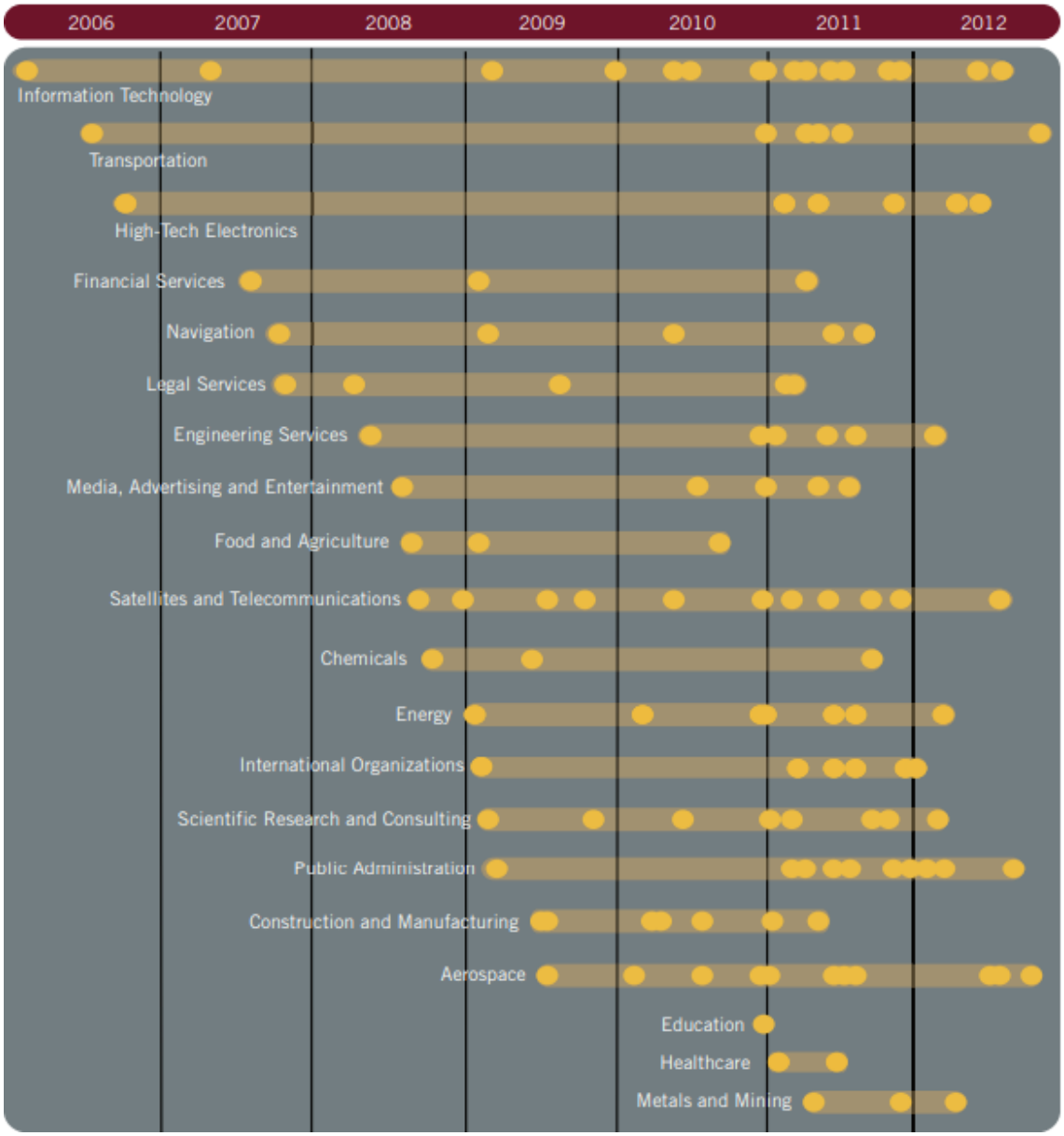
teknologi informasi. APT 18 atau Wekby merupakan tersangka utama dalam kasus serangan terhadap *Community Health System*, sebuah perusahaan yang bergerak dalam penyediaan layanan kesehatan (Mimoso, 2014). Menurut Charles Carmakal, Direktur Unit Forensik dari Fireeye, serangan tersebut merupakan serangan yang dilakukan oleh APT 18 (Finkle & Humer, 2014). Kelompok ini berhasil mencuri data 4,5 juta pasien dari jaringan komputer perusahaan yang memiliki jaringan rumah sakit sebanyak 206 tersebut. Data yang dicuri termasuk nama, alamat, dan nomor identitas. (Frizell, 2014). Meskipun biasa mencuri kekayaan intelektual milik perusahaan, pada kasus peretasan *Community Health System* APT 18 memfokuskan pada pencurian identitas untuk dijual.

Terakhir ada APT 10 atau Menupass Team yang menjadi tentara siber Tiongkok untuk mengejar ketertinggalan dalam hal teknologi dan ekonomi. Dalam usaha meningkatkan PDB-nya dua kali lipat, Tiongkok menggunakan kelompok ini untuk menyerang sektor-sektor yang menjadi fokus untuk rencana lima tahunan ke-13 Tiongkok (PricewaterhouseCooper , 2017, p. 15) Perusahaan keamanan siber Fireeye mengklaim telah mengusut kelompok ini sejak 2009 lalu. Menurut Fireye, kelompok ini mengincar jaringan perusahaan konstruksi, teknik, dirgantara, telekomunikasi dan pemerintah AS (FireEye iSight Intelligence, 2017). Selain mengincar AS, kelompok yang berbasis di Tianjin ini juga mengincar Eropa. Kolaborasi FireEye dan Mandiant dalam menelusuri kelompok ini lebih lanjut menemukan bahwa sejak 2016, kelompok ini juga mengincar Jepang. Pada penemuan awal, kelompok ini hanya mengincar universitas-universitas di Jepang namun belakangan kelompok ini juga mengincar pemerintah Jepang dan berusaha mendapatkan data dalam isu maritim, diplomasi dan bahkan Korea Utara (Matsuda & Muhammad, 2018).

Gambar 2.3 Sektor yang menjadi target dari APT10 (PricewaterhouseCooper , 2017, p. 10)

2.3 Tren Peretasan dan Pencurian KI oleh Tiongkok serta Kebijakan Obama dan Trump untuk menghadapinya

Pada era Obama peretasan Tiongkok berfokus pada penyerangan terhadap perusahaan-perusahaan teknik, energi, manufaktur, militer dan teknologi tinggi milik AS sebagai upaya Tiongkok dalam mengejar ketertinggalan teknologi dan ekonomi AS. Aktifitas APT pemerintah Tiongkok mewarnai tren peretasan di era Obama. Mandiant, sebuah perusahaan keamanan siber dalam laporannya tahun 2010 menjelaskan bahwa kemampuan APT Tiongkok berkembang ketika melakukan aktifitas ilegal dalam jaringan biasa (Mandiant, 2010). Pada awal-awal tahun kepemimpinan Obama, penyerangan mayoritas dilakukan oleh APT1 (2006-2013) (Mandiant, 2014, p. 23). Sejak 2006, APT1 telah melakukan penyerangan ke berbagai sektor di AS mulai dari sektor pendidikan, hingga teknologi informasi. Meskipun banyak perusahaan sektor yang menjadi korban, namun pada tahun-tahun awal pemerintahan Obama tidak disebutkan nama-nama perusahaan yang menjadi korban demi kepentingan bisnis.



Tabel 2.2 Sektor yang menjadi target APT1 (Mandiant, 2014, p. 23)

Pada 2009 terjadi operasi Night Dragon. Serangkaian serangan ini menyerang sektor-sektor penting seperti perusahaan kimia, energi dan minyak global (PricewaterhouseCooper , 2017, p. 14). Selain perusahaan, serangan ini menyerang individu maupun eksekutif dari perusahaan tersebut yang berada di Kazakhstan, Taiwan, Yunani dan AS. Dengan memanfaatkan cara seperti kelemahan Sistem Operasi Windows dan *spearphishing*, serangan ini mencoba mendapatkan dan mengambil informasi yang berkenaan dengan operasi eksklusif dan informasi keuangan milik perusahaan perusahaan-perusahaan tersebut (McAfee, 2011, p. 3). Serangan ini pertama kali diidentifikasi pada Maret 2009 oleh McAfee dan berlangsung terus hingga laporan diterbitkan pada tahun 2011.

Dalam laporannya McAfee secara menjelaskan bahwa mereka berhasil mengidentifikasi lokasi setidaknya satu penyerang berasal dari Tiongkok,

> *Sementara kami percaya banyak aktor yang terlibat dalam penyerangan ini, kami dapat mengidentifikasi satu individu yang menyediakan infrastruktur C&C kepada penyerang-individu ini berbasis di Kota Heze, Provinsi Shandong, Tiongkok. walaupun kami tidak yakin bahwa individu ini merupakan dalang dariserangan ini, tapi kami yakin bahwa orang ini memiliki informasi mengenai individu atau sekelompok individu yang melakukan intrusi.* (McAfee, 2011, p. 18).

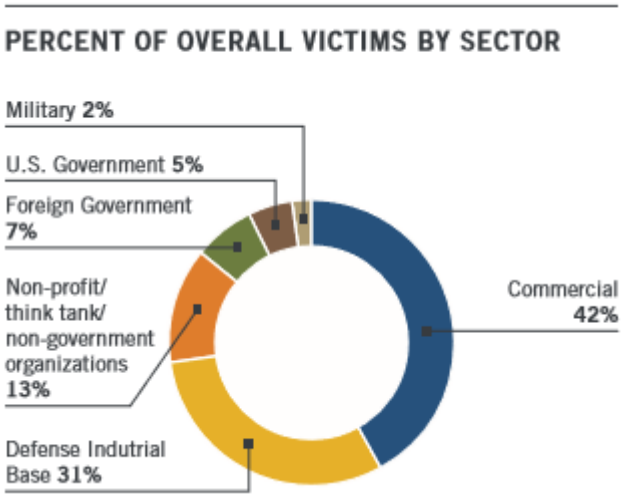
Selain lokasi, McAfee juga memperkirakan bahwa pelaku adalah pekerja kantoran dibuktikan dengan waktu terjadinya serangan dan eksfiltrasi data yaitu pada pukul 9 pagi sampai 5 sore (McAfee, 2011, p. 18). Dalam laporannya, McAfee menjelaskan bahwa individu tersebut bekerja di sebuah perusahaan yang menyediakan server AS dengan biaya $10 per 100 MB per tahun.

Pada tahun yang sama terjadi insiden penyerangan yang ditujukan kepada jaringan pemerintah AS, indusri pertahanan, firma hukum, dan perusahaan pertambangan. Serangan yang disebut sebagai Operasi Aurora dilakukan oleh kelompok yang dinamakan sebagai APT 17. Operasi tersebut dinamakan Aurora oleh Dmitri Alperovich yang mengidentifikasi file-file bekas operasi dan menemukan nama Aurora pada file tersebut. Serangan tersebut diketahui oleh publik pertama kali melalui pengumuman oleh Google dan McAfee pada awal 2010. Dalam pengumumannya, Google menjelaskan bahwa selain Google ada sekitar 20 perusahaan multinasional yang bergerak dalam bidang keuangan, teknologi, kimia, dan internet telah menjadi korban juga (Google, 2010). Google merupakan satu-satunya perusahaan yang berani mengungkap kasus ini, sedangkan perusahaan lainnya memilih bungkam karena khawatir tidak mendapatkan akses pasar Tiongkok bagi produk mereka.

Selain perusahaan multinasional, serangan tersebut juga menargetkan kelompok aktivis HAM yang bermarkas di Tiongkok (US-China Economic Relations Commission, 2009). Menurut Dmitri Alperovich, analis dari perusahaan keamanan siber Crowdstrike, APT 17 mendapatkan data dengan memasukan *malware* secara otomatis ketika pengguna mengunjungi situs-situs yang tidak aman (Zetter, 2010). Operasi ini dianggap telah merubah model serangan terhadap situs-

situs komersial, mengingat serangan semacam ini biasanya digunakan untuk menyerang situs militer.

Pada tahun 2011, Mandiant, konsultan keamanan siber melaporkan bahwa terjadi perubahan dalam target serangan baik entitas korban maupun informasi incarannya. Dalam laporannya, Mandiant menjelaskan bahwa serangan APT Tiongkok yang tadinya berfokus pada situs-situs pemerintah menjadi situs-situs bisnis. Sektor-sektor yang menjadi target dari serangan APT pada tahun 2011 adalah situs pemerintah AS, situs pemerintah asing selain AS, situs industri pertahanan, organisasi non-profit dan komersial (Mandiant, 2011). Namun, sektor komersial memiliki porsi paling besar dalam daftar target serangan APT Tiongkok pada tahun 2011 yaitu sebesar 42 persen.

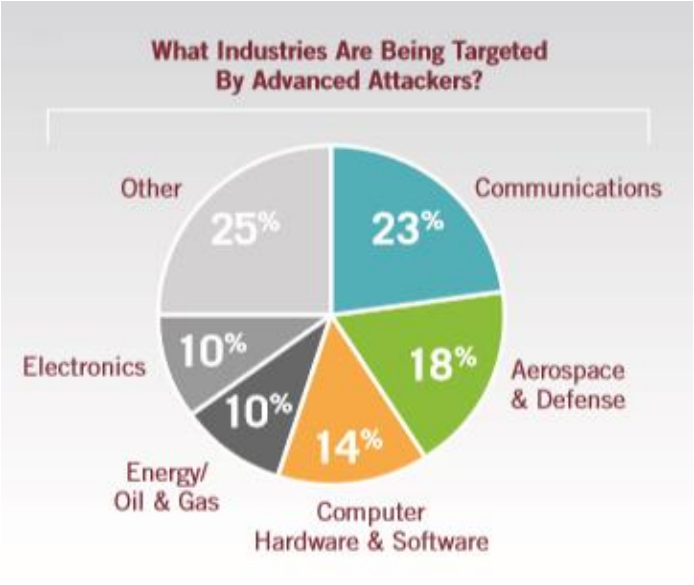


Tabel 2.3 Presentasi Sektor yang menjadi target serangan APT pada tahun 2011 (Mandiant, 2011, p. 5)

Contoh serangan yang terjadi pada 2011 adalah serangan terhadap Westinghouse Electric Corporation. Serangan terjadi ketika Westinghouse mengadakan kerjasama dengan salah satu perusahaan milik negara Tiongkok untuk membangun pembangkit listrik tenaga nuklir AP1000 di Tiongkok. Pada saat itu Sun Kailang yang menjadi pejabat unit 61398 meretas jaringan komputer milik Westinghouse dan mengakses email dari pejabat tinggi Westinghouse Electronic (Department of Justice, 2014). Sun yang didakwa pada tahun 2014 oleh Departemen Kehakiman AS dihukum karena berbagai tindak kriminal termasuk

akses komputer tanpa izin, konspirasi untuk mengakses komputer tanpa izin, dan spionase ekonomi (FBI, 2014). Sun dituduh mencuri informasi rahasia berupa spesifikasi pipa, pendukung pipa dan jalur pipa dalam pembangkit listrik AP 1000. Akibatnya, Tiongkok membatalkan pembangunan 36 reaktor nuklir dari 40 reaktor yang direncanakan pada 2017 karena telah dapat membangun sendiri (Cohen, 2017). Belakangan, pada 2017 Westinghouse dinyatakan bangkrut karena kesalahan penunjukan perusahaan untuk membangun dua reaktor di Georgia dan North Carolina, AS (Conca, 2017). Meskipun penyebab utama kebangkrutan adalah kesalahan interal, namun pembatalan pembangunan 36 buah reaktor di Tiongkok juga berpengaruh bagi kebangkrutan perusahaan ini karena pemasukan yang seharusnya bisa menambal kerugian akibat kesalahan internal ini tidak pernah sampai.

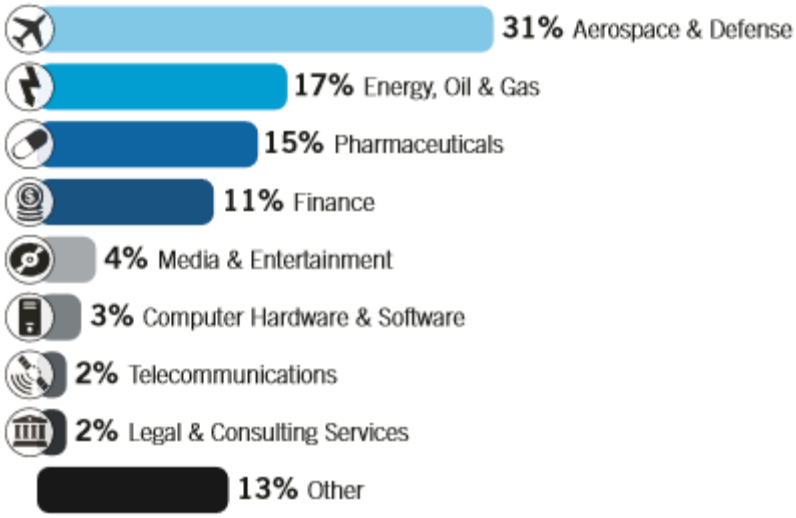
Pada 2012 tren serangan terhadap jaringan komputer industri semakin canggih. Akan tetapi, kesadaran perusahaan-perusahaan akan pentingnya keamanan siber belum terlalu tinggi. Hal ini dibuktikan dari jumlah perusahaan yang sadar akan adanya serangan terhadap jaringan komputernya. Menurut Mandiant dalam laporan tahunan edisi 2012, sebanyak 94 persen dari korban baru mengetahui bahwa telah diserang setelah diberitahu oleh pihak ketiga (Mandiant, 2012). Selain itu pada tahun ini, sektor komunikasi menjadi favorit bagi APT untuk diserang mengingat pertukaran informasi terjadi pada sektor ini.



Tabel 2.4 Persentase industri yang menjadi target APT pada tahun 2012 pada sektor ini (Mandiant, 2012, p. 2)

Pada 2012, FBI memanggil pejabat eksekutif Solar World. Pada saat itu, FBI memberitahukan bahwa jaringan komputer Solar World telah diretas dan peretas berhasil mencuri informasi berharga berkaitan rahasia dagang (Harris, 2014). Dalam kasus ini, APT 1 lagi-lagi menjadi aktor dari serangan tersebut. Pelaku dari penyerangan ini diketahui bernama Lao Wen, seorang perwira Departemen Ketiga Tentara Pembebasan Rakyat (Department of Justice, 2014). Pada 2014, Wen diadili atas tuduhan spionase ekonomi melalui jaringan komputer. Wen diketahui telah mencuri serangkaian informasi berharga diantaranya aliran dana Solar World, metrik manufaktur, garis produksi, dan biaya produksi. Dengan informasi tersebut, perusahaan sejenis milik pemerintah Tiongkok dipercaya dapat memenangkan persaingan bisnis dengan Solar World dari berbagai sisi. Ben Santarris, perwakilan dari Solar World menjelaskan, serangan ini tidak lepas dari aktifitas perusahaan yang vokal terhadap praktik dagang curang yang diterapkan oleh pemerintah Tiongkok (Shick, 2014). Pada 2017, Solar World dinyatakan bangkrut karena kalah bersaing dengan produk Tiongkok yang membanjiri pasar AS dengan harga yang lebih murah.

Tahun 2013 menandai mulai meningkatnya kesadaran akan keamanan siber. Pada tahun ini perusahaan-perusahaan mulai meningkatkan kemampuan keamanan sibernya sehingga mulai banyak perusahaan yang dapat mendeteksi serangan terhadap jaringan mereka secara internal. Menurut data dari laporan tahunan Mandiant tahun 2013, perusahaan yang dapat mendeteksi serangan secara internal meningkat jadi sebanyak 37 persen dari yang sebelumnya enam persen pada tahun 2012 (Mandiant, 2013, p. 2). Kasus yang menimpa Solar World dan Westinghouse Electric menjadi salah satu alasan peningkatan kesadaran ini. Pada tahun 2013, target dari APT Tiongkok juga masih berorientasi untuk kepentingan strategis industri Tiongkok seperti industri kapal terbang, farmasi, dan energi (Mandiant, 2013, p. 8).



Tabel 2.5 Industri yang menjadi target APT pada tahun 2013 (Mandiant, 2013, p. 9)

Pada 2013 data rahasia program pesawat tempur F-35 berhasil diretas oleh kelompok peretas yang dipercaya berasal dari Tiongkok. Franck Kendall, pejabat Pentagon yang mengurus akuisisi teknologi militer menjelaskan di hadapan senat saat ditanya mengenai perkembangan program pesawat tempur F-35: "*I'm not at all confident that our unclassified information is as well-protected. A lot of that is being stolen right now and it's a major problem for us*" (Alexander, 2015). Meskipun tidak dijelaskan kelompok peretas Tiongkok mana yang menjadi pelaku, tetapi serangan peretasan ini setidaknya berhasil menadapatkan informasi teknologi militer AS. Selain program pesawat tempur F-35, serangan ini juga mendapatkan informasi mengenai THAAD(*Terminal High Altitude Aeril Defense*), sistem pertahanan Balistik PAC-3 dan sistem pertahanan balistik Aegis (Dewey, 2013).

Selain target tersebut, tahun 2013 menjadi awal dimulainya operasi Iron Tiger, serangkaian serangan peretasan yang mengincar berbagai target penting di AS. Berdasarkan investigasi TrendMicro, sebuah perusahaan Jepang dalam bidang keamanan siber, serangan ini berasal dari Tiongkok kelompok APT 31. (Chang, et al., 2015, p. 3). Operasi ini menyerang email milik manajer dan direktur berbagai perusahaan termasuk pertahanan, elektronik, energi, telekomunikasi, dan kontraktor persenjataan Pemerintah AS (Chang, et al., 2015, p. 3). Operasi ini diketahui mulai terjadi sejak 2010 namun pada awalnya hanya menyerang demi keuntungan politik saja, sedangkan mulai tahun 2013 mulai menargetkan sektor-sektor strategis untuk kepentingan Tiongkok. Sebagaimana serangan khas APT

lainnya, operasi Iron Tiger dilakukan dengan menyebar *spear phishing* kepada target-target yang telah ditentukan, lalu peretas mengakses email yang berisi dokumen-dokumen penting termasuk kekayaan intelektual milik perusahaan yang menjadi korban seiring target membuka email-email tersebut (Chang, et al., 2015, p. 4).

Tahun 2014 bisa disebut sebagai tahun yang cukup sepi dari serangan-serangan siber terhadap AS. Penuntutan terhadap lima pejabat Tentara Pembebasan Rakyat oleh pengadilan Pensylvania pada Mei 2014 mungkin menurunkan aktifitas dari peretasan yang dilakukan oleh Tiongkok. Dakwaan ini merupakan kasus pertama dimana AS secara resmi mendakwa pejabat pemerintah asing dengan tuduhan peretasan terhadap komputer perusahaan AS dan pertama kalinya FBI menyebut Tiongkok sebagai "penjahat siber" (Ackerman, 2014). Tuduhan ini membuat hubungan kedua negara merenggang ketika pemerintah Tiongkok melayangkan protes resmi kepada otoritas AS.

Namun, 2014 bukanlah tahun tanpa peretasan. Pada tahun ini APT 18 melakukan peretasan kepada perusahaan penyedia layanan kesehatan AS, Community Health. Seperti yang telah dijelaskan sebelumnya, kelompok peretas ini mencuri data milik perusahaan tersebut yang berkaitan dengan pasien termasuk nama, alamat, dan nomor kartu jaminan sosial. Selain itu kelompok ini juga mengincar teknologi fasilitas kesehatan milik perusahaan tersebut.

Tahun 2015 merupakan tahun dimana kemajuan bagi hubungan antara Tiongkok dan AS terjadi. Pada tahun tersebut kesepakatan antara kedua negara mengenai peretasan berlangsung. Dalam kunjungannnya ke AS, Presiden Xi Jinping sepakat dengan Obama untuk tidak mendukung peretasan untuk mencuri kekayaan intelektual milik perusahaan di kedua negara (Rosenfeld, 2015). Kesepakatan ini layaknya setitik cahaya di tengah suramnya ketegangan hubungan kedua negara karena berbagai spionase ekonomi yang terjadi selama bertahun-tahun.

Menurut laporan khusus Fireeye tahun 2016, terjadi penurunan kasus peretasan kepada AS yang berasal dari Tiongkok. Tercatat dari pertengahan 2015 sampai awal 2016 hanya terjadi 13 kasus peretasan oleh Tiongkok, itupun jumlah kasus peretasan yang mencakup serangan terhadap Eropa dan Jepang (FireEye, 2016, p. 4). Penurunan ini, lanjut laporan tersebut disebabkan oleh dua hal yaitu

faktor internal dan eksternal. Faktor internal yang dianggap sebagai penyebab dari menurunnya serangan adalah reformasi pada jajaran pejabat Tentara Pembebasan Rakyat yang dilakukan oleh Xi Jinping sejak tahun 2014, sedangkan faktor eksternalnya adalah kesepakatan yang tercapai antara Barack Obama dan Xi Jinping tahun 2015 (FireEye, 2016, p. 4).

Tahun 2017 menjadi tahun yang cukup menggembirakan dalam hal kemampuan deteksi serangan peretasan. Tahun ini juga merupakan tahun pertama bagi pemerintahan Donald Trump. Menurut data dari laporan FireEye tahun 2017, sebanyak 53 persen deteksi serangan terhadap peretasan dilakukan oleh internal keamanan perusahaan sendiri (FireEye, 2017). Namun tetap terjadi peretasan terhadap penyedia layanan internet, yaitu Operasi Cloud Hopper. Operasi ini mengincar penyedia layanan teknologi informasi yang menjadi tempat berbagai perusahaan menyimpan berbagai dokumen resmi yang berisi rahasia dagang, paten dan berbagai kekayaan intelektual lainnya. Operasi ini diklaim dilakukan oleh APT 10, kelompok peretas yang berasal dari Tiongkok yang dikenal sebagai pengincar berbagai kekayaan intelektual milik barat sebagai upaya Tiongkok mengejar ketertinggalan teknologi dan ekonomi barat. Identifikasi APT 10 dilakukan berdasarkan waktu penyerangan terjadi dimana mayoritas serangan terjadi pada jam kerja waktu Tiongkok (PricewaterhouseCooper , 2017, p. 6). Operasi ini mengincar berbagai perusahaan termasuk energi, pertahanan, teknologi tinggi dan konstuksi dan manufaktur. Sektor-sektor ini oleh ahli dianggap sebagai sektor yang menjadi fokus dalam rencana lima tahunan Tiongkok ke-13 dengan tujuan Made in China 2025.

Respon terhadap perilaku Tiongkok berbeda antara pemerintahan Obama dan Trump. Obama lebih menekankan diplomasi dan kerjasama sehingga menghasilkan kesepakatan antara Obama dan Xi Jinping dalam hal keamanan siber. Dalam kesepakatan tersebut kedua negara berkomitmen dalam empat hal yaitu menyediakan respon cepat terhadap permintaan informasi dan bantuan terkait penanganan aktifitas jahat digital, tidak mendukung pencurian Kekayaan Intelektual melalui media siber, melanjutkan usaha untuk mengidentifikasi dan mempromosikan norma kepantasan perilaku dalam dunia siber dan membentuk mekanisme dialog tingkat tinggi untuk membicarakan kejahatan siber dan hal terkait(Office of the Press Secretary, 2015).

Sejak disepakatinya kerjasama ini, kedua negara memiliki sambungan komunikasi langsung untuk komunikasi darurat jika terjadi serangkaian peretasan seperti yang telah terjadi sebelumnya. Pemerintah Tiongkok akan mendelegasikan Kementrian Keamanan Publik , Kementrian Keamanan Nasional, Kementrian Kehakiman, dan Kantor Negara untuk Internet dan Informasi sedangkan Pemerintah AS akan mendelegasikan Kementrian Keamanan Dalam Negeri dan Hakim Agung AS akan memimpin dilalog berkala yang akan dilakukan untuk membahas ketepatan waktu dan kualitas respon yang diharapkan kedua negara terkait laporannya terhadap aktifitas siber jahat dan kejahatan terkait yang diidentifikasikan masing-masing negara. Selain itu, dialog ini juga akan dihadiri pula oleh perwakilan FBI dan komunitas intelijen AS(Office for the Press Secretary, 2015). Kesepakatan ini dianggap sebagai keberhasilan diplomasi pemerintah Obama mengingat perilaku Tiongkok selama ini yang terkesan kurang antusias untuk membicarakan pencurian Kekayaan Intelektual.

Berbeda dengan Obama, Donald Trump terlihat tidak percaya dengan Tiongkok walaupun AS telah memiliki kesepakatan ini. Pada Agustus 2017, Donald Trump menandatangani Executive Memorandum yang berisi perintah penyelidikan terhadap praktik dagang Tiongkok terhadap perusahaan-perusahaan AS. Dalam pernyataannya, Donald Trump menegaskan pentingnya negara dalam menjaga kekayaan intelektual perusahaan-perusahaan nasional (Wroughton & Mason, 2017). Maret 2018, seiring dengan keluarnya hasil penyelidikan tersebut, Donald Trump menerapkan tarif impor sebesar 25 persen kepada produk Tiongkok. Dalam keterangan persnya, Donald Trump menjelaskan alasan dari diberlakukannya tarif ini adalah pencurian kekayaan intelektual milik perusahaan AS. Trump mengatakan, "*kami memiliki masalah pencurian kekayaan intelektual yang serius. (tarif)ini akan membuat kami menjadi negara yang lebih kuat dan kaya*." (Diamond, 2018). Kebijakan ini diterapkan ketika AS masih memiliki kesepakatan dengan Tiongkok perihal spionase ekonomi melalui media siber.