PENANGANAN *CYBER ATTACKS* OLEH PEMERINTAH TIONGKOK MELALUI KEBIJAKAN *NETWORK SECURITY* TAHUN 2000-2015

Nadia Talita Putri[1)], Idin Fasisaka[2)], A.A.B. Surya Widya Nugraha[3)]

[1,2,3)] Fakultas Ilmu Sosial dan Ilmu Politik Universitas Udayana

Email: talitaputrinadia@gmail.com[1], idinfasisaka@yahoo.co.id[2],

aabasuwinu@gmail.com[3]

ABSTRACT

The development of Information and Communication Technology provide benefit and threat simultaneously for the countries that using it. China is one of the country that has been using Information and Communication Technology and China also claimed that the country has become world's biggest victim of cyber attacks. Increasingly complexity of the problem in the security area, needed a respon to tackle cyber attacks and the Chinese government has a distinctive way to handle this problem. The research aims to describe the efforts to tackle cyber attacks by the Chinese government through the network security policy. This research using qualitative method and assessed by using concepts of network security and cyber security cooperation. The locus of this research is from 2000 until 2015.

Key Word: China, network security, cyber security cooperation

1. PENDAHULUAN

Globalisasi menghadirkan kemajuan teknologi informasi dan komunikasi (TIK) kearah yang semakin praktis bagi para penggunanya. Kecanggihan dan kemudahan yang ditawarkan ini tidak seutuhnya hanya memberikan sisi positifnya saja, namun juga menciptakan sisi negatif secara bersamaan, terutama dalam bidang keamanan jaringan (*cyber security*). C*yber attacks* dapat mengganggu aktivitas jaringan informasi serta data digital suatu negara yang menggunakannya sebagai alat pengontrol infrastruktur vital, seperti: suplai listrik, komando militer, kontrol radioaktif nuklir, pelepasan limbah beracun industri kimia, pengaturan lalu lintas, pengaturan bursa saham dan berbagai aktivitas lainnya. Tidak hanya itu, IP (*internet protocol address*) suatu negara yang terdeteksi melakukan penyerangan terhadap IP negara lain, walaupun penyerangan dilakukan bukan oleh negara yang bersangkutan, tentu akan mengakibatkan citra buruk dan ketegangan hubungan antara negara yang diserang dengan negara yang menerima tuduhan.

Dunia maya pada era digital ini, telah menjadi domain baru setelah darat, laut, udara dan luar angkasa yang akan diperjuangkan oleh negara-negara yang memanfaatkannya. Menurut Kshetri (2014), hal ini disebabkan dunia maya sebagai domain kelima memiliki hubungan yang kompleks dengan keamanan nasional dan

hubungan internasional. Kshetri juga menambahkan dengan mengambil pemahaman Adam Cobb (1999), bahwa konflik yang terjadi di dunia maya merupakan ancaman yang sangat besar dampaknya dibandingkan pembangunan senjata nuklir pada tahun 1940an. Berdasarkan realita yang ada, *cyber attacks* dapat mengganggu aktivitas jaringan informasi serta data digital suatu negara yang menggunakannya sebagai alat pengontrol infrastruktur vital. Tidak hanya itu, IP (*internet protocol address*) suatu negara yang terdeteksi melakukan penyerangan terhadap IP negara lain, walaupun penyerangan dilakukan bukan oleh negara yang bersangkutan, tentu akan mengakibatkan citra buruk dan ketegangan hubungan antara negara yang diserang dengan negara yang menerima tuduhan.

Telah banyak negara-negara yang merasakan dampak dari *cyber attacks* tersebut*,* salah satunya adalah Tiongkok yang mengaku dirinya sebagai "*the biggest victim*" (Xinhua, 2012). Klaim ini pertama kali dinyatakan oleh Zhou Yonglin selaku Ketua departemen pengoperasian *China National Computer Network Emergency Response Technical Team* (CNCERT/CC) berdasarkan 21.618 laporan yang telah diterima oleh CNCERT/CC. Zhou Yonglin juga menambahkan bahwa permasalahan di Tiongkok lebih serius dibandingkan di Amerika Serikat, Jepang dan Korea Selatan (Jie, 2010). Menteri Keamanan Publik Tiongkok juga mengatakan hal yang serupa, hal ini dikarenakan Lebih dari 80 persen komputer dan *websites* di Tiongkok mengalami *cyber attacks,* bahkan tahun 2011 *e-commerce, microblogging,* jaringan sosial dan *gaming websites* di Tiongkok diretas (Lieberthal & Singer, 2012, hal. 4).

Dunia maya telah dimanfaatkan oleh pemerintah Tiongkok untuk pelayanan kepada masyarakat, pembangunan ekonomi, peningkatan kinerja pemerintah, dan juga merambah ke bidang militer dengan dibentuknya gerakan *Revolution in Millitary Affairs* (RMA) sebagai strategi modernisasi militer nasional Tiongkok (Fritz, 2008). Internet juga dimanfaakan oleh masyarakat Tiongkok untuk *e-commerce* atau transaksi ekonomi secara *online*, *e-banking,* sebagai alat komunikasi, serta untuk mendapatkan informasi pendidikan, berita, hiburan dan informasi lainnya (Lau, 2005). Berdasarkan hasil survei yang dilakukan oleh *Internet World Stats,* jumlah pengguna internet baru di Tiongkok meningkat tiap tahunnya dan Tiongkok tercatat menduduki peringkat pertama pengguna internet aktif terbesar di dunia (Internet World Stats, 2010).

Penyerangan yang terjadi dan semakin melekatnya penggunaan terhadap dunia maya, membuat pemerintah Tiongkok gencar menangani permasalahan *cyber attacks.* Bahkan pengamanan terhadap dunia maya termasuk dalam agenda keamanan nasional Tiongkok yang tertuang pada *National Security Law of the People's Republic of China* artikel 25 mengenai upaya proteksi keamanan *cyber security* dengan menjunjung tinggi *cyberspace sovereignty*, keamanan dan perkembangan *interest* Tiongkok (Xinhua, 2015). Dalam penanganan *cyber attacks* ini, Tiongkok memiliki caranya sendiri yang khas dengan

memegang teguh prinsip Konfusianisme dan menganut sistem politik otokratis, dimana Partai Komunis Tiongkok (PKT) memiliki andil yang besar dalam mengatur pemerintahan. Hal ini diutarakan oleh Joan Liu (2010) dalam artikelnya yang berjudul "*finding Chinese law on internet"*, bahwa karakteristik dan sumber hukum di Tiongkok, termasuk hukum dan kebijakan mengenai *cyberspace,* merupakan kombinasi dari budaya tradisional Tiongkok yang direfleksikan dari ajaran Konfusianisme dan model Soviet yang otokratis. Sehingga tidak dapat dipungkiri, bahwa hal inilah yang mempengaruhi Tiongkok dalam memilih langkah penanganan *cyber attack* yang damai dan memungkinkannya hubungan kerjasama demi mengejar kepentingan nasional, namun tetap adanya kontrol ketat dari pemerintah yang dikenal dengan nama hukum *network security.*

2. TINJAUAN PUSTAKA

Kajian pustaka pertama yang digunakan dalam penelitian ini adalah skripsi karya Puspaningrum (2015) yang berjudul "Upaya Pemerintah Shinzo Abe dalam Meningkatkan Keamanan Nasional Jepang dari Ancaman Kejahatan Dunia Maya". Karya Puspaningrum ini membantu dalam memahami upaya yang dilakukan negara untuk menjamin keamanan *cyber* nasionalnya. Dalam menjamin keamanan *cyber* nasional, haruslah dilakukan upaya secara domestik dan internasional. Terkait dengan upaya secara internasional, menurutnya negara-negara akan cenderung melakukan kerjasama internasional dalam sebuah permasalahan karena memiliki kepentingan yang sama. Sama halnya dengan Jepang, Tiongkok juga melakukan upaya secara domestik dan internasional baik kerjasama bilateral maupun multilateral terkait keamanan jaringan. Namun dalam penanganan *cyber attacks* ini, PKT dan prinsip Konfusian memiliki andil yang sangat besar, sehingga upaya yang dilakukan oleh Tiongkok memiliki warna yang berbeda. Penelitian ini juga menggunakan konsep kerjasama namun lebih khusus dengan menggunakan konsep *cyber security cooperation.*

Karya kedua yang digunakan adalah *report* Amy Chang (2014) yang berjudul "*Warring State: China's Cybersecurity Strategy".* Penelitian Chang ini membantu dalam memahami konsep *network security* yang akan digunakan dalam menganalisa penelitian yang akan dikaji. Selain itu, penelitiannya juga memberikan pemahaman secara jelas mengenai karakteristik Tiongkok dalam menentukan kebijakan dan pola kerjasama yang dilakukan dengan negara kompetitornya. Perbedaannya, Chang hanya membahas mengenai motivasi dan pandangan Tiongkok terhadap aktivitas *cyberspace* yang dilakukan oleh Amerika Serikat, sedangkan penelitian ini akan membahas lebih detail cara kerja *network security* yang digunakan oleh Tiongkok untuk menjaga *cyberspace* dari *cyber attacks*.

Kerangka pemikiran dalam penelitian ini menggunakan konsep *network security* yakni *cyber law* milik Tiongkok yang sekaligus menerangkan strategi keamanan nasional ala Tiongkok dalam bidang

keamanan jaringan, dan konsep *cyber security cooperation* dalam menjelaskan mekanisme serta hal-hal lainnya yang berhubungan dengan penanganan *cyber attack* melaui kerjasama bilateral maupun multilateral.

3. METODOLOGI PENELITIAN

Penelitian ini merupakan penelitian kualitatif dengan menggunakan analisa deskriptif. Menurut Satori dan Komariah (2013), penelitian kualitatif merupakan pendekatan penelitian yang mendeskripsikan realita yang ada dengan sebenar-benarnya, disusun dengan kata-kata berdasarkan teknik pengumpulan dan analisis data yang saling berhubungan dari situasi yang alamiah. Oleh sebab itu, penelitian ini akan mendeskripsikan mengenai penanganan *cyber attacks* oleh pemerintah Tiongkok melalui kebijakan *network security* tahun 2000-2015.

4. HASIL DAN PEMBAHASAN

1. Upaya pemerintah Tiongkok dalam memproteksi jaringan informasi serta data digitalnya dari *cyber attacks* secara domestik

Berdasarkan hukum *network security,* upaya penanganan *cyber attacks* yang dilakukan secara domestik oleh pemerintah Tiongkok adalah dengan mengambil langkah-langkah strategis, seperti: mengatur tindakan yang diperbolehkan untuk dilakukan agar dapat menjaga stabilitas keamanan yang dikenal dengan isolasi jaringan dan kontrol akses, membentuk lembaga khusus yang menangani permasalahan *cyberspace*, dan memberikan sanksi bagi para pelanggar aturan hukum *network security* baik yang dilakukan oleh masyarakat sipil ataupun departemen atau pegawai yang bertugas untuk menjaga keamanan *cyber.*

A. Isolasi Jaringan dan Kontrol Akses

Tiongkok telah melakukan kebijakan isolasi jaringan dan kontrol akses sejak tahun 2000 yang dikenal dengan nama *the Great firewall of China* atau kebijakan *Internet Censorship* untuk meningkatkan keamanan *cyber* (Zhen, 2015, hal. 1). Kebijakan ini merupakan bagian dari *The Golden Shield Project* yang bertujuan untuk menjaga keamanan nasional karena adanya kekhawatiran reformasi ekonomi Tiongkok yang dilakukan pada masa pemerintahan Deng Xiao Ping. Inti dari kebijakan *Internet Censorship* ini adalah seluruh masyarakat Tiongkok diberikan kebebasan untuk mengakses dan mengembangkan *web page* miliknya sendiri, namun tetap adanya kontrol pada beberapa laman situs dan kata kunci yang dianggap ‘berbahaya’ bagi pemerintah Tiongkok. Inilah perbedaan Tiongkok dengan negara lain, selain konteks yang berhubungan dengan pornografi, terorisme dan kekerasan, pemerintah Tiongkok juga melakukan isolasi terhadap konten kritik terhadap otoritas dan legitimasi PKT, serta isu sosial yang dapat mengganggu stabilitas sosial demi persatuan dan kesatuan negara.

Pemerintah Tiongkok juga membuat *The Great Cannon* sebagai Alat yang memiliki kemampuan untuk melakukan sensor dan pengawasan secara berasamaan. Perangkat dasar dari alat ini

memungkinkan pemerintah mengatur lalu lintas dunia maya, baik yang berasal dari *server* asing menuju situs yang berada di dalam Tiongkok, maupun sebaliknya.

Selain itu, pemerintah Tiongkok juga memilih untuk menggunakan hasil karya anak bangsa, dibandingkan menggunakan aplikasi produk dari luar negeri. Penggunaan aplikasi yang dibuat didalam negeri ini selain dikarenakan mempermudah pengguna internet dengan penggunaan bahasa mandarin, hal ini juga guna memproteksi gelombang virus, konten-konten berbahaya dan penyalahgunaan dari pihak luar. Tiongkok menyediakan seluruh fasilitas yang dibutuhkan oleh pengguna, seperti misalnya Google digantikan dengan Baidu untuk mesin pencari, Facebook digantikan dengan Renren, dan masih banyak lagi fasilitas media sosial lainnya yang dibentuk oleh Tiongkok (Yusrizal, 2014).

B. Lembaga Khusus yang Menangani Permasalahan *Cyberspace*

Departemen yang memiliki tanggung jawab untuk membuat rancangan, koordinasi, memproteksi, mengawasi dan mengatur keamanan *cyber security* di Tiongkok adalah Kementerian yang berada di dalam naungan *the State Council* seperti Kementerian Pendidikan, Kementerian Industri dan Teknologi Informasi, dan Kementerian Keamanan Publik. Berikut lembaga khusus yang dibentuk oleh masing-masing Kementrian:

(1) Kementerian Pendidikan membentuk CCERT CERNET *Computer Network Emergency Response Team*. Pelayanan CCERT ini hanya diperuntukan untuk para member CERNET atau pengguna .edu.cn yang terdaftar di kampus-kampus di Tiongkok saja. CCERT memiliki tugas untuk membuat penelitian mengenai *network security,* memberikan pelayanan respon cepat terhadap insiden yang terjadi, memberikan informasi penanganan serta bantuan secara teknis, memberikan pelayanan bantuan keputusan, dan memelihara pertukaran informasi dan kerjasama dengan CSIRT jaringan kampus di seluruh wilayah atau provinsi di Tiongkok (Zhu, Susan, & Li, 2001).

(2) Kementerian Industri dan Teknologi Informasi membentuk CNCERT/CC (*China National Computer Network Emergency Response Technical Team/ Coordination Center*) yang memiliki fungsi sebagai lembaga *monitoring, early warnings,* dan *emergency responses* di Tiongkok berskala nasional. Pelayanan CNCERT/CC diperuntukan untuk siapa saja yang merasa perlu menggunakan jasa pelayanan keamanan jaringan. CNCERT/CC juga melakukan kolaborasi dan kerjasama dengan CERT (*Computer Network Emergency Response*) negara lain untuk meningkatkan kinerja dan menghasilkan respon cepat terhadap penanganan permasalahan *cyber.* Selain itu, CNCERT/CC juga menjadi representatif Tiongkok dalam menghadiri berbagai pertemuan internasional dan mengikuti berbagai organisasi internasional dan kawasan terkait CERT seperti FIRST (*Forum of Incident Response and Security Teams*), serta,

(3) Kementerian Keamanan Publik mendirikan polisi internet yang bertugas untuk mengawasi dan mengadministrasi kinerja dalam memproteksi TIK yang berada di teritorial Tiongkok. Pasukan polisi internet ini hanya bertugas untuk menginvestigasi penyalahgunaan dan kejahatan TIK, penangkapan para pelaku kejahatan tersebut akan dilakukan oleh kepolisian dari divisi lain. Kepolisian internet ini tidak hanya berkerja sendiri, namun dibantu oleh masyarakat sipil yang memiliki kesadaran untuk melaporkan tindak kejahatan di Tiongkok.

Pemerintah Tiongkok juga memberlakukan pemberian sanksi untuk menimbulkan efek jera kepada para pelanggar aturan dunia maya dan bagi para *network operators* yang tidak menjalankan tugas dengan baik yang dapat mengakibatkan timbulnya ancaman keamanan *cyber* milik Tiongkok. Pemerintah Tiongkok menerbitkan aturan secara legal mengenai pemberian sanksi tersebut dalam hukum *network security* yang tercantum pada Bab 6 mengenai *legal responsibility.* Dalam hukum *network security,* sanksi dan denda yang diberikan hampir kebanyakan diberikan kepada para *network operator* yang tidak menjalankan tugas perlindungan terhadap keamanan jaringan dengan semestinya, dibandingkan bagi para pelaku kejahatan dalam domain *cyberspace.*

2. Upaya pemerintah Tiongkok dalam memproteksi jaringan informasi serta data digitalnya dari *cyber attacks* secara internasional

Penanganan *cyber attacks* yang dilakukan oleh pemerinttah Tiongkok secara internasional adalah dengan cara menjalin hubungan kerjasama dengan berbagai negara, baik secara bilateral maupun multilateral yang berada dibawah naungan institusi internasional yang berkaitan dengan keamanan *cyber*. Berdasarkan konsep *cyber security cooperation*, cara kerja kerjasama keamanan *cyber* ini diawali dengan mengidentifikasi tujuan yang ingin dicapai negara untuk menjadi acuan untuk membuat aturan legal, kemudian melakukan *sharing information* untuk menambah wawasan*,* dan *capacity building* dengan cara latihan bersama serta kegiatan lainnya untuk meningkatkan *skill.*

A. Hubungan Bilateral Tiongkok-Rusia

kedua negara menandatangani pakta kerjasama *cyber security* yang memiliki dua kunci utama yakni *mutual assurance on non-aggression in cyberspace* dan *language advocating internet sovereignty*. Kunci *mutual assurance on non-aggression in cyberspace* ini membahas mengenai *sharing information*, peningkatan kerjasama ilmiah dan akademik (*capacity building*), serta tidak saling melakukan spionase. Menurut Wei (2016) kesepakatan *non-aggression* bukanlah inti kerjasama kedua negara, sebenarnya fokus utama dari kerjasama kedua negara adalah konsep *internet sovereignty* itu sendiri. Dukungan mengenai konsep *internet sovereignty* ini merupakan upaya kedua negara untuk menyeimbangi dominasi tatanan dunia Amerika Serikat terkait *internet freedom*

yang diterima sebagai norma universal oleh PBB. Pasalnya, Amerika Serikat merupakan negara yang memotori manuver penyingkiran Tiongkok dan Rusia dari forum-forum kerjasama Informasi Internasional.

B. Hubungan Bilateral Tiongkok-Amerika Serikat

Hubungan kerjasama terkait keamanan *cyber* kedua negara ini, diawali oleh terdeteksinya aktivitas *malicious* (program penginfeksi komputer) kedua negara pada domain *cyberspace* pada tahun 2007-2008. Pada tahun 2009, Tiongkok mengirimkan laporan kepada FBI mengenai 13 kasus *website* bank palsu dan pornografi anak untuk diinvestigasi, namun Tiongkok tidak menerima balasan apapun dari FBI. Keyakinan bahwa akan sulitnya mencapai kesepakatan bersama, maka kedua negara mengunakan *track* ke-2 dalam *multi-track* diplomasi untuk menjalin hubungan kerjasama. Pada 17 Desember 2009, Tiongkok dan Amerika Serikat mengadakan pertemuan secara formal yang bertema "*Track 2 Sino-U.S. Cybersecurity Dialogue*". Pertemuan ini dihadiri oleh kalangan cendekiawan dari lembaga CSIS (*Center of Strategic and International Studies*) yang berasal dari Amerika dan CICIR (*China Institutes of Contemporary International Relations*) yang berasal dari Tiongkok di bawah naungan Keamanan Tiongkok yang diawasi langsung oleh PKT. Pejabat yang bertanggung jawab dalam keamanan *cyber* juga turut hadir dan terlibat langsung dalam pertemuan tersebut (Ardiansyah, 2016). Kerjasama ini bertujuan saling *sharing information* untuk mengurangi kesalahpahaman, meningkatkan transparansi pemerintah kedua negara, memahami pendekatan *cyber security* kedua negara, membangun kepercayaan dan kesepakatan mengenai norma serta aturan terkait *cyber security* (CSIS, 2009).

Melihat semakin kompleksnya permasalahan yang terjadi di kedua negara dan semakin masifnya serangan yang berasal dari kedua belah pihak, pada akhirnya kedua Kepala Negara memutuskan untuk duduk bersama membahas permasalahan *cyber*. Dialog mengenai isu *cyber* ini dihadiri oleh Presiden Barak Obama dengan Presiden Hu Jintao pada tahun 2011 (Chang A. , How the 'internet with chinese characteristic' is rupturing the web, 2014, hal. 28). Pertemuan yang dilakukan tersebut membahas mengenai *code of conduct* yang berhubungan dengan penggunaan *cyberspace* dan saling bertukar informasi.

Walaupun telah mengadakan pertemuan dan diskusi, hal ini tidak

menghasilkan titik temu dan kerjasama yang signifikan. Amerika Serikat memiliki pemahaman yang berbeda dengan Tiongkok terkait istilah bahkan kebijakan mereka masing-masing yang saling berbeda arah, Amerika menganut *internet freedom* sedangkan Tiongkok menerapkan *internet sovereignty*. Hal ini dikarenakan Tiongkok dan Amerika Serikat memiliki ideologi dan institusional yang berbeda yang mengakibatkan berbedanya pemahaman konsep dasar mengenai *network security.* Perbedaan inilah yang kemudian membuat komunikasi antara dua negara lemah, sehingga mekanisme dialog yang dilakukan sulit untuk membangun *mutual trust* dalam bidang *network security* (Yuxiao & Lu, 2015, hal. 239-240).

C. *Shanghai Cooperation Organization* (SCO)

Kerjasama *cyber security* mulai dilakukan oleh negara-negara anggota SCO pada tahun 2008. Kerjasaman ini ditandai dengan adanya *agreement International Information Security* yang menekankan bahwa seharusnya tidak boleh pada *digital gap* antara negara-negara maju dan berkembang. Negara maju seharusnya tidak memonopoli pasar dan memaksa negara berkembang untuk mengimplementasi apa yang dianggap negara maju benar. Negara anggota SCO mempercayai bahwa *code of conduct* Konvensi Internasional mengenai *International Information Security* kurang memadai dalam menjebatani komunikasi antara negara-negara yang berbeda, oleh sebab itu SCO menghilangkan keseluruhan spektrum dari penyalah gunaan keamanan *cyber* yang akan memicu eskalasi menuju *cyber-conflict* (Kizekova, 2012).

Pada tahun 2010, negara-negara anggota SCO mulai membahas permasalahan *cyber* secara lebih serius dengan merancang *draft* alternatif Budapest *treaty* yang bertujuan menciptakan perdamaian, pembangunan, keamanan dan kemakmuran dalam domain *cyberspace* (Ministry of Foreign Affairs of the People's Republic of China, 2010). Pada tahun 2011, negara-negara anggota SCO mengusulkan *draft Code of Conduct for Information Security* kepada Majelis Umum PBB karena menganggap bahwa Budapest *treaty* telah melanggar norma hukum internasional dan kedaulatan negara-negara. *Draft* tersebut membahas mengenai rancangan kode etik internasional mengenai keamanan *cyber* yang meliputgi larangan kegiatan bermusuhan atau tindakan agresi, tindakan yang dapat menimbulkan ancaman perdamaian serta keamanan (General Assembly of United Nations, 2011). Anggota SCO bersama Afghanistan, India Iran, Mongolia, dan Pakistan selaku observer serta Belarus, Sri Lanka dan Turki selaku rekan dialog dalam pertemuan *Regional Counter-Terrorism Structure* (RCTS), secara bersama-sama berjuang memberantas terorisme, separatisme dan ekstrimisme yang menggunakan kecanggihan TIK untuk menyebar luaskan propaganda, perekrutan dan hal-hal lainnya yang dapat mengancam. Negara-negara dalam pertemuan RCTS juga melakukan *sharing information* terkait rekomendasi

hukum legal dan standar kerjasama (CCDCOE, 2013).

D. *International Telecommunication Union* (ITU)

Peran ITU untuk menjamin keamanan dan membangun kepercayaan dalam penggunaan TIK adalah dengan cara membentuk *World Summit on the Information Society* (WSIS) sebagai mandat PBB untuk mewujudkan masyarakat informasi di dunia secara merata dan komprehensif (Broto, 2005). WSIS I diselenggarakan pada 12 Desember 2003 di Geneva yang dihadiri oleh Kepala Negara dan menteri yang berhubungan dengan TIK, penyelenggara telekomunikasi, kalangan LSM, dan pebisnis. Pada WSIS I menghasilkan sebuah dokumen yang bernama *Declaration of Principles* dan *Plan of Action* yang berisikan deklarasi yang mencerminkan cita-cita dan komitmen pemerintah dalam pembangunan masyarakat informasi secara holistik, serta rancangan visi dan prinsip umum yang diharapkan dapat mewujudkan pencapaian dan pengembangan TIK tanpa adanya kesenjangan digital. WSIS II dilaksanakan pada 17 November 2005 di Tunisia yang menghasilkan *Tunis Commitment* dan *Tunis Agenda for Actions* yang membahas mengenai payung politik para Kepala Negara untuk mewujudkan masyarakat informasi dan rancangan bentuk operasional untuk mewujudkannya yang meliputi *financial mechanism, internet governance and implementation*, dan *follow-up*.

Keanggotaan Tiongkok pada organisasi ini, sudah dilakukan jauh sebelum Tiongkok resmi menjadi Negara Republik Rakyat Tiongkok, yakni pada tahun 1920. Pemerinah Tiongkok secara aktif telah terlibat dalam WSIS sejak awal pembentukannya, hanya saja banyak pihak yang menyayangkan atas sikap Tiongkok mengenai *internet sovereignty* yang dianggap telah melanggar HAM karena intervensinya terhadap kebebasan yang tidak sesuai dengan pemahaman negara-neagara Barat. Tiongkok juga dianggap gagal dalam mendukung hubungan multilateral yang demokratis dan transparan (Kaspar, 2015, hal. 19).

E. *International Police* (Interpol)

Interpol mulai gencar menangani permasalah *cyber* sejak 2005. Namun tahun 2013 merupakan tahun terbentuknya divisi khusus yang menangani permasalah *cyber* yang dikenal dengan *Interpol Global Complex for Innovation* (IGCI) yang berada di Singapura dan mulai beroperai pada tahun 2014. Divisi ini memiliki laboratorium khusus yang memfasilitasi riset dan pengembangan (*research and development*) bagi Interpol.

Tiongkok mulai ikut serta dalam memberantas *cyber attacks* bersama Interpol pada tahun 2007, jauh sebelum IGCI dibentuk. Hal ini bertujuan agar Tiongkok yang direalisasikan oleh kepolisian, dapat menindak kejahatan yang telah melewati otoritas negara melalui otoritas Interpol yang memiliki legitimasi untuk menangkap para pelaku kejahatan diluar batas negara Tiongkok. Selain itu,

Interpol juga secara rutin melakukan latihan bersama untuk melakukan pengujian dan penelitian terkait penanganan permasalahan *cyber attacks* sehingga diharapkan akan meningkatkan wawasan para anggota Interpol (Guneev, 2013).

5. KESIMPULAN

Pemerintah Tiongkok dalam menangani permasalahan *cyber attacks* untuk memproteksi jaringan informasi serta data digitalnya, tidak lepas dari kontrol PKT dan prinsip Konfusian yang harmoni. Hukum *network security* juga diwarnai dengan pengaplikasian kedua sumber tersebut sehingga menciptakan aturan yang khas ala Tiongkok. Secara domestik pemerintah Tiongkok mengatur tindakan yang diperbolehkan untuk dilakukan yang dikenal dengan isolasi jaringan dan kontrol akses, membuat lembaga khusus yang menangani permasalahan *cyber,* yakni: (1) CCERT sebagai lembaga CERT nasional di bidang pendidikan, (2) CNCERT/CC sebagai lembaga *monitoring, early warnings,* dan *emergency responses* nasional, dan (3) polisi internet yang bertugas untuk menginvestigasi penyalahgunaan dan kejahatan TIK, namun penangkapan para pelaku kejahatan dilakukan oleh kepolisian dari divisi lain. Pemerintah Tiongkok juga memberikan sanksi bagi para pelanggar aturan hukum *network security* baik yang dilakukan oleh masyarakat sipil ataupun departemen maupun pegawai yang bertugas untuk menjaga keamanan *cyber.*

Sedangkan secara internasional, pemerintah Tiongkok melakukan kerjasama dengan pihak lain berdasarkan hukum *network security* yang menerapkan tiga cara (*ways*) terbaik, yakni: (1) membuat aturan legal (*legal measure*) untuk mengatur *cyberspace* dengan memformulasikan standar, (2) melakukan s*haring information*, dan (3) melakukan *capacity building* dengan cara meningkatkan *skill* dan latihan bersama melalui *research and development of network technologies*. Kerjasama yang dilakukan oleh pemerintah Tiongkok baik secara bilateral maupun multilateral selalu menjunjung tinggi nilai *internet sovereignty.*

6. DAFTAR PUSTAKA

Ardiansyah, M. D. (2016). *Upaya Center of Strategic and International Studies (CSIS) salam membangun kerjsama cybersecurity antara Amerika Serikat dan Cina Periode 2010-2013.* Jakarta: UIN Syarif Hidayatullah.

Broto, G. S. (2005, 14 November). *Partisipasi delegasi Indonesia dalam rangka menghadiri WSIS (World Summit on the Information Society) 2005 di Tunisia-Tunisia*. Dipetik Mei 7, 2016, dari Direktorat Jenderal Sumber Daya ddan Perangkat Pos dan Informatika: www.sdppi.kominfo.go.id/berita-partisipasi-delegasi-indonesia-dalam-rangka-menghdiri-wsis-world-summit-on-26-1313

Cai, C. (2015). Cybersecurity in Chinese context: changing concept, vital interest and cooperative willingness. *international dimentions of national (in)security concept, challanges and ways forward* (hal. 2-25). Berlin: Fudan University.

CCDCOE. (2013, April 2). *SCO Fighting Cyber Terrorism*. Dipetik Juni 3, 2016, dari CCDCOE NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia:

https://ccdcoe.org/sco-fighting-cyber-terrorism.html

Chang, A. (2014, Desember 15). *How the 'internet with chinese characteristic' is rupturing the web.* Dipetik Februari 19, 2016, dari huffpost: www.huffpost.com/us/entry/china-internet-sovereignty_b_6325192

Chang, A. (2014). *Warring state: China's cybersecurity strategy.* US: Research Associate at the Center for a New American Security.

Fritz, J. (2008). How China will use cyber warfare to leapfrog in military competitiveness. *Culture Mandala, Vol.8, No.1* , 28-80.

General Assembly of United Nations. (2011, September 14). Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. *Developments in the field of information and telecommunications in the context of international security* , hal. 1-5.

Guneev, S. (2013, Maret 22). *Net is closing in on cybercriminals-Kaspersky Lab stands by INTERPOL*. Dipetik Oktober 5, 2016, dari RT News: www.rt.com/news/kaspersky-interpol-singapore-igci-666/

Huikang, H. (2012, Oktober 9). *Statement at Budapest Conference on Cyber Issues.* Dipetik September 23, 2016, dari Permanent Mission of The People's Republic of China to The United Nations and other International Organizations in Vienna: http://www.chinesemission-vienna.at/eng/zgbd/t977627.htm

Internet World Stats. (2010). *China Internet, Telecommunications and Market Report.* Dipetik Juni 1, 2015, dari Internet World Stats: http://www.internetworldstats.com/asia/cn.htm

Jie, Y. (2010, Januari 25). *China 'biggest victim' of cyber attacks*. Dipetik Januari 2, 2016, dari china daily: www.chinadaily.com.cn/china/2010-01/25/content_9368402

Kaja, A., & Luo, Y. (2015, Agustus 10). *China issues draft network security law.* Dipetik Desember 5, 2015, dari Global Policy Watch: www.globalpolicywatch.com/2015/08/china-issues-draft-network-security-law

Kaspar, L. (2015). *The road to WSIS+10: Key country perspective in the ten-years review of the World Summit on the Information Society.* Londoon: Global Partners Digital.

Kizekova, A. (2012). *The Shanghai Cooperation Organisation: challenges in cyberspace.* Singapore: Rajaratnam School of International Studies.

Kshetri, N. (2014). Cybersecurity and International Relations: the U.S.engagement with China and Rusia.

Lieberthal, K., & Singer, P. W. (2012). *Cybersecurity and U.S.-China Relations.* Brookings: The John L. Thornton China Center and the 21st.

Liu, J. (2010, Mei 31). *China's leader in online legal research*. Dipetik November 1, 2016, dari Finding Chinese law on internet: www.lawinfochina.com/Articel/Artikel2.shtm

Ministry of Foreign Affairs of the People's Republic of China. (2010, Juni 11). *Declaration of the 10th Meeting of The Council of Heads of State of the SCO Member States*. Dipetik September 23, 2016, dari Ministry of Foreign Affairs of the People's Republic of China: www.fmprc.gov.cn/mfa_eng/zxxx_662805/t711709.shtml

Permanent Mission of the people's Republic of China to the United Nations Office at Geneva and other international organizations in Switzerland. (2004, April 19). *China's relationship with the International Telecommunication Union (ITU).* Dipetik September 2, 2016, dari Permanent Mission of the people's Republic of China to the United Nations Office at Geneva and other international organizations in Switzerland: www.china-un.ch/eng/zmjg/jgjblc/t85564.htm

Satori, D., & Komariah, A. (2013). *Metodologi Penelitian Kualitatif.* Bandung: Alfabeta.

Wamala, F. (2011). *ITU national cybersecurity strategy guide.* Geneva: ITU.

Wei, Y. (2016, Juni 21). *China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty*. Dipetik Juli 23, 2016, dari The Henry M. Jackson School of International Studies, University of Washington: https://jsis.washington.edu/news/china-

russia-cybersecurity-cooperation-working-towards-cyber-sovereignty/

Xinhua. (2012, Juli 5). *China world's biggest cyber attacks victim, says report*. Dipetik Januari 3, 2016, dari Global Times: www.globaltimes.cn/content/719138

Xinhua. (2015, Juli 1). *National security law People's Republic of China released the full text of a total of 7 84*. Dipetik November 21, 2016, dari China daily: www.chinadaily.com.cn/hqcj/zzgjj/2015-07-01/content_1391

Xudong, W. (2003, Desember 10). *Strengthening cooperation, promotion development and moving towards the information society together: statement by H.E. Mr. Wang Xudong Minister of Information Industry Peoples Republic of China at the World Summit on the Information Society*. Dipetik Juni 27, 2016, dari www.itu.int/net/wsis/geneva/coverage/statements/china/cn.html

Yusrizal, M. (2014). Dampak implementasi kebijakan the great firewall oleh pemerintah China terhadap aktivitas google inc di China. *Jom FISIP Volume 1 No. 2* , 1-14.

Yuxiao, L., & Lu, X. (2015). China's cybersecurity situation and the potential for international cooperation. Dalam J. R. Lindsay, T. M. Cheung, & D. S. Reveron., *China and cybersecurity : espionage, strategy, and politics in the digital domain* (hal. 225-241). USA: Oxford University Press.

Zhen, S. K. (2015). An explanation of self-censorship in China: the enforcement of social control through a panoptic infrastructure. *Inquiries Journal/ Student Pulse 7(9)* , 1-5.

Zhu, S., Susan, & Li, X. (2001). *Computer security incident response in China.* Tsinghua: CERNET Center, Tsinghua University Network Abuse BoF.