BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Fenomena hubungan internasional adalah fenomena yang mengalami perkembangan dan dinamika yang sangat cepat. Berkembangnya globalisasi dan kemajuan teknologi informasi membawa dampak besar terhadap berkembangnya ilmu hubungan internasional. Seperti yang terjadi dengan perkembangan konsep *power* yang mengalami evolusi akibat pesatnya penggunaan *Cyberspace* dalam hubungan internasional sehingga menciptakan suatu cabang *power* yang baru yaitu, *Cyberpower.*

Power merupakan kata kunci yang paling sering ditemukan di dalam hubungan internasional. *Power* digunakan sebagai konsep yang dikenal dengan kekuasaan politik *(power politic). Power* berbagi peran dengan konsep "negara" sejak lahirnya ilmu hubungan internasional dan dianggap sebagai konsep dasar dari hubungan internasional. Tujuan suatu negara dan *power* tidak dapat dipisahkan. Dengan kata lain, tujuan dari setiap aktor (negara) adalah *power* (Perwita dan Yani, 2005:13).

Penggunaan *cyberspace* dalam hubungan internasional akibat majunya teknologi membentuk suatu konsep baru tentang penggunaan *power* yang dapat dicapai melalui *cyberspace*. Hal inilah yang pada akhirnya melahirkan konsep *cyberpower* yang artinya adalah sebagai suatu kemampuan untuk menggunakan

cyberspace untuk meraih berbagai keuntungan dan pengaruh sesuai dengan target dan keinginannya (Nye, 2010: 3)

Penggunaan Komputer dan infrakstruktur internet, selain memberikan manfaat ekonomi, sosial dan politik yang diciptakan untuk para aktor masyarakat internasional, juga dapat menyebabkan naiknya tensi pada bidang politik dan militer , mispersepsi dalam hubungan internasional bahkan konflik, hal ini menjadi tangtangan baru bagi keamanan nasional dan internasional. Bersamaan dengan terorisme dan non-proliferasi senjata nuklir dan senjata pemusnah masal lainnya, *cyberspace* mewakili satu dari banyak ancaman inkonvensional terhadap kemanan internasional (NATO Review, 2011 http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/EN/index.htm [12/3/17]).

Fitur-fitur khusus dari *cyberspace* dan dampak serangan *cyberattack* multinasional inilah yang menekankan perlunya kebijakan publik dengan komponen internasional yang lebih kuat, *cyberattack* menjadi alat instrument untuk menyampaikan *cyberpower*. Karena dari sifat *cyberspace* yang asimetris dan transnasional, ancaman *cyber* mewakilkan sebuah tantangan untuk para pemimpin politik dunia, yang memerlukan upaya diplomasi mirip dengan upaya dalam memerangi terorisme (Maiorescu, 2015:1).

C*yberspace* bisa digunakan sebagai alat sebuah ancaman dari kalangan teroris, kriminal, atau dari prespektif polikal-militer, tergantung pada maksud dan tujuan dari si penyerangnya sendiri. Berkenaan dengan aktor yang menggunakan *cyberspace* sebagai wilayah militer, serangan dapat di lancarkan oleh badan struktur pemerintah, baik militer, intelejen atau badan lainnya. Serangan

dilancarkan oleh para peretas *(hacker)* yang loyal terhadap pemerintah atau yang disponsori oleh pemerintah dan oleh aktor-aktor non-negara, termasuk teroris (Halle, 2009:1).

Salah satu kasus yang menarik perhatian dunia terjadi pada 1 November 2005 kasus *Cyberattack* yang dilakukan oleh Tiongkok ke Amerika Serikat, serangan ini memiliki *codename* (kata sandi) *"Titan Rain".* Serangan ini bertujuan untuk menyusup dan memetakan jaringan komputer angkatan bersenjata Amerika Serikat (Halle, 2009:12). *Titan Rain* secara khusus menargetkan beberapa jaringan militer dengan cepat. Pada pukul 10.23 malam, serangan tersebut mengenai US Army Information Systems Engineering Command di Fort Huachuca, Arizona. Pada pukul 01:19, ditemukan kerentanan yang sama di dalam komputer di Defense Information Systems Agency di Arlington, Virginia. Pukul 3.25, serangan tersebut menginfeksi Naval Ocean Systems Center, di San Diego, California. Akhirnya, serangan tersebut berhenti pada pukul 4:46, setelah menemukan kerentanan yang sama di instalasi Pertahanan Luar Angkasa dan Pertahanan Angkatan Darat Amerika Serikat di Huntsville, Alabama (Thornburgh, 2005 http://content.time.com/time/nation/article/0,8599,1098371,00.html [12/3/17]).

Serangan *Titan Rain* ini sangat merugikan Amerika serikat, menurut Mayor Jenderal Willim Lord, angkatan udara Amerika Serikat serangan ini telah menyebabkan terdownloadnya 10 hingga 20 terabyte data dari DoD's Non-Classified Internet Protocol Router Network (NIPRNet) (Onley, 2006 http://gcn.com/articles/2006/08/17/red-storm-rising.aspx, [12/3/17]). *Titan Rain* terbukti sangat efektif dalam urusan *cyberespionage*. Setelah ditelusuri ternyata

terlacak bahwa IP *Address*-nya beralamat di Tiongkok, namun belum dapat dipastikan jika memang pemerintah Tiongkok yang berada dibelakang semua ini. Tetapi Amerika Serikat yakin jika pemerintah Tiongkok turut andil dalam serangan *Titan Rain* tersebut, meskipun belum ada konfirmasi lebih lanjut. Dalam kasus ini *cyberpower* terbukti efektif untuk menjadi instrument yang koersif (Halle, 2009:19-20).

Contoh kasus lainnya yang terkenal adalah *Estonia Web War* yang terjadi pada 2007. Estonia merupakan negara pecahan Uni Soviet, semenjak merdeka pada tahun 1991 Estonia mulai membangun negaranya sendiri untuk menjadi negara yang mandiri. Namun perkembangan dan pengelolaan Internet di Estonia pada saat itu masih masih bergantung pada negara tetangganya Rusia. Padahal Estonia merupakan negara pengguna internet terbesar perkapitanya dibanding dengan negara lain. Hal ini menjadikan Estonia rentan terhadapa *cyberattack* dan *cyberthreat* dari negara lain (Halle, 2009:24)

Estonia Web War berawal dari keinginan pemerintah Estonia berkeinginan untuk memindahkan monument perang peninggalan Uni Soviet di kota Tallinn pada 2007. Monument tersebut dianggap sebagai bekas pengaruh komunisme yang pernah disebarkan oleh Uni Soviet dan perlu disingkirkan karena sekarang Estonia telah menjadi negara merdeka dan liberal. Rusia sebagai negara pewaris dari Uni Soviet merasa keberatan dengan hal tersebut dan berencana untuk memperotes keras usaha dari Estonia tersebut. Enggan menggunakan cara *hard power* karena akan meningkatkan tensi di dunia, Rusia menggunakan konsep *cyberpower* dengan cara menalcarkan *cyberattack* untuk menyerang Estonia dan menyampaikan

maksud dan kepentingan Rusia disana. Selain itu ini juga merupakan upaya agar Estonia kembali bergabung dengan Rusia. (Halle, 2009:26)

Serangan tersebut melumpuhkan fasilitas-fasilitas publik dan pemerintahan Estonia selama beberpa bulan. Estonia yang kewalahan menangkal *cyberattack* Rusia akhirnya di bantu oleh *North Atlantic Treaty Organization* (NATO) dan berhasil untuk menangkal serangan tersebut. Pada akhirnya upaya yang dilakukan Rusian tidak membawakan hasil dan Estonia pun akhirnya mendirikan *Estonian Cyber Defense Center* yang disponsori oleh NATO. Dalam kasus ini *cyberpower* terbukti tidak efektif dalam menjadi instrument yang koersif (Halle, 2009:24-32).

Berkembangnya *cyberpower* menjadikannya instrumen yang tepat, efektif dan akurat untuk meraih berbagai keuntungan dan pengaruh sesuai dengan target dan keinginan. Penggunaan *cyberpower* terbukti lebih efektif daripada harus melakukan serangan fisik, karena tidak harus menggunakan pasukan nyata dan tidak perlu adanya korban jiwa. Hal ini berkaitan dengan apa yang akan diteliti peneliti, yaitu Amerika Serikat yang menggunakan *Cyberpower* untuk menghentikan program nuklir Iran.

Berawal dari rencana Iran untuk mengembangkan teknologi nuklir pada awal 1956 dengan didirikannya "Pusat Atom Universitas Teheran", Amerika Serikat dan Iran berkerjasama meluncurkan program nuklir (Crail, 2011: 7). Saat itu, Iran yang dipimpin Shah, memang memiliki hubungan baik dengan Amerika Serikat. Kerjasama tersebut diwujudkan dengan dibangunnya *The Teheran Nuclear Research Center* (TNRC) yang dioperasikan oleh *Atomic Energy Organization Of Iran* (AEOI) pada tahun 1974. TNRC dilengkapi dengan suplai 5 Mega Watt

reaktor nuklir. Reaktor tersebut biasa bekerja dengan uranium yang diperkaya sebanyak 93%, padahal uranium yang berada di atas 90% dapat digunakan dalam pembuatan bom atom (Cordesman and Al Rodhan, 2006: 59).

Namun begitu, Amerika Serikat tetap memberikan pembatasan dalam kerjasama dan mekanisme keterlibatan para teknisi Iran. Amerika Serikat tidak memperkenankan para teknisi Iran untuk terlibat langsung dalam penginstalan dan pengoperasian reaktor nuklir. Sementara ketika menjalin kerjasama dengan Perusahaan Reaktor Nuklir Framatome dari Perancis, 350 teknisi Iran mendapat pelatihan khusus untuk masalah nuklir (Cordesman and Al-Rodhan, 2006:60).

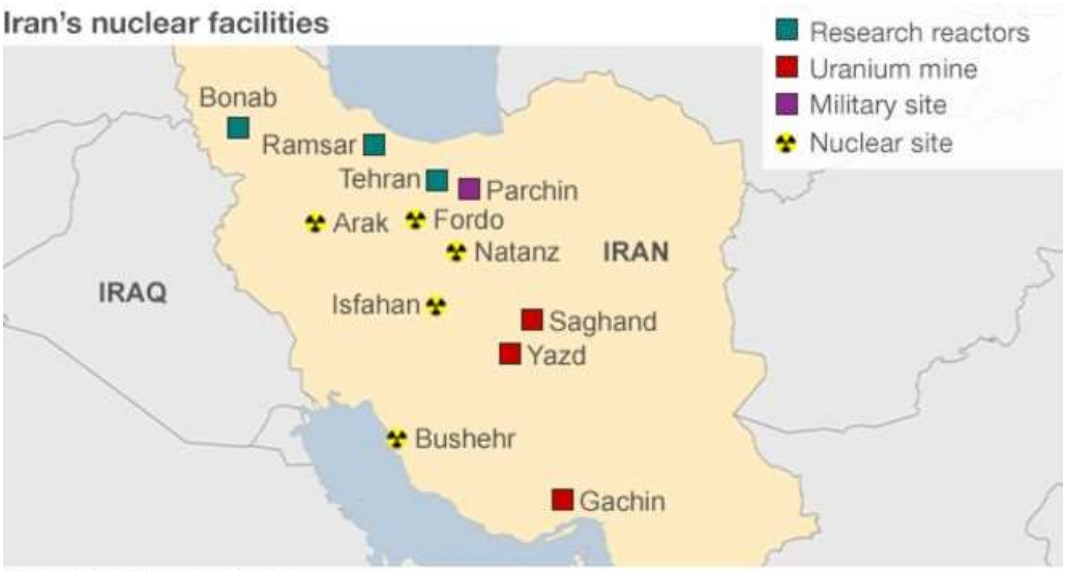
Setelah didirikannya AEOI, pemerintah Iran mulai menginvestasikan modal yang besar untuk mendirikan 23 reaktor atom dengan kapasitas 23.000 MW. Semenjak itu, Iran tidak hanya bekerjasama dengan Amerika Serikat saja, tapi dengan Jerman, Inggris, Perancis, Kanada, Italia, dan Belgia. Hal ini dilakukan dalam pengiriman tenaga ahli nuklir Iran untuk mengikuti pelatihan dan kontrak kerjasama pembangunan reaktor. Mulai tahun 1974 hingga 1978 didirikan Pembangkit Listrik Tenaga Atom Bushehr (Iran I dan II) oleh Jerman, Pembangkit Listrik Tenaga Atom Karun (Iran III dan IV) oleh Perancis, Pembangkit Listrik Tenaga Atom Isfahan (Iran V dan VI) oleh Jerman, dan Saveh (Iran VII dan VIII) oleh Jerman (Cordesman and Al Rodhan, 2006: 61).

Pada tahun 1980 pembangunan tersebut terhenti karena terjadi perang antara Iran dan Irak. Reaktor yang masih dalam proses penyelesaian dibom oleh Irak yang mengakibatkan kerusakan parah. Pada masa Presiden Ali Akbar Rafsanjani, Iran berupaya untuk melakukan pembangunan reaktor nuklir Bushehr

yang sempat terhenti. Iran meminta Jerman dibawah perusahaan Kraftwerk Union untuk melakukan kerjasama dalam pembangunan reaktor Bushehr (Global Security. 2013 http://www.globalsecurity.org/wmd/world/iran/bushehr.htm [5/4/17]). Akan tetapi, Jerman kemudian membatalkan perjanjian tersebut karena mendapat tekanan dari Amerika Serikat. Iran terus berupaya untuk melakukan kerjasama dengan Italia, Republik Ceko, Spanyol serta Argentina, agar mereka mau membantu penyelesaian pembangunan reaktor Bushehr. Akan tetapi, Amerika Serikat terus saja menekan negara-negara tersebut yang akhirnya mengakibatkan kegagalan kerjasama.

Proyek pembangunan reaktor nuklir Iran yang terhambat karena pemutusan kerjasama oleh beberapa negara Barat, ternyata tidak menghentikan Iran dalam membangun reaktor nuklir tersebut. Dengan memanfaatkan kekayaan intelektual anak bangsa sendiri, Iran mampu menguasai teknologi eksplorasi pengayaan uranium dan mengkonversikan uranium menjadi konsentrat uranium. Akhirnya pada 11 Februari 2003, Iran mendeklarasikan kemampuannya dalam memperkaya uranium (Tempo. 2004. http://majalah.tempointeraktif.com/id/arsip/2004/09/27 [12/3/17]).

Iran berusaha untuk mengembangkan pengayaan uraniumnya secara mandiri karena sikap ketergantungan akan bahan bakar nuklir dari asing akan menghambat pasokan bahan bakar nuklir. Pengembangan nuklir Iran ini kemudian mendapat protes dari berbagai pihak yang mencurigai adanya kepentingan militer



Sumber: http://www.bbc.com/news/world-middle-east-11927720

Gambar 1.1
Peta Fasilitas Nuklir Iran

Setelah Revolusi Islam, Iran semakin mengembangkan tenaga nuklir yang mereka klaim untuk dijadikan sebagai tenaga pembangkit listrik. Namun badan rahasia Amerika Serikat, *Central Intelligence Agency* (CIA), menilai bahwa Negara tersebut belum perlu mengganti tenaga listriknya dengan nuklir. Sehingga memunculkan kecurigaan dari Negara-negara barat terutama Amerika Serikat bahwa pengembangan nuklir Iran bertujuan untuk membuat bom atom. Pada tahun 2003, *Internasional Atomic Energi Agency* (IAEA) menyatakan bahwa mereka menemukan pabrik uranium berkadar tinggi di Natanz, Iran. IAEA menemukan bahwa Iran telah melakukan pelanggaran aturan teknis yang telah digariskan NPT, karena Iran terbukti mengimpor sebanyak 1,8 ton material nuklir dari Cina dalam bentuk unsur (UF6, UF4 dan UO2) yang digunakan untuk manufaktur logam dan kandungan uranium yang diperkerjakan dalam reaktor nuklir tersebut sebesar 93% yang biasanya dapat dibuat untuk menjadi bom atom (*The Nuclear Threat Initiative*,

2011 http://www.nti.org/e_research/profiles/Iran/Nuclear/index.html [5/4/17]). Produksi uranium Iran sempat di berhentikan, namun pada tahun 2006 Iran kembali memproduksi setelah mengadakan perjanjian dengan *International Atomic Energy Agency* (IAEA) (CNN Indonesia. http://www.cnnindonesia.com/internasional/20140922155915-120-3985/10-fakta-mengenai-nuklir-iran/ [10/4/17]).

Pada tanggal 23 Desember 2006, Dewan Keamanan PBB mengeluarkan resolusi 1737 yang isinya menyuruh Iran untuk menghentikan proses pengayaan uraniumnya. Namun Iran mengacuhkan resolusi ini dan tetap mempertahankan haknya untuk menggunakan energi nuklir demi tujuan-tujuan damai sebagaimana yang dijamin di dalam *Non-Ploriferation Treaty*. Pada tanggal 23 April 2007, Dewan Keamanan Perserikatan Bangsa-bangsa (PBB) mengeluarkan resolusi 1747 dan memberikan tenggat waktu dua bulan bagi Iran untuk menghentikan proses pengayaan yang ditambah dengan tekanan terhadap Iran untuk menanggalkan haknya dalam penggunaan energi nuklir untuk tujuan-tujuan damai (LIPI. 2007 http://lipi.go.id/berita/keserakahan-as-dan-nuklir-iran/1842 [10/4/17]).

Iran yang masih menjalankan pengembangan nuklirnya membuat Negara-negara barat khawatir terutama Amerika Serikat. Kegiatan program nuklir yang dilakukan Iran diangga oleh Amerika Serikat dapat mengancam kepentingan utama Amerka Serikat di Timur Tengah. Pertama, adalah kepentingan untuk mengamankan dan memastikan kelancaran distribusi minyak dari kawasan teluk Persia ke Amerika Serikat dan negara-negara industri lainnya. Kepentingan kedua adalah memastikan bahwa baik aktor negara maupun non-negara di kawasan

tersebut tidak mengembangkan, memperoleh, atau menggunakan senjata pemusnah massal atau *Weapon of Mass Destruction.* Kekhawatiran Amerika Serikat terhadap nuklir Iran tentunya mempunyai alasan karena ditakutkan Iran akan menyerang Israel, yang kemudian berpotensi mengundang aksi balasan dari Israel dan akhirnya berujung pada perang nuklir (Bowman dan Biden. 2008:85). Kemudian kepentingan yang ketiga adalah membantu kawasan tersebut agar tidak menjadi sarang, panggung aksi, ataupun pengekspor ekstrimis Islam yang mengandalkan kekerasan. Kebencian Amerika Serikat terhadap teroris dan usaha mereka dalam memberantas teroris dilandasi oleh aksi-aksi nekat kelompok teroris yang dapat membuat kekacauan dan akhirnya mengganggu kepentingan Amerika Serikat (Bowman dan Biden. 2008:90). Belum lagi ketakutan Amerika Serikat jika sampai senjata pemusnah massal seperti teknologi nuklir jatuh ke tangan teroris, tentu akibat buruknya akan berlipat ganda.

Israel yang merasa terancam akan program nuklir Iran terus menerus meminta bantuan Amerika Serikat untuk membantu menyerang Iran agar menghentikan program nuklirnya dengan cara meluncurkan serangan udara ke fasilitas-fasilitas reaktor nuklir Iran. Hal ini menjadi dilema tersendiri bagi Amerika Serikat yang diantaranya adalah Amerika harus mempertahankan eksistensi dan keamanan sekutunya Israel di Timur Tengah dan mempertahankan hubungan keduanya agar tetap terjaga. Disisi lain Amerika Serikat sudah terlibat dalam 2 peperangan di Timur Tengah dengan Irak dan Afganistan yang dianggapnya sudah cukup menyita banyak tenaga militernya dan ekonomi negaranya. Dengan mempertimbangkan hal tersebut, Bush dengan lugas menyatakan bahwa Amerika

Serikat tidak bisa melakukan serangan udara ke Iran. Amerika Serikat pun tidak menyerang Iran secara langsung. Tetapi, menggunakan cara lain untuk memenuhi permintaan Israel yakni dengan memanfaatkan program *cyber* yang telah mereka susun pada tahun sebelumnya (Zetter, 2014:212).

Dalam upaya menghentikan program nuklir Iran, pada akhir tahun 2007 Bush menerima dana 400 juta US dollar untuk mendanai operasi terkait nuklir Iran. Dana tersebut digunakan untuk pencarian data intelejen, operasi politik untuk mengganggu kestabilan politik dan pemerintahan Iran dan juga upaya sabotase terkait. (Pratama 2016:382) Salah satu upaya tersebut adalah menggunakan *cyberpower* dengan cara melancarkan *cyberattack* terhadap fasilitas pengembangan program nuklir Iran. Dibawah pimpinan presiden George W.Bush, Amerika memulai membangun c*yberweapon* yang rumit untuk mencegah Iran menyelesaikan pengembangan senjata nuklir tanpa mengambil resiko serangan militer melawan pasukan Iran (http://www.antaranews.com/berita/254567/as-dan-israel-dalangi-virus-stuxnet [10/4/17]).

Senjata tersebut bernama “Stuxnet” yang merupakan virus komputer yang sangat sulit dipecahkan oleh para ahli keamanan komputer. Tujuannya adalah untuk menghancurkan peralatan *centrifuge* (alat pemisah molekular untuk memurnikan uranium) nuklir Iran dengan mengeluarkan perintah khusus ke perangkat keras kontrol industri yang bertanggung jawab atas tingkat putaran mesin tersebut. Dengan demikian Amerika berharap dapat segera menyusun kembali program penelitian Iran, dan AS berharap agar Israel tidak meluncurkan serangan militer

pre-emptive (https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/ [10/4/17]).

Keuntungan dari operasi *cyberattack* ini bila dibandingkan dengan bentuk serangan langsung bisa dilihat dari adanya kemungkinan *zero victim* baik dari target maupun pihak penyerang. Stuxnet memiliki cara kerja yang digambarkan bisa menghancurkan sebuah infrastruktur tanpa menimbulkan indikasi yang mencurigakan bagi target karena serangn ini akan berjalan secara sistematis dan diam-diam. Secara lebih lengkap, yang coba ditawarkan pada saat itu adalah sebuah serangan yang melibatkan proses pengkodean digital yang sangat presisi, yakni sebuah serangan yang hanya akan berjalan ketika menemukan situasi atau kondisi tertentu di dalam fasilitas target. Serangan ini juga diyakini bisa menimbulkan efek merusak pada piranti fisik, bukan melalui ledakan, namun melalui serangkaian proses sabotase yang cukup panjang. Bila serangan ini berjalan secara lancar, maka infrastruktur nuklir Iran pun akan mengalami masalah yang berimbas pada mundurnya target produksi yang diharapkan oleh Iran. Dan meskipun nantinya serangan ini diketahui Iran, maka mereka akan kesulitan untuk menyelesaikan dan menghapus akar dari permasalahan ini. Selain itu, mereka akan menemui kesulitan untuk mengidentifikasi asal serangan hal ini mengingat tujuan AS yang nampaknya ingin menghindari timbulnya medan perang baru di Timur Tengah (Pratama, 2016:382)

Tidak seperti kebanyakan malware, Stuxnet tidak dimaksudkan untuk menciptakan uang atau mencuri data kepemilikan. Para ahli telah menyimpulkan, setelah mempelajari Stuxnet selama berbulan-bulan bahwa virus ini merupakan

jenis malware baru yang bisa menjadi template bagi penyerang yang ingin meluncurkan serangan digital pada target fisik di seluruh dunia. Bahkan tidak memerlukan internet untuk memulai serangan. Jadi dengan kata lain, Stuxnet dapat menghancurkan target fisik/perangkat fisik bukan hanya untuk merusak perangkat digital (The Christian Science Monitor. 2010 https://www.csmonitor.com/USA/2010/1116/... [10/4/17]). Hal ini diperkuat oleh pernyataan Kim Zetter, bahwa Stuxnet yang masuk ke fasilitas nuklir di Natanz, masuk melalui piranti USB. USB yang telah terkena virus Stuxnet dari internet ini selanjutnya dibawa oleh pegawai Natanz dan secara tidak sadar membawa masuk ke Natanz melalui laptop mereka yang digunakan untuk mengatur system operasi yang ada di sana. Stuxnet pada periode ini melakukan serangan ke Natanz dengan cara memanipulasi arus gas di dalam mesin pengelolah uranium (Zetter 2014:317).

Mesin pengolah uranium yang ada di Natanz memiliki beberapa susunan rangkaian yang terdiri dari beberapa pasang *centrifuge*, dan masing-masing rangkaian tersebut memiliki fungsinya masing-masing. Stuxnet tidak menyerang semua rangkaian ini, ia hanya menyerang beberapa bagian dengan mengirim sinyal palsu untuk menutup rangkaian agar tekanan gas yang ada di dalam rangkaian tersebut meningkat dan menyebabkan gas ini gagal diolah dan dibuang. Namun dalam proses serangan ini, Stuxnet membutuhkan waktu yang cukup lama untuk menjalankan serangan ini — sekitar 35 hari untuk mengumpulkan data dan ketika sebuah serangan telah dilakukan, stuxnet kembali mebutuhkan 35 hari lagi untuk melakukan serangan baru (Zetter 2014:317).

Selama kurun waktu 2007, Iran melakukan penambahan *centrifuge* sebanyak 2952 unit. Pemasangan unit ini memang berjalan lancar, akan tetapi, setelah semua unit terpasang di bulan November di tahun yang sama, mulai muncul beberapa masalah. Bila berdasarkan perkiraan teknisi Iran, seharusnya mereka bisa memproses sebanyak 1670 kg gas dalam kurun waktu Februari hingga November, namun dalam kenyataan yang terjadi, mereka hanya mampu memproses sebanyak 1240 kg saja (Zetter 2014:507). Jumlah kerusakan centrifuge pada tahun tersebut pun disinyalir sebesar 20% lebih tinggi dari perkiraan akibat pemakaian rutin. Stuxnet melakukan tugas ini dengan cara mengirim perintah yang salah ke *Programmable Logic Controller* (PLC) yang menyebabkan beberapa katup di *centrifuge* tidak terbuka sehingga tekanan udara didalamnya menjadi meningkat dan mengakibatkan materi di dalam *centrifuge* tersebut dianggap sebagai proses yang gagal dan dibuang secara percuma.

Untuk memantapkan penggunaan *cyberpower*-nya terhadap Iran, Amerika Serikat mengkampanyekan tentang protesnya menentang program nuklir Iran menggunakan media yang ada di *cyberspace*. Seperti postingan di website pemerintah Amerika tentang 2010 Quadrennial Diplomacy and Development Review (QDDR) sebagai dasar untuk menanggapi ancaman *nonproliferation weapon* seperti Nuklir yang dimiliki Iran (*U.S Government.* 2010 www.state.gov/s/dmr/qddr/241018.htm [15/4/17]). Dan postingan Amerika lainnya yang merilis daftar negara-negara yang mensponsori aksi terorisme, salah satunya adalah Iran dan program nuklirnya sebagai salah satu rencananya untuk mensponsori terorisme (U.S. Departement of State

https://www.state.gov/j/ct/rls/crt/2010/170260.htm). Lalu berbagai statement Amerika Serikat yang menentang program nuklir Iran yang diviralkan melalui media berita di *cyberspace* asal Amerika, seperti CNN dan VOA. Amerika juga mem-*blow up* protest yang di lakukan masyarakat Iran yang disebut dengan "Iranian Green Movement" yang menuntut turunnya presiden Ahmadinejad. Dalam protesnya, selain menuntut turunnya Ahmadinejad sebagai presiden, mereka juga menyuarakan ketidak peduliannya lagi dengan apa yang dilakukan rezim tersebut mengenai program nuklir Iran. Meskipun kabar ini berusaha di redam oleh pemerintah Iran dari dunia luar, Amerika Serikat melalui CNN mampu menyebar luaskan berita ini ke dunia luar (CNN: Iran protests, 11 Feb 2010 https://www.youtube.com/watch?v=dfxYfYsVc5U dan Iran Protest: Live Blog https://www.theguardian.com/news/blog/2010/feb/11/iran-protests-22-bahman [15/4/17]).

Upaya pengembangan program nuklir Iran memicu berbagai reaksi element masyarakat, khususnya masyarakat Amerika Serikat yang mengecam keras tindakan Iran untuk mengembangkan nuklir. Penggiringan opini masyarakat global mengenai bahayanya Iran jika memiliki senjata nuklir oleh pemerintah Amerika Serikat juga di bantu berbagai elemen masyarakat salah satunya organisasi *United Against Nuclear Iran* (UANI) yang merupakam organisasi advokasi non-partisan dan non-profit di Amerika Serikat yang berusaha "mencegah Iran memenuhi ambisinya untuk menjadi negara adidaya regional yang memiliki senjata nuklir". UANI terus menyuarakan agar Iran menghentikan program nuklirnya baik di dunia

nyata atau di *cyberspcace* (UANI http://www.unitedagainstnucleariran.com/about [15/4/17]).

UANI gencar mengkampanyekan suaranya tentang bahayanya jika Iran memiliki senjata nuklir di *cyberspace*. Melalui websitenya www.unitedagainstnucleariran.com, UANI terus mengupdate perkembangan program nuklir Iran dan kampanyenya ke seluruh dunia untuk mencegah Iran memiliki senjata nuklir (http://www.unitedagainstnucleariran.com/). Reaksi serupa juga di tunjukan oleh masyarakat Iran, mereka mendirikan *Campaign Against Sanctions and Military Intervention in Iran* (CASMII) yang merupakan sekelompok akademisi, pelajar dan profesional latar belakang Iran dan non-Iran yang dibentuk untuk menentang sanksi terhadap Iran oleh Amerika Serikat. Melalui websitenya CASMII mengkampanyekan perdamaian di Iran, protes terhadap sanksi dan intervensi Amerika Serikat terhadap iran keseluruh dunia (http://www.campaigniran.org/casmii/ [15/4/17]).

Memasuki tahun 2009, AS memiliki presiden baru, Barrack Obama. Sebelum Bush lengser, ia sempat mengundang Obama untuk membahas masalah yang sedang dihadapi di Natanz. Ia mengatakan bahwa operasi yang dilakukan oleh Stuxnet memang berhasil melemahkan produksi nuklir di Iran, akan tetapi Stuxnet masih membutuhkan waktu lagi untuk bisa benar-benar menghentikan produksi nuklir di Iran. Untuk melanjutkan stuxnet yang sedang berlangsung di Iran, tentu akan membutuhkan persetujuan dari presiden terpilih selanjutnya, oleh karena itu ia ingin agar Obama tetap melanjutkan dan mengembangkan proyek Stuxnet tersebut (Zetter, 2014:512).

Setelah resmi menjabat, presiden Obama mempercepat rencana presiden Bush. *Cyberattack* yag dilakukan Amerika ini telah berhasil menunda program nuklir Iran selama 5 tahun. Stuxnet berhasil membelikan mereka waktu. Yang pertama adalah memberikan Amerika waktu untuk berpindah administrasi pemerintahan Bush ke Obama tanpa memiliki masalah Isu penghentian program nuklir Iran oleh Amerika melalui Stuxnet terbongkar ke publik. Dan yang kedua memberikan waktu untuk Obama mencari alternatif lain untuk menghentikan nuklir Iran, seperti pemberian sanksi dan sebagainya. (The Jerusalem Post. http://www.jpost.com/Iranian-Threat/News/Obama-secretly-ordered-cyber-attacks-on-Iran [15/4/17]).

Setelah kekacauan yang terjadi di fasilitas program nuklir Iran di Nathanz, Iran akhirnya mengetahui penyebab kekacauan ini disebabkan oleh malware. Butuh waktu hampir setahun untuk Iran mengidentifikasi jenis virus apa yang menyerang dan dari mana asalnya. Setelah diteliti, virus yang menyerang itu memiliki tanda enskripsi yang spesial. Enskripsi ini hanya dimiliki oleh negara yang memilik kekuatan teknologi dalam bidang *cyber* yang maju. Melalui proses penelitian yang panjang Iran menarik kesimpulan bahwa Amerika Serikat berada dibelakang semua ini (Zetter, 2011 https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/ [15/4/17]).

Protes keras dilancarkan Iran terhadap Amerika Serikat mengenai *cyberattack* ke fasilitas nuklir Iran. Dilansir dari media Aljazeera, Iran menuduh Amerika melakukn serangan tersebut akibat merasa terancam kepentingannya ditimur tengah. Namun tuduhan itu jelas disangkal oleh Amerika, meskipun

Amerika mengakui jika mereka mampu untuk melakukan *cyberattack* ke Iran (Aljazeera News http://www.aljazeera.com/news/middleeast/2010/09/201099.html [15/4/17]).Untuk mengantisipasi serangan selanjutnya Iran belajar dari pengalman dalam menghadapi virus Stuxnet. Mereka memperkuat sistem pertahanan *cybersecurity*-nya dan mengklaim berhasil menangkal serangan virus stuxnet yang terbaru pada 2012. Iran kembali mengecam tindakan Amerika tersebut, namun Amerika enggan berkomentar banyak soal masalah itu. Presiden Amerika Serikat berkomentar "Amerika akan melakukan apa yang harus Amerika lakukan untuk menghentikan Iran mendapatkan senjata nuklir" (BBC News, 2017 http://www.bbc.com/news/world-middle-east-20842113 [15/4/17]).

Hingga akhirnya pada 14 Juli 2015, Iran menyepakati Kesepakatan Nuklir Iran *(Iran Nuclear Dead Framework)* dengan anggota P5+1 (Amerika, Inggris, Russia, Prancis, Tiongkok + Jerman) untuk menghentikan program nuklir Iran dengan imbalan mengangkat seluruh sanksi ekonomi yang pernah dijatuhan ke Iran (VOA Indonesia. 2015 http://www.voaindonesia.com/a/kesepakatan-nuklir-dengan-iran-berhasil-dicapai/2860802.html [8/4/17]).

Untuk menjaga originalitas maka menggunakan beberapa penelitian terdahulu sebagai acuan dan pembanding dalam mengkaji penelitian *cyberpower* Amerika Serikat dalam upaya penghentian program nuklir Iran,. Beberapa penelitian terdahulu yang akan digunakan peneliti yang pertama adalah penelitian yang dilakukan oleh Major Ann M.Halle, seorang senior pilot angkatan udara amerika serikat dan mahasiswi dari School of Advance Air and Space Studies Air

University di Alabama, Amerika Serikat pada tahun 2009 dalam tesis yang berjudul *"Cyberpower As a Coercive Instrument".*

Dalam penelitiannya, Halle memfokuskan untuk menjembatani celah antara ilmu *cyberspace* dan kegunaan praktik dari *cyberpower* sebagai instrument koersif. Dalam analisisnya Halle berpendapat bahwa, walaupun *cyberpower* memiliki potensi sebagai intstrumen koersif namun masih diperlukan pengembangan yang lebih lanjut untuk menjadi sebuah kekuatan yang lebih kuat dan efektif. Halle menyimpulkan dalam penelitiannya penggunaan *cyberpower* tanpa instrument yang lainnya belum membuktikan kemampuan koersifnya begitupun dengan penggunaannya bersamaan dengan instrument lainnya (serangan fisik atau diplomasi). Namun *cyberpower* sudah dapat menjadi iinstrumen yang menjanjikan dimasa depan nanti, penggunaan yang bijak dan tepat sasaran diyakini mampu menjadikannya instrument yang koersif.

Persamaan peneliti dengan penelitian Halle adalah sama-sama membahas tema *cyberpower*. Namun peneliti lebih berfokus pada penggunaan *cyberpower* Amerika Serikat dalam penghentian program nuklir Iran. Sedangkan Halle lebih berfokus pada pembahasan *cyberpower* sebagai instrument yang koersif serta praktiknya di dunia nyata dan studi kasusnya tentang masalah serangan *cyber* terhadap Amerika Serikat, Estonia dan Georgia

Penelitian yang kedua adalah sebuah jurnal yang ditulis oleh Munish Sharma dari Institute for Defence Studies and Analyses yang berada (IDSA) di New Delhi, India. Sharma merupakan seorang rekan kerja dan pemikir di ISDA, jurnalnya yang berjudul *"China's Emergence as a Cyberpower"* diterbitkan pada

maret 2016. Dalam penelitiannya, Sharma menyebutkan bahwa *cyberspace* sudah menjadi area pertarungan antar negara bangsa. Mirip dengan ranah fisik seperti darat, laut dan udara. Keunggulan dalam ranah *cyberspace* memungkinkan suatu negara untuk menggunakan *cyberpower*-nya.

Dalam beberapa tahun terakhir, China telah berinvestasi dalam jumlah yang besar untuk membangun infrastruktur dan kemampuan yang diperlukan angkatan bersenjatanya dalam menggunakan *cyberspace* agar mampu memperkuat *cyberpower*-nya. Dalam penelitiannya, Sharma menyimpulkan bahwa China yang memulai "informatisasi"-nya pada tahun 1982 yang awalnya hanya digunakan sebagai pelayanan sosial dan pemerintah kini telah muncul sebagai negara yang *cyberpower*-nya patut diperhitungkan. seiring dengan bangkitnya perkembangan teknologi di China seperti mengglobalnya Lenovo, Huawei, ZTE dan Alibaba membuat China merasa yakin untuk memulai era *cyber*-nya.

Pembekalan ilmu dan fasilitas untuk mengelolah *cyberpower* telah diberikan kepada angkatan bersenjata China. Munculnya China sebagai kekuatan *cyberpower* baru di dunia patut di perhitungkan. Masih banyak isu yang berkaitan dengan perolehan teknologi China dan praktik spionase ekonomi. Jika tuduhan terhadap China melakukan upaya hacking - seperti Titan Rain dan NetTraveller - adalah benar, maka China telah menunjukkan niatnya untuk menggunakan *cyberpower*. Pada tingkat strategis, organisasi memainkan peran penting; Mereka mencerminkan tujuan, tujuan dan perspektif *power*. Dalam kasus China, tujuan dan perspektif kekuatan *cyber* seolah-olah berbentuk dan didorong oleh kepentingan militer dan ekonomi

Perbedaan peneliti dengan penelitian Sharma adalah dalam konteks studi kasusnya. Sharma lebih memfokuskan pada motif, ancaman, sasaran, strategi dan maksud yang mendorong China untuk mengumpulkan *cyberpower*. Sedangkan peneliti lebih ke penggunaan *cyberpower* Amerika Serikat dalam upaya penghentian program nuklir Iran.

Penelitian yang ketiga dilakukan oleh Herlambang Wisnu Wardhana, seorang alumni Universitas Komputer Indonesia prodi Hubungan Internasional. Beliau merupakan angkatan tahun 2004 dan lulus pada tahun 2009. Skripsi yang berjudul *"Pengaruh Pengembangan Instalasi Nuklir Iran Terhadap Kepentingan Nasional Amerika Serikat Di Timur Tengah"* diterbitkan pada tahun 2009.

Dalam penelitiannya, Herlambang menuliskan tentang pengemembangan instalasi nuklir Iran membawa pengaruh yang besar terhadap kepentingan nasional Amerika Serikat. Timur Tengah mempunyai banyak arti bagi Amerika Serikat, baik itu kepentingan politik, ekonomi, dan keamanan.

Kepentingan politik itu adalah menjaga dan melindungi eksistensi sekutu Amerika Serikat, Israel sebagai representasi Amerika Serikat di Timur Tengah, kepentingan ekonominya berusaha menjamin dan menguasai suplai minyak bagi industri Amerika Serikat, serta kepentingan keamanannya adalah melindungi pangkalan militer Amerika Serikat di Timur Tengah dan mempersenjatai sekutu Amerika Serikat di Timur Tengah sebagai bentuk antisipasi terhadap kekuatan militer Iran.

Penelitian yang diambil oleh Herlambang memiliki kesamaan dengan peneliti yaitu membahas tentang program nuklir Iran dan pengaruhnya terhadap

kepentingan Amerika Serikat. Namun perbedaannya adalah peneliti lebih menekankan terhadap *cyberpower* Amerika Serikat dalam upaya penghentian program nuklir Iran. Herlambang tidak mejabarkan upaya apa yang dilakukan Amerika Serikat untuk menghentikan Iran dalam mengembangkan program nuklir tersebut secara jelas. Beliau lebih focus terhadap dampak dari pegaruh pengembangan nuklir Iran terhadap kepentingan Amerika Serikat.

Berdasarkan alasan-alasan tersebut yang menjadi dasar pertimbangn peneliti untuk mengadakan penelitian dengan judul:

"*Cyberpower* Amerika Serikat Dalam Upaya Penghentian Program Nuklir Iran".

Adapun ketertarikan peneliti untuk meneliti dan mengangkat isu tersebut didukung oleh beberapa mata kuliah disiplin Ilmu Hubungan Internasional, diantaranya adalah sebagai berikut:

1. Hubungan Internasional di Kawasan Amerika, merupakan matakuliah yang menjelaskan tentang profil Amerika dalam bidang politik,ekonomi, social dan budaya. Terutama tentang kebijakan-kebijakan yang biasa di ambil oleh Amerika Serikat dalam menanggapi fenomena hubungan internasional dunia.
2. *Information and Communication Technology for International Relation*, dalam mata kuliah ini mempelajari berbagai kegunaan teknologi informasi dan komunikasi dalam Hubungan Internasional. Serta memperkenalkan bentuk-bentuk penerapannya dalam Hubungan Internasional seperti, *E-diplomacy, digital Diplomacy, Cyber Diplomacy, Cyber Security* dll.

3. Komputer Aplikasi HI-VI *(Cyberlaw & Cybercrime (Organized Crime))*, merupakan mata kuliah yang menjelaskan tentang kasus *Cybercrime* dan *cybersecurity* yang ada di dunia, serta menjadi acuan terhadap peran Amerika dalam menggunakan kekuatan *Cybersecurity*-nya dalam menjalankan *cyberpower* Amerika Serikat terhadap upaya menghentikan program nuklir Iran.
4. Hubungan Internasional di Timur Tengah dan Afrika, merupakan mata kuliah yang membahas dinamika perkembangan hubungan internasional di Timur Tengah. Mata kuliah ini menjadi pendukung penelitian karena Iran merupakan negara yang terletak di wilayah Timur Tengah serta pernah di pelajari di mata kuliah tersebut.
5. Studi Keamanan Internasional, dalam mata kuliah ini mempelajari konsep keamanan suatu Negara yang menjadi faktor penting dalam kehidupan bernegara suatu bangsa. Berdasarkan mata kuliah ini peneliti menilai pentingnya kesepakatan dan persetujuan dari Negara-negara di dunia jika suatu Negara mengembangkan sebuah teknologi (senjata Nuklir) yang dapat mengancam keamanan Negara lainnya.

1.2 Rumusan Masalah

1.2.1 Rumusan Masalah Mayor

"Bagaimana *cyberpower* Amerika Serikat dalam Upaya Penghentian Program Nuklir Iran?"

1.2.2 Rumusan Masalah Minor

1. Bagaimana Amerika Serikat menggunakan *cyberpower* untuk menghentikan program nuklir Iran?
2. Apa alasan Amerika Serikat menggunakan *cyberpower* untuk menghentikan program nuklir Iran?
3. Apa hasil *cyberpower* Amerika Serikat terhadap penghentian program nuklir Iran?

1.2.3 Pembatasan Masalah

Isu tentang rencana penggunaan *cyberpower* Amerika Serikat dalam upaya penghentian program nuklir Iran sudah muncul sejak dari era kepemerintahan Presiden George W.Bush pada Tahun 2007. Stuxnet berhasil melakukan tugasnya untuk memperlambat produksi urainium dengan merusak peralatan *centrifuge*. Pada tahun 2009, Obama terpilih menjadi presiden dan segera melaksanakan kembali rencana presiden Bush dalam menggunakan *cyberpower* untuk menghentikan program nuklir Iran. Dengan penggunaan *cyberpower* Amerika mampu memperlambat Iran menciptakan senjata nuklir dan memberi waktu Amerika serikat untuk menyusun rencana yang kongkrit untuk menghentikan program nuklir Iran, dan pada Juli 2015 Iran menyetujui kesepakatan *Iran Nuclear Deal Framework.* Sehingga batasan masalah yang diambil peneliti adalah mulai dari 2007 hingga 2015.

1.3 Maksud dan Tujuan Penelitian

1.3.1 Maksud Penelitian

Penelitian ini dimaksudkan untuk mengetahui sejauh mana *cyberpower* Amerika Serikat dalam Upaya Penghentian Program Nuklir Iran.

1.3.2 Tujuan Penelitian

Penelitian ini memiliki beberapa tujuan antara lain:

1. Mengetahui bagaimana Amerika serikat menggunakan *cyberpower* untuk menghentikan program nuklir Iran .
2. Mengetahui alasan Amerika Serikat menggunakan *cyberpower* untuk menghentikan program nuklir Iran.
3. Mengetahui hasil *cyberpower* Amerika Serikat terhadap penghentian program nuklir Iran

1.4 Kegunaan Penelitian

1.4.1 Kegunaan Teoritis

Secara teoritis, hasil dari penelitian ini diharapkan dapat memperkaya kajian *cybepower* dalam Hubungan Internasional dan menjadi sumber referensi pengetahuan terkait perkembangan studi hubungan internasional di kawasan Amerika Serikat terutama bagaimana *cyberpower* menjadi sarana baru bagi Amerika Serikat untuk mencapai kepentingan nasionalnya. Serta dapat menambah keilmuan mengenai penggunaan konsep *cyberpower* yang di laksanakan oleh negara-negara di dunia untuk menyampaikan tujuan kebijakan luar negerinya.

1.4.2 Kegunaan Praktis

1. Diharapkan menambah wawasan dan ilmu pengetahuan serta dapat bermanfaat bagi para pembaca khususnya Program Studi Ilmu Hubungan Internasional mengenai *cyberpower* yang di lakukan oleh Amerika Serikat.
2. Sebagai bahan referensi bagi penstudi Hubungan Internasional.
3. Sebagai bahan referensi bagi Pemerintahan Republik Indonesia, dan Kementrian Luar Negeri dalam mengkaji isu *cyberpower* terutama dalam studi kasus Amerika Serikat.