

## **BAB I**

### **PENDAHULUAN**

#### **A. Alasan Pemilihan Judul**

Dunia cyber merupakan tempat atau server penyimpanan data-data intelijen negara. Negara-negara seperti AS ataupun China memanfaatkan celah atau bug yang ada untuk mencuri data-data penting saingannya. Tak pelak, hal tersebut menjadi pemicu perang cyber. Yang patut disoroti adalah kepentingan kedua negara dalam aksi perang cyber tersebut.

Ada beberapa poin yang menarik untuk dijadikan penelitian, salah satunya adalah kemunculan China sebagai negara super power juga merupakan hal yang menarik dan tidak terduga. Tampilnya China sebagai negara yang kuat membuat AS terpacu untuk semakin meningkatkan kekuatannya dan kewaspadaannya terhadap rivalnya yang baru.

Hal lain yang membuat penulis tertarik untuk mengangkat isu ini adalah kenapa baru di pemerintahan Obama, AS mencoba untuk membuka pintu kerja sama dengan negara lain terkait keamanan Cyber. Padahal isu tentang cyber security ini sudah mulai berkembang pada masa pemerintahan Bush Jr.

Dan lagi, AS malah menggandeng China yang mulai dianggap sebagai rival berat, dalam segala hal termasuk cyber military. Meski, sebelumnya rutin terjadi aksi saling serang diantara keduanya dalam dunia cyber. Juga aksi saling kecam yang berakibat pasang-surutnya hubungan keduanya. Tidak

lupa bahwa kepentingan dua negara yang saling bersaing ini juga bisa dijadikan bahan penelitian.

Pertimbangan lain yang membuat penulis berniat untuk melakukan riset ini adalah karena topik yang berhubungan dengan kerja sama di ranah dunia cyber masih tergolong baru. Jadi penulis beranggapan bahwa masih belum banyak mahasiswa yang meneliti/mengkaji masalah tersebut.

Dan di era yang teknologinya telah maju, seorang individu memiliki hak atau kebebasan untuk dapat mengakses informasi-informasi penting yang dapat membantu dalam penyusunan skripsi ini. Literatur seperti buku-buku, jurnal-jurnal ataupun majalah kini telah banyak tersedia dengan bermacam-macam pembahasan serta mudah untuk didapatkan. Juga pemanfaatan internet untuk mencari data-data penting yang sulit ditemukan di media lain.

Berlandaskan pada konsep kerja sama, tentulah ada kepentingan atau tujuan yang ingin dicapai oleh AS. Atas dasar diatas, penulis memutuskan untuk mengangkat judul "**kepentingan Amerika dalam kerja sama dengan China di bidang keamanan cyber di era Obama**".

## **B. Latar Belakang Masalah**

Beberapa dekade ke belakang, tidak dapat yang menyangkal bahwa AS merupakan negara terkuat di dunia. Perang dingin merupakan bukti Shahih, untuk menggambarkan seberapa besar kekuatan militer antara Uni Soviet dengan AS. Pengembangan gila-gilaan teknologi nuklir membuat negara-negara di dunia merasa khawatir dan terancam keselamatannya. Faktor pendorong terjadinya persaingan senjata nuklir adalah karena senjata

dianggap penting dan pada akhirnya tidak ada yang dapat dicapai dan yang dapat mengakhiri perlombaan hanyalah kehancuran salah satu atau keduanya.<sup>1</sup> Negara-negara lain takut bahwa dampak yang ditimbulkan kelak dari persaingan dua negara adidaya ini akan menjadi pemicu bagi terjadinya perang dunia ke-3. Kekhawatiran ini bisa dibilang wajar, bila melihat rentang waktu antara berakhirnya perang dunia ke-2 dengan periode persaingan Uni Soviet-AS terbilang singkat. Namun, ekspor demokrasi yang dilancarkan AS cukup untuk membuat Mikhail Gorbachev menegaskan bahwa akan terjadi fenomena Glassnot, sebagai pertanda runtuhnya komunis dan datangnya era baru, yaitu demokrasi dalam sistem pemerintahan Russia. Runtuhnya Uni Soviet, hingga penyerbuan kepada negara-negara di timur tengah cukup menjadi bukti superioritas AS. Dalam hal ini, tidak hanya militer saja yang berperan dalam keberhasilan amerika dalam melakukan penyerangan. Justru informasi yang dimiliki AS lah yang menjadi kartu truf keberhasilannya menaklukkan negara- negara timur tengah dan menguasai ladang minyak.

Memasuki milenium baru, peta kekuatan mulai sedikit berubah dengan tampilnya China sebagai kekuatan baru di level Asia dan dunia. Tidak hanya dalam hal ekonomi, China juga berkembang menjadi negara yang adidaya di bidang teknologi dan informatika. Fakta yang mengarah kesana adalah kehadiran perusahaan Lenovo yang menguasai saham IBM, yang merupakan perusahaan asal AS. Perjanjian senilai \$1.25 milyar pada tahun 2004 yang menjadi awal dari jatuhnya IBM, dimana Lenovo membeli saham

---

<sup>1</sup> Dorothy Pickles, *Pengantar Ilmu Politik*, Rineka Cipta, Jakarta, 1991, Hal. 113.

untuk kelas business PC.<sup>2</sup> Dampak yang ditimbulkan dari transaksi jual - beli tersebut adalah semakin hebat pengaruh China di AS dan semakin menguasai perdagangan alat- alat teknologi dalam skala global.

Di era globalisasi sekarang ini, perkembangan teknologi dan informasi tak dapat terelakkan. Malahan muncul tren belakangan ini bahwa perkembangan teknologi dan informasi bergerak sangat cepat. Utamanya adalah perkembangan gadget, yang semakin banyak membanjiri pasaran dunia. Internet pun merupakan media yang kebagian jatah sebagai teknologi yang selalu diperhatikan dan dikembangkan terus menerus, dibuktikan dengan pengembangan 4G atau LTE yang mana merupakan pusat lalu lintas data dalam server. Sekarang ini, internet merupakan media yang sangat penting kehadirannya bagi dunia. Lewat internet, tidak ada lagi tapal batas yang menghalangi seseorang untuk dapat berinteraksi dengan orang lain kapan pun dan dimana pun mereka berada.

Atas perhatian besar yang dicurahkan oleh para pengembang, hari ini internet memiliki berbagai fungsi dan kegunaan yang sangat membantu kehidupan sehari-hari. Apabila di awal tahun 2000 internet hanya dapat dinikmati sebagai media chatting yang sederhana atau browsing dengan kecepatan yang terbilang lambat, sekarang ini hal tersebut sudah dapat dipastikan tidak akan terjadi lagi. Internet yang tersedia saat ini selain sebagai media sosial, menyebarkan wawasan kepada masyarakat berupa pemberitaan via online atau yang kerap disebut e-news. Juga sosial media yang sangat

---

<sup>2</sup> Martyn Williams dan Paul Kallender, "China's Lenovo to buy IBM's PC business", dalam <http://www.infoworld.com/article/2681991/computer-hardware/china-s-lenovo-to-buy-ibm-s-pc-business.html/>, diakses pada tanggal 14 Oktober 2014.

digandrungi anak muda untuk mencurahkan perasaan, Media penyimpanan data-data seperti foto, video yang gratis dan mudah untuk digunakan dan kegunaan lain.

Berkat perkembangan teknologi tersebutlah serangan atau invasi ke negara lain tidak hanya berasal dari sektor militer saja. Teknologi juga bisa menjadi senjata yang sangat ampuh dalam menaklukkan negara lain. Terlebih, dengan perang menggunakan teknologi tidak perlu terjadi pertumpahan darah yang jelas-jelas melanggar HAM. Jalan perang, yang menghalalkan kekerasan telah membuat para peneliti studi tentang perang setuju bahwa kekerasan telah menjadi ciri khas sistem internasional yang kedudukannya terbilang penting.<sup>3</sup> Pertimbangan lain adalah faktor kemudahan dalam menjalankan operasi penyerangan berbasis internet yang bisa dikatakan mudah, cukup dengan memerintahkan tentara yang bekerja dipertahanan militer cyber dan resiko yang terbilang rendah. Resiko disini adalah, ada kemungkinan jika China, sebagai contoh mencuri data milik pemerintahan Indonesia. Pemerintah Indonesia bisa saja tidak menyadari bahwa selama ini China telah melakukan aksi cyber espionage. Tetapi karena perangkat militer cyber China lebih hebat, tetap ada kemungkinan bahwa tindakan China tersebut tidak dapat tercium oleh Indonesia.. Di antara kemudahan dan kelebihan yang didapat dari cyber military, jangan lupakan juga bahwa biaya yang harus ditanggung oleh negara-negara yang mengembangkan militer cyber terbilang besar.

---

<sup>3</sup> Holsti, K.J., *Politik Internasional: Kerangka Untuk Analisa I*, terjemahan M.Tahir Azhary, S.H, Erlangga: Jakarta, 1988, hal.31.

Awal dari kemunculan China sebagai cyber power dimulai pada saat tahun 1994. Pada masa itu, China menginvestasikan sebesar \$ 200 juta untuk mengimport produk-produk seperti CPU, server, database dan lain-lain.<sup>4</sup> Produk-produk teknologi tersebut dibeli dari pengembang yang merupakan pemain utama pasar teknologi yang berasal dari barat seperti Microsoft, Cisco, IBM, Intel dan Apple. Ide mengucurkan dana besar-besaran untuk mengimport produk-produk teknologi tersebut berawal dari kekhawatiran akan rentan dan lemahnya cyber security China. Jika hal ini dibiarkan terus-menerus, China akan rentan terhadap segala aktivitas dalam dunia cyber, seperti tindakan mata-mata dari negara lain, serangan cyber atau bahkan aksi hacking.

Ambisi China untuk menjadi negara super power tidak dapat diremehkan. Pada 20 tahun belakangan China menghabiskan dana sebesar \$100 milyar untuk di investasikan ke sektor militer, dan semakin bertambah besar menjadi \$600 milyar dalam 10 tahun belakangan ini.<sup>5</sup> China sangat getol untuk menjadikan dirinya sebagai role model dalam sektor ekonomi dan militer dunia. Investasi gila-gilaan tersebut dilandasi oleh pemikiran bahwa AS akan terus meningkatkan hegemoninya di dunia melalui jalur militer.<sup>6</sup> Dan hal tersebut dianggap sebagai sebuah tantangan yang serius bagi China.

---

<sup>4</sup> Zhu Ningzhu, "China Voice: Drop Cold War mentality on China's cyber security", dalam [http://news.xinhuanet.com/english/china/2014-04/22/c\\_133280867.html](http://news.xinhuanet.com/english/china/2014-04/22/c_133280867.html), diakses pada tanggal 15 Oktober 2014.

<sup>5</sup> Grant Brunner, "China's growing military might obscures the real threat of cyberwar", dalam <http://www.extremetech.com/extreme/143804-chinas-growing-military-might-obscures-the-real-threat-of-cyberwar>, diakses pada tanggal 21 Oktober 2014.

<sup>6</sup> Nick Hopkins, "US and China engage in cyber war games", dalam <http://www.theguardian.com/technology/2012/apr/16/us-china-cyber-war-games>, Diakses pada tanggal 21 Oktober 2014.

Di pembukaan kongres tahunan partai komunis pada 8 November 2012, Hu Jintao menyatakan China akan mempercepat pengembangan teknologi dan informatika sebagai usaha untuk meningkatkan kekuatan militer China.<sup>7</sup> penggunaan teknologi mesin, manajemen logistik, dan operasi gabungan menjadi sektor yang mendapat perhatian khusus, karena dianggap sebagai kelemahan terbesar China jika dibandingkan dengan AS yang sudah memiliki pondasi kuat di ketiga sektor tersebut.

Pernyataan Hu Jintao didasarkan pada kenyataan bahwa sekarang ini jumlah pengguna internet di China telah menginjak angka yang fantastis, yaitu sebesar 618 juta pengguna internet. Juga karena secara keseluruhan kekuatan militer amerika lebih unggul dari China, juga kekuatan diplomasi AS serta persaingan industri yang kompetitif menjadi alasan yang kuat bagi rencana pengembangan teknologi informasi yang cepat di China. Sudah jelas, bahwa konsentrasi China selama 10 tahun kedepan adalah untuk bersaing dengan AS sebagai negara superpower.<sup>8</sup>

Sedangkan AS, sebagai pemain lama dalam politik internasional tentu sangat memperhatikan militer cyber. Program kurikulum sekolah NSA menjadi bukti shahih bahwa AS memberikan perhatian yang sangat serius kepada militer cyber. Sekolah NSA didirikan pada tahun 1998 dan telah mengintegrasikan kurikulum cyber ke semua universitas di AS, baik

---

<sup>7</sup> Adam Segal, "The 18th Party Congress and Chinese Cyberpower", dalam <http://blogs.cfr.org/asia/2012/11/13/the-18th-party-congress-and-chinese-cyberpower/>, Diakses pada tanggal 22 Oktober 2014.

<sup>8</sup> BBC Monitoring, "China media: Cyber Power", dalam <http://www.bbc.co.uk/news/world-asia-china-26379813>, Diakses pada tanggal 22 Oktober 2014.

Universitas umum atau swasta.<sup>9</sup> Rencana untuk menambahkan 6000 prajurit dan suntikan dana sebesar \$5 milyar untuk meningkatkan unit pentagon cyber warfare merupakan ambisi besar dari secretary of defense Chuck Hagel.<sup>10</sup> Usaha itu terjadi setelah DOD bekerja sama dan mendapat aliran dana dari beberapa perusahaan swasta dan pihak-pihak lain.<sup>11</sup> Rencana tersebut muncul setelah AS sadar bahwa tanpa adanya rencana tambahan dan bantuan dari pihak-pihak lain, tidak mungkin dapat menandingi kekuatan militer cyber China. Semakin lama, AS menganggap China adalah negara yang sangat berbahaya dan semakin meningkatkan kewaspadaannya.

Langkah lain yang diambil oleh AS adalah dengan merekrut anak-anak SMP dan SMA untuk berkecimpung dalam militer cyber.<sup>12</sup> Bahkan The Air Force pun mengadakan kompetisi bernama "cyber patriot", untuk menjaring anak-anak seusia SMA yang memiliki minat dan bakat dalam dunia cyber untuk kemudian dipekerjakan dalam badan keamanan cyber AS.<sup>13</sup> Sejak Januari 2013 Army's Cyber Command sibuk melakukan perubahan kurikulum bagi anak-anak SMP dan SMA yang berpotensi supaya dapat menghadapi serangan cyber atau menghadang serangan cyber.<sup>14</sup> Huntsville City Schools menjadi sekolah digital terbesar di AS yang memiliki

---

<sup>9</sup> Aliya Sternstein, "China Wants To Replicate NSA's Cyber Schools", dalam <http://www.defenseone.com/threats/2014/09/china-wants-replicate-nas-cyber-schools/94475>, diakses pada tanggal 22 Oktober 2014.

<sup>10</sup> David Francis, "U.S. Plays Catch-Up with China on Cyber Warfare", dalam <http://www.thefiscaltimes.com/Articles/2014/05/11/US-Plays-Catch-China-Cyber-Warfare>, diakses pada tanggal 21 Oktober 2014.

<sup>11</sup> Ibid

<sup>12</sup> Corey Mead, "Military Recruiters Have Gone Too Far", dalam <http://ideas.time.com/2013/09/17/military-recruiters-have-gone-too-far>, diakses pada tanggal 22 Oktober 2014.

<sup>13</sup> Ibid.

<sup>14</sup> Ibid.

24 ribu murid yang mana kurikulum dan mentor-mentor dari militer disediakan oleh Army Cyber Command yang bekerja sama dengan West Point.

Isu tentang serangan cyber dianggap sebagai isu yang sangat serius. Bahkan isu ini dianggap lebih berbahaya dari ancaman terorisme.<sup>15</sup> Kekhawatiran ini jelas berdasar, karena AS merupakan negara yang paling banyak mendapat serangan cyber dari penjuru dunia, sama seperti China. Tiga area yang menjadi perhatian utama AS untuk dikembangkan adalah sektor jaringan listrik, institusi finansial, pelayanan pemerintah.<sup>16</sup> Ketiga sektor tersebut masih dilapisi oleh sistem perlindungan yang lemah. Penyerangan terhadap Wall Street kerap terjadi, yang paling menjadi ancaman adalah serangan dari Iran, karena hubungan diantara keduanya tidak harmonis. Serangan yang dilancarkan pada server pemerintahan AS juga sering terjadi, membuat sarana publik tidak dapat dimanfaatkan dan dapat membahayakan masyarakat. Alasan yang cukup logis, mengingat perusahaan air, pemadam kebakaran dan lampu lalu-lintas memanfaatkan internet dalam praktiknya. Sektor jaringan listrik juga cukup rawan. Apabila sampai terjadi serangan, bukan tidak mungkin koneksi internet di AS akan mati total dan tidak dapat terhubung ke internet.

---

<sup>15</sup> Michael Pizzi, "Cyberwarfare greater threat to US than terrorism, say security experts", dalam <http://america.aljazeera.com/articles/2014/1/7/defense-leaders-saycyberwarfaregreatestthreattous.html>, diakses pada tanggal 22 Oktober 2014.

<sup>16</sup> Matt Vasilogambros, "America's 3 Biggest Cybersecurity Vulnerabilities", dalam <http://www.nationaljournal.com/whitehouse/america-s-3-biggest-cybersecurity-vulnerabilities-20130313>, diakses pada tanggal 22 Oktober 2014.

Berbagai macam agenda melatar belakangi penyerangan berbasis teknologi (Cyber attack). Salah satunya adalah untuk mencuri data-data penting negara atau untuk memata- matai aktivitas para elit di sebuah negara. Tindakan semacam itu dikenal sebagai spionase cyber. Spionase cyber seolah menjadi hal yang jamak dilakukan oleh badan intelijen negara untuk mengetahui segala rencana atau kebijakan yang dijalankan di suatu negara. Aksi mata- mata ini juga memicu terjadinya aksi balasan dari negara yang merasa menjadi korban. Tak pelak, jika kemudian terjadi perang Cyber karena benturan kepentingan masing-masing negara.

Akibat yang ditimbulkan dari serangan cyber tidak dapat dipandang sebelah mata, karena dapat membahayakan sektor militer, ekonomi, sosial bahkan politik suatu negara. Karena tindakan mata-mata dengan cara spionase cyber sendiri membuat negara lain bisa memiliki data-data penting suatu negara. Menjadikan negara yang menjadi korban rentan. Selanjutnya data-data yang dicuri tersebut bisa digunakan untuk memonopoli atau melakukan ancaman kepada negara yang bersangkutan supaya dalam perjanjian kerja sama negara yang datanya dicuri dapat tunduk kepada negara yang melakukan pencurian data. Dengan begini, kepentingan nasional negara yang data-datanya dicuri tidak dapat terlaksana. Kepentingan nasional yang merupakan cita-cita tidak dapat terwujud, dan masyarakat dalam negeri hanya dapat menuntut kepada negara, terutama para elit politik yang telah gagal dalam memenuhi kebutuhan dalam negeri.

Beberapa tahun yang lalu, tepatnya pada tahun 2011, Hacker China berusaha untuk mengganggu satelit milik AS.<sup>17</sup> Sebuah tindakan yang tentunya sangat mengancam AS. Serangan-serangan seperti itu sebenarnya merupakan hal yang cukup wajar, mengingat serangan cyber terbanyak berasal dari AS maupun China, dan AS lah yang menjadi negara paling banyak mendapat serangan cyber.<sup>18</sup>

Di tahun 2012 pun, China mencoba untuk melakukan mata-mata dengan cara menembus jaringan keamanan AS, meski gagal.<sup>19</sup> meski begitu usaha yang dilakukan China tidak dapat dipandang sebelah mata. Penyebabnya adalah karena kurangnya ahli dalam serangan cyber. Sejak saat itu, Perkembangan cyber militer China menjadi sangat cepat, karena isu dalam dunia cyber dianggap sebagai isu yang sangat penting dimasa mendatang. Bisa dikatakan,,negara-negara yang rawan terhadap serangan China adalah negara-negara yang mengadakan hubungan kerja sama di bidang politik maupun ekonomi.<sup>20</sup>

Merujuk pada peristiwa diatas, negara-negara lain juga mulai menganggap bahwa isu kriminal cyber merupakan sesuatu yang berbahaya dan mengancam kedaulatan negara. Semula, banyak para pakar atau intelektual

---

<sup>17</sup> Grant Brunner, "The Obama administration takes on Chinese cyberwarfare ", dalam <http://www.extremetech.com/internet/153965-the-obama-administration-takes-on-chinese-cyberwarfare>, diakses pada tanggal 21 Oktober 2014.

<sup>18</sup> Sebastian Anthony, "How to watch hacking, and cyberwarfare between the USA and China, in real time", dalam <http://www.extremetech.com/extreme/185125-how-to-watch-hacking-and-cyberwarfare-between-the-usa-and-china-in-real-time>, diakses pada tanggal 21 Oktober 2014.

<sup>19</sup> Grant Brunner, "US Congress: China's cyberwarfare is becoming a serious problem for the United States", dalam <http://www.extremetech.com/extreme/139722-us-congress-china-cyberwarfare-is-becoming-a-serious-problem-for-the-united-states>, diakses pada tanggal 21 Oktober 2014.

<sup>20</sup> Ibid.

menganggap bahwa kejahatan cyber atau perang cyber hanyalah angan-angan atau imajinasi saja. Negara-negara mulai menyadari bahwa kerja sama di sektor keamanan cyber merupakan suatu hal yang wajib dilakukan.

Ketegangan yang terjadi antara AS dan China tak kunjung usai. Tetapi kedua belah pihak pernah bertemu dalam U.S.-China internet industry forum.<sup>21</sup> Topik utama yang menjadi pembahasan dalam pertemuan ini adalah cyber affairs. Faktor yang membuat hubungan keduanya tidak dapat akur adalah faktor ketidakpercayaan dan komunikasi yang bisa dibilang kurang efektif. Hasil pertemuan yang nihil ini membuat kedua negara setuju untuk melakukan beberapa pertemuan lagi di tahun ini untuk mencapai kesepakatan bersama.

Pada tanggal 13 April 2013, sekretaris negara AS, John Kerry mengumumkan terbentuknya Working group bagi China dan AS yang berfokus pada permasalahan cyber. Lalu pada tanggal 7-8 Juni 2013 terjadi pertemuan empat mata antara Obama dan Xi Jinping di Sunnylands, California. Bagaimana pun juga, kerja sama telah terjalin dan menarik untuk di analisa motif-motif AS di balik hubungan dengan China. Kerja sama ini dapat terjalin karena beberapa waktu yang lalu, pada 2012 China mengatakan siap untuk bekerja sama dengan negara manapun untuk menjaga perdamaian dan keamanan cyber yang berlandaskan hubungan sama-sama untung.<sup>22</sup>

---

<sup>21</sup> Shao Yuqun and Lu Chuanying, "Sino-US cyber controversy", [Http://www.china.org.cn/opinion/2014-04/11/content\\_32064041\\_3.html](http://www.china.org.cn/opinion/2014-04/11/content_32064041_3.html), diakses pada tanggal 22 Oktober 2014.

<sup>22</sup> Grant Brunner, "The Obama administration takes on Chinese cyberwarfare", dalam <http://www.extremetech.com/internet/153965-the-obama-administration-takes-on-chinese-cyberwarfare>, diakses pada tanggal 21 Oktober 2014.

Pertemuan lanjutan pada 8-12 Juli antara terjadi pertemuan S&ED di Washington, AS, membuat kedua negara resmi menjalin kerja sama.<sup>23</sup>

### **C. Rumusan Dasar Masalah**

Berdasarkan latar belakang yang telah tertera sebelumnya mengenai hubungan kerja sama Amerika Serikat dengan China di bidang keamanan cyber, maka permasalahan tersebut dapat dirumuskan sebagai berikut:

**"Apa kepentingan AS dalam kerja sama keamanan cyber dengan China di masa Pemerintahan Obama?"**

### **D. Landasan Teori**

#### **1. Kepentingan Nasional**

Kepentingan nasional menurut Jack C. Plano dan Roy Olton sebagai sebuah panduan dan landasan bagi para pembuat keputusan dalam negeri membuat kebijakan politik luar negeri.<sup>24</sup> Kepentingan nasional secara umum merupakan konsepsi dari elemen-elemen yang mewakili kebutuhan paling penting bagi negara. Dalam pembuatan keputusan, tidak hanya satu agenda saja yang dianggap penting, melainkan terdiri dari beberapa agenda, sehingga disebut sebagai kepentingan-kepentingan nasional.<sup>25</sup>

Sedangkan Hans J. Morgenthau mendefinisikan kepentingan nasional sebagai "usaha untuk menjaga kelangsungan hidup negara-bangsa melalui pemenuhan kepentingan yang vital dengan menggunakan kekuasaan secara

---

<sup>23</sup> Li Zheng, "A Setback in China-US Cyber Cooperation", dalam <http://www.chinausfocus.com/peace-security/a-setback-in-china-us-cyber-cooperation>, diakses pada tanggal 22 Oktober 2014.

<sup>24</sup> Jack C. Plano & Roy Olton, *The International Relations Dictionary*, Western Michigan University, California, 1969, hal. 128.

<sup>25</sup> Ibid.

bijaksana.<sup>26</sup> Morgenthau juga menyatakan bahwa dalam berkecimpung dalam politik internasional, negara memiliki tujuan yang harus terpenuhi, yaitu mencapai kepentingan nasional, bukan kepentingan "sub-nasional" dan juga "supra-nasional".<sup>27</sup>

Dari sini sudah jelas, kepentingan nasional tidak akan dapat terpisahkan dari politik luar negeri. Karena politik luar negeri merupakan cerminan dari kepentingan nasional, juga merupakan sarana untuk mewujudkan cita-cita negara. Sedang politik luar negeri merupakan kebijakan yang diberlakukan kepada negara lain, dengan melihat kondisi dalam negeri dan luar negeri.

Karena sebuah negara di analogikan seperti seorang manusia, maka sifat egois dan anarkhis juga ada dalam diri negara. Sifat egois inilah yang selalu muncul jika dihadapkan pada keadaan berlangsungnya negosiasi dalam hubungan kerja sama antar negara. Maka penggunaan militer sebagai ancaman atau sekedar gertak sambal bukan hal yang asing terjadi. Karena kaum realis sendiri, salah satunya adalah Nicholas N. Spykman dan penganut lainnya sepakat menyatakan bahwa satu-satunya variabel yang dapat menjabarkan perilaku negara dilingkup politik internasional adalah penggunaan power atau kekuasaan.<sup>28</sup> Serangkaian tindakan yang dilakukan

---

<sup>26</sup> Mohtar Mas'oed, *Ilmu Hubungan Internasional: Disiplin Dan Metodologi*, Lp3es, Jakarta, 1990, hal. 18.

<sup>27</sup> Ibid.

<sup>28</sup> Ibid.

sebuah negara adalah berdasar pada kondisi yang ada dalam negeri, seperti kondisi politik, sosial dan juga ekonomi.<sup>29</sup>

Dalam kerangka kerja sama pastilah akan ada benturan pendapat dari masing-masing pihak. Penyebabnya adalah masing-masing pihak ngotot untuk memenuhi kebutuhan negeri melalui kepentingan nasional. Perselisihan tersebut tidak akan memiliki jalan keluar, sehingga nantinya akan dicari jalan tengah guna membuat putusan yang dapat memuaskan masing-masing pihak. Kesepakatan berdasarkan jalan tengah tersebut akan membuat tiap pihak memiliki peran untuk dapat berbuat objektif demi berjalannya hubungan kerja sama. Namun, ada kalanya bahwa kebutuhan akan pemenuhan kepentingan nasional begitu mendesak, sehingga kepentingan nasional suatu negara akan lebih diutamakan dari pada peran nasional.<sup>30</sup>

Bagaimanapun, negara tidak akan mungkin dapat berbuat objektif dalam lingkup kerja sama. Negara tidak akan memperdulikan kelangsungan hidup mitranya, karena pada dasarnya mengorbankan pihak lain demi meraih kekuasaan atau keuntungan merupakan ciri dari politik internasional.<sup>31</sup>

## **2. Politik Luar Negeri**

Setiap negara di dunia pasti memiliki kepentingan masing-masing. Dan salah satu cara untuk memenuhi kepentingan nasional negara tersebut adalah dengan melakukan interaksi atau kerja sama dengan negara lain melalui kebijakan yang tercantum dalam politik luar negeri. Jack C. Plano

---

<sup>29</sup> Jack C. Plano, dkk., Op. Cit., hal.160.

<sup>30</sup> Holsti K.J, Op.Cit, hal. 84.

<sup>31</sup> Holsti K.J, Op.Cit., hal. 209.

dan Roy Olton mendefinisikan politik luar negeri sebagai "strategi ataupun tindakan yang dirancang oleh pembuat keputusan dalam suatu negara guna menghadapi negara lain untuk mencapai serangkaian tujuan yang tercantum dalam kepentingan nasional."<sup>32</sup>

Tokoh lain yang mendefinisikan politik luar negeri adalah Miriam Budiardjo, yang menyatakan, "kebijakan atau policy merupakan sekumpulan keputusan yang diambil untuk memilih tujuan serta cara mencapainya dan dilakukan oleh seseorang atau kelompok."<sup>33</sup>

Mochtar mas'oeed berpendapat bahwa politik luar negeri merupakan tindakan atau kebijaksanaan yang diberlakukan kepada pihak atau keadaan yang berada diluar lingkup wilayah suatu negara dalam kerangka hubungan kerja sama.<sup>34</sup>

Secara umum, tujuan utama negara dalam politik luar negeri menurut Jack C. Plano dan Roy Olton adalah untuk meraih kebutuhan negara di bidang keamanan nasional, ekonomi, harga diri negara, perlindungan dan pengembangan teknologi, penggunaan kekuatan dan pertahanan diri.<sup>35</sup>

Kebijakan luar negeri dihasilkan oleh serangkaian diskusi yang dilakukan oleh elit pemerintah suatu negara. Sering kali sifat negara disamakan dengan sifat dasar manusia, yang mana manusia selalu berusaha sekeras mungkin untuk memperoleh kebutuhannya. Karena itu penting bagi

---

<sup>32</sup> Jack C. Plano & Roy Olton, Op. Cit., hal. 127.

<sup>33</sup> Miriam Budiardjo, *Dasar-Dasar Ilmu Politik*, PT. Gramedia Pustaka, Jakarta, 2008, Hal. 20.

<sup>34</sup> Mochtar Mas'oeed, *Studi Hubungan Internasional : Tingkat Analisis Dan Teorisi*, Pusat Antar Universitas-Studi Sosial Universitas Gajah Mada, Yogyakarta, 1989, hal.87.

<sup>35</sup> Jack C. Plano & Roy Olton, Op.Cit, hal. 128.

suatu negara memiliki seorang warga negara yang paham akan kebutuhan negara dan kondisi politik internasional, sehingga berbagai kebijakan luar negeri yang dirancangnya benar-benar untuk menguntungkan negaranya sendiri.

Dalam hubungan kerja sama, pastilah ada pihak yang lebih kuat atau dominan atas pihak lain. Berbagai faktor yang mendasari hal tersebut adalah karena tangguhnya militer dan atau kemampuan ekonomi yang dimilikinya. Militer maupun ekonomi dapat dipandang sebagai sebuah "power", yang mana power dapat diartikan sebagai kekuasaan juga pengaruh. Dengan tangguhnya kekuatan militer, sudah cukup untuk membuat negara yang lebih lemah militernya untuk takut dan timbul rasa khawatir. Karena "power" sendiri merupakan sebuah keahlian untuk membuat pihak lain atau lawan menuruti permintaan kita dengan cara mempengaruhinya.<sup>36</sup> Sehingga negara yang lemah tersebut bisa diperas kekayaan alamnya atau membuat negara tersebut menjadi takluk pada sistem atau aturan yang sebenarnya hanya menguntungkan pihak yang kuat. Argumen diatas diperkuat dengan pernyataan Morgenthau, bahwa power atau kekuasaan merupakan "kemampuan yang dimiliki seseorang untuk mengendalikan pikiran dan tindakan lain".<sup>37</sup>

Dalam menjalin hubungan dengan negara lain, suatu negara akan dihadapkan pada permasalahan tentang peran nasional. Peran nasional disini maksudnya adalah tindakan yang berupa kewajiban suatu negara atas negara

---

<sup>36</sup> Jack C Plano, Dkk., *Kamus Analisa Politik*, PT. Raja Grafindo Persada, Jakarta, 1982, hal. 185

<sup>37</sup> Mohtar Mas'oeed, *Op.Cit.*, hal. 18.

lain sesuai dengan aturan atau norma yang telah disepakati atau berlaku dalam framework kerja sama. Beberapa hal yang dapat menjadi acuan dalam menjabarkan tentang peran nasional diantaranya, yaitu kondisi eksternal kedua belah pihak, atribut nasional masing-masing pihak dan atribut sikap atau ideologis.<sup>38</sup> Poin pertama yaitu kondisi eksternal. Kondisi eksternal jelas berpengaruh dalam tindakan suatu negara dalam politik internasional. Timbulnya persepsi akan datang ancaman dari pihak lain atau pihak yang menjalin hubungan kemitraan juga dapat mengubah atau menghentikan aktivitas politik luar negeri suatu negara. Faktor perubahan kondisi politik luar negeri juga dapat mempengaruhi. Poin kedua, yaitu atribut nasional suatu negara.

Faktor yang terkait dengan atribut nasional salah satunya adalah kepentingan luar negeri suatu negara, yang didasarkan pada kebutuhan ekonomi terutama, juga keadaan sosial serta politik. Power yang dimiliki suatu negara juga memegang peranan penting dalam berjalannya peran nasional suatu negara. Seperti penjelasan diatas, dimana dengan power yang lebih kuat dari negara lain, suatu negara dapat mendominasi dan mengarahkan ke kebijakan yang dapat menguntungkan negara kuat. Arah pandang suatu bangsa juga turut berpengaruh dalam peran nasional. Indonesia misalnya, yang membenci Israel tidak akan mungkin menjalin hubungan kerja sama dan tidak akan tercipta peran nasional. Poin terakhir, yaitu atribut ideologis atau sikap. Peran nasional juga sangat berhubungan dengan ideologi

---

<sup>38</sup> Holsti K.J, Op.Cit., hal. 83.

suatu negara. Tanpa adanya kesinambungan ideologi, peran nasional tidak akan terbentuk dan terlaksana.

### 3. Aktor Rasional

Untuk memahami perilaku sebuah negara dalam politik internasional, Graham T. Allison mengajukan tiga model pembuatan keputusan. Disini, model yang akan digunakan adalah model teori aktor rasional. Model ini bertujuan untuk menjelaskan proses pembuatan keputusan luar negeri suatu negara.

Teori aktor rasional sendiri dianggap sebagai teori yang paling mampu dan pas untuk menjelaskan tentang aktivitas negara dalam politik luar negeri. "Berotak" dan terkoordinasi, tidak terpecah belah atau monolith itulah gambaran singkat tentang pemerintahan dalam suatu negara.<sup>39</sup> Dengan bersifat rasional dan mengutamakan kepentingan nasional diatas segalanya dalam pembuatan kebijakan. Maka politik luar negeri merupakan hasil tindakan dari aktor-aktor rasional.

Terkoordinasi dan logis merupakan analogi bagi perilaku pemerintah. Menggunakan metode penalaran, individu melakukan tahap-tahap intelektual dan berusaha untuk menetapkan suatu kebijakan dari bermacam-macam pilihan atas alternatif yang memungkinkan untuk mencapai tujuan<sup>40</sup>. Pilihan alternatif itulah yang dianggap sebagai pilihan yang paling ideal atau optimal untuk meraih kepentingan nasional.

---

<sup>39</sup> Mohtar Mas'oe'd, Op.Cit, hal. 235.

<sup>40</sup> Ibid, hal. 234.

Dalam hal ini, tugas seorang pembuat keputusan sangatlah berat. Para pembuat keputusan tidak hanya harus paham betul masalah kebutuhan negara dan mencapainya, tapi juga harus paham akan kondisi politik internasional. Para pembuat keputusan dapat disebut gagal apabila gagal dalam mengutamakan kepentingan nasional dan mewujudkannya karena kepentingan nasional sendiri merupakan cita-cita negara. Pembuat keputusan harus paham betul kepentingan nasional dan tujuannya, lalu kemudian pembuat keputusan juga harus mencari alternatif-alternatif kebijakan yang dapat diterapkan dan melakukan kalkulasi mengenai untung-rugi atas masing-masing alternatif kebijakan yang tersedia.<sup>41</sup>

Politik luar negeri selalu terikat oleh tuntutan domestik. Ada kalanya bahwa kebijakan yang telah dirumuskan dan disepakati oleh pembuat keputusan tidak tepat sasaran atau salah. Kemungkinan-kemungkinan untuk terjadi kesalahan tetap ada, karena pada dasarnya pembuat keputusan adalah manusia biasa. Oleh karena itu biasanya para pembuat keputusan menggunakan metode "optimalisasi hasil", untuk melakukan perubahan atau tindakan penyesuaian terhadap kebijakan yang mereka tetapkan.<sup>42</sup>

Asumsi yang mendasari bahwa negara perlu memenuhi kebutuhan untuk mempertahankan kelangsungan hidup karena negara dianggap sebagai individu yang memiliki sifat manusia. Kebutuhan negara, yang tertuang dalam kepentingan nasional merupakan "given" alias sudah dari sananya. Adanya kebutuhan yang harus terpenuhi merupakan hal yang

---

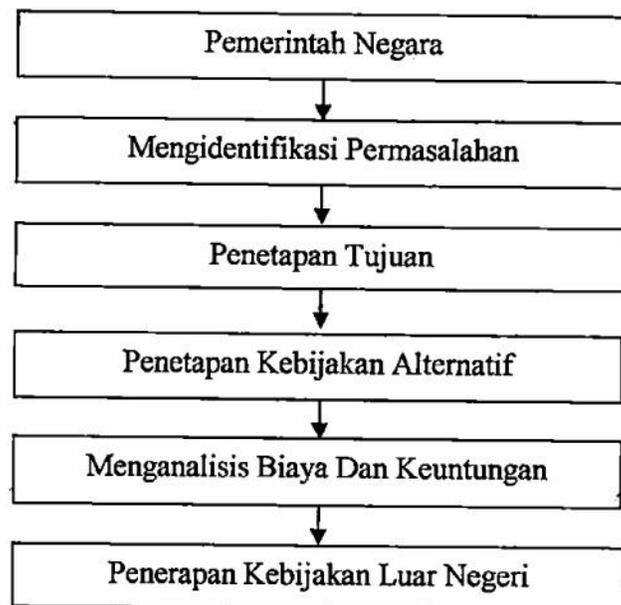
<sup>41</sup> Ibid.

<sup>42</sup> Ibid.

lumrah, sama seperti seseorang yang harus makan untuk bertahan hidup. Kebutuhan negara ada jauh sebelum interaksi antar negara terjadi, seperti di era sekarang. Sedangkan struktur internasional juga merupakan struktur anarkis yang memang sudah sejak awal ada seperti itu.

Berdasar hal tersebut, diberlakukan lah hubungan kerja sama antar negara untuk pemenuhan hasrat akan kebutuhan nasional yang wajib terpenuhi. Kerangka kerja sama terjadi secara langsung diantara dua negara melalui interaksi atau transaksi yang didasarkan atas persamaan permasalahan atau kepentingan yang dapat diselesaikan bersama.<sup>43</sup>

Proses pembuatan keputusan menurut Graham T. Allison, yaitu:<sup>44</sup>



Para pembuat keputusan membuat kebijakan luar negeri nya berdasar kepentingan nasional AS, yaitu pengembangan dan perlindungan teknologi, pengembangan cyber economic, dan pertahanan nasional. Dalam memenuhi

<sup>43</sup> Holsti K.J, Op.Cit, hal. 210.

<sup>44</sup> Mochtar Mas'oeed. Studi *Hubungan Internasional: Tingkat Analisis Dan Teorisasi*, Hal. 90-91.

kepentingannya, AS tidak melihat bahwa dengan terus bersaing dengan China, hal tersebut dapat terpenuhi. Oleh karena itu, muncul alternatif lain dalam upaya pemenuhan kepentingan tersebut. Yaitu dengan menjalin kerja sama dengan China yang merupakan saingan berat AS dalam dunia cyber. Hubungan kerja sama ini dianggap sebagai alternatif yang paling ideal atau optimal dalam mencapai kebutuhan yang paling vital menurut negara AS.

Jadi, berdasar model aktor rasional, tentu AS sudah melakukan hitung untung-rugi bila melakukan hubungan kerja sama dengan China. Jika kerja sama resmi terjalin, maka AS tidak perlu khawatir akan mengalami penyerangan cyber dari China, yang berarti keamanan nasional AS terbilang aman. Juga kerja sama ini menginisiasi pengembangan teknologi bersama-sama diantara kedua negara. Selain itu, cyber economic juga merupakan hal penting yang dapat dikembangkan jika terjadi hubungan diantara keduanya. Jadi menurut pemaparan diatas, AS terbilang untung menjalin hubungan kerja sama dengan China.

Hal sebaliknya dapat terjadi bila hubungan kerja sama antara AS dan China tidak terjalin. Kemungkinan besar kedua nya akan terlibat aksi saling serang dan berujung pada aksi saling curiga dan melemparkan kecaman, yang mana akan semakin menurunkan kepercayaan diantara keduanya. Persaingan keduanya juga pasti akan semakin memanas karena kedua nya merupakan negara super power. Kemajuan teknologi dan dunia cyber juga akan lebih lambat karena hubungan kerja sama tidak pernah terjadi.

### **E. Hipotesa**

Berlandaskan latar belakang yang telah dipaparkan diatas, kepentingan AS dalam hubungan kerja sama dengan China adalah:

1. Menjaga keamanan nasionalnya, cyber economic dan pengembangan dan perlindungan teknologi.
2. Kepentingan AS tetap terjaga jika menjalin kerja sama dengan China setelah melalui pertimbangan untung-rugi.

### **F. Tujuan Penulisan**

Dalam penelitian ini, penulis bertujuan untuk memberikan penjabaran tentang:

1. Untuk mengetahui konflik antara AS dengan China di dunia cyber.
2. Untuk memaparkan kepentingan AS didalam hubungan kerja sama dengan China.

### **G. Batasan Penelitian**

Supaya pembahasan dalam penelitian ini tidak terlalu melebar atau keluar dari topik, penulis mencoba memberikan batasan penyusunan di skripsi ini. Penulis hanya akan membahas hubungan kerja sama antara AS dengan China dibidang cyber security di era Obama. Namun, penulis tetap akan menambahkan data-data dan beberapa kejadian yang masih memiliki sangkut paut dengan dunia cyber atau tindakan yang dilakukan oleh AS atau China sebelum terjadinya perjanjian kerja sama keamanan cyber.

## **H. Teknik Pengumpulan Data**

Dalam melakukan penelitian ini, penulis menggunakan studi penelitian kepustakaan yang memanfaatkan data-data yang bersumber dari buku-buku, jurnal-jurnal, dokume, surat kabar dan juga internet yang memiliki kaitan dengan studi kasus yang dibahas.

## **I. Sistematika Penulisan**

BAB 1 merupakan pembukaan penelitian ini, memaparkan latar belakang penelitian secara mendalam.

BAB II akan membahas tentang definisi, perkembangan, keamanan dan ancaman cyber.

BAB III akan membahas organisasi dan isu cyber di AS dan China serta konflik yang terjadi diantara keduanya dan upaya penyelesaiannya.

BAB IV akan membahas kepentingan AS dalam kerja sama dengan China dibidang cyber security.

BAB V merupakan kesimpulan dari penelitian ini.