Journal of International Relations, Volume 2, Nomor 4, Tahun 2016, hal 213-220
Online di http://ejournal-s1.undip.ac.id/index.php/jihi

ANALISIS PENGGUNAAN *OFFENSIVE CYBER OPERATIONS* MENGHADAPI ANCAMAN NUKLIR IRAN

Ary Melysa

Program Studi Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik
Universitas Diponegoro
Jalan Prof. H. Soedarto, SH, Tembalang, Semarang, Kotak Pos 1269
Website: http//www.fisip.undip.ac.id Email: fisip@undip.ac.id

ABSTRACT

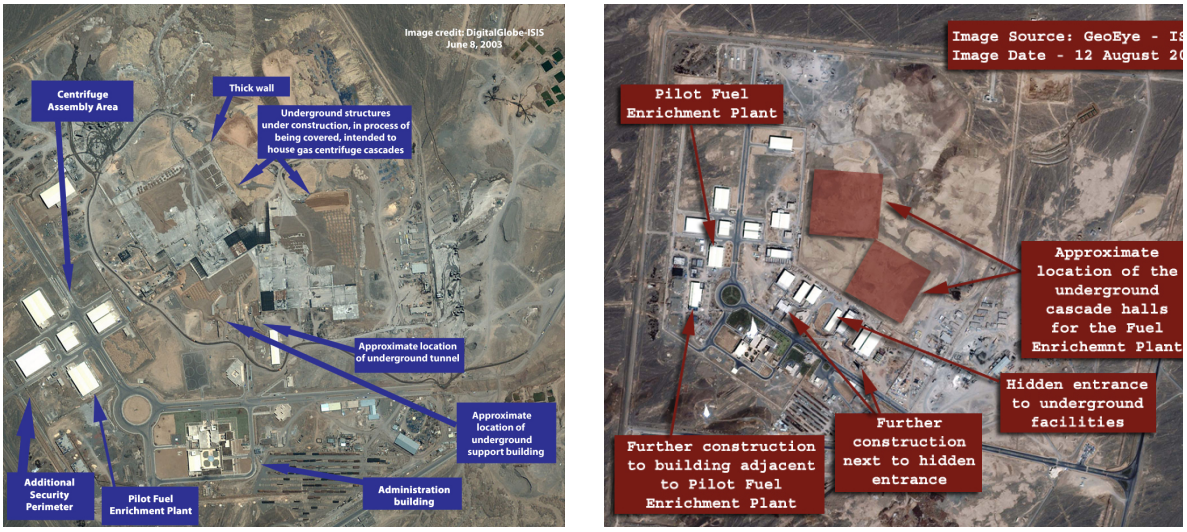
Iran's nuclear program was first initiated by joining the U.S. Atoms For Peace program. It however, changed when Iranian Revolution was occuring in 1979. Since then, the U.S has withdrawn its support to Iran's nuclear program. Although the program has been suspended, Iran continues its development after war with Iraq. The U.S. concerned that Iran's new nuclear program was built to produce nuclear weapons. After failing to prevent Iran from developing its nuclear program through diplomatic approaches, the U.S. was seeking a new alternative by using Offensive Cyber Operation or also known as Olympic Games. Together with Israel, the U.S. created the first ever cyber weapon called Stuxnet. The target of this operation is Uranium Enrichment Facility in Natanz, Iran. Specifically, Stuxnet has damaged around 1000 centrifuges whose primarily function is to enrich the uranium. This research aims to find out the reason of the U.S. in using Offensive Cyber Operations instead of Conventional Military Operations with regard to Iran's nuclear threat. To do so, this research uses Offensive Realism theory with qualitative method. The outcome of this research is: the U.S. as a rational actor has chosen Offensive Cyber Operations because the operation has brought the U.S. a number of strategic gains that cannot be necessarily achieved by Conventional Military Operations. These strategic gains are 1) Anonimity 2) Practicality in terms of distance, cost and risk 3) Execution easiness and 4) Political and bureaucracy leeway.

Keywords: *Cyber Operation*, *Offensive Cyber Operation*, *threat, Iran, nuclear*

PENDAHULUAN

Program nuklir Iran diawali dengan kerjasama Iran-Amerika Serikat dalam program *Atoms For Peace* besutan Presiden Dwight Eisenhower pada tahun 1957 (Bruno 2010). Namun program nuklirnya dihentikan karena pemimpin Revolusi Iran tidak menyetujui penggunaan program nuklir Iran. Selain itu, Amerika Serikat (AS) menarik dukungannya akibat pemimpin baru Iran yang anti-barat. Semenjak saat itu pula hubungan diplomatis Iran-Amerika Serikat terputus akibat peristiwa penyanderaan terhadap kedubes Amerika Serikat di Iran saat revolusi terjadi. Pada tahun 2002, *National Council Resistance of Iran* membocorkan kabar bahwa Iran sedang mengembangkan program nuklir secara diam-diam (NCRI 2013). Kabar tersebut diperkuat dengan bukti-bukti gambaran satelit yang diperoleh *Institute of Strategic and International Studies*.

Gambar 1 Foto Satelit Fasilitas Natanz



Sumber: (Institute for Science and International Security 2009)

Mendengar kabar tersebut, IAEA langsung meminta Iran untuk mengklarifikasi kabar tersebut. Iran kemudian mengakui bahwa negaranya memang sedang mengembangkan program nuklir. IAEA kemudian mengunjungi fasilitas pengayaan uranium di Natanz. Ternyata perkembangan nuklir Iran sudah cukup maju. Program nuklir yang dikembangkan Iran sontak membuat Amerika Serikat merasa terancam. Iran merupakan salah satu dari tiga negara yang tergabung dalam kelompok *axis of evil* seperti yang sering dikemukakan oleh Presiden George W. Bush. Selain itu, hubungan diplomatis kedua negara telah terhenti sejak tahun 1980. Amerika Serikat juga memandang Iran sebagai musuh karena negara tersebut kerap mendukung kegiatan terorisme terutama kelompok Hamas dan Hezbollah (Bruno, State Sponsors: Iran. 2011).

Amerika Serikat kemudian mulai melakukan pendekatan diplomatis dengan meminta PBB untuk segera menyelesaikan masalah tersebut (Bolton 2006). Akhirnya pada tahun 2006, Dewan Keamanan PBB mengeluarkan resolusi 1696 yang berisi permintaan kepada Iran untuk menghentikan program nuklirnya. Iran menolak resolusi tersebut dengan alasan negaranya membangun proyek nuklir hanya untuk diversifikasi energi saja dan bukan untuk senjata. Namun karena nuklir untuk energi dan nuklir untuk senjata hampir tidak bisa dibedakan, hal tersebut membuat AS tetap tidak percaya pada perkataan Iran.

Akhirnya PBB kembali mengeluarkan Resolusi 1737 yang berisi ancaman pemberian sanksi jika Iran tidak mematuhi permintaan PBB. Ahmadinejad kembali menolak resolusi tersebut dan mengatakan PBB menerapkan *double standard* karena Israel juga mengembangkan nuklir namun tidak ditentang oleh PBB. Menghadapi sikap Iran tersebut, PBB kemudian terpaksa mengeluarkan Resolusi 1747 yang berisi pemberian sanksi ekonomi serta embargo senjata demi menghambat perkembangan nuklir Iran. Israel juga termasuk salah satu negara yang merasa terancam dengan nuklir Iran. Israel menyalahkan AS yang terlalu lembek terhadap Iran. Israel bahkan sempat mendemonstrasikan kekuatan militernya dengan harapan Iran akan menghentikan proyek nuklirnya. Namun Iran tetap melanjutkan proyek nuklirnya.

Melihat hal tersebut, AS kemudian mencari cara menghadapi nuklir Iran. George W. Bush pada waktu itu hanya memiliki dua pilihan (Sanger 2012). Pilihan pertama adalah melakukan operasi militer sebagaimana yang disarankan oleh *National Security*

*Advisor*nya. Sedangkan pilihan kedua diajukan oleh *United States Strategic Command* (USSTRATCOM) adalah menggunakan *Offensive Cyber Operation*. Akhirnya Bush memilih *Offensive Cyber Operation* untuk menghadapi ancaman nuklir Iran yang lebih dikenal sebagai *Olympic Games Operation*.

PEMBAHASAN

Gambaran Umum Olympic Games Operation

Olympic Games Operation merupakan operasi gabungan yang dilakukan oleh Amerika Serikat dan Israel yang persiapannya dimulai dari tahun 2006. Amerika Serikat berperan sebagai pembuat Stuxnet sedangkan Israel berperan untuk memperbaharui Stuxnet serta menyelundupkan Stuxnet ke dalam jaringan komputer fasilitas nuklir Iran. Target dari operasi ini adalah fasilitas pengayaan uranium Natanz. Fasilitas tersebut merupakan elemen yang paling penting dalam pengembangan nuklir Iran. Fasilitas tersebut terdiri dari tiga bangunan bawah tanah yang didesain untuk menyimpan 50.000 sentrifuse dan enam bangunan di atas tanah (The Institute for Science and International Security 2016). Dua bangunan diatas tanah digunakan untuk menampung aliran gas. Empat bangunan lainnya digunakan sebagai tempat riset dan administrasi. Demi keamanan, komputer-komputer di fasilitas Natanz tidak terhubung dengan jaringan Internet. Dalam memperkaya uranium, fasilitas ini menggunakan sistem pengendali industri bernama Siemens S7-417 dan S7-315 yang mengendalikan ratusan alat pengayaan uranium atau yang disebut sebagai sentrifuse (Zetter 2014).

Senjata yang digunakan dalam operasi ini bernama *Stuxnet* yang merupakan *cyber weapon* pertama di dunia. *Stuxnet* adalah sebuah *malware* berbahaya yang berukuran 500 *kilobyte* (kb) atau 10 kali lebih besar dari *malware* biasa (Langner 2013). Selain itu, *Stuxnet* juga sangat canggih karena dilengkapi dengan empat buah *zero day* dan dua sertifikat digital. Zero day adalah sebuah celah yang tidak diketahui oleh pembuat software sampai serangan tersebut terjadi . Sehingga secara harafiah, zero day memiliki arti pembuat *software* memiliki *zero day* untuk mencegah serangan tersebut terjadi. Sedangkan sertifikat digital adalah sebuah "paspor" bagi *Stuxnet* agar dirinya dapat menginstal dirinya sendiri tanpa dicurigai ataupun dicegah oleh antivirus apapun.

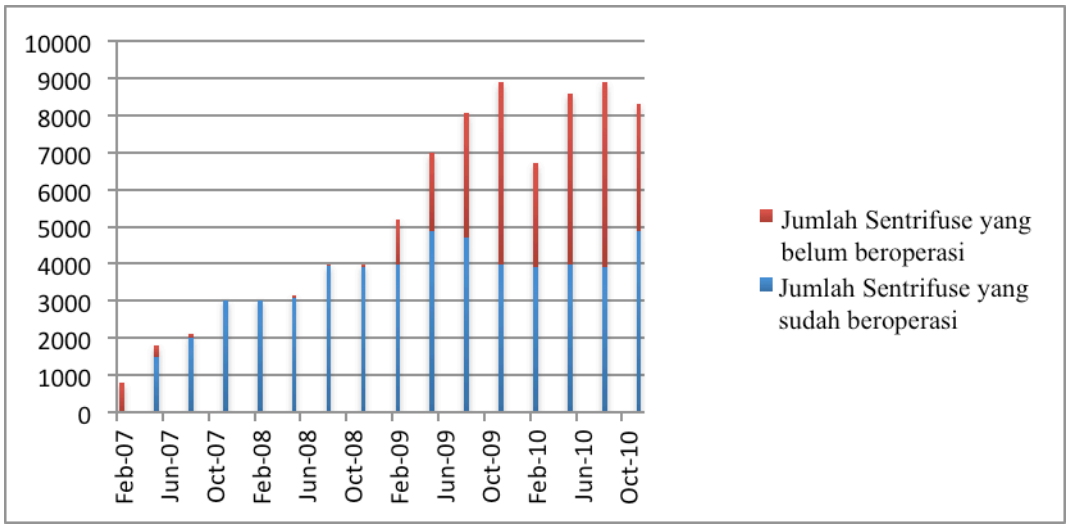
Seperti yang sudah disebutkan sebelumnya, komputer di fasilitas Natanz tidak terhubung dengan jaringan Internet. Sehingga proses persebaran Stuxnet memanfaatkan media *flashdisk*. Penyelundupan *flashdisk* berisi *Stuxnet* tersebut dilakukan oleh *double agent* dari Israel. Selain menggunakan *flashdisk*, *Stuxnet* juga memanfaatkan *network shares* untuk menginstal dirinya sendiri di puluhan komputer sekaligus. Setelah terinstal, *Stuxnet* kemudian mencari komputer mana saja yang memiliki akses terhadap sistem pengendali industri yang mengendalikan sentrifuse. Jika komputer yang ia tempati tidak memiliki akses terhadap *software* tersebut, Stuxnet tidak melakukan apa-apa.

Serangan *Stuxnet* sendiri terjadi pada dua gelombang. Gelombang pertama, Stuxnet menggunakan teknik *overpressurize* dengan terlebih dahulu meretas software pengendali sentrifuse bernama Siemens S7-417 yang mengendalikan 984 sentrifuse (Falliere, Murchu dan Chien 2011). Setelah berhasil diretas, Stuxnet memerintah sentrifuse-sentrifuse tersebut untuk menutup katup aliran gas. Selain memerintah, Stuxnet juga mengelabui operator seolah-olah semua baik-baik saja. Serangan tersebut membuat tekanan di dalam sentrifuse semakin tinggi namun tidak cukup tinggi untuk meledakkan sentrifuse yang ada. Dampak dari serangan pertama ini hanya hasil pengayaan uranium yang berkualitas rendah.

Serangan yang kedua, Stuxnet mengincar software yang lebih kecil yaitu Siemens S7-315 yang hanya mengendalikan 164 sentrifuse saja (Langner 2013). Rotor pada sentrifuse yang biasanya hanya berputar pada kecepatan 63,000 revolusi/menit, dipercepat menjadi 84,000 revolusi/menit kemudian tanpa jeda waktu yang cukup, diperlambat

hingga 120 revolusi/menit. Serangan tersebut terus diulang-ulang oleh Stuxnet sampai akhirnya sekitar 1,000-1,800 sentrifuse rusak parah (Zetter 2014).

Grafik 1 Jumlah Sentrifuse di Natanz



Sumber: (Albright, Brannan dan Walrond 2010)

Pada grafik di atas terlihat bahwa performa nuklir Iran sedang berada pada puncaknya saat bulan November tahun 2009 dengan jumlah sentrifuse mencapai 8,692 buah. Tetapi kemudian pada bulan Februari tahun 2010, jumlah sentrifusenya menurun hingga ke angka 6,888 buah. Menurut *International Atomic Energy Agency* (IAEA) angka penurunan ini jauh di atas normal. Namun IAEA sendiri tidak berkapasitas untuk menginvestigasi peralatan yang rusak. Tugas IAEA hanyalah mengawasi penggunaan uranium saja.

Iran pada waktu itu tidak menyadari bahwa negaranya mengalami *cyber attack*. Iran menyangka penurunan tersebut terjadi akibat kesalahan teknis. Barulah pada pertengahan tahun 2010 saat *Cyber Security Analyst* menemukan Stuxnet yang tersebar di internet, Iran menyadari bahwa dirinya diserang. Menanggapi hal tersebut, Iran kemudian memperkuat *cyber defensenya* dan membentuk *cyber police* yang bernama *The Iranian Cyber Police* FATA.

Alasan Penggunaan Offensive Cyber Operations

Amerika Serikat (AS) merupakan salah satu negara yang mulai mengakui *cyber space* sebagai domain yang menjadi wewenang *Department of Defense* setelah darat, laut, dan udara. Oleh karena itu, AS giat meningkatkan kemampuan *cyber capabilities*nya terutama kemampuan ofensifnya.

Tabel 1 *Cyber Capabilities* Negara

Negara	Kemampuan Ofensif	Kemampuan Defensif	Ketergantungan terhadap *Cyber*	Total
Amerika Serikat	8	1	2	11
Rusia	7	4	5	16
Tiongkok	5	6	4	15
Korea Utara	2	7	9	18

Sumber: (Clarke dan Knake 2010)

Dari tabel diatas dapat dilihat bahwa AS lebih mementingkan kemampuan ofensifnya. Hal tersebut dikarenakan kemampuan ofensif jauh lebih murah dibandingkan kemampuan defensif. Pertahanan yang baik harus mampu menghadapi semua serangan. Berbeda dengan kemampuan ofensif dimana AS hanya perlu berhasil menyerang sekali (National Research Council 1999). Selain itu Perwakilan AS di *Cyber Center* Estonia menyatakan bahwa sifat asimetris di dalam *cyber operations* sangat menguntungkan penyerang (Geers 2011).

Amerika Serikat (AS) merupakan negara pertama yang menggunakan *Offensive Cyber Operations*. Berdasarkan teori Realisme Ofensif, penggunaan *Offensive Cyber Operation* dipandang sebagai alat untuk memaksimalkan kesempatannya untuk bertahan di dalam sistem internasional yang anarki (Freyberg-Inan, Harrison dan James 2009). Oleh karena itu, AS sebagai aktor rasional memilih menggunakan *Offensive Cyber Operations* dibandingkan military operations biasa karena *Offensive Cyber Operations* memiliki keunggulan-keunggulan yang tidak dimiliki oleh *Conventional Military Operation*. Keunggulan-keunggulan tersebut adalah anonimitas, praktis dari segi jarak, efisiensi biaya, minimalisir kerusakan fisik, minimalisir korban jiwa, masih lemahnya *cyber defense* negara lain serta kemudahan proses birokrasi dalam pelaksanaan operasi.

Anonimitas

Salah satu keuntungan *Offensive Cyber Operations* dibanding *Offensive Military Operations* pada umumnya adalah anonimitas. Sifat alamiah dari teknologi memungkinkan identitas pengguna didalam *cyberspace* ditutupi dalam fitur anonimitas. Dalam pelaksanaan sebuah *cyber operation*, fitur ini sangat menguntungkan AS sebagai negara penyerang. AS dapat menyerang Iran tanpa diketahui oleh Iran. Hal tersebut memungkinkan AS mencapai kepentingannya tanpa harus bertanggung jawab atas apa yang sudah dilakukannya. Selain itu, saat persiapannya pun fitur ini menguntungkan penggunanya. Tidak akan ada yang tahu jika suatu negara sedang merencanakan *cyber operations* karena pengembangannya sendiri hanya dilakukan di komputer saja. Berbeda dengan pengembangan *military operations* yang dapat diketahui oleh negara lain dari anggaran belanja militer yang ditingkatkan, pembelian pesawat tempur, ataupun senjata lainnya.

Praktis dari Segi Jarak

Di dalam cyberspace tidak ada yang namanya batasan wilayah. Siapapun dapat berinteraksi dengan orang lain di negara manapun selama ada koneksi internet. Sayangnya selain bisa berinteraksi, siapapun juga dapat menyerang orang lain di negara manapun. Hal tersebut memungkinkan penyerangan dilakukan dari jarak jauh tanpa perlu repot-repot pergi ke tempat sasaran. Hal ini berbeda dengan military operations yang mengharuskan AS untuk membangun military base di negara tujuan, mengirimkan logistik serta mengirimkan tentaranya. Cara seperti itu jelas tidak efisien dalam hal waktu dan biaya.

Selain itu, karena dilakukan dari jarak jauh maka persiapannya pun tidak akan diketahui oleh negara lain. AS bisa mempersiapkan *cyber operation*nya tanpa takut aksinya diketahui oleh negara lain. Hanya saat serangan dilakukanlah korban baru menyadari apa yang terjadi dan karena sifatnya yang muncul tiba-tiba, negara yang tidak memiliki *cyber defense* yang bagus akan kewalahan menghadapi serangannya.

Efisiensi Biaya

Meskipun *cyber operations* membutuhkan teknologi dan tenaga ahli tetapi dibandingkan dengan pengeluaran operasi militer biasa *cyber operations* jauh lebih murah karena tidak harus mengganti biaya kerusakan yang ditimbulkan oleh *military operations*.

Cyber operations memiliki biaya yang sangat murah dengan tingkat resiko yang lebih rendah. Menurut sebuah laporan dari *U.S Air Force Research Laboratory*, *cyber operations* merupakan cara yang murah untuk mencapai kepentingan nasional AS dibandingkan dengan membeli senjata, tank, pesawat terbang maupun melatih ribuan tentara.

Setiap tahunnya AS menganggarkan USD 708 miliar untuk bidang militer. Sedangkan US Cyber Comand yang berwenang atas cyber operations hanya diberikan anggaran sebanyak USD 105 juta saja. Biaya yang mahal tersebut menguras anggaran belanja AS dan kadang hasilnya tidak sesuai keinginan. Padahal uang sebanyak itu dapat dialokasikan untuk hal lain seperti kesehatan, pendidikan ataupun yang lainnya.

Tabel 2 Perbandingan Biaya

Offensive Cyber Operations	*Conventional Military Operations*
USD 48,4 juta* *Termasuk gaji tahunan *cyber army* dan biaya peralatan yang dibutuhkan	USD 731 miliar* *termasuk biaya pembelian perlengkapan perang, senjata, pelatihan tentara, gaji tentara, pembangunan markas militer, logistik dan pemeliharaan infrastruktur
Sumber: (Miller 2013)	Sumber: (Epstein dan Williams 2016)

Jadi jika dibandingkan dengan pengeluaran *Conventional Military Operations*, *Cyber Operations* jauh lebih murah dan lebih efisien dalam urusan dana. Hal tersebut dikarenakan serangannya dapat dilakukan dari jarak jauh dan hanya menggunakan peralatan yang lebih sedikit dari *Conventional Military Operations*.

Minimalisir Kerusakan Fisik

Dalam *Olympic Games Offensive Cyber Operations* dampak kerusakan fisiknya hanya pada sentrifuse yang memang menjadi target utama AS. Hal ini berbeda jika AS menggunakan *Conventional Military Operations*. Tujuan AS adalah untuk menghambat perkembangan nuklir Iran. Jika menggunakan *Conventional Military Operations* maka AS akan mengirimkan rudal ataupun bom ke fasilitas Natanz yang dampaknya bisa meruntuhkan bangunan fasilitas nuklir dan dapat menyebabkan kontaminasi radioaktif.

Minimalisir Korban Jiwa

Seperti yang sudah disebutkan sebelumnya, operasi militer terkenal dengan resikonya yang besar. Selain kerusakan fisik, operasi militer seringkali menyebabkan korban jiwa baik dari pihak penyerang maupun korbannya. Contohnya *Iraqi Freedom Operation* yang memakan korban jiwa dari pihak AS dan koalisi sebanyak 196 dan korban luka-luka 551 orang (Bacevich, et al. 2013). Sedangkan dari pihak Irak, operasi tersebut memakan korban jiwa sebanyak 7500 warga sipil (Bacevich, et al. 2013).

Jika AS tetap menggunakan operasi militer maka dipastikan serangan tersebut akan membunuh ratusan ilmuwan dan pekerja yang ada di fasilitas nuklir Iran. Tentu saja, AS akan menghindari hal tersebut karena tidak ingin terus-terusan dikecam pihak internasional. Apalagi sebelumnya AS telah dikecam atas apa yang dilakukannya di Irak dan Afghanistan. Selain itu, dengan menggunakan *cyber operations*, AS dapat meminimalisir resiko kematian dari anggota tentaranya sendiri serta warga sipil. Seperti yang kita tahu ratusan ribu tentara AS mati di medan perang. Protes dari dalam negeri pun bermunculan

karena banyak tentara AS yang mati sia-sia. Hal tersebut tentu tidak efektif apalagi negara masih harus membayar kompensasi ataupun membiayai tentara-tentara yang terluka di medan perang. Sehingga, menggunakan *Offensive Cyber Operations* dipandang lebih efisien dibandingkan menggunakan *Conventional Military Operations.*

Lemahnya *Cyber Defense* Korban

Sebelum Stuxnet terjadi, banyak negara yang mengabaikan keamanan *cyber space*nya. Negara-negara masih terfokus pada keamanan wilayah dan tidak mementingkan *cyber defense*nya meskipun negaranya memiliki *cyber dependence* yang cukup besar. Selain itu, tidak ada satupun yang menyangka bahwa fenomena semacam *Stuxnet* dapat terjadi. Meskipun *cyber crime* sudah terbilang umum terjadi namun tidak ada satupun yang menyangka ada yang mampu mengakibatkan kerusakan fisik di *critical infrastructure* dengan hanya melalui sebuah komputer saja. Banyak yang menganggap fenomena seperti *Stuxnet* hanya ada di film-film holywood saja. Hal ini kemudian dilihat sebagai kesempatan bagi AS untuk meraih keuntungan strategis demi mencapai kepentingan nasionalnya.

Kemudahan Proses Birokrasi

Selain keuntungan-keuntungan yang sudah disebutkan diatas, masih ada satu keunggulan lagi yang dimiliki oleh *Cyber Operations*. Keunggulan tersebut adalah kemudahan dalam pengesahan tindakan. Proses pengesahan *cyber operations* jauh lebih mudah dan tidak bertele-tele. *Cyber operations* itu sendiri merupakan wewenang dari *the United States Cyber Command* (USCYBERCOM) yang berada di bawah kepemimpinan *the United States Strategic Command* (USSTRATCOM).

Proses pengesahannya dimulai dari usulan pelaksanaan *cyber operations* oleh USCYBERCOM yang kemudian disampaikan kepada Presiden. Setelah itu presiden dan tim dewan keamanan nasionalnya akan menentukan apakah *cyber operations* dapat dilaksanakan atau tidak. Jika diterima oleh Presiden, maka *cyber operations* dapat dilaksanakan. Dalam kasus *Olympic Games Operations*, usulan tersebut dibuat oleh General E. Cartwright yang merupakan pemimpin dari USCYBERCOM. Ia mengusulkan penggunaan *cyber operations* sebagai alternatif dalam menghadapi ancaman nuklir Iran. Presiden Bush saat itu hanya memiliki pilihan yang terbatas. Bush hanya dapat memilih antara penggunaan kekuatan militer atau *Offensive Cyber Operations*. Setelah berdiskusi dengan timnya, akhirnya Bush menyetujui operasi tersebut.

Hal ini berbeda dengan pengusulan *Conventional Military Operations*. Semenjak Perang Dunia II, AS belum pernah lagi mendeklarasikan perang ke negara manapun. Tetapi sejak peristiwa 9/11, AS menggunakan istilah baru yaitu *Authorization of Using Military Force* (AUMF) (Gude 2014). Proses pengesahan AUMF tidak semudah pengesahan *cyber operations*. Pada AUMF, Presiden Bush mengusulkan draftnya kepada kongres. Setelah itu, *House of Representative* melakukan voting terkait draft tersebut. Di sisi lain, Senat juga melakukan *roll call vote* atas draft tersebut. Setelah melewati proses *lobbying* yang panjang dan penuh amandemen, akhirnya draft tersebut di*voting*. Setelah itu barulah draft tersebut disahkan dan presiden diperbolehkan melaksanakan operasi militer tersebut.

PENUTUP

Program nuklir Iran memiliki banyak pro dan kontra. Iran secara tegas menyatakan program nuklir miliknya secara murni hanya demi kepentingan diversifikasi energi saja. Namun karena penggunaan uranium untuk program energi dan senjata tidak dapat dengan jelas dibedakan, hal itu membuat AS merasa terancam. Hubungan kedua negara sudah

tidak harmonis sejak peristiwa penyanderaan di kedutaan besar AS di Iran pada tahun 1980. Semenjak saat itu, setiap tindakan Iran mulai dari mendukung kegiatan terorisme hingga pengembangan proyek nuklir dianggap sebagai ancaman bagi AS.

Menghadapi ancaman tersebut AS merasa harus melakukan tindakan demi menghambat proyek nuklir Iran. Jika biasanya, AS melakukan operasi militer dengan mengirimkan tentaranya, mengebom dan menghancurkan infrastruktur milik musuh. Kini AS menggunakan *Offensive Cyber Operations* bernama *Olympic Games*.

Hasil dari penelitian ini menunjukkan bahwa Amerika Serikat menggunakan *Offensive Cyber Operations* karena hadirnya beberapa keunggulan jika dibandingkan dengan *conventional military operations*. Keunggulan-keunggulan tersebut adalah: 1) anonimitas, 2) praktis dari segi jarak, biaya dan resiko, 3) mudah untuk dioperasikan 4) mudah dalam proses politik dan birokrasi. Karena keunggulan-keunggulan inilah AS lebih memilih *cyber operations* ketimbang *conventional military operations*.

Referensi

Bolton, John R. "Adoption of Resolution 1696 on Iran." *U.S Department of State.* 31 Juli 2006. http://2001-2009.state.gov/p/io/rls/rm/69788.htm (diakses Agustus 17, 2016).

Bruno, Greg. "Iran's Nuclear Program." *Council on Foreign Relations.* 10 Maret 2010. http://www.cfr.org/iran/irans-nuclear-program/p16811 (diakses September 18, 2016).

Bruno, Greg. "State Sponsors: Iran." *Council on Foreign Relations.* 13 Oktober 2011. http://www.cfr.org/iran/state-sponsors-iran/p9362 (diakses September 18, 2016).

Falliere, Nicolas, Liam O Murchu, dan Eric Chien. *W.32 Stuxnet Dossier.* California: Symantec, 2011.

Freyberg-Inan, Annette, Ewan Harrison, dan Patrick James. "Rethinking Realism in International Relations: Between Tradition and Innovation." Dalam *Elaborating on Offensive Realism*, oleh Patrick James, 45-62. Maryland: The Johns Hopkins University Press, 2009.

Gude, Ken. "Understanding Authorizations for the Use of Military Force." *American Progress.* 24 September 2014. https://www.americanprogress.org/issues/security/report/2014/09/24/97748/understanding-authorizations-for-the-use-of-military-force/ (diakses September 20, 2016).

Institute for Science and International Security. "Excerpts from Internal IAEA Document on Alleged Iranian Nuclear Weaponization." *ISIS Nuclear Iran.* 22 Oktober 2009. isisnucleariran.org/assets/pdf/IAEA_info_3October2009.pdf (diakses September 29, 2016).

Langner, Ralph. *To Kill A Centrifuge.* Analysis Technical, California: Langner, 2013.

NCRI. "Non Nuclear Iran." *National Council of Resistance in Iran.* 16 Februari 2013. http://www.ncr-iran.org/en/issues/non-nuclear-iran (diakses Juni 24, 2016).

Sanger, David E. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power.* New York: Crown Publishers, 2012.

The Institute for Science and International Security. "Natanz Facility." *ISIS Nuclear Iran.* 12 Agustus 2016. http://www.isisnucleariran.org/images/gallery/natanz/geoeye_natanz_iran_12_aug_2006.jpg (diakses Juni 15, 2016).

Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.* Chicago: Crown Publishers, 2014.