Transformasi No. 28 Tahun 2015
Volume I. Halaman 1 - 88

UPAYA AMERIKA SERIKAT DALAM MENJAGA KEAMANAN NASIONAL DARI *CYBER WAR* TAHUN 2009-2013

Oleh
Achmad Sholeh Abubakar[1], Halifa Haqqi[2], Setyasih Harini[3]

Abstract

The evolution of Information Technology of the 21st century growing increasingly. Cyberspace has become into a new arena in the dynamics of International relations. The United States notice a "Wake-up Call" when The hacking of military base in the Middle East in 2008 and NASA's Jet Propulsion Laboratory in China's Internet Protocol address in 2012. This research focuses about the effort of The United State's National Security of Cyber War in 2009-2013 by President Obama. This efforts it's to response cyber attack conducted by the State or cyber terrorism.

This research's objective was to understand cyber security of the United State by President Obama in 2009 to 2013 against the threats of cyber war to protect the national interest in this case about the power of cyber security. The concept of national security and cyber security were used for further discussion. This descriptive analytical research used secondary data sources while its data collecting technique was library research. Data analysis technique included data reduction, data display, conclusions and verification. The results of this research indicate that the efforts made by President Obama in The United States cyber security in political and economic sector by increasing military resistance and technology, cyber diplomacy and keeping The Critical Infrastructure.

***Keywords** : cyber security, cyber war, national security, The United States*

Pendahuluan

Proses penyebaran teknologi pada abad-21 telah melampaui imajinasi manusia dalam melakukan komunikasi dan pertukaran data serta informasi lintas negara. Peningkatan penggunaan media sosial mulai dari *Facebook*, *Twitter*, *Youtube*, *Instagram*, *E-mail*, bahkan penyimpanan data berbasis awan atau sering kita kenal dengan *cloud computing* menjadi perhatian penting saat ini. Informasi dan teknologi telah menyerap dan mengubah setiap aspek kehidupan manusia di abad 21 ini. Saat ini jumlah pengguna internet global diperkirakan 2,4 Miliar, nilai tersebut lebih dari sepertiga total penduduk dunia.

Selama lebih dari satu dekade, Amerika Serikat bergantung pada penggunaan ruang lingkup *cyberspace* hampir di setiap kegiatan mereka. Presiden Obama melihat hal ini sebagai salah satu *point* penting keamanan *cyber* di masa depan. Pada tanggal 29 Mei 2009, Presiden Obama menegaskan perhatian Pemerintah Amerika Serikat terkait pentingnya penggunaan jaringan komputer untuk memberikan dan menyalurkan minyak, gas, listrik, air, dan transportasi umum. Presiden Obama juga menegaskan kerentaan dan investasi yang lebih untuk menjaga fasilitas-fasilitas umumdemi kepentingan rakyat Amerika Serikat yang lebih baik.

Pada tahun 2008, insiden peretasan terjadi pada fasilitas militer Amerika Serikat di Timur Tengah. Wakil Menteri Pertahanan Amerika Serikat, William J. Lynn III merilis dokumen yang mencerminkan bahwa terdapat kode berbahaya di *server* Pentagon. Penyebarannya melalui *Universal Serial Bus* (USB), *Flash Driv*e yang tidak terdeteksi oleh sistem keamanan Pentagon.(http://www.nytimes.com/ diakses tanggal 13 Juni 2014)

Pada bulan November tahun 2011, terungkap bahwa 2 satelit pencitraan lingkungan milik Amerika Serikat *Landsat-7* dan *Terra* telah diretas. Penyerang memperoleh akses ke sistem

[1] Penulis
[2] Pembimbing 1
[3] Pembimbing 2

kendali satelit. Pada bulan Februari 2012 Inspektur Jenderal NASA mengungkapkan bahwa komputer dengan alamat *Internet Protocol (IP)* yang berbasis di China telah mendapatkan akses penuh ke sistem *Jet Propulsion Laboratory* yang memungkinkan penyerang untuk memodifikasi, menyalin atau menghapus *file* penting tersebut. (http://www.defensenews.com diakses tanggal 12 Juli 2014)

Selain itu, penting bahwa setiap pendekatan komperhensif terhadap isu keamanan *cyber* mempertimbangkan tentang Keamanan Nasional, kedaulatan negara, serta perlindungan *Critical Infrastructure* Amerika Serikat. Peneliti membatasi permasalahan ancaman *cyber* yang terjadi selama kurun waktu tahun 2008-2013. Peneliti juga membatasi jangka waktu penelitian ini selama tahun 2009-2013 pada masa Pemerintahan Presiden Obama.

Peneliti dalam penelitian ini juga membatasi upaya yang dilakukan oleh Pemerintah Amerika Serikat menghadapi ancaman *cyber war* di bidang politik dan ekonomi. Maksud dari pembatasan penelitian ini dikarenakan luasnya cakupan pembahasan mengenai keamanan nasional dan keamanan *cyber* serta bentuk-bentuk ancamannya. Dari penjelasan latar belakang diatas, maka peneliti mengambil rumusan masalah tentang Bagaimana Upaya Amerika Serikat menjaga Keamanan Nasional dari *Cyber War* Tahun 2009-2013?

Metode Penelitian

Penelitian ini termasuk penelitian deskriptif kualitatif dikarenakan topik yang dibahas dalam penelitian ini tidak berhubungan langsung dengan proses perhitungan angka-angka maupun statistik, tetapi lebih mengacu pada penjelasan /deskripsi

Penelitian ini bersifat studi kepustakaan, yang berarti bahwa peneliti mengumpulkan data-data dari buku-buku terkait teori-teori mengenai hubungan internasional, dokumentasi *cyber attack*, jurnal penelitian terdahulu yang terkait dengan upaya Amerika Serikat di masa pemerintahan Presiden Obama untuk menjaga Keamanan Nasional dari *cyber war*, dan dari situs-situs berita *online* yang terpercaya serta dapat dipertanggung jawabkan terkait dengan permasalahan yang dibahas dalam penelitian ini.

Kerangka dalam obyek penelitian ini, terkait upaya Amerika Serikat menjaga Keamanan Nasional dari *cyber war* dalam kerangka *cyber security* pada masa pemerintahan Presiden Obama.Teknik pengumpulan data yang peneliti gunakan dalam penelitian ini adalah teknik studi pustaka *(Library Research)*. Teknik analisa data yang peneliti gunakan dalam penelitian ini adalah teknik analisa kualitatif.

Hasil Penelitian dan Pembahasan

Keamanan *cyber* merupakan dimensi keamanan yang relatif baru di dunia Internasional dalam konteks Keamanan Nasional. Selama lebih dari satu dekade, musuh telah mengeksploitasi sejumlah besar data intelektual Amerika Serikat lewat dunia maya. Pada bulan Februari 2003, Presiden Bush menerbitkan *The National Strategy to Secure Cyberspace*. Tujuan dari dokumen tersebut adalah untuk mengamankan dunia maya di sektor swasta guna membela dan mencegah potensi serangan *cyber*.

Berikut ini Lembaga/Departemen di Amerika Serikat sebagai garda depan untuk menjaga keamanan *cyber* dan Keamanan Nasional Amerika Serikat: (1) *Department of Defense* (DoD) adalah Departemen Eksekutif pemerintah Federal Amerika Serikat yang ditugaskan untuk mengkoordinasikan dan mengawasi semua lembaga. DoD dibentuk pada tanggal 10 Agustus 1949 bermarkas di Pentagon. DoD dipimpin oleh Menteri Pertahanan Chuck Hagel, sedangkan kepala setingkat Kabinet bertanggung jawab langsung dengan Presiden Amerika Serikat.

Department of Defense (DoD) mengoperasikan jaringannya sendiri di seluruh dunia, yang dikenal dengan *Global Information Grid* (GIG).Tujuan DoD adalah untuk menyediakan pasukan militer yang diperlukan untuk mencegah perang dan melindungi keamanan Amerika Serikat.; (2) *Department of Homeland Security* (DHS) dibentuk tanggal 25 November 2002 melalui Undang-Undang keamanan dalam negeri merupakan sebuah departemen yang terdiri dari beberapa divisi yang berupaya melindungi Amerika

Serikat dari serangan terorisme dan bencana alam. DHS diciptakan pada masa pemerintahan Presiden Bush sebagai respon terhadap serangan 9/11 tahun 2001.

1. Bentuk dan Dampak Ancaman *Cyber* di Amerika Serikat

Teroris menggunakan internet untuk melemahkan Keamanan Nasional Amerika Serikat.Al-Qaeda menggunakan alat enkripsi pertama kali pada tahun 2007 ketika *Global Islamic Media Front* mendistribusikan program propaganda untuk kelompok militan Islam lainnya sekaligus meluncurkan perangkat lunak enkripsi mereka.Istilah *E-Jihad* mengacu pada cara penggunaan informasi teknologi yang diterapkan oleh kelompok Jihad seperti Al-Qaeda untuk mengatur "kampanye" mereka melalui penggunaan *E-mail*, enkripsi *file* dan sarana untuk mengembangkan taktik strategi mereka.

Kombinasi karakteristik yang dijelaskan di atas membuat internet menjadi aset yang bernilai strategis bagi teroris.Jaringan Al-Qaeda juga telah berhasil dalam menggunakan propaganda multimedia dengan memproduksi kaset, *CD-Rom*, DVD, foto, dan dokumen tulisan untuk menyebarkan ideologi radikal mereka dan untuk menjangkau simpatisan. Kelompok teroris telah menciptakan ribuan situs *website* untuk menggalang dana, merekrut, dan mendidik anggota baru. Beberapa individu teroris juga menggunakan game terpoputer seperti *Second Life* dan *World of Warcraft* untuk merencanakan pertemuan. Dalam konteks dunia maya, teroris dapat bertemu dalam bentuk perwujudan mereka secara *online* melalui *avatar*.

Pada tahun 2012, *National Aeronautics and Space Administration* (NASA) mengungkapkan penyusupan jaringan *cyber Jet Propulsion Laboratory (JPL)*yang ada di laboratorium NASA dengan alamat *Internet Protocol (IP)* berbasis di China.Dalam insiden tersebut, penyusup memperoleh kendali penuh fungsional melalui jaringan, memungkinkan mereka menyalin, menghapus, atau memodifikasi *file* sensitif. Menurut laporan Washington Times bahwa Amerika Serikat sejak awal 2007 jaringan *cyber* China berulang kali menyusup jaringan kontraktor terkait rencana desain *F-35 Joint Strike Fighter*. Pada bulan November 2011, terungkap bahwa dua satelit pencitraan lingkungan milik Amerika Serikat Landsat-7 dan Terra telah diretas oleh China. Penyerang memperoleh akses ke sistem kendali satelit.

Lebih dari 3.000 perusahaan mengoperasikan sistem jaringan pipa Amerika Serikat. Para pelaku *spionase cyber* biasanya memasang *malware* yang dapat mencari perusahaan jaringan pipa manapun dengan kode "SCADA" secara otomatis. SCADA merupakan sebuah sistem yang mengatur, memantau dan mengoperasikan stasiun jaringan pipa secara otomatis.

Saat ini sektor jaringan listrik Amerika Serikat sedang bertumbuh dan membuat *cybersecurity* juga semakin penting terkait Keamanan Nasional maupun internasional. Komponen jaringan listrik Amerika Serikat saling bergantung satu sama lain. Serangkaian tindakan *hacker* dilakukan terhadap apa yang disebut dengan "*Smart Meter*" yang selama beberapa tahun terakhir dibangun oleh pemerintah Amerika Serikat untuk meningkatkan efektifitas penggunaan listrik rumah tangga dengan mengontrolnya melalui jaringan *online*. Peneliti mengamati ancaman yang dilakukan oleh negara maupun individu di bidang politik dan ekonomi berakibat terhadap stabilitas dan keamanan dalam negeri Amerika Serikat.

2. Upaya Pemerintah Amerika Serikat

Presidential Policy Directive 8/PPD-8: National Preparedness ditandatangani dan dirilis oleh Presiden Obama pada tanggal 30 Maret 2011.PPD-8 menggambarkan sebuah pendekatan negara untuk mempersiapkan ancaman dan bahaya yang menimbulkan resiko terbesar bagi keamanan Amerika Serikat. Peneliti mengamati selama bertahun tahun pasca terjadinya serangan 11 September 2001, dunia telah menyaksikan gangguan tidak sah dan *hackingweb* dari berbagai aktor termasuk spionase industri. Orang-orang ini menggunakan banyak taktik dan prosedur seperti penggunaan *virus* komputer, *worm*, dan perangkat lunak

tertentu untuk melakukan serangan. Tantangan dari semua gangguan tersebut memungkinkan seluruh *Critical Infrastructure* Amerika Serikat harus dipertahankan. Informasi dan komunikasi, distribusi fisik, energi, perbankan, dan keuangan adalah prioritas kesiapan nasional Amerika Serikat untuk menghadapi ancaman *cyber* di masa sekarang dan yang akan datang.

Presiden Obama menandatangani *Presidential Policy Directive/*PPD-20*: U.S. Cyber Operation Policy* di tahun 2012 yang mengarahkan Dewan Keamanan Nasional untuk bertindak tegas menghadapi ancaman *cyber*. PPD-20 mengarahkan respon militer terhadap sebuah serangan *cyber*. Secara keseluruhan, peneliti melihat PPD-20 yang dibentuk adalah untuk mengarahkan pemerintah Amerika Serikat guna menyiapkan *counter-cyberattack* terhadap ancaman asing dan memungkinkan tindakan pencegahan terhadap serangan *cyber*. Ancaman terorisme melalui media internet menjadi salah satu landasan PPD-20 ini dibuat.

Menyadari konsekuensi potensi dari serangan *cyber*, *Department of Defense* DoD menyadari adanya kebutuhan untuk membentuk sebuah strategi *cyber*.Wakil menteri pertahanan William Lynn menyatakan bahwa strategi *cyber* ini memungkinkan pasukan maya sebuah bangsa untuk secara efektif sebagai atribut serangan *cyber*. Jenderal Keith Alexander menggambarkan kemitraan keamanan *cyber* Amerika Serikat sebagai salah satu dimana *Department Homeland Security* memimpin menciptakan infrastruktur yang aman untuk melindungi kepentingan Amerika Serikat, *Cyber Command* mempertahankan terhadap segala bentuk serangan *cyber*, FBI melakukan investigasi kriminal dan komunitas intelijen untuk mengumpulkan informasi luar negeri yang berindikasi menyebabkan terjadinya sebuah serangan *cyber*.

Diplomasi *cyber* adalah bentuk diplomasi baru untuk memasukkan dan menggunakan perangkat baru komunikasi di abad 21. Diplomasi *cyber* yang dilakukan Amerika Serikat dipimpin oleh Departemen Luar Negeri dan merupakan alat baru untuk memenuhi misi diplomasi. Meskipun Amerika Serikat telah terlibat dalam diplomasi *cyber* di bawah pemerintahan Presiden Bush pada tahun 2006, namun Amerika Serikat secara resmi meluncurkan kampanye diplomasi *cyber* di tahun 2009. Peneliti menemukan perkembangan diplomasi *cyber* Amerika Serikat terkait respon terhadap perubahan dalam hubungan internasional dengan memperluas jangkauan diplomasi Amerika Serikat diluar komunikasi pemerintah antar pemerintah.

Pada tanggal 12 Februari 2013, Presiden Obama menandatangani *Presidential Policy Directive*-21, keamanan *Critical Infrastructure* dan ketahanan yang Amerika Serikat bangun. *Department of Homeland Security* (DHS) mendirikan *Critical Infrastructure Partnership Advisory Council* (CIPAC) untuk memfasilitasi dan mengkoordinasi antara program perlindungan infrastruktur sektor swasta dan negara. Dilihat dari kerentaan *Critical Infrastructure* Amerika Serikat yang peneliti jelaskan sebelumnya, membuat pemerintah mengupayakan keamanan *Critical Infrastructure* tersebut.

Peneliti menemukan bahwa kerugian yang diakibatkan oleh sebuah serangan *cyber* bisa mencapai jutaan dolar. Kekayaan dan kerahasiaan sebuah informasi milik negara maupun perusahaan swasta bisa dijadikan senjata untuk menyerang kestabilan ekonomi Amerika Serikat.

Presiden mengeluarkan *Executive Order (E.O.) 13636: Improving Critical Infrastructure Cybersecurity* pada tanggal 13 Februari 2013 yang menyerukan pemerintah untuk berkoordinasi dengan pemilik dan operator *Critical Infrastructure* untuk meningkatkan keamanan informasi *cyber* dan bersama-sama mengembangkan dan menerapkan pendekatan berbasis resiko untuk *cybersecurity*. *Executive Order (E.O) 13636* menunjuk *National Institute of Standards and Technology* (NIST) untuk mengembangkan kerangka *cyber security* untuk memetakan mengenai resiko *cyber* dan berlaku untuk berbagai sektor yang signifikan.

Ruang lingkup *cyberspace* tidak sepenuhnya hanya sebatas virtual, namun juga terdiri dari komputer (*hardware*), sistem operasi (*software*), jaringan internet, dan jaringan kabel *fiber*/serat optik.Selama

beberapa tahun terakhir, pemerintah Amerika Serikat telah mengembangkan penggunaan *Internet Protocol Version* 6 (IPv6) pada jaringan DoD.

Penutup

Standar keamanan mengenai perangkat lunak sebuah perusahaan untuk keamanan *cyber* menjai perhatian khusus Presiden Obama dan perusahaan swasta. Pasal 204 dari Undang-Undang *cybersecurity* menegaskan bahwa akan memberdayakan NIST untuk mengenali dan mempromosikan langkah-langkah manajemen resiko serangan *cyber* serta upaya-upaya terbaik untuk melindungi sistem informasi penting pemerintah maupun swasta. Dalam hal ini NIST sebagai salah satu sektor standarisasi perangkat *smart meter* mengembangkan protokol yang menempatkan prioritas *smart grid* sebagai sumber daya penting nasional.

Daftar Pustaka

A.Baldwin, D. (2013). Power and International Relations. In W. Carlsnaes, T. Risse, & B. A. Simmons, *Handbook of International Relations* (2nd ed., pp. 273-297). Thousand Oaks, California: SAGE Publications.

Berg, B. (2001). *Qualitative Research Methods for the Social Sciences* (4th ed.). Needham Heights: Allyn & Bacon.

Choucri, N. (2012). *Cyberpolitics in International Relations.* London, Massachusetts, England: The MIT Press.

Clarke, R., & Knake, R. (2010). *Cyberwar: The Next Threat to National Security & What to Do About It.* New York: HarperCollins Publishers Inc.

Kuehl, D. (2009). From Cyberspace to Cyberpower: Defining the Problem. In F. D. Kramer, S. H. Starr, & L. K. Wentz (Eds.), *Cyberpower and National Security* (1st ed., pp. 24-42). Washington: National Defense University Press.

McGraw, G. (2006). *Software Security: Building Security in.* Addison: Wesley Professional.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar:What Everyone Needs To Know.* New York, United States of America: Oxford University Press.

"Cover Story: Hacking Cases Draw Attention To Satcom Vulnerabilities | Defense News | Defensenews.com." Accessed July12, 2014. http://www.defensenews.com/article/20120123/C4ISR02/301230010/Cover-Story-Hacking-Cases-Draw-Attention-Satcom-Vulnerabilities.

"Military Computer Attack Confirmed - NYTimes.com." Accessed June13, 2014. http://www.nytimes.com/2010/08/26/technology/26cyber.html?_r=5&.&.&.