Aktifitas Spionase Republik Rakyat Tiongkok ke Amerika Serikat (*Cyber* Spionase RRT ke Amerika Serikat terkait Proyek Militer Pesawat F-35 *Joint Strike Fighter* 2014- 2017)

Muhamad Helmi Kaffah Nur Iman[1]
Andrea Abdul Rahman Azzqy[2]

Abstract
This study aims to analyze the Chinese Spying Activities against the United States Related Military Projects F-35 Joint Strike Fighter. In analyzing the case the author uses the concept of Action-Reaction Model and Information Warfare. This type of research is qualitative research. The results of this study indicate that Tiongkok is currently a US espionage threat, in this focus stole secret data F-35 Joint Strike Fighter by phishing that can open access to secret aircraft data F-35 Joint Strike Fighter jet. In its action, Chinese representatives stole the data by sending emails to Lockheed Martin staff or officials who contained malware called spyware and trojans to access data that was stored neatly and strictly as a safeguard against expensive data such as the production cost of F-35 fighter jets The Joint Strike Fighter.

Keywords*: PRC, USA, cyber espionage, F-35 joint strike fighter, phishing*

Pendahuluan

Masa kini membawa pembaruan yang berdampak pada pergeseran dalam kehidupan sehari-hari. Munculnya teknologi informasi yang membawa fungsi untuk mempermudah dalam pertukaran informasi dan berkomunikasi. Fungsi teknologi ini di gunakan tidak hanya di kalangan masyarakat tapi di institusi negara, militer dan lainnya sebagainya pun memanfaatkan kemajuan yang ada. Kemajuan ini menimbulkan dampak baik maupun dampak buruk, baiknya mempermudah dalam komunikasi, dan mencari informasi namun buruknya pun begitu banyak yang dapat ditimbulkan seperti disalahgunakan seperti penipuan, tindakan hacking, dan serangan lewat Cyberspace lainnya. Cyberspace dalam bahasa Indonesia itu dunia maya, dunia dimana adanya hubungan dua arah atau satu arah yang dihubungkan lewat jaringan komputer. Menurut Perry Barlow dan Bruce Sterling dalam bukunya yang berjudul The Hacker Crackdown Online and Disorder On The Electronic Frontier, kedua tokoh itu menyebutkan bahwa "Cyberspace merupakan ruang yangtidak dapat dilihat "(Perry Barlow & Bruce Sterling, 1992:1). Dalam hubungan internasional peran teknologi dimanfaatkan untuk memaksimalkan suatu negara dalam

[1] Mahasiswa, Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Budi Luhur. Email: balcony@budiluhur.ac.id
[2] Dosen, Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Budi Luhur.

melakukan hubungan diplomatik dan lain sebagainya yang mendukung untuk terjalinnya hubungan antar negara tersebut.

Cyberspace dalam urusan kenegaraan dan militer merupakan ruang baru yang memanfaatkan dunia cyber yang kasat mata. Dengan hadirnya ruang ini menimbulkan masalah baru yang beralih dari konvensional kepada hal yang lebih modern seperti spionase yang pada saat ini dilakukan secara cyber (Sindonews, https://nasional.sindonews.com/read/1248299/14/bentuk-satuan-siber-tni-siap hadapi-serangan-di-dunia-maya-1507966324/). Pembaruan ini tidak semata-mata mendatangkan kemudahan dan dampak baik lainnya namun dibarengi dengan masalah baru seperti penyerangan suatu system informasi atau sistem komputerisasi atau yang biasa disebut cyber attack seperti yang terjadi di Estonia pada tahun 2007 (Merdeka, https://www.merdeka.com/teknologi/kasus-estonia- dan-georgia-jadi-sejarah-kelam-cyber-crime-dunia.html). Sebagai bentuk solidaritas untuk negara-negara sekutunya AS dalam organisasi NATO (North Atlantic Treaty Organization) dan Estonia merupakan pusat cyber anggota NATO maka dari itu AS meningkatkan keamanan cyber nya karena ini merupakan ranah baru dalam kedaulatan negara setelah darat, laut dan udara. Pada tahun 2011 Obama menerbitkan formulasi kebijakan yakni International Strategy for Cyberspace untuk membendung kejahatan-kejahatan yang berasal dari ranah cyber yang dapat mengancam keamanan dan kedaulatan negaranya tersebut (The WhiteHouse, 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/International_Strategy_Cyberspace_Factsheet.pdf). Formulasi kebijakan ini menandakan bahwa AS sedang mengetatkan keamanan cyber nya yang sering dibobol oleh para penyerang cyber atau hacker dari pemerintahan dan industri pertahanan AS, maka dari itu dibuat kebijakan ini.

Penyerangan via cyberspace seperti ini lebih efisien dan efektif karena hanya melewati serangkaian keamanan dalam sistem yang tidak kasat mata. Contoh dalam kasus ini adalah spionase secara cyber yang merupakan masalah baru yang ada didunia internasional. Dalam penelitian ini akan membahas tentang spionase secara cyber yang dilakukan oleh Republik Rakyat Tiongkok terhadapindustri militer Amerika Serikat terkait proyek militer pesawat F-35 Joint StrikeFighter yakni pesawat generasi kelima yang diproduksi oleh Lockheed Martin yang merupakan industri militer milik AS yang juga merupakan salah satu industri yang paling produktif dalam menciptakan inovasi-inovasi baru yang hadir untuk pertahanan AS sendiri atau untuk di komersilkan oleh AS guna mendapatkan penghasilan negara paman sam tersebut. (Sindonews, https://international.sindonews.com/read/632058/9/as-tuding-Tiongkok-agresor- cyber-terbesar-di-dunia-1337425975). Dalam kasus ini Tiongkok menggunakan warga negara Tiongkok yang merupakan pengusaha bidang penerbangan yang memiliki pabrik di California yang bernama Su Bin. Dalam aktifitasnya Su Bin dibantu oleh perwira militer Tiongkok untuk mengawasi tindakan Su Bin tersebutyang dilakukan diranahdunia maya. (Vice News,https://news.vice.com/article/man-who-sold-f-35-secrets-to-Tiongkokpleads-guilty).

Dari fenomena yang terjadi dimana Tiongkok melakukan cyber espionage terhadap AS terkait data F-35, dari siitu penulis merumuskan masalah sebagai berikut: Bagaimana strategi Tiongkok dalam meretas data proyek militer Amerika Serikat F-35 *Joint Strike Fighter*?

Dalam penelitian ini, penulis menggunakan teori realisme, action reaction model dan Information Warfare. Teori Realisme digunakan untuk menjelaskan tentang kedua negara yang saling bersaing namun persaingannya tersebut dapat mengancam keamanan nasional dan kelangsungan hidup bagi AS dan dalam hal ini Tiongkok yang menjadi ancaman terhadap keamanan nasional bagi negeri paman sam tersebut karena

melakukan cyber espionage terhadap industri militer yakni proyek militer pesawat F-35 JSF milik negeri paman sam tersebut, AS yang merupakan salah satu penyumbang pemasukan negara terbesar bagi AS. (Robert Jackson, Georg Sorenson,2011:112). Lalu action reaction model digunakan untuk menjelaskan persaingan dalam persenjataan yang dilakukan kedua negara yakni Tiongkok dan AS. Tiongkok melakukan hal semacam ini untuk menyaingi kehebatan persenjataannya untuk pertahanannya untuk menahan hegemoni AS dipasifik. Dalam kasus ini pesawat F-35 dalam kasus ini dicuri datanya dan digunakan untuk memproduksi pesawat dalam negerinya oleh Tiongkok. (Barry Buzan, 1987 : 76, https://link.springer.com/chapter/10.1007/978-1-349-18796-6_6). Kemudian Information Warfare menjelaskan bahwa perang informasi pada pasca perang dingin masih sering terjadi seperti yang terjadi pada kasus cyber espionage Tiongkok terhadap Amerika Serikat terhadap proyek militer pesawat F-35 ini, dimana informasi suatu bangsa yang didapatkan negara lain merupakan suatu ancaman terhadap keamanan nasional suatu negara (Martin Libicki, 1996 : 26).

Artikel ini menggunakan pendekatan kualitatif yang diperoleh dari hasil wawancara dan studi pustaka dan menggunakan metode studi kasus untukmenjelaskan kasus ini secara lebih mendalam. Penulis meneliti dengan menyelidiki aktifitas yang dilakukan oleh Su Bin dan oknum militer Tiongkok dalammendapatkan data rahasia dari pesawat jet F-35 Joint Strike Fighter (Pakar Komunikasi, https://pakarkomunikasi.com/pengertian-studi-kasus-menurut-para- ahli). Dalam tulisan ini, data yang digunakan bersifat primer dan sekunder. Dataprimer diperoleh dari hasil wawancara kemudian data sekunder diperoleh dengan cara studi literatur yang didapatkan dari buku, jurnal-jurnal ilmiah, dokumen resmi negara dan berita-berita dari media online.

Pembahasan

Sejarah dan Perkembangan Cyberspace

Dalam kemajuan teknologi pada era modern ini setiap elemen dalam negara wajib untuk mempertahankan kedaulatan, keamanan dalam setiap aspek seperti dalam cyberspace yang merupakan ranah atau bagian baru dalam mempertahankan kelangsungan hidup negara. Untuk itu sebagian negara yang telah sadar bagaimana vitalnya dunia cyber dalam kehidupan berbangsa dan bernegara. Kemajuan dunia maya tidak bisa dilepaskan oleh perkembangan internet karena pada umumnya orang mengenal dunia maya itu dari internet.

Internet singkatan dari interconnected network, yang merupakan suatu perangkat yang dapat terhubung melalui sistem jaringan. (New Media Institute, 2017, http://www.newmedia.org/history-of-the-internet.html) Internet pada awalnya diciptakan untuk kepentingan militer dan kepentingan pendidikan di Amerika Serikat. Internet awalnya dibuat oleh departemen pertahanan AS yang menemukan sebuah perpaduan antara teknologi dan telekomunikasi dari sebuah riset yang diadakan oleh DARPA (Defence Advanced Research Project Agency)yang dipimpin oleh Robert Taylor dan Larry Robert dari MIT(Massachusetts Institute of Technology) membuat badan riset yang berjalan dibawah naungan DOD(Department of Defence) pada 1960. Dari riset ARPA (Advance Research Project Agency) tersebut berhasil dibuat sebuah sistem yang menghubungkan antar jaringan, lalu dari hasil temuan tersebut itu dinamakan ARPANET. Awalnya ARPANET berjalan dari University of California Los Angels ke Stanford Research Institute, dan pada tahun 1981 berkembang pesat dan banyak yang menggunakan sampai ke seluruh dunia sehingga jaringannya yang meluas dan menjadi satu koneksi berubah sebutan menjadi internet.

Perkembangan Cyberspace

Internet yang kini menjadi sebuah perangkat yang diperlukan semua kalangan pun memiliki pengaruh pada bergesernya pola komunikasi jarak jauh. Itu hanya sebagaian dampak positif yang didapat oleh pengguna namun ada pula dampak buruk yang merugikan pengguna seperti hacking, espionage dan lain sebagainya. Penyerangan dalam ranah cyber ini sulit dideteksi maka dari itu pada era modern dengan segala kemajuan teknologi yang ada dimanfaatkan oleh oknum-oknum untuk mendapatkan keuntungan pribadi, kelompok maupun suatu bangsa atau negara. Pada perkembangannya cyberspace dibagi menjadi dua lapisan yaitu Surface Web dan Deep Web yang termaktub dalam WWW(World WideWeb).(CambiaResearch,https://www.cambiaresearch.com/articles/85/surface- web-deep-web-dark-web----whats-the-difference) Surface Web merupakan suatu lapisan dimana bisa kita gunakan dalam browsing internet yang sehari-hari digunakan oleh pengguna. Sedangkan Deep Web merupakan lapisan web yang dapat mencakup sebagian besar yang terdapat di internet, dari lapisan ini dapat kita temui berbagai kegiatan yang negatif atau tidak legal. Hal ini dapat dimanfaaatkan oleh oknum penjahat hacker karena lapisan ini sulit untuk di sulit untuk dilacak. Presentase yang bisa didapatkan dari internet lebih besar dari Deep Web daripada dari Surface Web. Namun bila ingin mengakses internet melalui Deep Web harus menggunakan aplikasi tersendiri salah satunya TOR Web yang dapat mengakses situs-situs ilegal.(Service Care Solution, www.servicecare.org.uk-61792715468)

Cyber Attack Menjadi Ancaman Keamanan Nasional

Dunia cyber memiliki ancaman dari serangan-serangan yang datang dari berbagai penjuru baik itu berupa virus, hacking dari individu atau kelompok yang tidak bertanggung jawab karena begitu sulitnya mengidentifikasi penyerang cyber tersebut. Cyber Attack ini terjadi karena begitu kompleksnya dunia cyber sehinggasulit dibendung dalam perkembangannya. Kemudian pembangunan infrastruktur ini bisa terganggu dengan terjadinya cyber attack, karena saat ini semua kegiatan terhubung dengan suatu jaringan untuk mempermudah pekerjaan yang sebelumnya menggunakan cara yang konvensional. (Techopedia, https://www.techopedia.com/definition/24748/cyberattack) Dalam penyeranganmacam ini biasanya menggunakan berbagai macam malware, dan yang paling sering digunakan untuk menyerang atau meretas individu, institusi negara atau perusahaan seperti Worm, Trojan dan Spyware. Worm merupakan sebuah jenis malware yang serupa dengan virus komputer yang bisa merusak bagian-bagian dalam komputer dan sifatnya mandiri karena jika sudah terjangkit worm di dalam komputer, worm akan hinggap ke bagian-bagian lain tanpa harus ada yang mengontrol worm tersebut. Sedangkan Trojan merupakan jenis malware yang bisa memakan data-data yang tersimpan oleh komputer yang terserang. Trojan bisa tersimpan ditempat yang tak terduga seperti di email, dan di tempat lain yang tidak bisa di tebak. Lalu spyware merupakan malware yang sesuai dengan namanya spy yang mengumpulkan informasi riwayat penelusuran secara diam- diam lewat internet yang langsung menyampaikan kepada pihak ketiga tanpa disadari tentang informasi dari perusahaan, lembaga dan negara. Jenis malware inibisa menyerang identitas ketiga hal tersebut lewat email dan lain-lain. Spyware digunakan untuk kepentingan suatu pihak dalam melakukan spionase yang menyebabkan kerugian bagi suatu negara yang diserang malware jenis ini (Avast, http://www.avast.com/c-trojan). Ancaman cyber kini begitu nyata karena telah terjadi aksi spionase secara cyber kepada negara lain demi mengetahui kegiatan dari negara lain baik di bidang politik, ekonomi maupun militer. Dunia cyber pada saat ini lebih sering digunakan untuk berbagai tindakan yang dapat merugikan salah satu pihak seperti

spionase via cyber seperti yang terjadi kepada AS yang terserang cyber spionase Tiongkok dalam hal ini industri militer. Praktik spionase sangat sering terjadi pada sejarah dalam hubungan internasional seperti pada perang dingin yang melibatkan dua magnet dunia yakni AS dan Uni Soviet. Kedua negara besar ini berebut pengaruh negara-negara didunia.

Namun tidak hanya sampai situ, praktik spionase pun sampai sekarang masih sering terjadi didunia, seperti yang dilakukan oleh Republik Rakyat Tiongkok kepada AS yang merupakan negara pesaing dalam hal industri militer pada saatini. Negeri panda tersebut menjadi penantang serius yang berambisi menjadinegara yang lebih kuat untuk menghadapi hegemoni AS dikawasan dan dalam pasar senjata global, maka dari itu Tiongkok terus meningkatkan kapasitas dan kapabilitas pada institusi militernya. (The Global Review, http://theglobalreview.com/lama/content_detail.php?lang=id&id=10979&type=4#.WkXnp9-WbIU).

Aktifitas Cyber Spionase Tiongkok Terhadap Amerika Serikat di bidang Militer

Tiongkok mengalami peningkatan dalam hal ekonomi berkat revolusi yang dijalankan pada masa Deng Xiaoping yang menganut sistem pasar bebas. Efek dari revolusi yang dilakukan Deng terasa hingga kini yang menjadi lebih maju ketika Tiongkok bergabung bersama WTO (World Trade Organization) dengan begitu pasar Tiongkok menjadi luas. Dengan begitu pendapatan Tiongkok pun meningkat, yang kemudian keuntungan yang diperoleh dimanfaatkan untuk memperbaiki pertahanan Tiongkok dan produksi dalam negeri dalam hal persenjataan. Terbukti Tiongkok mampu mengurangi impor alutsista dengan lebih memilih produksi sendiri, terlebih lagi Tiongkok mampu mengekspor alutsista ke negara lain. Tiongkok hingga 2015 telah mengekspor senjata ke negara lain yang terus meningkat, "menurut Stockholm International Peace Research Institution ekspor dalam bidang militer Tiongkok meningkat drastis diangka 88% dalam rentang waktu 2011-2015 "(CNNIndonesia,https://www.cnnindonesia.com/internasional/20160222114703-113-112511/ekspor-senjata-Tiongkok-meningkat-dua-kali-lipat/). Dengan peningkatan yang begitu signifikan Tiongkok menjadi negara pengekspor senjata terbesar ketiga didunia. Hal ini menjadi ancaman tersendiri bagi AS karena muncul aktor baru pesaing setelah Rusia. Namun dalam perkembangannya Tiongkok diduga melakukan spionase secara cyber terhadap AS yang merupakan negara yang sedang bersaing. Spionase dilakukan Tiongkok untuk dapat menyaingikedigdayaan AS dalam pasar senjata global.

Tidak sedikit kasus spionase yang melibatkan Tiongkok terhadap negara-negara lain khususnya AS. Seperti pada tabel di bawah ini:

Tabel 1 Sejumlah Spionase Cyber Tiongkok Terhadap Amerika Serikat

Tahun	Target	Asal Serangan
2007 – 2013	Data Desain dan Sistem Radar F-35 Joint Strike Fighter	Tiongkok
2007	Desain H-20 Northtropp Grumman, BAE System	Tiongkok

2007	Desain QinetiQ Bidang Militer(Robotika,Satelit, dan Helikopter Tempur	Tiongkok
2012	Sistem Rudal Patriot, Sistem Pertahanan Rudal Balistik Aegis, V-22 Osprey, F/A-18 Tempur, Kapal Tempur Littoral 17	Tiongkok

Sumber: Committee on Energy and Commerce Subcommittee on Oversight Investigations

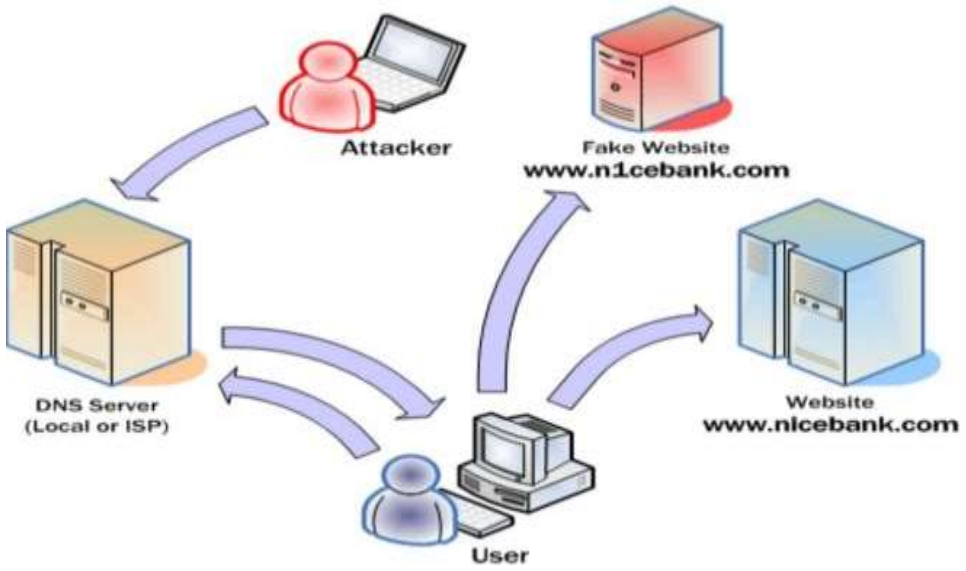
Pada tahun 2007 negeri tirai bambu mendapatkan data H-20 yang diproduksi oleh Northtropp Grumman dan BAE System yang dilakukan oleh seorang mantan kontraktor Northtropp Grumman sendiri yakni Noshir Gowaida. Noshir bekerja sama dengan Tiongkok terkait data pesawat berhulu ledak nuklir tersebut (BBC,http://www.bbc.com/news/world-asia-pacific-12272941). Ini merupakan suatu kejadian dimana penghianatan terjadi dimana mantan kontraktor Northtropp Grumman yang bekerja sama dengan negara rival Amerika Serikat yakni Tiongkok. Ditahun yang sama pun terjadi banyak kasus spionase yang dilakukan oleh oknum dari Tiongkok. F-35 yang merupakan pesawat generasi kelima milik Amerika Serikat. Pesawat ini menjadi pesawat dengan teknologi yang mumpuni karena telah memasukan teknologi sistem anti radar, elektro optik, dan nozel mesin F-35. (Vice News, https://news.vice.com/article/man-who-sold-f-35- secrets-to-Tiongkok-pleads-guilty) Seperti yang diungkapkan oleh Snowden yang merupakan mantan kontraktor dari NSA(National Security Agency) pada majalah der spiegel, Snowden mengatakan bahwa mengatakan bahwa "Desain Radar dan jenis modul F-35 Joint Strike Fighter telah dicuri oleh peretas yang berasal dari Tiongkok". (Freebeacon,http://freebeacon.com/national-security/Tiongkok-hacked- f22-f35-jet-secrets/). Pernyataan tersebut menjadi sebuah peringatan bagi keamanan nasional di bidang cyber AS.

Indikator Tiongkok Melakukan Cyber Spionase Kepada Amerika Serikat

Tiongkok yang sedang dalam tahap peningkatan kapasitas dan kapabilitas untuk mendapatkan kepercayaan dari negara-negara yang ada didunia bahwa Tiongkok telah menjadi negara yang superior. Salah satu indikator Tiongkok melakukan spionase terhadap AS yaitu agar dapat menciptakan alutsista yang memiliki kapabilitas yang dimiliki oleh alutsista produksi AS. Negeri paman Sam yang kini masih menjadi negara yang paling inovatif dalam persenjataan berteknologi canggih menjadikan faktor pendorong Tiongkok melakukan spionase terhadap industri persenjataan dari AS. Modernisasi yang dilakukan negeri Panda itu sedang dalam proses dengan cara mempercanggih persenjataan, merampingkan jumlah pasukan disemua matra laut, udara dan darat. Modernisasi militer Tiongkok pada era Xi Jinping lebih ditekankan untuk membuat PLA lebih kompeten dalam melaksanakan tugasnya dengan memasukan unsur teknologi didalam persenjataannya yang membuat pertahanan Tiongkok yang lebih mampu untuk menghadapi ancaman baru yang datang yaitu dari cyberspace. Pada perkembangannya PLA mengalami peningkatan signifikan pada serangkaian bagian tentara pembebasan rakyat tersebut (Kabar24, http://kabar24.bisnis.com/read/20171020/19/701409/Tiongkok-bangun-kekuatan-militer-xi-jinping-kekuatan-dibangun-untuk-melawan).

Aktifitas Cyber Spionase Tiongkok Ke Amerika Serikat Terkait Proyek Militer Pesawat F-35 Joint Strike Fighter

F-35 Joint Strike Fighter merupakan pesawat jet generasi kelima yang diproduksi oleh Lockheed Martin, pada saat ini merupakan pesawat tempur berbasis kapal induk tercanggih. Produksi pesawat ini telah lama dijalankan namun banyak kendala yang dihadapi selama masa produksi. Biaya produksi pesawat ini pun sampai saat ini masih yang tertinggi dari yang sebelumnya. Dengan hadirnya pesawat jet terbaru AS ini, membuat Tiongkok ingin pula menciptakan pesawat yang dapat disejajarkan dengan pesawat tersebut. Namun dalam perkembangannya Tiongkok melakukan spionase terhadap data-data pesawat F-35 tersebut dengan menyertakan Su Bin yang merupakan pengusaha asal Tiongkok yang berdomisili di Vancouver, Kanada dan disana pula industri aviasi miliknya berdiri.(Microdata, http://blog.microdata.com/how-the-chinese-stole-the-secret- f35-fighter-plans-and-why-it-matters-to-you/) Su Bin dalam melakukan aksi cyber spionase ini terhadap F-35 INI dengan cara phishing. Phishing merupakan Praktik Curang dengan cara penyerang menyamar sebagai orang yang memiliki reputasi lewat surat elektronik atau email dan media lainnya. (Search Security, http://searchsecurity.techtarget.com/definition/phishing)

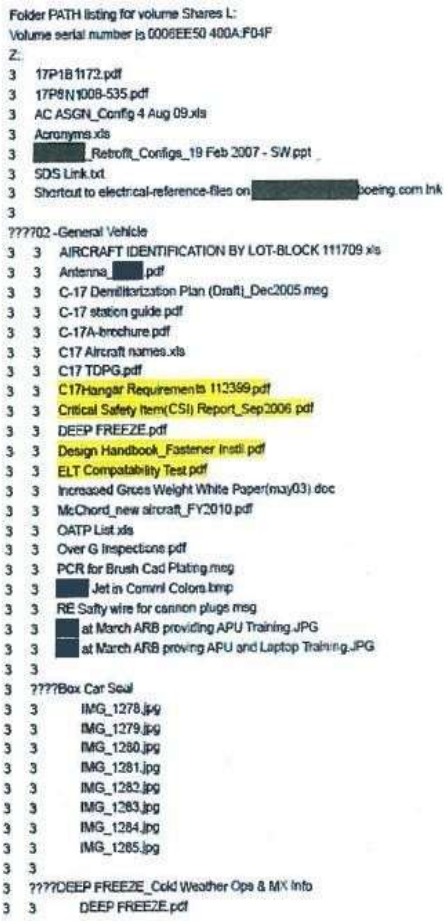


Gambar 1 Teknis Dalam Aktifitas Phishing
Sumber : Cyber Secure Asia, 2015

Anatomi Phishing diatas menggambarkan bagaimana langkah-langkah yang ditempuh pelaku sampai mendapatkan data dari target. Pelaku dapat mengakses data target dengan leluasa karena tindakan ini sulit diidentifikasi. Ini merupakan strategi yang digunakan oleh Tiongkok dalam mendapatkan data-data F-35. (Cyber Secure Asia, https://www.cybersecureasia.com/blog/phishing-and- pharming) Dalam aksinya Su Bin dipantau oleh dua perwira militer Tiongkok mengawasi Su dalam mendapatkan data tersebut. Su Bin menjalani misinya dengan mengirim email yang disebut sebagai phishing kepada pejabat kontaktor. Su mengirimkan email kepada kontraktor dan staff dari kontraktor pertahanan milik AS dengan memasukan malware dalam email tersebut yang menuntun staf dan pejabat kontraktor AS untuk membuka akses agar bisa diambil data serta informasinya terkait blueprint F-35. Pelaku ini menggunakan email yang terlegitimasi oleh kontraktor pertahanan AS dengan menyamakan nama,

tempat tinggal, posisi dan lainnya dengan tokoh yang terpercaya dari kontraktor pertahanan AS yang meyakinkan untuk bisa mendapatkan akses mengetahui data-data rahasia tersebut. Su Bin melakukan pencurian dengan menjebak kontraktor pertahanan AS dengan mengirimkan email yang berisi malware yang bisa membuka akses untuk Su Bin bertindak lebih jauh untuk mengambil data rahasia tersebut. Yang dilakukan Su Bin bersama rekannya dari Tiongkok mengakses jaringan komputer kontraktor pertahanan AS untuk mengambil data terkait sistem anti radar yang merupakan pembaruan dari pesawat generasi kelima ini. Sebagai hasil dari pencurian data-data rahasia terkait Lockheed Martin F-35 Joint Strike Fighter dibawah ini merupakan yang didapat dari sumber yang bersangkutan melalui surat kabar yang meliput tentang masalah yang terjadi terhadap kontraktorpertahanan. (Santosa, 2017)

Gambar 2 Blueprint Data F-35 Yang TercuriSumber : Bussiness Insider, 2015



Gambar 3 Data F-35 Joint Strike Fighter Sumber: Vice News, 2014

Data diatas diambil dari kejaksaan yang merupakan bukti dari tindak kriminal yang dilakukan oleh Su Bin. Gambar diatas merupakan bagian-bagian yang tercuri dari komponen F-35 JSF yaitu bagian sistem radar, elektro optik dan nozel mesin. Hal ini pada dasarnya merupakan tindakan yang mengancam keamanan informasi suatu negara dalam hal ini Amerika Serikat.

Reaksi Amerika Serikat Terhadap Aksi Cyber Spionase Tiongkok Terkait Proyek Militer Pesawat F-35 Joint Strike Fighter

Amerika Serikat yang merupakan salah satu negara yang begitu bergantung terhadap cyberspace, karena AS menggunakan sistem komputerisasi dalam menyimpan data-data sensitif dan rahasia pemerintahan. Maka dari itu Amerika membuat suatu formulasi kebijakan yang fokus pada keamanan cyberspace yang diberi nama International Strategy For Cyberspace yang diterbitkan pada tahun 2011 pada masa kepemimpinan Barrack Obama. Dalam kebijakan ini pula dituliskan tentang memperkuat kemitraan, dan hubungan trilateral dengan langkah tersebut dapat memperkecil risiko masalah cyber yang datang dari negara lain. (US Department Of State, 2011, https://2009-2017.state.gov/s/cyberissues/strategy/index.htm).

Tidak hanya membuat kebijakan, Amerika Serikat pun menjatuhkan sanksi terhadap Tiongkok yang telah melakukan spionase via cyberspace yang merugikan AS begitu besar. Sanksi yang dijatuhkan Amerika Serikat berupa sanksi ekonomi kepada Tiongkok sebagai reaksi atas spionase cyber yang dilakukan negara panda tersebut kepada Amerika Serikat. Sanksi dijatuhkan sebelum berlangsungnya pertemuan pemimpin kedua negara pada Konferensi Tingkat Tinggi di California. Sanksi dijatuhkan kepada pihak tersangka berupa pembekuan aset dan transaksi finansial.(VOA Indonesia, https://www.voaindonesia.com/a/as-siapkan-sanksi- peretasan-oleh-china-/2939473.html).

Kemudian pada tanggal 24-25 September 2015 diadakan pertemuan dalam Konferensi Tingkat Tinggi yang diadakan di California pun membahas tentang beberapa poin seperti perdamaian regional dan global, Memperkuat kerjasama pembangunan, memperkuat hubungan bilateral dalam bidang militer, keamanan cyber, dan pemberantasan terorisme. Keamanan cyber disini menjaga segala serangan-serangan cyber agar tidak terjadi lagi antara kedua negara (The White House, 2015, file:///C:/Users/acer/Documents/FACT%20SHEET_%20President%20Xi%20Jinping%E2%80%99s%20State%20Visit%20to%20the%20United%20States%20_%20whitehouse.gov.html). Untuk itu kedua negara setuju untuk mengentaskan kejahatan cyber yang merugikan negara. Selanjutnya dalam pertemuan ini kedua negara menyetujui agar dibuat forum antara kedua negara untuk membahas lebih jauh terkait cyber threat, dalam pertemuan ini Amerika Serikat dan Tiongkok membawa kementerian-kementerian terkait kedua negara, badan intelijen untuk berkomunikasi dalam rangka mengurangi ancaman kejahatan dunia maya.

Kesimpulan

Praktik Spionase yang dilakukan lewat cyberspace merupakan masalah yang sangat rumit untuk diselesaikan karena begitu kompleks didalam dunia maya dan cukup sulit untuk mencari bukti tentang tindakan tersebut. Teknologi informasi pada masa sekarang ini sangat dibutuhkan untuk mempermudah dan mempercepat dalam proses komunikasi yang begitu penting dalam menjalankan roda pemerintahan. Dalam masalah ini penulis berpendapat bahwa spionase dalam hubungan antar negara hanya untuk memanfaatkan kelemahan dari suatu negara yang berdampak buruk pada hubungan antar negara yang seharusnya diwarnai dengan tindakan saling menguntungkan satu sama lain justru berbanding terbalik dengan fakta yang terjadi dilapangan seperti dalam kasus didalam tulisan skripsi ini. Dalam perkembangannya hubungan antara Tiongkok dan Amerika Serikat begitu baik dalam hubungan perdagangan, namun tidak dibarengi dengan hubungan diplomatik kedua negara yang berbeda ideologi politik.

Tiongkok yang kini mulai berkembang pesat dalam bidang ekonomi dan pertahanannya. Dalam ekonomi Tiongkok mulai berkembang ketika negara tersebut membuka diri dalam pasar bebas yang mengikuti tren internasional. Perkembangan yang baik di bidang ekonomi Tiongkok ini membawa dampak yang baik bagi pertahanan Tiongkok yang mulai diberlakukan reformasi militer yang membuat Tiongkok kuat dalam pertahanan mulai dari produksi jet tempur hingga kapal induk yang menunjukan kekuatan pertahanan Tiongkok. Dalam mengembangkan pertahanannya Tiongkok diwarnai oleh tindak spionase cyber yang sering menyerang Amerika Serikat yang telah terlebih dahulu menjadi negara yang secara militer kuat dengan berbagai alutsista yang mumpuni yang dibuat oleh industri pertahanannya sendiri dan AS pun merupakan pengekspor alutsista di levelinternasional yang bernilai ekonomi tinggi. Tindakan spionase bila tidak diketahui merupakan hal yang biasa dan tidak menjadi masalah walaupun

melemahkan kedudukan negara yang terkena spionase. Maka dari itu spionase dalam hubungan internasional memerlukan aturan yang jelas agar bisa setidaknya mengurangi kegiatan spionase ini. Tiongkok dan AS yang kini menjadi negara yang kuat dalam hal pertahanan seharusnya tidak melakukan spionase tersebut secara berlebihan karena tindakan tersebut hanya bisa menurunkan kepercayaan suatu negara yang menjadi teman atau sekutunya.

Daftar Pustaka

Buzan B. (1987) The Action-Reaction Model. In: An Introduction to Strategic Studies. International Institute for Strategic Studies Conference Papers. Palgrave Macmillan, London, https://link.springer.com/chapter/10.1007/978-1-349-18796-6_6 diakses 1 November 2017.

Jackson, Robert dan Georg Sorensen, (2013), Elemen-elemen realisme dalam Pengantar Studi Hubungan Internasional, Oxford University Press. hal.112 Libicki, Martin.(1995). What is Information Cyberwarfare. National Defence Security, hal 26 diunduh 15 Oktober 2017.

Sterling, Bruce (1992). Hacker Crackdown Online and disorder on the electronic frontier: "Introduction". http://www.gutenberg.org/files/101/101-h/101-h.htm diunduh pada 10 Oktober 2017.

The White House. 2015. Fact Sheet: President Xi Jinping's State Visit The United States". file:///C:/Users/acer/Documents/FACT%20SHEET_%20President%20Xi%20Jinping%E2%80%99s%20State%20Visit%20to%20the%20United%20States%20_%20whitehouse.gov.html diakses 21 Desember 2017.

The White House, 2011. "Launching the International Strategy For Cyberspace". https://obamawhitehouse.archives.gov/blog/2011/05/16/launching-us-international-strategy-cyberspace diakses 19 Desember 2017.

US Department Of State, 2011, https://2009-2017.state.gov/s/cyberissues/strategy/index.htm\

US Department Of State, 2011, "Pillars of The International Strategy For Cyberspace", https://2009- 2017.state.gov/s/cyberissues/strategy/index.htm diakses 19 Desember 2017.

Novan Iman Santosa (2017). Senior Political and News Editor at The Jakarta Post Jakarta: The Jakarta Post, Wawancara, 13 Desember.

Larry M Wortzell. (2013). "Cyber Espionage And The Theft of US Intellectual Property And Technology: Commitee on Energy and Commerce Sub Commitee on Oversight and Investigations". file:///C:/Users/acer/Documents/Wortzel-OI-Cyber-Espionage-Intellectual- Property-Theft-2013-7-9.pdf diakses pada 13 Desember 2017.

Avast. "Trojan, Worm. Spyware definition". http://www.avast.com/c-trojan diakses pada 29 Oktober 2017.

Business Insider. (2014, 16 Juli). "FBI: A Chinese Hacker Stole Massive Amounts Of Intel On 32 US Military Projects". http://www.businessinsider.com/chinese- hackers-stole-f-35-data-2014-7/?IR=T diakses 22 Desember 2017.

BBC, (2011, 25 Januari "US Spy for Tiongkok Noshir Gowaida Jailed For 32 Years",http://www.bbc.com/news/world-asia-pacific-12272941 diakses 17 Desember 2017.

Cambia Research.(2016, 22 April). "Surface Web, Deep Web, Dark Web – What's The Difference?". https://www.cambiaresearch.com/articles/85/surface-web-deep-web-dark-web----whats-the-difference diakses 29 Oktober 2017.

CNN Indonesia. (2016, 22 Februari). "Ekspor Senjata Tiongkok Meningkat Dua Kali Lipat" https://www.cnnindonesia.com/internasional/20160222114703- 113-112511/ekspor-senjata-Tiongkok-meningkat-dua-kali-lipat/ diakses 7 Desember 2017.

Cyber Secure Asia, (2015, 2 Desember) Understanding The Difference Between Phishing

And Pharming https://www.cybersecureasia.com/blog/phishing-and-pharming diakses 18 Desember 2017.

Free Beacon. (2016, 24 Maret). "Tiongkok Hacked F-22, F-35Stealth Jet Secret". http://freebeacon.com/national security/Tiongkok- hacked-f22-f35-jet-secrets/ diakses 14 Desember 2017.

Kabar24. (2017, 20 Oktober). "Tiongkok Bangun Kekuatan Militer, Xi Jinping: Kekuatan Dibangun Untuk Melawan". http://kabar24.bisnis.com/read/20171020/19/701409/Tiongkok-bangun- kekuatan-militer-xi-jinping-kekuatan-dibangun-untuk-melawan diakses 15 Desember 2017.

Merdeka. (2013,23 Oktober). "Kasus Estonia dan Georgia Jadi Sejarah Kelam Cyber Crime Dunia https://www.merdeka.com/teknologi/kasus- estonia-dan georgia-jadi-sejarah-kelam-cyber-crime-dunia.html diakses 16 September 2017.

New Media Institute. "History Of the Internet". http://www.newmedia.org/history-of-the-internet.html. di akses 1 November 2017.

Pakar Komunikasi. (2017,17 Mei). 15 pengertian studi kasus menurut para ahli. https://pakarkomunikasi.com/pengertian-studi-kasus-menurut-para-ahli di akses pada 29 Oktober 2017

Sindonews. (2017, 14 Oktober)." Bentuk Satuan Siber, TNI Siap Hadapi Serangan Dunia Maya". https://nasional.sindonews.com/read/1248299/14/bentuk- satuan-siber-tni siapa- hadapi- serangan-di-dunia-maya 1507966324/13diakses 10 September 2017 diakses 10 September 2017.

Sindonews. (2012, 19 Mei). "AS Tuding Tiongkok Agresor Cyber terbesar di Dunia". https://international.sindonews.com/read/632058/9/as-tuding-Tiongkok- agresor-cyber- terbesar-di-dunia-1337425975 diakses 5 Desember 2017.

Service Care Solution. (Juni, 27 2016). " Surface Web vs Deep Web vs Dark Web".www.servicecare.org.uk-61792715468. diakses pada 30 Oktober 2017.

Search Security. (2017, 31 Oktober). "Definition of Phishing". http://searchsecurity.techtarget.com/definition/phishing diakses 18 Desember 2017.

Techopedia. "What Does Cyber Attack Mean". https://www.techopedia.com/definition/24748/cyberattack diakses pada 1 November 2017.

The Global Review.(2013, 29 Januari). "Tiongkok Potensial Sebagai Superpower". http://theglobal-review.com/lama/content_detail.php?lang=id&id=10979&type=4#.WkS55 N-WbIU diakses 4 Desember 2017.

Vice News. (2014, 24 Maret). "Man Who Sold F-35 Secrets To Tiongkok PleadsGuilty". https://news.vice.com/article/man-who-sold-f-35-secrets-to- Tiongkok-pleads-guilty diakses 20 Desember 2017.

VOA Indonesia. (2015, 31 Agustus). "Pemerintah Amerika Serikat Siapkan Sanksi Atas Peretasan Oleh China". https://www.voaindonesia.com/a/as- siapkan-sanksi-peretasan-oleh-china-/2939473.html, diakses 20 Desember 2017.