IMPLIKASI PERANG SIBER ANTARA ISRAEL, AMERIKA SERIKAT DAN IRAN MELALUI *OLIMPIC GAME OPERATION* TERHADAP FASILITAS PROGRAM NUKLIR IRAN PADA PERIODE PEMERINTAHAN MAHMOUD AHMADINEJAD: PERANG SIBER STUXNET 2010

Ayunita Harianja[1], Adi Rio Arianto[2], M. Chairil Akbar Setiawan [3]
Fakultas Ilmu Sosial dan Ilmu Politik Universitas Pembangunan "Veteran Jakarta"
ayunitaharianja43@gmail. com, arianto. adirio@gmail. com, mchairilakbars@upnvj. ac. id

ABSTRACT
Iran's nuclear program is the most collaborative in the Middle East region. International criticism regarding the development of the program did not make Ahmadinejad to stop the nuclear program in Iran. The United States decided to take action regarding Iran's nuclear program by cooperating with Israel to carry out attacks on nuclear facilities Israel is located in the Natan region. This attack is known as the Olympic Game Operation with the code "olympics, by creating a dangerous malware virus called Stuxnet, designed with the aim of taking over control over remote industrial systems. This attack is expected to be capable of nuclear facilities in the Natanz region as a whole, but in reality, this attack was only able to have a short-term impact on the damage caused. This study aims to find out how the impact of cyber war involving Israel, the United States, and Iran on Iranian power in the Middle East region. The author uses 3 frameworks of thought in this research, namely International Security, Cyber War, and Cyber Attacks. In this study, the author uses 2 data sources, namely primary data and secondary data. Iran's nuclear facilities are able to have both short and long-term impacts in several fields and are able to influence the position of Iran's power in the Middle East region.

Keywords: Nuclear, Stuxnet Virus, International Security, Cyber War, Cyber Crime, Olympic Game Operation

ABSTRAK
Program nuklir Iran merupakan fenomena yang paling kontroversial di kawasan Timur Tengah. Kecaman dari dunia internasional terkait pengembangan program nuklir tidak membuat Ahmadinejad untuk menghentikan program nuklir di Iran. Amerika Serikat memutuskan untuk mengambil tindakan terkait program nuklir Iran dengan melakukan kerjasama dengan Israel untuk melakukan serangan terhadap fasilitas nuklir Israel yang berada di wilayah Natanz. Serangan ini dikenal dengan nama Olympic Game Operation dengan sandi "olimpiade, dengan menciptakan sebuah virus malware berbahaya yang diberi nama Stuxnet, dIrancang dengan tujuan mengambil alih kontrol atas sistem industri jarak jauh. Serangan ini diharapkan mampu untuk menghentikan fasilitas nuklir di wilayah Natanz secara menyeluruh, namun pada kenyatannya, serangan ini hanya mampu memberikan dampak jangka pendek terhadap kerusakan yang ditimbulkan. Penelitian ini bertujuan untuk mengetahui bagaimana dampak perang siber yang melibatkan Israel, Amerika Serikat dan Iran terhadap kekuatan Iran di kawasan Timur Tengah. Penulis menggunakan 3 kerangka pemikIran dalam penelitian ini yaitu Keamanan Internasional, Perang Siber dan Kejahatan Siber. Dalam penelitian ini, penulis menggunakan 2 sumber data yaitu data primer dan data sekunder. Hasil dari penelitian ini menyatakan serangan siber Stuxnet terhadap fasilitas nuklir Iran mampu memberikan dampak baik jangka pendek maupun panjang dalam beberapa bidang serta mampu mempengaruhi posisi kekuatan Iran di kawasan Timur Tengah.

Kata Kunci: Nuklir, Virus Stuxnet, Keamanan Internasional, Perang Siber, Kejahatan Siber, Olympic Game Operation

PENDAHULUAN
Kajian Nuklir timbul menjadi sebuah fenomena baru ketika nuklir dialih fungsikan sebagai senjata nuklir. Senjata nuklir mampu menghancurkan sebuah wilayah dengan dampak kerusakan yang besar. Senjata nuklir menjadi salah satu senjata yang diminati oleh negara sejak hadirnya kajian aspek keamanan dalam perjanjian Westphalia yang ditandatangani

oleh negara-negara eropa. Isu pengembangan senjata nuklir merupakan isu yang menjadi perhatian sejak pengembangan nuklir muncul pada tahun 1945 yang membuat konteks nuklir selalu dikaitkan dengan militer dan politik suatu negara. Motivasi dari pengembangan senjata nuklir pun menjadi bervariasi. Hal ini menggeser pandangan senjata nuklir yang pada awalnya bertujuan untuk menciptakan rasa aman dan tentram dalam sebuah negara menjadi ajang untuk menunjukkan betapa kuatnya kekuatan militer negara tersebut. Ada beberapa faktor yang mendorong sebuah negara mengembangkan senjata nuklir. Pertama, alasan strategi. Senjata nuklir digunakan sebagai *deterrence* untuk mencegah ancaman militer dari pihak lain, baik ancaman fisik dan non fisik. Selain itu adalah alasan politik. Secara sederhana nuklir menjadi keuntungan bagi negara yang memilikinya untuk menaikkan posisi negara tersebut kedalam pencaturan internasional (Puwanto, 2011 : 3-5).

KekhawatIran dunia internasional akan senjata nuklir dan upaya untuk mencegah pengembangan senjata nuklir yang tidak terkontrol, maka dibuatlah Treaty on the Non-Proliferation of Nuclear Weapons atau lebih dikenal dengan Non-Proliferation Treaty (NPT). Non-Proliferation Treaty merupakan perjanjian yang bertujuan untuk mengatur dan mencengah pengembangan senjata nuklir tanpa pengawasan oleh dunia. Selain itu NPT juga mengatur kerjasama dalam penggunaan nuklir sebagai proses pembuatan senjata nuklir untuk menjaga keutuhan dan kedamaian dunia. NPT sendiri diawasi oleh International Atomic Energy Agency (IAEA) untuk mengecek kepatuhan setiap negara anggota melalui pengawasan yang dilakukan oleh IAEA (Affairs, 2020).

Iran merupakan salah satu negara di Timur Tengah yang memiliki potensi dan kemampuan dalam mengembangkan program nuklir. IAEA menyatakan bahwa Iran memiliki cadangan uranium sebanyak 37 ton. Uranium tersebut dimanfaatkan untuk memenuhi kebutuhan penelitian maupun kebutuhan peningkatan kemampuan teknologi Iran sendiri (Akbar, 2012). Pada masa pemerintahan Sah Pahlevi Iran yang disponsori oleh Amerika Serikat Program *Atom For Peace* untuk terlaksananya program nuklir demi masa depan perdamaian dunia. Dikarenakan hal ini pula hubungan Amerika dengan Iran semakin meningkat. Bila dibandingkan dengan Pemimpin Iran sebelumnya, Presiden Mahmoud Ahmadinejad merupakan Presiden dengan program yang paling kontroversial. Setelah masa kepemimpinan Mohammad Khatami selesai, Mahmoud Ahmadinejad naik untuk menggantikan posisi Khatami.

Ahmadinejad merupakan salah satu Presiden yang kembali menjalankan program nuklir Iran tanpa memperdulikan sanksi dan tanggapan negara lain dan berani menentang Amerika Serikat dan Israel. Kecaman dari dunia internasional tidak membuat Ahmadinejad untuk mengurungkan niatnya. Program nuklir ini juga berkaitan dengan tujuan utama Ahmadinejad dalam janjinya untuk meningkatkan kesejahteraan dan mengurangi tingginya kemiskinan di Iran. Ahmadinejad juga menggunakan program nuklir Iran tersebut sebagai harapan baru untuk menstabilkan kondisi akibat kerusuhan yang terjadi. Permasalahan konflik internal di Iran yang tidak berhenti membuat Mahmoud harus mengambil kebijakan yang bertujuan untuk menjaga keamanan negaranya. Salahsatu konflik domestik yang mampu mengganggu stabilitas Iran adalah kebocoran mengenai data dua program nuklir Iran oleh seorang pemberontak Iran. Mahmoud juga menjadikan program nuklir sebagai alat untuk mencapai persetujuan perdamaian dan penghentian serangan. Pada tahun 2005 IAEA mengeluarkan resolusi dalam menanggapi ketidakpatuhan Iran, namun Ahmadinejad menolak resolusi dengan alasan resolusi tersebut tidak logis. Penolakan yang dilakukan pemerintah Iran ini berhasil membebaskan Iran dari resolusi IAEA. Pada tahun 2006 Iran membuka fasilitas nuklir yang awalnya disegel oleh IAEA. Ketiga progam nuklir ini berada di Natanz, Isfahan dan Pars Tash. Ahmadinejad melalui Dewan Tinggi Kemanan Nasional Iran memberitahukan pembukaan 3 lokasi pengayaan menandakan Iran siap untuk memulai kembali program nuklirnya dan akan

membuka kerjasama dengan Rusia terkait pengembangan program nuklir (Yaphe, 2010).

Sikap Iran yang terus mempertahankan pilihan untuk mengembangkan program nuklir membuat dunia internasional semakin berang. Negara-negara yang mempunyai kepentingan di Kawasan Timur Tengah serta negara negara barat seringkali menunjukkan rasa kekhawatIran mereka menggunakan media massa atas pengembangan program nuklir Iran. Negara-negara yang mempunyai kepentingan di kawasan Timur Tengah juga memberikan respon yang sama seperti negara barat. KekhawatIran ini akhirnya membuat PBB mengambil tindakan dengan memberikan sanksi embargo dan pencabutan ijin serta pemberhentian pengoperasian nuklir di Iran. Sanksi yang diberikan PBB tidak menghentikan tujuan Iran untuk mengembangkan program nuklirnya. Iran yang menunjukkan ketidakpedulian atas respon dunia internasional terkait dengan program nuklirnya membuat dunia internasional kecewa.

Bush yang kala itu menjadi Presiden Amerika Serikat menilai bahwa Iran adalah bagian dari Axis of Evil (Poros Kejahatan). Melihat peristiwa 9/11 yang terjadi beberapa tahun silam membuat Bush berpendapat bahwa Iran mempunyai potensi yang sangat besar untuk menjadi sarang terosisme dan musuh yang berpotensi membahayakan Kawasan Timur Tengah. Bush melihat Iran yang mengembangkan program nuklir sebagai upaya Iran untuk mengancam stabilitas dan perdamaian dunia sekaligus untuk mempersenjatai kelompok teroris di kawasan Timur Tengah (PBS, 2021). Amerika Serikat memutuskan untuk mengambil tindakan terkait program nuklir Iran dengan melakukan kerjasama dengan Israel untuk memberhentikan program nuklir Iran. Amerika Serikat dan Israel membuat virus malware yang bernama Stuxnet (Melysa, 2016). Stuxnet merupakan virus malware berbahaya yang dIrancang untuk mengambil alih kontrol atas sistem industri jarak jauh. Virus ini disebarkan dengan menggunakan perangkat perantara seperti Universal Serial Bus (USB) untuk mendapatkan akses dan membuat pengawasan. Virus Stuxnet menggunakan default Symantec Siemens untuk mendapatkan jalan masuk ke Sistem Windows Corp tersebut untuk menyebarkan virus dan menyerang serta mengatur ulang target komputer. Tujuan virus Stuxnet dimaksudkan untuk memberhentikan program nuklir di wilayah Natanz (Sembiring, 2020).

Serangan ini dikenal dengan Olympic Game Operation dengan sandi "olimpiade". Olympic Game Operation melibatkan dua badan intelijen besar yaitu NSA (National Security Agency) dan CIA (Central Intelligence Agency) dan organisasi rahasia Israel. Amerika mengumpulkan semua berkas dan data tentang Natanz yang akan berguna dalam mempengaruhi perangkat penghasil uranium (lebih dikenal dengan istilah sentrifugal). Dalam hal ini virus Stuxnet telah dimasukkan yang selanjutnya akan dikembangkan oleh unit Israel 8200 bersama dengan NSA yang selanjutnya menciptakan bug. Tujuan dari pengembangan virus diprioritaskan untuk melumpuhkan setrifugal di Natanz. Serangan Stuxnet menghancurkan sekitar 1.000 sentrifugal di Natanz dan menyerang hamper 100.000 komputer di seluruh dunia. Kerusakan ini menimbulkan kekacauan di wilayah Natanz yang berdampak terhadap terhentinya program nuklir Iran di wilayah Natanz (Kamiński, 2020). Namun kenyataannya serangan ini tidak banyak menyebabkan kerusakan yang mempengaruhi untuk melumpuhkan secara permanen. Serangan ini memberhentikan program nuklir selama satu tahun. Ahmadinejad melihat serangan ini mengambil tindakan cepat utuk memperbaiki sistem komputer dan sistem operasi dengan memulihkan sumber daya dan memprogram ulang sistemnya.

KERANGKA TEORI

Kejahatan Siber (Cyber Crime)

Istilah *cyber* menjadi istilah yang sering dipakai dalam seluruh lapisan dunia global. Untuk menjelaskan kejahatan siber, maka yang ahrus kita ketahui adalah *cyberspace. Cyber Space* merupakan sebuah dunia bukan ruang yang

mempunyai pengertian umum sebuah "ruang maya" yang menjadi simbolis bagi tempat bertemu nya jutaan manusia. Ketika seseorang sedang berkomunikasi di internet, maka orang tersebut akan bertemu dalam ruang simbolis dimana orang tersebut mampu berbagi informasi dan lain-lainnya. *Cyber Space*, menurut Alisjahban, merupakan ruang yang selalu berada pada sekeliling kawat telepon, kabel fiber optic dan gelombang elektromagnetik. Dunia cyberspace dihuni seluruh ilmu pengetahuan baik pengetahuan yang baik ataupun pengetahuan yang buruk. Ruang ini nantinya akan dihubungkan dengan dunia luar melalui pintu dimana manusia dapat melihat dan mengetahui untuk memasukkan pengetahuan baru, mengubah pengetahuan yang ada didalamnya, atau mengeluarkan pengetahuan tersebut dari ruang tersebut. Pintu yang dimaksud adalah alat teknologi seperti televisi, gadget, pemancar dan lain lainnya. Dengan muncul dan menyebarnya *cyber space* kedalam seluruh lapisan dunia global, dunia global secara tidak langsung dituntut untuk mengubah nilai dan perilakunya dalam kehidupan sehari-harinya akibat penggunaan alat teknologi tersebut (Hadi A. , 2005).

Beberapa peneliti memberikan pendapat mengenai defenisi dari kejahatan siber. Menurut Casey, kejahatan siber atau *cyber crime* merupakan segala kejahatan baik pencurian data, sabotase, pengrusakan dan kejahatan lainnya yang menggunakan komputer. Dalam hal ini komputer bisa memiliki peran yang penting ataupun peran yang tidak penting. Dalam tujuannya untuk mendapatkan target, beberapa teknik dan langkah dilakukan untuk mendapatkan akses informasi yang dibutuhkan. Dalam hal ini kejahatan siber melibatkan komputer untuk mencapai tujuannya (Moore R. , 2011). Di sisi lain, *cyber crime* bukan hanya melibatkan kecanggihan teknologi komputer saja, melainkan juga melibatkan teknologi komunikasi dalam peroperasiannya. Hal ini dikarenakan *cyber crime* berkaitan dengan pemanfaatan teknologi komunikasi yang mengandalkan pada tingkat keamanan yang tinggi dan kredibilitas informasi. Perang Siber (Cyber Warfare)

Konsep perang siber tau yang lebih dikenal dengan *cyberwarfare* merupakan konsep yang memiliki defenisi yang masih diperdebatkan sampai saat ini. Hal ini didukung dengan fakta bahwa defenisi cyber dan defenisi warfare masih didiskusikan oleh beberapa aktor internasional. Cyberwafare sendiri sering melibatkan negara-bangsa atau organisasi internasional untuk menyerang demi mencapai tujuan nya. Dikutip dari **artikel yang ditulis oleh** Jason Andress dan Steve Winterfeld dalam bukunya berjudul "*Cyber Warfare:Techniques, Tactics and Tool for Security Practitioners*" menjelaskan cyberwarfare dapat digunakan sebagai alat untuk melakukan spionase, terror dan peperangan. Dalam buku ini menjelaskan cyberwarfare menggunakan konsep *cyberspace*. Cyberspace sebagai ruang yang menjadi domain dengan penggunaan elektronik untuk menyimpan, mengatur ulang, memodifikasi melaui jaringan. Defenisi Cyberspace dalam Memorandum berjudul " *National Military Strategy for Cyberspace Operation*" adalah sebagai berikut (Pace, 2006) :

> "*A domain characterized by the use of electronics and the electromagneti spectrum*
> *to store, modify, and exchange data via networked systems and associated physical infrastructures"*

Dalam hal ini cyberspace memiliki defenisi sebagai ruang atau media yang digunakan para pengguna elektronik dalam jaringan internet yang digunakan untuk mengumpulkan, menyimpan, memodifikasi data, maupun jalinan komunikasi satu arah atau sebaliknya secara tidak langsung atau *online*. Dalam hal ini Cyber space akan dijadikan wadah sebagai tempat terjadinya cyber warfare. Jason juga menjelaskan bagaimana strategi dan taktik yang diambil dalam cyberwarfare.

Dikutip dari jurnal yang ditulis oleh Kartika Eliva Angel Tampubulon berjudul "*Perbedaan Cyber Attack, Cyber Crime dan Cyber Warfare"* UNTERM dan UNICJRI memberikan defenisi cyber yang

berbeda. Cyber warfare menurut UNTERM sebagai berikut (Tampubolon, 2019):

> "*The offensive and defensive use of information and informations system to deny, exploit, corrupt or destroy an adversary's computer based network while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries"*

Kemudian UNICJRI memberikan defenisi Cyberwarfare sebagai berikut (Tampubolon, 2019):

> *"any action by a nation-state to penetrate another nation's computer networks for the purpose of causing some sort of damage".*

Bedasarkan defenisi dari kedua organisasi tersebut, dapat disimpulkan bahwa keduanya mempunyai defenisi yang berbeda. Menurut UNTERM perang siber merupakan tindakan yang dilakukan dengan langkah agresif dan langkah pencegahan. Dalam hal ini tindakan agresif melibatkan militer untuk menyerang dengan menggunakan militer sedangkan langkah pencegahan seperti perlindungan sistem dari hal eksploitasi, pengrusakan dan penghancuran sistem informasi dan komunikasi untuk mewujudkan kepentingannya. Sedangkan defenisi perang siber menurut UNICJRI merupakan suatu tindakan yang dilakukan baik melibatkan aktor negara untuk masuk kedalam sebuah jaringan dengan tujuan merusak sistem jaringan informasi dan komunikasi yang ada didalamnya.

METODE PENELITIAN

Metode penelitian yang digunakan adalah metode kualitatif. Karena penelitian ini membahas secara detail mengenai fenomena-fenomena yang akan diteliti melalui berbagai aspek, opini, perspektif, tanggapan, kritikan, respon, dan keinginan baik dari individu maupun kelompok. Metode Kualitatif merupakan metode peneltian yang dikumpulkan dengan menggunakan analisis. Metode kualitatif biasanya bersifat deskriptif. Deskriptif ini sendiri merupakan cara dari penyajian gambaran lengkap dan eksplorasi mengenai suatu fenomena (Syafnidawaty, 2020). Peneliti yang menggunakan metode kualitatif biasanya untuk mengumpulkan, menyelidiki, dan menganalisis data baik secara infuktif dan deduktif terhadap objek dan tempat yang diteliti.

Bedasarkan dengan tujuan penulisannya, maka penulisan ini akan memaparkan penjelasan terkait berbagai data dan informasi lainnya untuk mampu menjawab pertanyaan dari permasalahan peneltian yang terdapat dalam penelitian ini. Bentuk peneltian yang dilakukan adalah dengan melakukan studi kepustakaan untuk mendapatkan informasi sesuai dengan tema yang diteliti. Informasi yang diperoleh berasal dari jurnal, artikel, buku, website resmi, laporan, media visual serta sumber-sumber tertulis baik cetak maupun elektronik lainnya.

HASIL DAN PEMBAHASAN

Pengembangan Fasilitas Program Nuklir Iran

Iran merupakan salah satu negara di kawasan Timur Tengah yang mempunyai kemampuan dan potensi dalam pengembangan nuklir. Salah satu hal yang menjadi perhatian dunia internasional terhadap Iran adalah pengembangan program nuklirnya. Pengembangan program nuklir Iran mulai diperlihatkan pada tahun 1950-an selama masa pemerintahan Shah Pahlavi. Iran memiliki hubungan yang sangat dekat dengan Israel, yang dimana saat itu Shah diperkenalkan kepada Amerika Serikat oleh Israel. Selama berlangsungnya perang dingin, Iran, Israel dan Arab Saudi menjadi pilar kekuatan Barat di Timur Tengah. Shah Pahlavi menjadi salah satu presiden Iran yang mempunyai hubungan baik dengan Amerika Serikat, sehingga Iran pada masa itu menerima bantuan untuk memproduksi energi nuklir. Adanya penemuan serta pengembangan teknologi nuklir, sebenarnya dapat menjadi sumber inspirasi bagi negara lain. Hal ini dikarenakan teknologi nuklir bisa dimanfaatkan untuk menjadi salah satu pasokan sumber melimpah. Dalam pemanfaatannya, tentunya juga terdapat keuntungan besar bagi negara yang

memiliki nuklir. Bagi negara yang memiliki nuklir pemanfaatan nuklir merupakan sumber alternatif dalam pasokan sumber daya energi yang melimpah. Penggunaan energi nuklir akan berdampak pada penghematan bahan bakar fossil yang berupa gas, batu bara dan minyak bumi, yang hampir sebagian besar digunakan sebagai bahan bakar pembangkit energi listrik. Pemanfaatan energi nuklir dapat mengurangi keperluan bahan bakar fossil, sehingga cadangan fossil mampu bertahan lama. Panas yang dihasilkan oleh reaktor nuklir juga dapat digunakan secara langsung untuk keperluan yang lain selain keperluan pasokan listrik. Misalnya di negara Swedia dan Rusia, panas dari reaktor nuklir digunakan untuk memanaskan bangunan dan untuk menyediakan panas untuk berbagai proses industri seperti desalinasi air. Selain itu, suhu panas yang tinggi yang berasal dari reaktor nuklir kemungkinan akan mampu dimanfaatkan ke dalam beberapa proses industri di masa depan, terutama untuk membuat hydrogen. Selain untuk pembangkit listrik dan penggunaan panas nya, nuklir juga mempunyai kegunaan lain (Basri, 2014).

Negara Iran sendiri merupakan negara yang termasuk kedalam perjanjian NPT, sehingga semua peraturan dan perjanjian terikat didalam NPT juga terikat dengan Iran. Dewan keamanan PBB melalui IAEA tetap terus meninjau perkembangan nuklir Iran secara berkala. Iran selalu memberikan klarifikasi mengenai program nuklir nya bahwa nuklir yang sedang dikembangkan Iran bertujuan untuk perdamaian dunia. Namun klarifikasi ini tidak pernah diterima dan dipercaya oleh PBB. Meskipun Iran telah menyatakan pendapat tersebut terus menerus, PBB melalui IAEA masih tetap tidak ingin mempercayai dan terus berasumsi bahwa pengembangan nuklir Iran harus terus diawasi dan dikontrol demi memastikan tidak adanya senjata nuklir yang tercipta. Dunia dan orgaisasi Internasional sudah pasti sangat mengharapkan tunduknya Iran pada perjanjian NPT. Oleh hal itu, kekhawatIran akan terjadinya perang nuklir bisa dihindari meskipun sejumlah negara yang mempunyai kemampuan nuklir masih belum menerima kenyataan bahwa mereka harus tunduk pada rezim ini. Ketegangan yang terjadi dikawasan Timur Tengah kerap dipicu oleh kepemilikan senjata, terutama senjata nuklir salah satu negara, sehingga dengan adanya kontrol pihak internasional ketegangan bisa diredam secara efektif. Dengan tercapainya perjanjian nuklir maka terdapat kemajuan dalam proses negosiasi para pihak yang selama ini cenderung saling curiga ketika duduk di meja-meja perundingan untuk membahas isu internasional.

Berbeda dengan negara-negara barat dan dunia yang memberikan penolakan terhadap program nuklir Iran, China dan Rusia mengambil tindakan yang berbeda. Kedua negara tersebut menunjukkan sikap penolakannya kepada Amerika Serikat. Meskipun China tidak secara langsung menyatakan dukungannya terhadap program nuklir Iran, namun China menolak usulan pemberian sanksi terhadap Iran dengan menyatakan bahwa saat ini bukan waktu yang tepat untuk memberikan sanksi karena Iran telah membuka pintu negosiasinya. Dalam menyikapi masalah nuklir Iran, China sangat hati-hati khususnya terhadap kemungkinan adanya kepentingan Amerika Serikat di Timur Tengah. China merupakan salah satu negara dengan pertumbuhan ekonomi yang pesat. Untuk terus meningkatkan pertumbuhan ekonominya, maka China harus mampu menjaga stabilitas pasokan energi dalam negeri. Untuk menjaga cadangan energi, China dalam hal ini membutuhkan pasokan minyak. Di China sendiri, pasokan minyak tidak sebanding dengan kebutuhan energi dalam negeri, hal tersebut membuat China harus menentukan sikap politik untuk menjalin kerjasama dengan semua negara yang memiliki sumber energi minyak. Kebutuhan akan minyak dan gas yang seiring berjalannya waktu mengalami peningkatan dari tahun, hal inilah yang menjadi alasan pengambilan kebijakan China menjadikan masalah keamanan energi sebagai agenda utama politik luar negeri. Iran merupakan salah satu negara yang memasok kebutuhan minyak bagi China hingga 12% dari total kebutuhan minyak di China. Selain itu, tejadinya

kekosongan investasi di negara Iran sebagai dampak dari perkembangan program nuklir Iran memberikan peluang kepada China untuk terlibat dalam eksplorasi ladang minyak baru di Iran serta menginvestasikan sekitar 50 miliar dollar dan mengerahkan ilmuan serta perusahaan raksasa yang ada di China untuk datang ke Iran. Sikap China dalam mendukung program nuklir Iran tidak terlepas dari hubungan kerjasama yang telah dijalankan oleh kedua negara ini. Meskipun begitu besar tekanan yang diberikan negara barat dan dunia internasional ke Iran terkait program nuklir, pada kenyataannya tekanan ini tidak memiliki dampak terhadap perubahan kebijakan politik China terhadap Iran. China sendiri juga tidak memiliki kepentingan strategis terhadap sanksi yang diberikan kepada Iran. KekhawatIran China lebih mengarah kepada dampak yang akan dihasilkan oleh tekanan barat ke negara Iran. Jika dilihat tekanan yang diberikan negara barat ke China untuk menghentikan kerjasama dengan Iran, maka tekanan yang diberikan barat terhadap Iran mempunyai pengaruh yang lebih besar terhadap kepentingan nasional Iran jika Iran merealisasikan ancaman nya untuk mengalihkan penjualan minyak dan gas (Nugroho, 2012).

Berdasarkan sejarah, hubungan Rusia dan Iran sudah terjalin sebelum abad ke-18. Letak wilayah yang berdekatan membuat kedua negara ini memiliki hubungan kerjasama dalam berbagai bidang. Letak geografis yang sama, membuat kedua negara ini mempunyai musuh yang sama yakni Amerika Serikat yang muncul sebagai kekuatan regional yang baru. Hal ini lah yang membuat Iran membangun reaktor nuklir di salahsatu kota di Pesisir Selatan bagian Barat Iran yaitu di kota Bushehr pada tahun 1974, Rusia menyatakan siap membantu pengembangan reaktor nuklir Iran. Adanya bantuan pengembangan nuklir Rusia terhadap Iran, sebenarnya memiliki beberapa keuntungan untuk Rusia. Bila dilihat dalam bidang ekonomi, Iran merupakan salah satu pasar terbesar dalam perdagangan persenjataan, hal ini membantu Rusia untuk mengekspor senjata demi meningkatkan kekuatan militernya. Selain itu, kerjasama dalam pengembangan nuklir ini juga mendorong peningkatan kerjasama dagang dalam bidang konstruksi pembangkit listrik, minyak dan gas, serta barang-barang konsumsi. Sebagai salah satu negara yang memiliki nuklir, Rusia memiliki pandangan tersendiri terhadap negara yang mengembangkan nuklir. Semakin buruknya hubungan Rusia dan Amerika Serikat setelah terjadinya Perang Dingin menyebabkan Rusia memandang Amerika Serikat sebagai salah satu musuhnya. Rusia juga memberikan bantuan militer terhadap Iran dengan kekuatan militer dalam bidang pertahanan pasukan darat dan pasukan udara.

Dalam hal ini, Rusia melakukan aliansi kuat yang baru terhadap Iran. Tujuan bantuan militer ini digunakan untuk mencegah ancaman seperti agresi militer, terorisme, kejahatan transnasional dan ancaman lainnya yang akan mengganggu keamanan Iran dan Rusia. Tindakan Rusia ini mendapat kecaman keras dari dunia internasional termasuk Amerika Serikat dan Israel. Amerika Serikat bahkan memberikan peringatan keras kepada Rusia bila Rusia tetap bersi keras untuk membantu Iran dalam pengembangan nuklirnya. Namun Rusia menyatakan bahwa bantuannya kepada Iran hanya demi kepentingan pembuatan reaktor dan siap untuk terbuka kepada IAEA tentang semua perkembangan pembangunan reaktor Bushehr. (Akbar, 2015)

Sebagian masyarakat dunia menganggap bahwa pengembangan program nuklir ini akan menjadi ancaman besar yang mampu membahayakan keselamatan jiwa umat manusia di dunia. KekhawatIran dunia adalah dengan berlanjutnya pengembangan program nuklir ini, dikhawatirkan akan mengulang peristiwa bom Hiroshima dan Nagasaki tahun 1945 yang menghancurkan dua kota tersebut dan menyebabkan menghilangnya ribuan nyawa seta korban jiwa tidak bersalah akibat luka ataupun radiasi yang ditimbulkan akibat ledakan bom nuklir pada kedua kota tersebut (Mikail, 2019). KekhawatIran yang muncul ini adalah hal yang wajar, mengingat dampak dari nuklir yang telah terjadi memberikan efek berkepanjangan dan sangat sulit bagi

wilayah yang menjadi target serangan nuklir untuk kembali ke keadaan seperti semula. Wilayah tersebut harus berjuang untuk mampu mengembalikan keadaannya seperti sebelum mendapatkan serangan nuklir. Dengan adanya kejadian tersebut, akibatnya teknologi yang berkaitan dengan nuklir akan selalu dianggap sebagai sesuatu yang sangat berbahaya. Masyarakat dunia internasional akan merasakan keresahan yang begitu luar biasa dengan adanya pengembangan program nuklir yang dapat membunuh umat manusia. Sehingga dengan adanya fakta ini, masyarakat dunia akan menganggap bahwa nuklir adalah senjata yang mematikan. Iran menjadi negara dengan kekuatan tak terbendung semenjak keinginan menjadikan negara mereka sebagai negara mandiri. Iran yang mengambil kebijakan "*inward looking* (strategi melihat kedalam)" dengan didasarkan pemanfaatan sumber daya yang dimiliki Iran, memberikan peluang bagi Iran untuk menyelesaikan dalam permasalahan ekonomi serta memperkuat hubungan Iran dengan negara lainnya di kawasan Timur Tengah. Kepemilikan nuklir Iran telah membawa banyak keuntungan yang besar dalam menjaga posisi Iran di Timur Tengah. Negara yang memiliki nuklir akan dianggap sebagai negara terkuat dan berada di posisi *top of the table* di dalam hubungan internasional. Hal ini akan menguntungkan Iran dalam posisi kerjasama dalam hubungan Internasional. Disisi lain, nuklir membantu Iran dalam melindungi identitas nasionalnya di Timur Tengah, hal ini juga akan memperkuat keamanan nasional Iran yang membantu menjaga keamanan domestik Iran jangka panjang (Sinaga, 2009).

Setelah Iran dicurigai oleh negara-negara Barat, maka aktivitas program nuklir Iran menjadi isu yang sangat kontroversi. Amerika Serikat yang dulu pernah mendukung program nuklir Iran, justru menjadi negara yang sangat keras menentang keberadaan nuklir Iran di kawasan Timur Tengah. Amerika Serikat sangat giat untuk menyuarakan Iran kedalam perundingan internasional untuk menghentikan program nuklir. Melalui PBB dan Uni Eropa, kasus Iran ini mengalami pasang surut dalam proses penyelesaiannya. Banyak kajian yang membahas mengenai hubungan Iran dan Amerika Serikat, namun belum ada literatur yang menjelaskan alasan Amerika Serikat begitu giat dan menentang keras pengembangan program nuklir yang dilakukan Iran. Dikutip dari jurnal yang ditulis oleh Rio Sundari yang berjudul*"Strategi Amerika Serikat Dalam Menekan Pengembangan Nuklir Iran"* yang mengutip kembali penjelasan artikel yang ditulis oleh Gawdad Bahgat yang berjudul *"Approaches toward Iran's Nuclear Progamme : The United State of America and China in Comparative Perspective"* berpendapat bahwa Amerika Serikat menggunakan cara yang salah dalam mendekati Iran. Berbeda dengan China yang menggunakan sikap "ramah" dalam mendekati Iran. Bahgat lebih melihat pandangan hubungan Amerika Serikat dan Iran kepada aspek ancaman kawasan Timur Tengah. Bahgat berpendapat, bahwa ancaman yang akan dihadapi Amerika Serikat setelah kelompok Taliban dan Irak adalah Iran. Amerika memiliki kekhawatiran tersendiri terkait dengan munculnya kelompok berkhianat dan pembangkang lainnya seperti kelompok Taliban dan Irak di kawasan Timur Tengah. Terlebih lagi Iran yang mempunyai kemampuan potensial untuk melakukan perubahan dari program energi nuklir ke program nuklir bersenjata, maka secara logika, tindakan Amerika Serikat melakukan tekanan dan desakan terhadap Iran merupakan hal yang tepat. Asumsi negative yang berkembang akibat program nuklir Iran tersebut, membuat Amerika juga membangun pangkalan militernya dikawasan Timur Tengah. Hal ini diakibatkan kekhawatiran program nuklir yang mengancam keamanan regional Timur Tengah (Sundari, 2020). Fakta keputusan yang diambil Iran bahwa Iran tidak ingin terbuka mengenai pengembangan program nuklir yang sedang dijalankan, membuat akhirnya Dewan Keamanan PBB memberikan sanksi kepada Iran. Sanksi yang diberikan terhadap Iran pun beragam. Sanksi pertama yang diberikan yaitu pembatasan Iran dalam perdagangan internasional untuk memenuhi kebutuhan program

nuklirnya dan ilmuan-ilmuan yang berperan dan terlibat dipindahkan keluar negeri. Sanksi kedua yang didapatkan adalah embargo yang dimana menyulitkan Iran untuk melakukan transaksi sumber daya minyak di pasar internasional. Sanksi yang diberikan Dewan Keamanan PBB terhadap Iran, membuat Iran harus pasrah dengan segala hal yang telah terjadi (Sya'roniRofii M. , 2015) .

Fasilitas nuklir Iran pertama didirikan di Teheran pada tahun 1967 dengan bantuan Amerika Serikat dan Jerman sebagai pemasok reaktor untuk perkembangan riset. Satu tahun kemudian Iran menandatangani perjanjian NPT. Dalam perjanjian NPT Pasal IV berisi, bahwa mengakui dan menerima hak semua negara untuk mengembangkan energi nuklir untuk tujuan damai dan juga mengakui "hak yang tidak dapat dicabut" dari penandatangan untuk pengembangan penelitian, produksi dan penggunaan energi nuklir untuk tujuan damai tanpa diskriminasi, dan untuk memperoleh peralatan, bahan dan informasi ilmiah dan teknologi (Kubbig, 2006). Hal ini membuat Amerika Serikat mendorong Iran untuk memperluas energi nuklirnya. Amerika juga turut ikut andil membantu dalam pembangunan reaktor nuklir tersebut. Rezim Pahlavi merupakan rezim yang dibangun dengan ideologi nasionalis. Kepemimpinan Pahlavi dikenal otoriter. Selain itu, Pahlavi juga melakukan beberapa kebijakan seperti adanya westernisasi yang berhasil menguasai suku-suku di Iran, kebijakan modernisasi ekonomi dan meluaskan penguasaannya terhadap ulama yang dilihat dari kebijakan-kebijakan Pahlavi semakin menyebarkan kontrolnya atas banyak bidang yang pada awalnya merupakan kekuasaan para ulama. Tahun 1970-an, Pahlavi menunjukkan kesewenangannya terhadap kekuasaannya di Iran. Militer dan kehadiran polisi rahasia (Savak), menjadi sosok hal yang sangat ditakuti dan dibenci dikarenakan mereka melancarkan penyidikan, intimidasi, pemenjaraan, penyiksaan dan pembunuhan terhadap musuh-musuh besar rezim Pahlavi. Selain itu, isu HAM yang disebarkan Amerika Serikat, menyebabkan jurnalis menuntut kebebasan media dan pers di Iran. Kelompok demonstran melakukan demonstrasi untuk menuntut diakhirinya rezim Pahlavi yang menurut mereka telah melakukan pelanggaran HAM berat selama berkuasa. Ditambah dengan adanya korupsi di kalangan pemerintah, menyebabkan pemerintahan Pahlavi diambang kemunduran dan memicu terjadinya Revolusi Iran pada tahun 1979. Revolusi Iran merupakan revolusi yang dipimpin Ayatullah Khomeini, yang dibentuk untuk melawan pemerintahan Shah Pahlavi saat itu. Ayatullah Khomeini terus memberi semangat perlawanan di tempat pengasingannya di Paris saat itu. Secara berkala, Ayatullah memberikan pidato-pidato politik yang berisi kecaman terhadap pemeritahan Pahlavi untuk memprovokasi dan menaikkan semangat massa untuk melakukan perlawanan kepada rezim Pahlavi (Mundzir, 2020). Ayatullah bahkan memberikan julukan Amerika Serikat sebagai *"Setan Besar"*. Akibat hal ini, Amerika Serikat selalu menyalahkan Iran sebagai penyebab membutuuknya kondisi Timur Tengah khususnya dikawasan Teluk. Hubungan Amerika Serikat dan Iran semakin memanas ketika Mahmoud Ahmadinejad terpilih sebagai presiden Iran. Amerika Serikat mulai mengganggu Ahmadinejad dengan berbagai isu, termasuk isu nuklir. Kontroversi program nuklir Iran oleh Amerika Serikat menjadi kekuatan revisionis dalam sistem regional Timur Tengah. Faktor inilah yang membuat Amerika melihat Iran sebagai ancaman serius bagi kepentingan Amerika Serikat di Timur Tengah. Menurut Amerika. Secara perlahan, Iran akan menjadi negara terdepan di kawasan Timur Tengah (Tarock, 2014).

Setelah terjadinya Revolusi Iran, Ayatullah mengambil tempat sebagai Presiden Iran setelah jatuhnya rezim Pahlevi. Iran pada masa kepemimpinan Ayatullah memutuskan untuk tidak melanjutkan reaktor nuklir karena Ayatullah apercaya Iran tidak membutuhkan energi nuklir (Mir, 2014). Terjadinya Perang Teluk I tahun 1980-1988 antara Iran dan Irak menyebabkan kemampuan militer Iran mengalami kemerosotan. Iran mengalami kemunduran dalam aspek persenjataan

militer. Adanya bantuan yang diberikan oleh Amerika Serikat secara politik dan militer membuat Iran memenangkan Perang Teluk tersebut. Kemunduran yang dialami Iran disebabkan oleh kerusakan dan kehancuran yang dialami negara Iran setelah terjadi nya Perang Teluk I yang berlangsung pada tahun 1980-1988. Hampir 60 persen senjata militer Iran yang dominan adalah persenjataan darat, rusak total akibat peranng melawan negara Irak. Selain persenjataan militer di darat, persenjataan militer di laut dan udara pun pengalami hal yang sama. Iran merasa terisolasi, dirugikan dan dikhianati oleh Barat. Ditambah dengan adanya pernyataan bahwa politisi Barat dan media menyalahkan Iran atas perang yang terjadi dan dengan demikian membebaskan Irak dari agresinya. Setelah invasi yang dilakukan terhadap Irak disambut dengan pergantian Rezim tahun 2003 dan posisi Iran yang terbendung oleh Amerika Serikat, Iran sangat merasa khawatir. Hal ini dikarenakan kekhawatiran Iran akan menjadi target negara selanjutnya untuk diinvasi. Terlebih lagi kekuatan militer Iran yang sudah hancur, akan membuat Iran lebih leluasa untuk diserang karena Iran tidak memiliki tameng persenjataan yang mumpuni. Untuk mengahadapi ancaman ini, maka salah satu hal yang harus dilakukan Iran adalah mempercepat pengembangan program nuklirnya. Melindungi keamanan nasional menggunakan program nuklir merupakan hal yang sangat penting dilakukan oleh Iran dari negara Timur Tengah lainnya (Sinaga, 2009).

Iran pada masa kepemimpinan Ahmadinejad, berani untuk tampil berbeda dengan melawan semua ketidakadilan yang diciptakan negara-negara barat dan dunia internasional terhadap negaranya. Ahmadinejad sangat gigih untuk menentang Amerika dan Israel dengan tetap menjalankan program nuklirnya tanpa melibatkan Amerika Serikat dan Israel dan mengambil alih keseluruhan pengelolaan program nuklir Iran. Ahmadinejad juga menjalankan progam nuklir ini tanpa sepengetahuan dunia internasional dan mengabaikan segala peraturan dan perjanjian yang telah dilakukan oleh PBB dan menentaang setiap masukan oleh Dewan Investigator IAEA. Ahmadinejad juga menggunakan PBB untuk mengkritisi setiap sikap berbeda negara-negara barat dan dunia internasional dalam memandang negara Iran yang dibandingkan dengan Israel. Konsistensi kebijakan dan keteguhan Iran dalam pandangannya terhadap nuklir yang dikembangkan bukan untuk tujuan perang dan mengancam perdamaian, terus berlaku hingga 2 periode masa Pemerintahan Ahmadinejad.

Ahmadinejad menjadikan program nuklir untuk menciptakan efek *deterrence* terhadap negara Iran. *Deterrence* sendiri berarti hubungan dimana negara X mampu memberikan ancaman terhadap negara Y dengan hukuman untuk meyakinkan negara Y agar tidak melakukan hal yang tidak diinginkan oleh negara X. Konsep deterrence ini kemudian mengalami perkembangan, yang dimana deterrence dibedakan menjadi dua jenis, yaitu *deterrence retaliation* dan *deterrence denial*. Deterrence sebagai retaliation ingin memperlihatkan kekuatan militer negara X dan memberikan ancaman hukuman yang keras sehingga dapat mencegah negara Y (dalam hal ini pihak yang dianggap mengancam) untuk tidak melakukan hal-hal yang tidak diinginkan. Dengan demikian dapat juga disebut sebagai ancaman balasan sebagai hukuman agar pihak lawan tidak melakukan hal - hal yang tidak diinginkan. Sedangkan *deterrence* sebagai *denial* yaitu kemampuan untuk menangkal secara langsung serangan yang dilancarkan oleh pihak musuh terhadap negara mereka. Esensi *deterrence* adalah menciptakan ancaman militer dalam rangka mencegah aktor lain untuk melakukan tindaka agresif, mencegah hal yang tidak diinginkan sebelum hal tersebut terjadi.

Pada tahun 2002, National Council Resistance of Iran memberitahukan bahwa Iran sedang mengembangkan program nuklir secara diam-diam. Kabar tersebut diperkuat dengan bukti-bukti gambaran satelit yang diperoleh Institute of Strategic and International Studies. Salah satu program nuklir yang ditanggap radar Institute of Strategic and International Studies adalah berada di wilayah Natanz. Diketahui bahawa Iran diam-diam

membuka dan menjalankan program nuklir di wilayah Natanz tanpa sepengetahuan IAEA selaku Dewan Inverstigator yang ditugaskan untuk mengawasi Iran. Penemuan informasi ini akhirnya diadukan oleh National Council Restitance of Iran kepada Dewan Investigator IAEA. (Melysa, 2016).

Mendengar kabar tersebut, IAEA meminta klarifikasi dari Iran. Presiden Mahmoud Ahmadinejad tidak membantah dan justru mengakui hal tersebut kepada IAEA bahwa Iran sedang mengembangkan program nuklirnya. Namun Ahmadinejad kembali menegaskan bahwa program nuklir yang sedang dikembangkan di wilayah Natanz bukan untuk kepentingan pembuatan senjata nuklir, melainkan untuk kepentingan domestik Iran dalam hal sumber energi dan menjadi jawaban dalam penyelesaian konflik domestik yang terjadi di Iran. Namun IAEA tidak menjadikan jawaban Ahmadinejad untuk tidak memberikan respon terhadap program nuklir yang sedang dikembangkannya. IAEA menganggap bahwa Iran telah melanggar perjanjian NPT. IAEA menyatakan bahwa Iran telah melanggar perjanjian non-proliferasi dan menuduh Iran gagal dalam mematuhi prosedur pengamanan dan juga menuduh program nuklir Iran ditujukan untuk memproduksi senjata nuklir. Akibat hal ini pula, Amerika Serikat berusaha untuk melakukan pendekatan diplomatis kepada Iran dengan tujuan agar Iran memberhentikan program nuklir di wilayah Natanz. IAEA juga mengambil keputusan untuk menyegel 3 fasilitas di Iran, yakni di wilayah Natanz, Ishafan dan Pars Tash. Namun hal ini tidak membuat Ahmadinejad menuruti keinginan Amerika Serikat dan IAEA. Sebaliknya, Ahmadinejad tetap berisikeras untuk menjalankan program nuklirnya. Pemerintahan Ahmadinejad melawan dengan keras sikap Barat khususnya Amerika Serikat. Hal ini dikarenakan tidak banyak pemerintahan negara di dunia ini yang berani melawan Barat dan Amerika Serikat. Sikap perlawanan Pemerintahan Ahmadinejad terhadap Amerika Serikat merupakan bentuk dari sikap anti-hegemoni Amerika Serikat. Iran membuka segel internasional yang dipasang pada program nuklir wilayah Natanz dan kembali untuk meneruskan proses pengadaan bahan bakar nuklir melalui pengawasan IAEA. Segel yang dibuka tersebut dari fasilitas di Natanz, fasilitas penyimpanan Isfahan, dan Pars Tash (Fauzi, 2018).

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 Amerika Serikat 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. Pilihan pertama adalah melakukan operasi militer sebagaimana yang disarankan oleh *National Security* 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*.

Gambaran Umum Olympic Game Operation

Olympic Game Operation adalah operasi gabungan antara Amerika Serikat dan Israel. Operasi ini dirancang sebagai sebuah serangan operasi siber yang menargetkan fasilitas nuklir Iran di wilayah Natanz. Untuk melaksanakan perang siber ini, Amerika bekerja sama dengan Israel untuk mempersiapkan

sebuah *cyber weapon* berupa sebuah program *(worm)*. Meskipun Iran memiliki program nuklir Iran di wilayah lainnya, namun wilayah Natanz adalah wilayah paling penting dalam pengembangan program nuklir Iran. Hal ini dikarenakan wilayah Natanz merupakan tempat berdirinya bangunan-bangunan penting pengembangan keseluruhan program nuklir negara Iran. Hal ini lah yang membuat program nuklir diwilayah Natanz tidak terhubung ke internet dengan alasan untuk melindungi sistem dari serangan negara lain

Operasi Olympic Game Operation ini dibagi kedalam dua tahap penyerangan. Tahap pertama adalah pembuatan *worm* yang berfungsi dalam memetakan posisi program nuklir Natanz Iran. Kemudian pada tahap kedua, akan dilakukan serangan terhadap fasilitas nuklir Iran di wilayah Natanz yang sudah ditargetkan. Amerika Serikat berperan sebagai pembuat Stuxnet dan Israel berperan untuk menyelundupkan Stuxnet ke fasilitas nuklir Iran yang berada di Natanz. Perusahaan asal Jerman yang bergerak dibidang teknologi yaitu Siemens, dilibatkan untuk membuat virus Stuxnet. Tujuan dari operasi penyerangan ini adalah menginfeksi sistem komputer yang menjalankan sentrifugal dan menghancurkan sentrifugal pada bangunan-bangunan penting yang mendukung berjalannya program nuklir Iran terkhususnya di wilayah Natanz.

Mekanisme Operasi Olympic Game Operation

Stuxnet adalah perangkat lunak berbahaya atau malware yang biasanya menyerang sistem kontrol industri. Para ahli mengatakan virus dapat digunakan untuk memata-matai atau sabotase. Perusahaan asal Jerman yang bergerak dibidang teknologi yaitu Siemens, dilibatkan untuk membuat virus Stuxnet. Stuxnet dirancang untuk tidak terdeteksi untuk waktu yang lama dan memberikan konsistensi untuk terus membebani sentrifugal. Ukuran Stuxnet lebih besar dari ukuran malware pada umumnya. Siemens mengatakan malware menyebar melalui perangkat memori USB thumb drive yang terinfeksi, mengeksploitasi kerentanan disistem operasi Windows Microsoft Corp. Program serangan perangkat lunak malware melalui *Supervisory Control and Data Acquisition* atau SCADA. Analis mengatakan penyerang akan menyebarkan Stuxnet melalui thumb drive karena banyak sistem SCADA tidak terhubung ke Internet, tetapi memiliki port USB. Setelah virus menginfeksi sistem, worm Stuxnet bekerja dalam memetakan nuklir Natanz Iran. Informasi dan data yang didapatkan akan memberikan tahap awal untuk serangan berikutnya, lalu dengan cepat membentuk komunikasi dengan komputer server penyerang sehingga dapat digunakan untuk mencuri data perusahaan atau mengontrol sistem (Wey, 2021). The Supervisory Control and Data Acquisition (SCADA) adalah sistem kontrol jaringan industri yang bertanggung jawab dalam 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 penggunaan teknologi tinggi dan manajemen otomatis dalam sektor ini, menyebabkan rentannya sistem dalam berbagai ancaman serangan siber, sehingga akan berdampak buruk pada dunia nyata (Syani Zuraida).

Agen yang telah disiapkan oleh Israel, kemudian menyelundupkan virus Stuxnet ke dalam sistem komputer Windows Iran. Setelah Virus Stuxnet masuk ke sistem komputer Iran, Stuxnet kemudian bekerja dengan cepat sambil me-replika serta menyebarkan dirinya ke sistem komputer secara keseluruhan, yang pada awalnya hanya menyerang windows, Stuxnet akan menyebar ke sistem software komputer lainnya. Penyebaran yang dilakukan akan memberikan kesempatan pada virus Stuxnet untuk memeriksa sistem kontrol mesin yang ditarget kan. Pada awalnya Stuxnet akan mengamati operasi dari sistem yang akan dijadikan target. Setelah mengamati sistem komputer yang menjalankan program nuklir Natanz, virus Stuxnet akan bekerja untuk mengambil alih dan mengendalikan sentrifugal.

Setelah sistem sentrifugal diambil alih, virus Stuxnet kemudian menginfeksi sistem tersebut dengan tujuan untuk membuat sistem operasi sentrifugal gagal beroperasi. Stuxnet merusak sentrifugal di Natanz dengan memprogram ulang PLC Siemens yang mengendalikannya. Untuk melakukan itu, pertama-tama Stuxnet harus mengkompromikan sistem Microsoft Windows dan kemudian perangkat lunak kontrol Siemens WinCC/PCS 7 SCADA yang berjalan di atasnya. Hal ini dilakukan dengan memanfaatkan beberapa kerentanan, salah satunya adalah hardcoded WinCC/SCADA password yang telah diposting di Internet. Selain menginfeksi sistemnya, virus Stuxnet juga bekerja untuk meledakkan beberapa sentrifugal penting di beberapa bangunan tersembunyi di wilayah Natanz. Setelah semua sentrifugal telah berhasil diledakkan, maka virus Stuxnet kemudian memberikan umpan balik palsu pada sistem kontrol di luar untuk memastikan dan memberikan perintah bahwa tidak terjadi peretasan dan sistem komputer dan sistem sentrifugal dalam keadaan baik baik saja (Kushner, 2019).

Tahap kedua dalam serangan dari Operasi Olympic Game Operation adalah hasil dari penyerangan tersebut. Dengan menggunakan virus Stuxnet sebagai senjata siber nya, virus Stuxnet berhasil memberikan efek terhadap fasilitas nuklir Natanz. Symantec mencatat pada Agustus 2010 bahwa 60% komputer yang terinfeksi di seluruh dunia berada di Iran. Kerusakan yang terjadi tidak berdampak ke negara lain kecuali program nuklir Iran. Operasi Olympic Game Operation berhasil untuk memberhentikan dan memberikan pengaruh terhadap sistem komputer program nuklir Iran. (Kamiński, 2020). Bedasarkan laporan internasional dan IAEA, virus Stuxnet berhasil untuk menginfeksi serta menghancurkan sistem operasi sentrifugal serta beberapa sentrifugal penting lainnya. Perusahaan keamanan Symantec asal Amerika mengidentifikasi bahwa virus Stuxnet telah menginfeksi sekitar 6.000 mesin dan merusak 1.000 sentrifugal di wilayah Natanz. Selain itu, virus Stuxnet merusak beberapa bangunan penting fasilitas nuklir Iran. Bangunan penting tersebut terdiri dari 3 bangunan bawah tanah yang berguna untuk menampung sentrifuse-sentrifuse progam nuklir wilayah Natanz, 2 bangunan diatas tanah yang berisi teknologi untuk menampung aliran gas serta 4 bangunan lain yang digunakan untuk keperluan analisis riset dan administrasi serta pengembangan fasilitas nuklir Iran di wilayah Natanz (Shakarian, 2011).

Akibat operasi serangan Olympic Game Operation dengan virus Stuxnet sebagai senjatanya, program nuklir Iran yang berada di wilayah Natanz berhenti total selama 2 tahun lamanya. Total angka persentase kerusakan yang menyerang program nuklir Iran Natanz adalah 10%. Meskipun kerusakan yang ditimbulkan oleh sernagan virus Stuxnet telah merusak sentrifugal dan menginfeksi sistem komputer yang menjalankan program nuklir di wilayah Natanz seperti yang dijelaskan penulis pada paragraf sebelumnya, Presiden Mahmoud Ahmadinejad mengklaim bahwa serangan ini menghasilkan dampak yang kecil terhadap kerusakan fasilitas nuklir Iran di wilayah Natanz. Beberapa petinggi Iran mengatakan dampak yang diberikan hanya memperlambat dan menonaktifkan sementara fungsi dari kontrol sentrifugal di wilayah Natanz. Pada kenyataanya, serangan virus Stuxnet tidak merusak program nuklir Iran secara menyeluruh. Hal ini sangat jauh bertentangan dengan apa yang diharapkan Amerika Serikat dan Israel dalam memberikan dampak nya terhadap program nuklir Natanz. Tindakan serangan operasi Olympic Game Operation yang melibatkan virus Stuxnet untuk menyerang program nuklir Natanz ditujukan dan dimaksudkan untuk menyerang Program nuklir Natanz terbukti jauh lebih mudah dari segi apapun. Terlepas dari fakta dan pengungkapan bahwa Amerika Serikat dan Israel merupakan pelaku dari serangan tersebut, Iran tidak menganggap dan menggunakan serangan tersebut sebagai alasan Iran menampilkan dirinya sebagai korban penyerangan dan tidak menyampaikan kemarahan dan keluhan tersebut kepada lembaga dan organisasi internasionaal.

Stuxnet sebagai *Cyber Weapon*

Teknologi lahir dari hasil kreativitas pemikiran manusia. Bila dilihat dari betapa pentingnya peran teknologi, maka bisa dikatakan bahwa semua lapisan masyarakat dari masyarakat biasa hingga para petinggi dunia sangat bergantung kepada teknologi baik hasilnya positif maupun negatif. Perang siber akan muncul bila suatu negara mencoba menyerang negara lain dengan mengunakan komputer dan internet (Rahmawati, 2017). Dinamika globalisasi membuat negara internasional tidak lagi menggunakan perang konvensional untuk mencapai kepentingannya. Hal ini mengakibatkan kekuatan sebuah negara tidak lagi dilihat oleh kekuatan militer dan alusista negara tersebut. Akibatnya konflik yang terjadi disuatu negara tidak lagi didonimasi oleh kekuatan militer, melainkan muncul kekuatan non-militer dengan melibatkan aktor non-negara. Dengan hal ini pula, aktor non-negara seperti hacker (baik individu ataupun kelompok), teroris, kelompok kriminal terorganisir dan lainnya menjadi aktor baru dalam kejahatan siber. Dampak yang ditimbulkan oleh perang siber pun tidak sama seperti perang konvensional seperti biasanya. Perang siber yang menyebabkan kerusakan fisik biasanya mampu untuk diperbaiki. Selain itu, perang siber sangat jarang menimbulkan korban manusia seperti pada perang konvensional, karena biasanya perang siber akan menyerang fasilitas dan bangunan-bangunan penting negara yang diserang.

Munculnya virus Stuxnet, merupakan salah satu bukti dari kejahatan siber menggunakan kecanggihan komputer yang terhubung dengan internet. Virus Stuxnet membuka jalan baru terhadap kemajuan perang dunia maya (perang siber) di masa depan. Virus Stuxnet adalah contoh serangan yang menghasilkan kerusakan fisik terhadap target yang ingin dituju tanpa menilbulkan korban manusia. Virus Stuxnet dipandang sebagai revolusi baru terhadap perkembangan kejahatan siber yang mengancam kekuatan militer yang paling hebat sekalipun. Stuxnet menujukkan bahwa perang masa depan tidak akan lagi menggunakan kekuatan militer dan persenjataan fisik. Penggunakan internet sebagai media akan memberikan keuntungan yang besar terlebih lagi bagi aktor yang mempunyai kekuatan militer yang lemah. Selain tidak mengeluarkan biaya yang besar, aktor yang terlibat pun tidak akan terjun langsung kelapangan untuk melakukan perang tersebut (Rohozinski, 2013).

Amerika dan Israel menggunakan virus Stuxnet sebagai senjata dalam menjalankan operasi tersebut. Dalam operasi serangan tersebut, Amerika Serikat dan Israel menggunakan operasi siber ofensif dalam menyerang fasilitas nuklir di Natanz. Amerika Serikat dan Israel mempunyai alasan tersendiri dalam memakai penggunakan siber ofensif. Salah satu nya yaitu operasi siber ofensif dipercaya mampu untuk memaksimalkan serangannya terhadap target yang ingin diserang. Selain itu akan lebih menguntungkan bila dibandingkan jika memakai kekuatan militer dan perang konvensional biasa. Salah satu kelebihan dari perang siber dengan menggunakan operasi siber ofensif adalah tertutupinya anonimitas si penyerang. Dalam pelaksanaan perang siber, keuntungan ini sangat menguntungkan Amerika Serikat dan Israel sebagai negara penyerang. Amerika Serikat dan Israel akan lebih leluasa untuk menyerang Iran demi mencapai kepentingan dan tujuannya tanpa harus diketahui. Hal ini pula akan mengurangi dugaan Amerika Serikat dan Israel harus bertanggung jawab secara langsung dari serangan yang telah dilakukan. Berbeda dengan perang konvensional yang melibatkan militer untuk turun secara langsung menyerang, yang dimana hal ini akan langsung diketahui oleh negara lain bahkan musuhnya sendiri. Dengan mempersiapkan diri dalam persenjataan fisik atau adanya belanja militer, maka negara tersebut akan dianggap sedang melakukan persiapan perang. Perang siber ini tidak akan diketahui oleh dunia luar karena perang siber menggunakan *cyber space* untuk melakukan serangannya (Langner, 2011).

Selain itu, keuntungan yang dapat dirasakan oleh Amerika Serikat dan Israel yaitu mudah dalam segi jarak. Ruang siber

tidak mengenal batas wilayah. Siapapun mampu untuk berinteraksi dengan seseorang di wilayah manapun selama koneksi internet berjalan (Mikail, 2019). Dengan adanya kemampuan interaksi tersebut, memungkinkan orang lain untuk menyerang orang yang lainnya tanpa harus pergi ke tempat musuh yang ingin di serang. Pelaku yang ingin melakukan penyerangan pun hanya perlu menggunakan ruang siber dan internet saja. Hal ini berbeda bila dibandingkan dengan perang konvensional biasa yang bilamana Amerika Serikat memakai cara ini, maka mengharuskan Amerika Serikat untuk membangun military base di negara tujuan, mengirimkan logistik serta mengirimkan tentaranya. Dengan menggunakan perang siber, maka persiapan yang sedang dilakukan pun tidak akan diketahui oleh negara lain karena sifat dari perang siber yang muncul secara tiba-tiba.

Perang siber juga akan mengurangi efisiensi biaya. Meskipun pada umumnya pelaksanakan operasi siber membutuhkan teknologi yang mendukung dan tenaga ahli yang bekerja dalam operasi militer tersebut, namun bila dibaandingkan dnegan operasi militer pada umumnya, pengeluaran yang terjadi dalam operasi siber akan jauh lebih murah bila dibandingkan dengan perang konvensional. Dalam pengoperasian perang siber, perang siber akan memiliki biaya yang sangat murah apabila terjadi kerusakan yang dihasilkan dari serangan siber tersebut. Jika dibandingkan dengan operasi militer biasa, kerusakan yang dihasilkan operasi militer akan jauh lebih mahal karena biaya yang dikeluarkan untuk memperbaiki alusista yang dipakai dalam operasi militer tersebut akan lebih mahal.

Keuntungan lainnya yang akan didapatkan dari operasi serangan siber Stuxnet yaitu meminimalisir kerusakan fisik dan korban jiwa (Melysa, 2016). Dalam operasi Olimpic Game Operation, dampak kerusakan fisik yang ditimbulkan hanya pada *sentfiruse* yang menjadi target utama penyerangan. Hal ini berbeda bila menggunakan perang konvensional. Apabila dalam penyerangannya ke Iran Amerika Serikat dan Israel memakai perang konvensional, maka yang harus dilakukan oleh Amerika Serikat dan Israel adalah mengirimkan rudal maupun bom pada fasilitas program nuklir Iran. Dan bila hal ini terjadi, maka resiko yang akan dialami pun bukan hanya mencakup negara Iran saja, melainkan akan melibatkan dunia internasional. Dampak yang diberikan juga bukan hanya kerusakan fisik terhadap bangunan yang diserang, namun akan menimbulkan korban jiwa tidak bersalah yang sangat banyak akibat terjadinya penyerangan tersebut. Sehingga, menggunakan operasi ofensif siber dipandang lebih efisien dibandingkan menggunakan operasi militer konvensional Sebelum Stuxnet terjadi, banyak negara yang mengabaikan keamanan ruang sibernya. 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 kejahatan siber 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.

Penggunaan Stuxnet sebagai senjata siber dalam operasi Olympic Game Operation, membawa revolusi baru terhadap perkembangan *cyberwar* dalam dunia internasional. Pada pengoperasiannya, malware Stuxnet bukanlah senjata area luas, karena pada saat peroperasiannya, Stuxnet dibatasi penyerangannya untuk menyerang target tertentu dan menghasilkan efek tertentu. Hal ini membuat Amerika Serikat dan Israel memiliki tanggung jawab untuk merancang senjata Stuxnet yang kuat untuk menyerang hanya sasaran yang dimaksudkan. Hal ini lah yang menjadi dasar para perencana dan desainer Stuxnet dalam menciptakan virus Stuxnet. Stuxnet telah menciptakan revolusi di bidang perang sebagai salah satu senjata yang dapat digunakan untuk mendapatkan akses ke pusat nuklir negara lain. Dengan adanya kemajuan ini, maka akan menjadi kemajuan yang paling berbahaya dan mematikan dalam taktik perang. Banyak

negara yang cinta damai telah bangkit untuk mencegah perkembangan seperti itu di masa depan dengan mengambil tindakan pencegahan.

Kekuatan Regional Iran di Timur Tengah

Iran mempunyai kekuatan yang besar sehingga memungkinkan Iran memainkan peran regionalnya. Di bidang ekonomi, Iran memiliki keunggulan dikarenakan letak geografisnya dalam cadangan minyak dan gas alam. Cadangan minyak dan gas alam yang sangat melimpah membuat Iran memainkan peran yang begitu penting dalam pasar internasional terkait hal penjualan minyak dan gas alam. Bedasarkan data pada tahun 2016 (Grafik 5. 1), Iran memiliki cadangan minyak sekitar 157.530.000.000 dan menyumbang sekitar 9, 5% dari total cadangan minyak dunia yaitu sekitar 1.650.585.140.000 barel (Worldmeter, n.d.).

Iran Juga mempunyai cadangan terbukti setara dengan 239,2 miliar barel kali konsumsi tahunannya. Ini berarti, tanpa adanya ekspor Neto, maka Iran memiliki cadangan sekitar 239 miliar barel minyak tersisa (pada tingkat konsumsi saat ini dan tidak termasuk cadangan yang belum terbukti. Sedangkan untuk cadangan gas Iran bedasarkan data dari tahun 1986-2014. Pada tahun 1986 Iran menghasilkan 211,29 ribu barel per hari dengan minimum 71 ribu barel per hari. Sedangkan pada tahun 2014 Iran menghasilkan sebesar 382,24 ribu barel per hari.

Namun, adanya sanksi dan embargo yang diberikan akibat pengembangan program nuklir Iran, membuat Iran ekonomi Iran mengalami ketidakstabilan. Ditambah dengan adanya permasalahan seperti inflasi, pengangguran dan pendapatan yang rendah membuat Iran bergantung terhadap manufaktur lokal untuk mengatasi masalah ekonomi. Iran juga menjalin kerjasama dengan beberapa negara asing seperti China dan Rusia. Iran memahami bahwa keamanan negaranya menjadi salah satu hal yang paling penting. Oleh sebab itu, dalam bidang militer, Iran berusaha menjadi negara kuat di kawasan Timur Tengah. Pasukan Iran terkenal sebagai pasukan yang paling kuat di kawasan Timur Tengah. Keseriusan Iran dalam meningkatkan kekuatan militernya dibuktikan dari pengeluaran yang diberikan untuk melengkapi beberapa alusista sebagai salah satu penunjang militernya.

Pada tahun 1988 hingga 1992, Iran menghabiskan sebanyak 3,6 miliar dollar (untuk harga tahun 1990-an) untuk mengimpor senjata. Dalam periode ini, pemasok senjata terbesar selama periode ini yaitu Rusia (yang pada masa itu dikenal dengan nama Uni Soviet) yang menyumbang sekitar 50,1 persen dari total impor senjata konvensional. Dalam hal ini, Rusia melibatkan penjualan senjata seperti pesawat tempur canggih MiG-29, tank T-72, sebanyak 300 artileri berat, kapal selam dan rudal. Selain itu Rusia juga setuju untuk memberikan suku cadang dan layanan teknis kepada Iran untuk menghadapi pesawat Irak yang diterbangkan ke Iran selama Perang Teluk I. Selain negara Rusia, beberapa negara lain yang membantu pasokan senjata adalah China dan negara-negara lain (Moore, 2016).

Terjadinya Perang Teluk I, membuat Iran harus membangun dan meningkatkan kembali kekuatan militernya. Setelah perang tersebut, Iran terus berusaha untuk memperbaiki kerusakan yang dialami dengan terus meningkatkan kerjasama dengan tujuan agar Iran dibantu dalam hal militer. Selain itu Iran juga mengembangkan persenjataan dan kemampuan program nuklir serta kekuatan non-konvensional. Iran juga sering mengadakan pelatihan angkatan laut yang provokatif di bagian Teluk dengan tujuan untuk menampilkan Iran sebagai sebuah kekuatan di Teluk serta memberikan tekanan kepada negara-negara Arab dan Teluk serta aliansi mereka. Meskipun militer Iran belum berteknologi maju, namun Iran mampu untuk memberikan ancaman dikarenakan kepemilikan atas nuklir, hal ini juga mampu menjadi kekuatan bagi Iran untuk mengintimidasi negara besar dan kawasan regional. Dalam bidang kerjasama di kawasan, negara Iran merupakan negara yang tidak ikut serta dalam keamanan regional atau pun organisasi ekonomi seperti Gulf Cooperation Council (GCC). Hal ini

dikarenakan beberapa alasan, salah satunya yaitu perbedaan pandangan terhadap ancaman dan kepentingan. Namun Iran tetap berusaha untuk membangun hubungannya dengan negara-negara GCC yang tidak mempercayai kepentingan regional Iran. Negara-negara Teluk dan Israel menunjukkan kekecewaannya dengan pengumuman program nuklir Iran. Israel menganggap program nuklir Iran sebagai ancaman eksistensial, dan beberapa kali mengancam akan membom fasilitas nuklir Iran. Sikap Israel terhadap Iran bertujuan untuk menjatuhkan sanksi. Israel bahkan tidak menyetujui Perjanjian Persiapan Jenewa antara Iran dan negara barat pada tahun 2013 dan Perjanjian Kerangka April 2015 (Raouf, 2019).

Dampak Virus Stuxnet terhadap Domestik Iran

Serangan siber yang dilakukan Amerika Serikat dan Israel dalam tujuannya menyerang fasilitas program nuklir Natanz Iran, ternyata memberikan dampak ke dalam beberapa bidang di negara Iran. Dampak-Dampak tersebut antara lain:

1) Dampak Sosial dan Politik

Dalam bidang politik internal, virus Stuxnet memberikan dampak tersendiri. Pihak berwenang Iran menyatakan bahwa Iran tidak mampu melindungi negaranya dari serangan siber negara lain. Akibat hal ini, masyarakat Iran menuduh Ahmadinejad sebagai orang yang paling bertanggung jawab dalam serangan yang dilakukan Amerika Serikat dan Israel ke negara Iran. Pemerintah Iran tampak ragu-ragu tentang bagaimana bereaksi secara resmi terhadap berita bahwa virus Stuxnet mungkin telah menginfeksi fasilitas nuklir Iran. Pemerintah Iran akhirnya meminimali informasi terkait dampak serangan virus tersebut ke dalam beberapa media lokal. Hal ini dilakukan untuk menghindari terlalu banyak kesalahan dari penduduk, dengan menyatakan bahwa virus Stuxnet hanya berdampak kepada komputer pribadi tanpa koneksi ke fasilitas nuklir dengan menunjuk negara Barat dan NATO sebagai pelaku. Baru beberapa bulan kemudian, akhirnya pemerintah Iran mengumumkan bahwa virus Stuxnet telah menyerang aktif program nuklir. Pihak berwenang Iran tidak membalas serangan siber karena identitas pelaku tidak diketahui atau tidak jelas dan karena tidak ada preseden tentang bagaimana negara harus menanggapi serangan tersebut. Kelambanan ini membuat pemerintah Iran terlihat lemah dan tampak sebagai sasaran empuk dan menciptakan pandangan buruk terhadap pemerintahan Iran. Kepemimpinan Mahmoud Ahmadinejad dipandang lemah dan menjadi sasaran empuk bagi rival lain untuk menggunakan kasus serangan virus ini untuk menjatuhkan Ahmadinejad dari kursi kepresidenan Iran pada masa itu. Dalam bidang sosial, Stuxnet tidak memiliki dampak langsung terhadap kehidupan sosial masyarakat Iran, hal ini dikarenakan tidak ada nya korban jiwa yang muncul akibat serangan tersebut, namun sebagian besar yang dirasakan adalah ketakutan dan perasaan tidak aman setelah terjadinya perang siber tersebut. Iran merasa dikhianati oleh langkah-langkah keamanan siber negara yang tidak efektif dan sikapnya yang lemah sehubungan dengan para pelaku. Meskipun virus Stuxnet hanya menargetkan fasilitas nuklir Iran, fakta bahwa malware menyebar ke komputer lain di dunia berkontribusi pada perasaan tidak aman secara global (Baezner & Robin, Stuxnet, 2017)

2) Dampak Ekonomi

Serangan Stuxnet memberikan dampak signifikan terhadap ekonomi Iran. Selain mendapatkan embargo internasional, Iran juga dilarang untuk memiliki akses memasuki pasar internasional untuk memenuhi keperluan Iran dalam kebutuhan perkembangan nuklirnya. Adanya pembatasan yang dilakukan ini berdampak terhadap stok material dan sumber daya Iran terkhususnya

uranium untuk peningkatan program nuklir Iran. Selain itu adanya larangan khusus terkait pembatasan pembelian sentrifugal pengganti untuk kerusakan yang ditimbulkan virus Stuxnet mendorong Iran membangun sentrifugal demi lancarnya program nuklir Iran khususnya diwilayah Natanz setelah serangan tersebut. Iran juga merasakan tekanan pada anggaran dana yang semakin meningkat akibat serangan virus Stuxnet. Artinya, Iran harus mengeluarkan dana yang sangat banyak untuk untuk mampu bertahan dan memperbaiki semua kerusakan yang ditimbulkan (Zetter, 2015).

Iran pun merasakan dampak ekonomi yang cukup lama dikarenakan Iran yang harus mengeluarkan dana untuk pengembangan keamanan siber demi mencegah terulangnya peristiwa yang sama kepada negara Iran yang tidak menutup kemungkinan mempunyai banyak rival. November 2011, Iran membentuk unit siber baru dalam Pengawal Revolusi Iran terkait serangan yang dilakukan Amerika Serikat dan Israel. Pengawal Revolusi Iran atau lebih dikenal dengan Islamic Revolutionary Guards Corps (IRGC) atau Garda Revolusi, merupakan organisasi militer dan semi-militer yang bergerak dalam bidang pertahanan untuk melindungi negara Iran dari serangan musuh. IRGC juga mencakup keamanan siber di bidang pertahanan Iran (Banerjea, 2015).

3) Dampak Teknologi

Serangan Stuxnet berdampak pada perusahaan-perusahaan yang mengembangkan perangkat lunak. Perusahaan-perusahaan yang mengembangkan perangkat lunak dengan kerentanan untuk dieksploitasi, menginfeksi dan mengendalikan komputer di Iran terpaksa bereaksi untuk mengembangkan malware. Microsoft mengeluarkan tambalan untuk menyelesaikan eksploitasi zero-day dan Siemens menawarkan tambalan dan alat penghapusan kepada pelanggan mereka untuk menghapus Stuxnet dalam beberapa bulan setelah ditemukannya virus malware tersebut. Segala bentuk lisensi dan sertifikat ijin perusahaan yang dicurigai akan membahayakan keamanan negara Iran dicabut dan diberhentikan. Bilamana perusahan-perusahaan perangkat lunak lamban dalam menanggapi kasus ini, maka akan menyebabkan hilangnya kepercayaan dari pelanggan dalam kemampuan mereka untuk menghasilkan perangkat lunak dan teknologi yang aman. Konsekuensi teknologi jangka panjang juga dapat dilihat dari masyarakat Iran yang meningkatkan kewaspadaan dan ketidakpercayaan mereka terhadap teknologi dan malware yang mereka gunakan. Setiap munculnya beberapa bug atau erornya sistem dalam teknologi akan selalu dicurigai sebagai tindak kejahatan siber oleh pihak asing (Baezner & Robin, Stuxnet, 2017).

Dampak teknologi secara langsung secara fisik yang dirasakan oleh Iran adalah kerusakan sentrifugal. Sentrifugal sendiri merupakan alat yang dibutuhkan Iran untuk mengolah uranium yang akan diubah menjadi bahan bakar reaktor pengolahan nuklir (BBC, Iran mengakui fasilitas nuklirnya rusak parah setelah disabotase, 2021). Malware Stuxnet tersebut diyakini mempengaruhi kecepatan sentrifugal sehingga membuat sistem sentrifugal mengalami pergantian kecepatan antara kecepatan tinggi dan rendah. Perubahan kecepatan ini ditutupi oleh rootkit Stuxnet, sehingga membuat operator berpikir bahwa sentrifugal berjalan dengan kecepatan normal. Perubahan kecepatan akan menyebabkan sentrifugal lebih cepat aus dan rusak tidak dapat diperbaiki. Meskipun angka kerusakan mesin dan kerusakan sentrifugal cukup besar, namun kerusakan tersebut tidak memberikan efek besar terhadap jumlah sentrifugal lainnya yang tidak terkena dampak sama sekali. Jumlah dari sentrifugal yang dimiliki oleh Iran juga cukup besar, yakni sekitar 6000-9000 sentrifugal, sehingga kerusakan ini bahkan tidak merusak setengah dari jumlah sentrifugal yang ada (Paul K.

Kerr, 2010). Laporan IAEA mengatakan bahwa kerusakan yang dihasilkan oleh virus Stuxnet hanya membawa dampak yang kecil terhadap operasi nuklir Iran. Alat yang dipergunakan untuk mengolah uranium cenderung stabil meskipun terjadi peningkatan secara substansial terhadap sentrifugal. Meskipun memberikan dampak yang kecil, namun program nuklir Iran sempat berhenti selama dua tahun lamanya akibat serangan tersebut (Shakarian, Stuxnet: Cyberwar Revolution in Military Affairs, 2011).

Dampak Virus Stuxnet terhadap Kekuatan Iran di Timur Tengah

Kejahatan dan ancaman global, ditambah dengan kemajuan teknologi dan informasi sekarang tidak hanya ditujukan untuk menyerang pemerintah dan militer nasional, namun dapat pula menimbulkan ancaman ke seluruh bidang seperti ekonomi, politik, budaya, dan keamanan suatu negara. Ancaman kejahatan siber muncul dan dapat terjadi dikarenakan adanya kepentingan dari berbagai individu atau kelompok pihak-pihak tertentu. Ancaman ini dalam aspek kehidupan masyarakat menimbulkan berbagai ancaman baik ancaman fisik baik maupun non-fisik dengan menggunakan *(software)* untuk melakukan pencurian informasi dan data yang dapat mengancam suatu negara. Peningkatan terhadap ancaman kejahatan siber oleh negara ataupun aktor non-negara berdampak terhadap terjadinya Perang siber. Hal yang harus dilakukan dalam menghadapi ancaman kejahatan siber harus bisa dimanfaatkan baik dari dalam maupun luar negara dengan memanfaatkan kondisi sosial, politik, budaya, ideologi, dan perkembangan teknologi (Rahmawati, 2017).

Dalam kawasan Timur Tengah, keamanan nasional merupakan salah satu aspek yang paling penting dalam menjaga serta melindungi kepentingan nasional negara-masing masing. Amerika Serikat menganggap Iran merupakan rival yang berat dikawasan Timur Tengah terlebih lagi Iran sudah menjadi kekuatan penyeimbang (balance of power) di Timur Tengah. Hal ini telah membuat hegemoni Amerika Serikat di Timur Tengah semakin menurun (Saragih, 2017). Kepemilikan nuklir Iran telah membawa banyak keuntungan yang besar dalam menjaga posisi Iran di Timur Tengah. Negara yang memiliki nuklir akan dianggap sebagai negara terkuat dan berada di posisi *top of the table* di dalam hubungan internasional. Hal ini akan menguntungkan Iran dalam posisi kerjasama dalam hubungan Internasional. Disisi lain, nuklir membantu Iran dalam melindungi identitas nasionalnya di Timur Tengah, hal ini juga akan memperkuat keamanan nasional Iran yang membantu menjaga keamanan domestik Iran jangka panjang (Sinaga, 2009).

Sama halnya dengan dampak dari perang siber lainnya, serangan siber Stuxnet juga memberikan pengaruh besar terhadap posisi dan kekuatan Iran di kawasan Timur Tengah (Hidayat, Kepentingan Siber Ofensif Iran Terhadap Arab Saudi Dalam Kasus Virus ShamoonTahun 2012, 2020). Akibat serangan ini, fasilitas program nuklir Iran mengalami kerusakan dan kelumpuhan operasi sistem. Kelumpuhan program nuklir Iran selama 2 tahun pasca serangan Stuxnet, sempat menjadikan posisi Iran kedalam posisi yang genting diakibatkan masyarakat serta dunia internasional menganggap melemahnya posisi kekuatan Iran di Timur Tengah. Dengan diserangnya fasilitas nuklir Natanz yang merupakan wilayah paling penting dalam pengembangan nuklir Iran, maka dominasi Iran di Timur Tengah sebagai negara yang berada di posisi atas dikarenakan program nuklirnya menjadi hilang. Hal ini merubah pandangan dunia internasional bahwa Iran tidak lagi menjadi rival terberat di kawasan Timur Tengah. Kepemilikan nuklir Iran selama ini memberikan efek *deterrence* yang menguntungkan bagi Iran untuk meningkatkan kekuatan Iran di Timur Tengah. Namun akibat adanya serangan ini, efek *deterrence* yang ingin

diciptakan oleh Ahmadinejad seketika menjadi hilang.

Tersebarnya peristiwa serangan siber Stuxnet ke dunia internasional mengancam posisi keamanan nasional Iran di Timur Tengah. Iran menjadi sasaran empuk bagi negara-negara tetangga dikawasan Timur Tengah untuk dijadikan target serangan. Serangan siber Stuxnet dipercaya telah melemahkan kekuatan militer Iran, hal ini menyudutkan posisi Iran di Timur Tengah. Selain itu, serangan Stuxnet berdampak pada ketakutan Iran tersendiri. Iran mempercayai bahwa virus Stuxnet yang menjadi senjata Amerika Serikat dan Israel akan membuka celah bagi Amerika Serikat untuk menanamkan gagasan, ideologi dan nilai-nilai asing yang dikhawatirkan akan memberikan pengaruh terhadap identitas negara Iran. Apabila ideologi asing tersebut telah memasuki Iran, maka akan menimbulkan masalah baru terhadap perpecahan domestik yang memungkinkan terjadi di Iran (McCombie, 2012). Disisi lain, virus Stuxnet juga berdampak terhadap masyarakat dan juga kebijakan politik Iran di Timur Tengah (Hidayat, Kepentingan Siber Ofensif Iran Terhadap Arab Saudi Dalam Kasus Virus ShamoonTahun 2012, 2020). Di kawasan Timur Tengah sendiri, Stuxnet menjadi sebuah *"wake up call for state"*. Negara-negara kawasan Timur Tengah dan juga internasional menyadari, bahwa negawa di kawasan Timur Tengah dan negra barat perlu untuk mengembangkan kebijakan maupun strategi kekuatan siber negara mereka sendiri. Stuxnet juga berdampak dalam menurunkan ketegangan di kawasan Timur Tengah. Hal ini dikarenakan kekhawatIran dunia terkait program nuklir Iran berkurang semenjak serangan siber Stuxnet di wilayah Natanz. (Baezner & Robin, Stuxnet, 2017).

Hal itu tidak membuat Ahmadinejad membiarkan posisi Iran terus berlarut dalam keadaaan seperti itu. Ahmadineja d berupaya untuk menaikkan posisi Iran di kawasan Timur Tengah dengan mengembangkan serta memperbaiki program nuklir yang dimiliki nya terutama di wilayah Natanz. Pengembangan nuklir Natanz yang menjadi wilayah penting dalam perkembangan program nuklir Iran membuat Mahmoud Ahmadinejad menyadari bahwa nuklir akan membantu Iran untuk memberikan efek *deterrence* bagi negara yang ingin menyerang Iran. Diserangnya fasilitas program nuklir Natanz Iran telah disadari oleh Presiden Ahmadinejad. Ahmadinejad pun berusaha untuk memperbaiki kerusakan yang dihasilkan. Butuh waktu yang lama bagi Ahmadinejad untuk mengembalikan program pengayan nuklir Natanz seperti semula. Iran pun membuka kembali fasilitas program nuklir baru di wilayah yang sama yaitu Natanz. Namun dalam pengembangan program nuklir baru ini, Iran kembali menegaskan bahwa pengembangan program nuklir ini tidak berkaitan dengan pengembangan senjata nuklir yang mengancam keamanan dunia internasional (CNN, 2018).

Dengan adanya perang siber stuxnet, menjadi motivasi inspirasi baru serta membuka jalan baru untuk Iran dalam meningkatkan kekuatannya di kawasan Timur Tengah. Iran menyadari selain perlunya peningkatan program Iran, hal yang harus dikembangkan Iran adalah kekuatan sibernya. Iran mengubah gagasan serta pandangannya terhadap perlunya peningkatan kekuatan siber negaranya sendiri untuk mampu melawan ancaman kejahatan siber seperti perang siber Stuxnet. Dalam upaya Iran untuk meningkatkan kapabilitas kekuatan sibernya, Iran harus mengeksplorasi kapabilitas Iran dalam siber baik dari sumber daya ataupun kemampuannya untuk meningkatkan kepentingan nasionalnya terhadap siber. Apabila kekuatan siber Iran mampu ditingkatkan kedalam kemampuan yang lebih, maka kekuatan siber ini akan menjadi senjata baru bagi Iran untuk menyerang negara lain serta mempermudah Iran untuk mencari titik lemah musuh nya.

Keputusan Ahmadinejad untuk melakukan pengembangan kekuatan siber

Iran ternyata memberikan hasil dan dampak terhadap serangan selanjutnya. Stuxnet dijadikan contoh oleh Iran untuk membuat virus yang sama dan melakukan serangan yang sama terhadap negara yang ingin diserang. Kemampuan kekuatan siber Iran yang baru mampu untuk menyerang Arab Saudi. Hal ini dibuktikan dengan kasus *virus Shamoon* terhadap negara Arab Saudi. Serangan yang dilakukan Iran ini selain mempunyai kepentingan tersendiri atas serangan tersebut, juga mempunyai tujuan untuk membuktikan bahwa Iran mampu untuk berbuat hal sama terhadap negara lain. Iran juga secara tidak langsung menghukum Amerika Serikat dan sekutu internasional lainnya atas berbagai sanksi ketidakadilan yang didapatkan Iran atas pengembangan nuklirnya (Hidayat, 2012). Dan untuk membalas serangan Stuxnet yang dikirim oleh Amerika Serikat dan Israel, Iran yang pada awalnya berisikeras bahwa program nuklir yang dikembangkannya bukan untuk kepentingan senjata nuklir dan menentang semua tuduhan yang dilayangkan ke negara Iran, kini bereaksi membalas serangan tersebut dengan membatalkan sejumlah komitmen dan perjanjian untuk taat kepada IAEA (BBC, 2021).

Kemajuan teknologi siber Iran mengalami perkembangan yang begitu pesat setelah terjadinya serangan Stuxnet. Meskipun aktivitas dari siber Iran tidak sebanding dengan negara yang memiliki kekuatan siber yang lebih maju, namun kapabilitas Iran dalam melakukan siber ofensif terhadap negara yang ingin diserangnya. Dengan adanya pengembangan kekuatan siber Iran, maka kepentingan nasional Iran akan semakin terlindungi. Dengan hal ini pula, maka Iran akan mampu untuk mengembalikan posisi kekuatannya seperti semula. Kepentingan nasional Iran akan menjadi salah satu aspek penting dalam pelaksanaan politik nya di kawasan Timur Tengah. Kebijakan nasional Iran bercita-cita ingin menjadi pemimpin utama dan mendominasi. Kemudian dirumuskan pada identitas budaya nasional untuk ambisi hegemonik dan didukung dengan organisasi militer kuat.

Masyarakat Iran tidak akan lupa kepada sanksi yang diberikan oleh Amerika Serikat dan akhirnya dijatuhkan oleh negara-negara lain yang turut mendukung Amerika Serikat. Iran menyatakan bahwa tidak akan menjalin hubungan diplomatik dengan Amerika Serikat adalah kebijakan utamanya. Sudah sejak lama Iran tidak begitu peduli dengan keinginan Amerika Serikat di kawasan Timur Tengah yang dianggap ingin melakukan westernisasi. Karenanya ancaman kehadIran Amerika Serikat yang berada tepat diperbatasan Iran adalah sesuatu yang perlu dicermati dan dikhawatirkan oleh Iran. Selain tekanan dan ancaman diberikan oleh Amerika Serikat, Iran memiliki ancaman lainnya dari wilayah yang sama yaitu dari Israel. Jika Amerika Sserikat disebut sebagai *Big Evil*, maka Israel diistilahkan sebagai musuh bebuyutan karena selalu didukung oleh Amerika Serikat dalam semua tindakannya. Hal ini menyiratkan bahwa ancaman dari Amerika Serikat dan Israel sejalan dalam menekan Iran untuk tidak memiliki perangkat pertahanan jika diserang, yaitu nuklir. Bagi Iran, cara terbaik mengatasi kemungkinan-kemungkinan yang buruk dan bisa saja terjadi, misalkan diinvasi Amerika Serikat, maka memiliki nuklir adalah sebuah hal yang diperlukan. Iran dapat dikategorikan sebagai negara yang tertinggal dalam pengembangan persenjataan militernya. Aspek militer sendiri adalah bagian penting bagi keamanan dan kekuatan nasional. Dan hal ini adalah potensi yang bisa dimiliki dengan kepemilikan senjata nuklir (Sinaga, 2009).

KESIMPULAN

Negara juga harus mampu meningkatkan keamanan siber mereka dengan membuat prosedur operasi pencegahan kejahatan siber untuk menanggapi serangan siber. Prosedur ini dapat dilakukan pada tingkat teknis

dengan pakar keamanan siber yang bertindak cepat untuk memecahkan masalah teknis yang terkait dengan serangan tersebut. Ketika Iran menyadari bahwa negara mereka telah menjadi sasaran serangan siber, tampaknya ada kebingungan di dalam otoritas Iran tentang cara untuk menanggapi serangan itu secara politis. Oleh karena itu, prosedur operasi standar di tingkat politik juga dapat membantu memberikan panduan kepada pihak berwenang tentang bagaimana menanggapi serangan siber yang dilakukan oleh negara lain.

Serangan siber virus Stuxnet merupakan salah satu bukti nyata perkembangan kejahatan siber dimasa depan. Stuxnet telah menggeser paradigma bahwa perang dimasa depan tidak lagi menggunakan kekuatan militer secara fisik dan menimbulkan korban jiwa. Stuxnet telah menciptakan revolusi di bidang perang karena salah satu senjata tersebut dapat digunakan untuk mendapatkan akses ke pusat nuklir negara lain, karena hal ini pula serangan siber dengan menggunakan virus sebagai senjata menjadi paling berbahaya dan mematikan kemajuan dalam taktik perang. Dunia internasional menjadikan peristiwa ini sebagai pelajaran pacuan untuk peningkatan kekuatan siber nasional negara untuk mencegahnya perkembangan peristiwa yang sama di masa depan dengan mengambil tindakan pencegahan ancaman siber.

Kerusakan yang disebabkan oleh Stuxnet pada sentrifugal Iran menunjukkan bahwa infrastruktur penting dapat menjadi sasaran ancaman siber. Fakta bahwa jaringan Natanz terpisah dari jaringan lain sehingga tidak cukup untuk melindungi program nuklir Natanz dari serangan virus Stuxnet. Oleh karena itu, negara harus mempertimbangkan bahwa infrastruktur penting harus diintegrasikan dalam strategi keamanan siber. Pertimbangan tersebut akan menyiratkan peningkatan perlindungan terkait dengan ancaman siber, dengan standar keamanan siber. Hal ini juga bertujuan untuk meningkatkan perlindungan terhadap ancaman siber, dan juga untuk meningkatkan ketahanan jika terjadi serangan siber.

Negara harus meningkatkan kekuatan sibernya agar mampu untuk melindungi negaranya dari serangan negara lain untuk menyerang negaranya. Perlu adanya peningkatan keamanan siber dengan melibatkan kebijakan siber kedalam peraturan dan aturan militer sebuah negara. Melihat perkembangan perang tidak lagi menggunakan perang konvensial di masa depan, maka negara harus mampu untuk mempersiapkan dirinya secara matang agar mampu menghadapi ancaman serupa.

DAFTAR PUSTAKA

BUKU

Agus Triartono, S. I. (2019). *Keamanan dan Sekuritisasi dalam Hubungan Internasional.* Jawa Barat: Melvana Publishing.

Baezner, M., & Robin, P. (2017). *Stuxnet.* Zürich: Security Studies (CSS), ETH Zürich.

Creswell, J. (1998). Research Design : Qualitative and Quantitative Approaches. *Thousand Oaks : Sage Production*.

Dr.Maskun S.H, L., Achmad S.H M, H., Dr.Naswar S.H, M., Hassidiq, H., Shafira, A., & Lubis, S. N. (2020). *Korelasi Kejahatan Siber & Kejahatan Agresi Dalam Perkembangan Hukum Internasional.* Makassar, Sulawesi Selatan, Indonesia: Nas Media Pustaka.

Hadi, A. (2005). *Matinya Dunia Cyberspace.* Sewon bantul,

Yogyakarta, Indonesia: LKiS Yogyakarta.

Moore, R. (2011). *Cybercrime : Investigating High-Technology Computer Crime.* United State of America: Anderson Publishing.

Pace, P. (2006). *National Military Strategy for Cyberspace Operation (NMS-CO).* Washington DC: Departmen Of Defense Washington.

Paul K. Kerr, J. R. (2010). *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability.* Congressional Research Service .

Rohozinski, J. P. (2013). *Stuxnet and the Future of Cyber War.* London: Routledge.

Sugiyono. (2013). *Metode Penelitian Kuantitatif,Kualitatif,dan R&D.* Bandung: Penerbit Alfabeta.

Supriyadi. (85). Community of Practitioners : Solusi Alternatif Berbagi Pengetahuan antar Pustakawan. *Lentera Pustaka*, 2016.

Syani Zuraida, Y. (n.d.). Stuxnet Amerika Serikat dalam Kerangka Neo-Realisme. 83.

Tampubolon, K. E. (2019). Perbedaan Cyber Attack,Cyber Crime dan Cyber Warfare. *Jurist-Diction Journal*, 546-547.

Tarock, A. (2014). *Iran's Nuclear Programme and The West.* London: Routledge.

W.Creswell, J. (2008). *Qualitative Inquiry & Research Design : Choosing Among Five Approaches.* United States of America: Sage Publication L.td.

Winterfeld, J. A. (2011). *Cyber Warfare : techniques,tatics and tools for security practitioners.* United State of America: Elsevier.

Yaphe, J. S. (2010). *Nuclear Politics in Iran.* Washington, D.C.: National Defense University Press.

JURNAL

Akbar, Z. E. (2015). Kepentingan Rusia dibalik dukungannya terhadap Program Nuklir Iran. *Jurnal Ilmu Hubungan Internasional*, 5-9.

Banerjea, U. (2015). Revolutionary Intelligence: The Expanding Intelligence Role of the Iranian Revolutionary Guard Corps. *Journal of Strategic Security*, 97-99.

Basri, T. H. (2014). Sejarah dan Pengembangan Senjata Nuklir. *Jurnal Seuneubok Lada, 2*, 98-100.

Eberle, C. J. (2013). Just Cause and Cyber War. *Journal of Military Ethics*, 8.

Frances Ryan, M. C. (2009). Interviewing in Qualitative Research : The one-to-one interview. *International Journal of Teraphy and Rehabilitation*, 310.

Hadi, S. (2016). Pemeriksaan Keabsahan Data Peneltiian Kualitatif pada Skripsi. *Jurnal Ilmu Pendidikan*, 75.

Hadžikadunić, E. (2014). Understanding Iranian Foreign Policy-The Case of Iranian Nuclear Program. *Journal of Transdiciplinary Studies*, 7-9.

Hidayat, A. (2012). Kepentingan Siber Ofensif Iran Terhadap Arab Saudi Dalam Kasus Virus ShamoonTahun 2012. *Global Political Studies Journal*, 106-108.

Hidayat, A. (2020). Kepentingan Siber Ofensif Iran Terhadap Arab Saudi Dalam Kasus Virus ShamoonTahun 2012. *Global Political Studies Journal*, 118-119.

Irawan, D. (2021). Dinamika Keamanan Kawasan Timur Tengah dalam Persaingan Kekuatan Iran dan Amerika Serikat. *Dauliyah*, 238-239.

Kamiński, M. A. (2020). Operation Olympic Games : Cyber Sabotage as a tool of American Intelligence aimed at counteracting the development of Iran's Nuclear Programme. *Security Defense Quartelly*, 65-66.

Kiki Mikail, A. F. (2019). Program Pengembangan Nuklir Iran dan Pengaruhnya terhadap Masyarakat Iran (1957-2006 M). *Jurnal Studi Sosial dan Politik*.

McCombie, S. C. (2012). Stuxnet: the emergence of a new cyber weapon and its implications. *Journal of Policing,Intelligence nd Counter Terrorism*, 80-89.

Melysa, A. (2016). Analisis Penggunaan Offensive Cyber Operations Menghadapi Ancaman Nuklir Iran. *Journal of International Relations*, 214.

Mikail, K. (2019). Program Pengembangan Nuklir Iran dan Pengaruhnya terhadap Masyarakat Iran. *Jurnal Studi Sosial dan Politik*, 7-10.

Mir, K. A. (2014). Iran Nuclear Programme: Revisiting the Nuclear Debate. *Journal of Power, Politics & Governance*, 224-226.

Mohamed Chawki, A. D. (2015). Cybercrime,Digital Forensics and Jurisdiction. 3.

Mulyadi, M. (2011). Peneltian Kuantitatif dan Kualitatif serta Pemikiran

Dasar Menggabungkannya. *Jurnal Studi Komunikasi dan Media*, 1-2.

Mundzir, C. (2020). Dimensi Islam dan Politik : Telaah Historis atas Revolusi Iran 1979. *Jurnal al-Hikmah*, 36-40.

Nahak, S. (2017). Hukum Tindak Pidana Mayantara (Cyber Crime) dalam perspektif akademi. *Jurnal Prasada*, 3-6.

Nugroho, A. (2012). Dukungan Cina Terhadap Program Nuklir Iran (2006-2009). *Jurnal Transnasional, 4*, 2-6.

Putri, G. E. (2016). Pandangan Politik Mahmoud Ahmadinejad Studi Kasus : Hubungan Iran-Amerika Serikat (2005-2009). *Dauliyah Journal of Islamic and International Studies*, 160-162.

Rahman, A. B. (2017). Editorial : Keamanan Internasional. *Journal of International Studies*, 1-3.

Rahmawati, I. (2017, Agustus). Analisis Manajemen Risiko Ancaman Kejahatan Siber (cyber crime) dalam peningkatan Cyber Defense. *Jurnal Pertahanan dan Bela Negara, 7*, 56-57.

Raodia. (2019). Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime). *Jurisprudentie*, 232-233.

Raouf, H. (2019). Iranian quest for Regional Hegemony : Motivations,Strategies and Contrains. *Journal Emerald*, 243-248.

Rashid.dkk, Y. (2019). Case Study Method: A Step-by-Step Guide. *International Journal of Qualitative Methods*, 5.

Rijali, A. (2018). Analisis Data Kualitatif. *Jurnal Alhadharah*, 94.

Riyadi. (2016). Kajian Ancaman Cyber Security Terutama apda Fasilitas Nuklir Untuk Meningkatkan Keamanan dan Ketahanan Nasional. *Pusat Pengkajian Sistem dan Teknologi Pengawasan Instalasi dan Bahan Nuklir*, 1.

Rosaliza, M. (2015). Wawancara,sebuah interaksi komunikasi dalam penelitian kualitatif. *Jurnal Ilmu Budaya*, 71-72.

S.Bachri, B. (2010). Meyakinkan Validitas Data Melalui Triangulasi Pada Peneltiian Kualitatif. *Jurnal Teknologi Pendidikan*, 55-56.

Saldanha, P. (2017). Keefektifan Konvensi NPT dalam Menangani negara Pengguna Senjata Nuklir. *Journal Islamic World and Politics*, 132-136.

Saragih, H. M. (2017). Perubahan Arah Kebijakan Luar Negeri Iran

Terhadap Amerika Serikat Dalam Progam Nuklir Iran pada masa pemerintahan Hassan Rouhani. *Jurnal Interdependence*, 17-19.

Sembiring, Z. (2020). Stuxnet Threat Analysis in SCADA (Supervisory Control And Data Aquisition) and PLC (Programmable Logic Controller) Systems. *Journal of Computer Science, Information Technology and Telecommunication Engineering (JCoSITTE)*, 98.

Shakarian, P. (2011). Stuxnet: Cyberwar Revolution in Military Affairs. *Small Wars Journal*, 4-5.

Shakarian, P. (2011). Stuxnet: Cyberwar Revolution in Military Affairs. *Small Wars Journal*, 2-7.

Sinaga, O. (2009). Kepemilikan Nuklir dan keamanan Nasional iran : Suatu Studi Kasus. *Sosiohumaniora*, 28.

Stevens, C. (2019). Assembling Cybersecurity : The Politics and materiality of technical malware reports and the Case of Stuxnet. *Contemporary Security Policy*, 2-4.

Subagyo, A. (2015). Sinergi Dalam Menghadapi Ancaman Cyber Warfare Synergy in Facing of Cyber Warfare Threat. *Jurnal Pertahanan*, 96-99.

Sundari, R. (2020). Strategi Amerika Serikat Dalam Menekan Pengembangan Nuklir Iran. *Frequency of International Relations*, 317-322.

Sya'roniRofii. (2010). Membayangkan DuniaTanpa Senjata Nuklir: NPTdan Post-agreement Negotiation. *Jurnal Multiversa*, 3-10.

Sya'roniRofii, M. (2015). Babak Baru Nuklir Iran:Memahami Manuver Irandan Dinamika Politik Kawasan Timur Tengah. *Jouranal of Integrative International Relations*, 29-31.

ARTIKEL

Fauzi, M. Z. (2018). Strategi Pemerintahan Ahmadinejad dalam Penolakan Penghentian Program Nuklir iran Yang Berdampak Terhadap Semakin Memburuknya Hubungan Iran dengan Amerika Serikat tahun 2005-2009. 3-15.

Ganji, B. (2006). Politics of confrontation: the foreign policy of the USA and revolutionary Iran.

Hikmatul Akbar, P. K. (2012). Perkembangan Nuklir Iran dan Diplomasi kepada IAEA. 19.

Kubbig, P. D. (2006, August 3). Iran and the Nuclear Non-Ploriferation Treaty.

Kushner, D. (2019). The Real Story of Stuxnet. 2.

Langner, R. (2011). *Stuxnet: Dissecting a Cyberwarfare Weapon.* THE IEEE COMPUTER AND RELIABILITY SOCIETIES.

SUMBER ONLINE

Affairs, O. O. (2020, March 16). *United Nations*. Retrieved from United Nation: https://www.un.org/disarmament/wmd/nuclear/npt/

BBC. (2021, April 14). *BBC News*. Retrieved 2 31, 2021, from bbc.com: https://www.bbc.com/indonesia/dunia-56713445

BBC. (2021, April 12). *BBC NEWS*. Retrieved 1 5, 2022, from BBC.com: https://www.bbc.com/indonesia/dunia-56713445

CNN. (2018, June 7). *cnnindonesia.com*. Retrieved 1 5, 2022, from CNN Indonesia: https://www.cnnindonesia.com/internasional/20180607153103-120-304333/iran-buka-fasilitas-nuklir-baru-di-natanz

PBS. (2021, April 13). *PBS Frontline*. Retrieved from pbs.org: https://www.pbs.org/wgbh/pages/frontline/shows/tehran/axis/map.html

Primer, T. I. (2020, March 17). *United States Institute of Peace*. Retrieved from The Iran Primer: https://iranprimer.usip.org/blog/2020/jan/22/iran-and-npt#:~:text=1968,develop%20or%20acquire%20nuclear%20weapons

Syafnidawaty. (2020, october 29). *Universitas Raharja*. Retrieved from raharja.ac.id: https://raharja.ac.id/2020/10/29/penelitian-kualitatif/

Worldmeter. (n.d.). Retrieved 1 14, 2022, from worldmeters.info: https://www.worldometers.info/oil/iran-oil/

Zetter, K. (2015, 10 02). *Wired*. Retrieved 12 31, 2021, from Wired.com: https://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/