Stuxnet Amerika Serikat dalam Kerangka Neo-Realisme

Syani Zuraida[1]
Yusran[2]

Abstract
This research discusses about the Stuxnet phenomena to remote the nuclear program of Iran. The advance of information and communication technology impacts the international relation. Those technological sophistication makes the country can attack another country virtually. Stuxnet is an example of cyber- attack done by United States of America to distract the Iran's nuclear program. His research uses qualitative methods with the framework of neo-realism to analyze and answer the question of the research. The result of this research is stuxnet as a cyber-weapon justifies the concept of neo-realism international system, power and its relation.

Keywords: *cyber weapon, neo-realism, Stuxnet, Iran, United States of America*

Pendahuluan

Hubungan internasional merupakan cabang disiplin ilmu yang terutama memperhatikan hubungan politik antar negara. Hubungan internasional mencakup pengkajian terhadap politik luar negeri dan politik internasional, dan meliputi segala segi hubungan diantara berbagai negara (Howard Lentner, 1974: 58). Hubungan tersebut kian hari kian beragam, baik hubungan yang bersifat kerjasama maupun hubungan yang bersifat konflik.

Pada umumnya, negara melakukan kerjasama didasarkan pada perbedaan berbagai faktor, yaitu faktor sumber daya manusia dan sumber daya alam. Letak geografis yang berbeda antara negara satu dengan negara lainnya menyebabkan perbedaan pada sumber daya suatu negara. Alhasil, untuk memenuhi kebutuhan akan suatu hasil bumi, negara kerap melakukan kerjasama perdagangan dengan negara lainnya. Kerjasama lain yang dilakukan negara antara lain kerjasama dalam bidang pendidikan yang pada umumnya diimplementasikan melalui pemberian beasiswa maupun pertukaran pelajar.

[1] Mahasiswi, Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Budi Luhur. Email: zuraidasyani@gmail.com
[2] Dosen Tetap, Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Budi Luhur

Namun, hubungan internasional tidak hanya diwarnai dengan hubungan kerjasama. Ada kalanya, hubungan tersebut bersifat konflik ataupun perang. Pada tahun 1957, Iran bersama Amerika telah menandatangani perjanjian program Atom untuk Perdamaian (Atom for Peace), sebagai bentuk kerjasama penelitian penggunaan energi atom secara damai (Greg Bruno, 2010). Kemudian, pada tahun 1974 Iran menyatakan keinginannya untuk mengembangkan senjata nuklir. Keinginan Iran tersebut disambut dengan respon negatif Amerika. Awalnya, Amerika menolak rencana Iran melalui perjanjian pembatasan nuklir dengan Iran. Namun, ternyata Iran tetap mengembangkan senjata nuklir. Dari masalah tersebut, maka timbulah pertanyaan penelitian, "Bagaimana strategi Amerika Serikat dalam mencegah pengembangan nuklir oleh Iran?"

Pembahasan

Program Nuklir Iran

Pada tahun 1957, Iran bersama Amerika telah menandatangani perjanjian program Atom untuk Perdamaian (Atom for Peace), sebagai bentuk kerjasama penelitian penggunaan energi atom secara damai (Greg Bruno, 2010). Dua puluh tahun kemudian, Iran bergerak cepat untuk mengembangkan pembangkit listrik tenaga nuklir (PLTN). Sehingga didirikanlah Tehran Nuclear Research Center (TNRC) pada tahun 1975. TNRC dilengkapi dengan reaktor penelitian nuklir sebesar 5 megawatt dari Amerika. Reaktor ini dikenal dengan sebutan Tehran Research Reactor (TRR) yang mengkonsumsi kadar uranium tinggi sebagai bahan bakarnya. Hal penting dalam perjanjian ini adalah, Iran akan mendapat dukungan nuklir dari Amerika apabila Iran menandatangani perjanjian non-proliferasi senjata nuklir (Non-Proliferation of Nuclear Weapons/NPT). Pada tahun 1968 Iran menandatangani NPT sehingga dibukalah program nuklir Iran untuk selalu di kontrol oleh International Atomic Energy Agency (IAEA) (Greg Bruno, 2010).

Di tengah pengembangan program nuklir tersebut, Iran menyatakan keinginannya dalam mengembangkan senjata nuklir. Hal ini diperkuat dengan komentar Presiden Iran, Shah Mohammad Reza Shah Pahlavi bahwa Iran harus menyiapkan diri untuk menciptakan senjata nuklir apabila negara non-anggota pengembang nuklir, menciptakan nuklir (William Burr, 2009: 34). Pernyataan tersebut muncul akibat adanya tes senjata nuklir oleh India pada 1974. Tes senjata nuklir tersebut merupakan tes senjata nuklir pertama oleh negara yang bukan merupakan anggota permanen Dewan Keamanan PBB (Nuclear Weapon Archive, 2001).

Menanggapi pernyataan Iran, Amerika memutuskan untuk membuat perjanjian lanjutan serta pembatasan pada program nuklir Iran. Namun, Iran merasa kebijakan Amerika menggambarkan ketakutan Amerika apabila negara lain juga mengembangkan senjata nuklir. Ditengah berbagai perselisihan, akhirnya pada tahun 1978 di tandatanganilah perjanjian yang mengizinkan Amerika untuk menggunakan hak veto dalam pengolahan ulang bahan bakar nuklir (William Burr, 2009: 34). Perjanjian tersebut menimbulkan tekanan diantara pemerintah Iran, beberapa beranggapan bahwa Shah terlalu tunduk pada kemauan Amerika.

Revolusi di Iran pada tahun 1979 membawa perubahan besar bagi program nuklir Iran. Sehingga dibawah pemerintahan Ayatollah Ruhollah Khomeini tahun 1990, Iran menandatangani perjanjian dengan Rusia untuk mendapatkan pakar nuklir Rusia serta informasi mengenai tenaga nuklir. Kemudian pada tahun 2002, sebuah kelompok yang disebut National Council of Resistance of Iran mengungkapkan keberadaan fasilitas pengayaan uranium di Natanz (Greg Bruno, 2010). Ketegangan antara Iran dan dunia barat tumbuh pesat pada 2006 ketika Presiden Iran, Mahmoud Ahmadinejad menyatakan bahwa Iran telah mencapai tujuannya dalam memperkaya uranium. Amerika adalah negara yang paling mengecam keputusan Pemerintah Irak untuk melanjutkan pengayaan uranium. Secara rahasia Amerika menyiapkan sebuah rencana untuk menghentikan program nuklir Iran. Rencana rahasia ini baru terungkap pada Juni 2010.

Munculnya Stuxnet

Pada era globalisasi yang ditandai dengan pesatnya perkembangan teknologi informasi dan komunikasi, perang tidak lagi dilakukan dengan berhadap-hadapan dengan senjata konvensional. Serangan dilakukan secara maya melalui internet dengan target operasi sistem jaringan suatu negara. Hal ini sangat berbahaya, mengingat dalam era globalisasi segala kegiatan ekonomi, sosial, politik, budaya terintegrasi dalam sebuah sistem jaringan. Sehingga serangan yang dilakukan dalam dunia maya/cyber attack merupakan ancaman bagi ketahanan nasional sebuah negara.

The Supervisory Control And Data Acquisition (SCADA) merupakan sistem kontrol jaringan industri yang bertanggung jawab pada proses kontrol industri seperti manufaktur, pembangkit listrik, berbagai infrastruktur seperti pipa minyak dan gas serta fasilitas seperti bandara, stasiun luar angkasa dan lain-lain. Sistem kontrol tersebut sangat penting bagi perekonomian dunia dalam berbagai sektor industri. Ketergantungan penggungan teknologi tinggi dan manajemen otomatis dalam sektor ini, menyebabkan rentannya sistem dalam berbagai ancaman serangan cyber/cyber attack. Sehingga terserangnya sistem oleh cyber attack tersebut akan berdampak buruk pada dunia nyata (T. Chen dan S. Abu-Nimeh, 2011: 91-93).

Cyber attack yang akan dibahas dalam pembahasan ini adalah serangan Stuxnet worm yang dilakukan Ameika-Israel terhadap reaktor nuklir Iran. Serangan ini telah direncanakan sejak masa pemerintahan George W. Bush, pada saat itu Bush merancang sebuah file virus dengan kode olimpic games. File virus ini lolos dan merambat ke komputer di seluruh dunia pada musim panas 2010 melalui internet setelah terjadi ketidaksengajaan pemrograman,(David E. Sanger, 2012) pakar keamanan komputer Amerika dan Israel mempelajarinya dan menyebutnya stuxnet (David E. Sanger, 2012)

Stuxnet mampu menyusup dan menyabotase sistem dengan cara memperlambat ataupun mempercepat motor penggerak reaktor nuklir, bahkan dapat membuatnya berputar diatas kecepatan maksimum. Kecepatan ini akan merusak komponen reaktor untuk memproduksi bahan bakar uranium. Presiden Barack Obama, menyebutkan bahwa serangan Stuxnet worm ini merupakan langkah untuk memperlambat kemajuan perkembangan program nuklir Iran. (Tikun Olam, 2010). Hal ini dikonfirmasi lewat investigasi Kaspersky Labs terhadap virus tersebut, "serangan worm seperti ini hanya dapat diwujudkan dengan dukungan sebuah negara." (William Mclean, 2010)

Para analis mengatakan bahwa Stuxnet dilengkapi berbagai fitur termasuk Windows Rootkit, perintah dan kontrol jaringan terdistribusi, kemampuan peer-to- peer, dan teknik penghindaran anti-virus (Nicolas Falliere, Liam O Murchu, dan Eric Chien, 2011). Windows rootkit membuat Stuxnet mampu menghidupkan dirinya kembali pada sistem yang teinfeksi setelah proses scanning malware. Sistem perintah dan kontrol jaringan membuat pencipta dan pengoperasi malware memberikan akses jarak jauh untuk memerintah dan memperbaruinya. Kemampuan peer-to-peer memberikan Stuxnet kemampuan untuk berkomunikasi dengan stuxnet lain bahkan dalam koneksi internet yang berbeda virus (Nicolas Falliere, Liam O Murchu, dan Eric Chien, 2011). Fitur-fitur yang dimiliki Stuxnet membuat Stuxnet menjadi malware yang luar biasa.

Melalui analisis yang ekstensif, para ahli percaya Stuxnet dikembangkan dan diuji coba sekitar tahun 2007. Infeksi awal pada jaringan Iran berlangsung pada 2009 (Elizabeth Montalbano, 2011) Pada awalnya, pemerintah Iran mengklaim tidak adanya infeksi. Ketika para ahli mengakui infeksi Stuxnet, pemerintah menyatakan bahwa tidak ada kerusakan yang diakibatkan oleh Stuxnet. Namun, bagaimanapun juga pada 29 November 2010, Presiden Iran Mahmoud Ahmadinejad mengakui bahwa Stuxnet telah menginfeksi fasilitas nuklir Iran dan merusak program melalui sabotase fasilitas sentrifungal (William Yong and Robert F. Worth, 2010). Satelit fotografi dan investigasi IAEA telah mengindikasikan bahwa setidaknya 1000 dari 9000 sentrifungal yang ada di Natanz rusak akibat infeksi Stuxnet. (David Albright, Paul Brannan, and Christina Walrond, 2010).

Selain itu para analis juga berpendapat bahwa Israel dan Amerika sebagai negara pencipta Stuxnet. (Masters, Jonathan, 2011) Hal ini dikonfirmasi pemerintahan Amerika dalam pertemuan di gedung putih. Pertimbangan Presiden Barrack Obama, wakil presiden Joseph R. Biden Jr dan Mantan Direktur CIA Leon Panetta dalam upaya memperlambat kemajuan perkembangan program nuklir Iran, maka dikirimlah serangan malware ke dalam jaringan program nuklir Iran. (David E. Sanger, 2012)

Paradigma Neo-Realisme Hubungan Internasional

Asumsi dasar neorealisme sama seperti pandangan realisme yakni, manusia pada dasarnya makhluk yang mementingkan diri sendiri (selfish). Namun, perbedaannya adalah neorealisme memandang sifat dasar negara berdasarkan pendekatan non-sistemik. Maksudnya adalah penyebab segala chaos di dunia internasional adalah aktor (baik negara sebagai aktor utama maupun sifat dasar manusia) (Kenneth Waltz, 1979). Neorealisme juga percaya adanya anarki atau tidak adanya istitusi sentral diatas negara. (Charles W. Kegley Jr; Eugene R. Wittkopf, 2001: 21). Negara tetap menjadi aktor utama, bertindak dengan memegang teguh prinsip 'self-help' dan memastikan mereka bisa survive atau bertahan hidup. Tapi yang dibedakan neorealis bukanlah masalah yang dihadapi suatu negara, melainkan kapabilitas mereka untuk menanganinya. Kapabilitas itu nantinya menentukan posisi negara bersangkutan dalam sistem global dan distribusi kapabilitas menunjukkan struktur dari sistem itu sendiri yang membentuk bagaimana unit-unit di dalamnya berinteraksi antara satu sama lain.

Power atau kekuasaan juga menjadi konsep sentral dari neorealisme, namun bukan sebagai bagian dari nature mereka melainkan menjadi sarana bagi negara untuk bertahan hidup. Pencetus neorealisme, Kenneth N. Waltz dalam bukunya Theory of International Politics (1979) menerangkan "sarana itu sendiri terbagi ke dalam dua kategori: upaya internal (peningkatan kapabilitas ekonomi, penambahan kekuatan militer, atau mengembangkan strategi yang lebih baik) dan upaya eksternal (memperkuat dan memperbesar aliansinya atau melemahkan musuh)".

Neo-realisme memandang bahwa, perilaku negara ditentukan oleh lingkungan internasional. Kenneth Waltz fokus membahas lingkungan internasional. Waltz berpendapat bahwa negara memiliki kecenderungan kearah politik internasional yang kompetitif. Sehingga dapat dipastikan kepentingan suatu negara mungkin sama atau bertentangan dengan kepentingan negara lain. Perbedaan kepentingan akan menimbulkan peperangan, sedangkan kepentingan yang sama akan menciptakan aliansi (Charles W. Kegley Jr; Eugene R. Wittkopf, 2001: 21).

Menurut Waltz ada dua alternatif untuk membentuk aliansi. Balancing alliance dan bandwagoning alliance. Balancing alliance yaitu keadaan ketika suatu negara bergabung pada sisi yang lemah untuk mencoba mengalahkan negara yang kuat. Sedangkan bandwagoning alliance merupakan keadaan ketika suatu negara bergabung dengan sisi yang kuat. Menurut neorealisme Waltz, negara lebih suka menerapkan balancing alliance daripada bandwagoning. Argumen inti dari pernyataan ini adalah kontribusi power yang diberikan suatu negara pada aliansinya. Pada balancing alliance, power negara akan sangat diperlukan untuk melawan pihak musuh yang kuat, sementara bandwagoning alliance sudah cukup kuat sehingga negara tidak memberikan kontribusinya untuk keamanan kolektif aliansi. Bahkan, dalam bandwagoning alliance, suatu negara dapat diserang oleh sekutunya sendiri. Sehingga dapat disimpulkan bahwa balancing alliance lebih menguntungkan.

Analisa Stuxnet dengan Paradigma Neo-realisme

Stuxnet merupakan sebuah malware (cyber attack) yang diciptakan oleh Amerika dan Israel untuk menyabotase program nuklir Iran. Menurut paradigma neo-realisme, negara bersifat selfish, yakni selalu mengutamakan kepentingannya sendiri. Pengembangan program senjata nuklir Iran dipandang sebagai suatu ancaman bagi Amerika-Israel sehingga Amerika-Israel berusaha untuk melakukan tindakan pencegahan terhadap ancaman tersebut.

Selain itu, stuxnet juga menjadi alasan survival suatu negara. Kapabilitas Ameika-Israel dalam menangani ancaman nuklir Iran menentukan posisinya dalam sistem global. Dengan diciptakannya Stuxnet membuka mata dunia bahwa serangan demi mencapai survive dan memajukan kepentingan nasional tidak lagi hanya dapat dilakukan di dunia nyata, tapi juga di dunia maya.

Stuxnet yang merupakan bentuk senjata cyber juga menjustifikasi konsep sistem internasional neo-realisme. Stuxnet yang bekerja di wilayah cyberspace telah menjadi sistem internasional baru. Hal ini dicirikan dengan ketiadaan badan pemerintahan yang mengatur sistem internasional tersebut. Atau dengan kata lain cyber space sangat cocok dengan model sistem internasional neo-realisme yang dicirikan dengan negara dan aliansinya lah kunci dari sistem internasional.

Kenneth Watlz menjelaskan sarana-sarana untuk mencapai power atau kekuasaan, antara lain:

1. Upaya internal dengan peningkatan kapabilitas ekonomi, penambahan kekuatan militer atau mengembangkan strategi yang lebih baik
2. Upaya eksternal dengan memperkuat aliansinya atau melemahkan musuh

Dalam rangka mendapatkan power tersebut, Amerika telah melaksanakan kedua upaya tersebut, yakni dengan mengembangkan Stuxnet yang merupakan salah satu contoh pengembangan strategi dan kekuatan militer (upaya internal), serta menggandeng Israel sebagai bandwagoning alliance (upaya eksternal).

Kesimpulan

Kemajuan teknologi informasi dan komunikasi membuat hubungan internasional menjadi semakin dinamis. Perang atau serangan yang dulu hanya mungkin dilakukan secara berhadap-hadapan, kini dengan kemajuan teknologi dapat terjadi lewat dunia maya. Kehadiran Stuxnet membuktikan bahwa serangan terhadap negara lain dapat dilakukan secara maya dan memberikan efek yang ril di kehidupan nyata.

Paradigma neo-realisme mengatakan bahwa Stuxnet yang tergolong ke dalam cyber-attack menjustifikasi model sistem internasional kaum neo-realis. Sistem internasional yang anarkis yang juga diartikan tidak ada kekuasaan tertinggi kecuali negara yang berperan dalam hubungan internasional.

Kemajuan teknologi informasi dan komunikasi menyebabkan hubungan internasional menjadi lebih rentan terhadap ancaman. Sehingga peningkatan kapabilitas pertahanan harus ditingkatkan seiring dengan perkembangan teknologi. Peningkatan pertahanan diperlukan agar kejadian serupa Stuxnet tidak terulang, sekaligus tetap mempertahankan kedaulatan negara dari negara lain.

Referensi

Albright, David Paul Brannan, and Christina Walrond, (2010) "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?" Institute for Science and International Security, diakses di http://isis-online.org/isis-reports/detail/did- stuxnettake-out-1000-centrifuges-at-the-natanz-enrichment-plant/#2.

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

Burr, William, (2009) "A Brief History of US-Iranian Nuclear Negotiations," Bulletin of the Atomic Scientists, 65, no. 1,

Chen T. dan S. Abu-Nimeh, (April 2011), "Lessons from stuxnet," Computer, vol. 44, no. 4

Falliere, Nicolas, Liam O Murchu, dan Eric Chien, (2011), "W32.Stuxnet Dossier," Symantec Security Response, diakses di http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_st uxnet_dossier.pdf.

Kegley Jr, Charles W; Eugene R. Wittkopf, (2001) World Politics: Trend and Transformation, (Boston: Bedford/St Martin's),

Lentner, Howard, (1974), Foreign Policy Analysis: A Comparative and Conceptual Approach, Ohio: Bill and Howell Co.

Maclean, William "Iran First Victim of Cyberwar", http://news.scotsman.com/world/Iran-39first-victim-of-cyberwar39.6550279.jp diakses 25 Desember 2015

Masters, Jonathan, (2011), Confronting the Cyber Threat , Council on Foreign Relations, diakses di http://www.cfr.org/technology-and-foreign- policy/confronting-cyber-threat/p15577

Montalbano, Elizabeth, (2011), "Stuxnet, Duqu Date Back to 2007, Research Says," Information Week, 29 Desember 2011, diakses di http://www.informationweek.com/news/security/vulnerabilities/232301131

Nuclear Weapon Archive, (2001) "Smiling Buddha: 1974," diakses di http://nuclearweaponarchive.org/India/IndiaSmiling.html

Olam, Tikun (2010) "Iran Confirms Stuxnet Damage to Nuclear Facilities," http://richardsilverstein.com/tikun_olam/2010/09/25/iran-confirms-stuxnet-damage-to-nuclear-facilities/

Sanger, David E. (2012) "Obama Order Sped Up Wave of Cyber attacks Againts Iran," The New York Times: Middle East, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyber-attacks-againts-iran.html?_r-2&

The Institute for Science and International Security, "Tehran Nuclear Research Center," diakses di http://www.isisnucleariran.org/sites/facilities/tehran-researchreactor-trr/

Waltz, Kenneth, (1979), Theory of International Politics, Reading, MA: Addison-Wesley Pub.Co

Yong, William dan Robert F. Worth, (2010) "Bombing Hit Atomic Experts in Iran Streets," The New York Times, 29 November 2010, diakses di http://www.nytimes.com/2010/11/30/world/middleeast/30tehran.html?_r=2&hp pada 26 Desember 2015