

# **BAB I**

## **PENDAHULUAN**

### **I.1 Latar Belakang**

Perkembangan teknologi dan informasi pada masa kini memberikan dampak dan pengaruh yang sangat besar terhadap globalisasi. Perkembangan yang dialami pada bidang komputer dan internet semakin memudahkan masyarakat untuk menjalankan aktivitas sehari-harinya dan mendapatkan informasi sebanyak-banyaknya tanpa ada batasan. Dengan menggunakan alat teknologi, apa yang kita inginkan bisa didapatkan tanpa harus pergi dan melihat secara langsung. Meskipun perkembangan teknologi semakin maju, tidak berarti bahwa pengaruh yang diberikan selalu positif. Aktor-Aktor dunia terkadang memanfaatkan pesatnya teknologi untuk menjalankan kepentingannya. Jaringan internet pada dasarnya merupakan media yang sangat mudah dipakai untuk tindakan kriminal. Masyarakat yang tidak bisa lepas akan media sosial dijadikan sebagai keuntungan bagi para oknum untuk melancarkan segala cara menjalankan setiap tujuan yang ingin dicapai. Internet yang seharusnya digunakan untuk menghasilkan dampak positif justru disalahgunakan sebagai alat propaganda dan menyerang negara lain. Pengembangan internet sebagai media informasi pada akhirnya berkembang menjadi kejahatan dunia maya yang digunakan untuk menyebarkan ancaman. Hal ini membawa potensi kejahatan siber baik dari skala yang rendah maupun tingkat yang tinggi.

Dengan perkembangan teknologi yang semakin tidak terkontrol ditambah dengan ketidaktersediaan pengawasan, maka kejahatan siber mampu mengganggu stabilitas dalam berbagai aspek baik dalam aspek politik, sosial-budaya, ekonomi, dan aspek keamanan nasional negara tersebut. Kejahatan siber akan dikatakan sebagai sebuah kejahatan bila mana terjadi sebuah “pelanggaran” yang menggunakan media komputer untuk meretas dan merugikan pihak lain (Chawki, 2015). Kejahatan siber pertama kali terjadi pada tahun 1990-an. Pada saat itu perkembangan teknologi digunakan untuk mencari keuntungan oleh pihak-pihak

tertentu. Adapun kejahatan yang dilakukan yaitu menyerang portal dan website publik maupun perorangan (Raodia, 2019). Hal ini membuktikan bahwa seiring dengan bertambahnya kualitas konektivitas, semakin besar peluang dari kejahatan siber meningkat. Peningkatan ini diikuti dengan bertambahnya berbagai jenis kejahatan seperti manipulasi data, menyebarkan propaganda, spionase, peretasan, penipuan, pencurian dan lainnya. Dalam beberapa dekade ini, ancaman dunia maya bahkan telah berdampak kepada kerusakan fasilitas nuklir diseluruh dunia. Hal ini dipercaya akan berdampak kepada stabilitas keamanan dan ketahanan suatu negara (Riyadi, 2016).

Kajian Nuklir timbul menjadi sebuah fenomena baru ketika nuklir dialihfungsikan 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 mencegah 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 kerusakan yang terjadi. Permasalahan konflik internal di Iran yang tidak berhenti membuat Mahmoud harus mengambil kebijakan yang bertujuan untuk menjaga keamanan negaranya. Salah satu 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 program nuklir ini berada di Natanz, Isfahan dan Pars Tash. Ahmadinejad melalui Dewan Tinggi Keamanan Nasional Iran memberitahukan pembukaan 3 lokasi pengayaan menandakan Iran siap untuk memulai kembali program nuklir nya 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 terorisisme 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 diseluruh 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 untuk memperbaiki sistem komputer dan sistem operasi dengan memulihkan sumber daya dan memprogram ulang sistemnya.

Dalam mendukung penelitian, penelitian ini disertakan dengan penelitian terdahulu yang didapatkan dari berbagai sumber. Pertama, pada tahun 2019 oleh Raodia yang berjudul “*Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara*”. Artikel ini membahas pengaruh kemajuan Teknologi Informasi dan Komunikasi (TIK) dalam peningkatan kejahatan siber di Indonesia, yang dalam hal ini memungkinkan untuk menciptakan ancaman kejahatan yang semakin luas dan menimbulkan jenis ancaman yang baru. Artikel ini juga mendiskusikan tentang pencegahan dan penanggulangan kejahatan mayantara (cybercrime) dengan melibatkan berbagai aspek. Pencegahan akan menjadi efektif

jika Ilmu Pengetahuan dan Teknologi (IPTEK) dimanfaatkan dengan baik dan diimplementasikan dengan tepat (Raodia, 2019).

Acuan penulis pada artikel tersebut adalah kejahatan mayantara yang ditimbulkan oleh kemajuan IPTEK yang dampaknya menimbulkan ancaman baru khususnya dalam dunia maya. Dengan hal ini membuktikan bahwa kemajuan Teknologi dan Informasi (TIK) tidak semuanya memberikan hasil yang positif, karena tidak dipungkiri beberapa aktor internasional masih ingin memainkan kepentingannya atas negara lain. Perbedaan yang terdapat dalam artikel di atas dengan tulisan ini berada pada objeknya. Tulisan ini menggunakan Iran sebagai objeknya, sedangkan artikel tersebut menggunakan Indonesia sebagai objek yang diteliti.

Kajian kedua ditulis oleh Paulino Saldanha pada tahun 2017 “*Keefektifan Konvensi NPT dalam Menangani Negara Pengguna Senjata Nuklir*”. Artikel ini fokus membahas mengenai keefektifan NPT dalam menangani senjata nuklir di dunia. Senjata nuklir pada umumnya dikenal sebagai senjata pemusnah massal. Peristiwa bom Hiroshima dan Nagasaki yang dilakukan Amerika Serikat pada tahun 1945 membuka mata dunia untuk menetapkan kebijakan untuk mengatur kepemilikan senjata agar tidak terulang terjadinya peristiwa yang sama dimasa depan. Dengan munculnya NPT sebagai suatu prosedur dan kebijakan maka aturan ini harus diikuti oleh negara yang memiliki senjata nuklir (Saldanha, 2017). Perbedaan artikel tersebut dengan tulisan ini berada pada focus pembahasan. Kajian ini berfokus kepada kesuksesan NPT dalam menekan dan mengontrol negara yang memiliki senjata nuklir agar tidak digunakan untuk kepentingan yang merugikan keamanan dan perdamaian dunia. Artikel tersebut menjelaskan bagaimana pengaruh NPT terhadap negara anggotanya dalam mencoba mengarahkan negara anggota NPT untuk patuh dan mengikuti aturan NPT. Namun ternyata tidak semua anggota mengikuti dan mematuhi NPT. Berawal dari ketidakpatuhan ini maka akan memungkinkan terealisasinya kepentingan aktor untuk memakai senjata nuklir dalam mencapai tujuannya. Dengan perkembangan peradaban manusia yang semakin modern, maka NPT harus semakin matang untuk

melakukan kontrol terhadap kepemilikan senjata nuklir dan memberikan sosialisasi secara global.

Kajian ketiga diambil dari artikel yang ditulis oleh Ary Melysa pada tahun 2016 dengan judul "*Analisis Penggunaan Offensive Cyber Operatios Menghadapi Ancaman Nuklir Iran*". Artikel ini memfokuskan pada strategi dan cara yang diambil oleh Amerika Serikat dan Israel dalam menanggapi ancaman nuklir di Iran. Artikel ini meninjau dan mendiskusikan langkah dan tindakan yang diambil untuk mencegah dan menghambat program nuklir Iran yang telah mengancam keamanan dunia internasional. Hal ini akan menjadi alat bantu yang penting bagi Iran untuk mengkaji bagaimana berjalannya *Offensive Cyber Operation* untuk menyerang dan memperkuat *Cyber Defense* dengan menggunakan dunia maya sebagai pertahanan keamanan nasional Iran. Selain itu artikel ini juga membahas keuntungan yang didapatkan dalam penggunaan operasi cyber ofensif yang ekonomis yang mampu untuk mengurangi kerusakan fisik dan meminimalisir timbulnya korban jiwa (Melysa, 2016).

Penulis menjadikan artikel ini sebagai acuan dalam hubungan kerjasama pemerintah secara Internasional dalam penggunaan cyber sebagai metode baru dalam menjaga keamanan nasional. Iran yang memiliki sumber daya yang begitu kaya diiringi dengan perkembangan teknologi yang semakin canggih akan membantu Iran dalam menggunakan nuklir nya sebagai alat untuk menjaga teritori dan menjadikan nuklir sebagai salah satu alat yang mampu digunakan untuk memajukan pertahanan nasional. Perbedaan antara artikel tersebut terhadap penelitian ini berada pada studi kasus. Artikel ini menjadikan Amerika Serikat dan Israel sebagai objek penelitian sedangkan penulis menjadikan Iran sebagai objek yang diteliti.

Selanjutnya, kajian keempat diambil dari artikel yang ditulis oleh Zulfikar Sembiring pada tahun 2020 dengan judul "*Stuxnet Threat Analysis in SCADA (Supervisory Control and Data Acquisition) and PLC (Programmable Logic Controller) System*". Artikel ini memfokuskan tentang cara kerja malware Stuxnet yang ditargetkan pada sistem SCADA (Supervisory Control And Data Acquisition) dan PLC (Programmable Logic Controller). Artikel ini juga menjelaskan

sistematika dan proses yang dilalui oleh virus Stuxnet dalam melumpukan program nuklir Iran di Natanz. Selain itu, artikel ini juga mendiskusikan pencegahan yang dapat dilakukan untuk melawan ancaman Stuxnet. Hal ini akan menjadi alat bantu yang cukup penting untuk pemerintahan Iran dalam memastikan keamanan negaranya dari ancaman siber dimasa depan (Sembiring, 2020).

Penulis menjadikan artikel tersebut menjadi acuan karena artikel tersebut menjelaskan bagaimana proses Stuxnet dalam menyebarkan virusnya pada SCADA dan PLC yang merupakan alat kontrol fasilitas Iran. Dalam hal ini Iran perlu untuk menilik kembali bagaimana kemampuan Iran dalam kemajuan sistem kontrol program nuklirnya. Perbedaan artikel tersebut terhadap penelitian ini berada pada focus pembahasan. Dalam artikel ini menjelaskan dengan seksama bagaimana virus Stuxnet bekerja untuk mengambil alih alat kontrol fasilitas program nuklir Iran, sedangkan tulisan ini membahas mengenai dampak yang ditimbulkan virus Stuxnet terhadap keefektifitasannya untuk melumpuhkan program nuklir Iran.

Sumber kajian kelima diambil dari artikel yang ditulis oleh Mariuz Antoni Kamiński pada tahun 2019 yang berjudul “*Operation Olympic Games.*” *Cyber-Sabotage as a tool of American intelligence aimed at counteracting the development of Iran’s Nuclear Programme*”. Artikel ini membahas sejarah terciptanya *Operation Olympic Games* sebagai alat untuk menyerang program nuklir Iran dengan bantuan badan intelijen Amerika Serikat dan Israel. Penggunaan *Operation Olympic Games* membuktikan bahwa operasi sabotase yang dilakukan dunia maya dengan skala yang luas mampu untuk mengakibatkan kerusakan infrastruktur penting dalam skala besar yang melibatkan berbagai sumber daya negara dan aktivitas dunia maya. Negara yang kuat dengan kepemilikan badan intelijen yang berkembang merupakan perpaduan yang baik dalam melakukan sabotase dengan tingkat kehancuran yang diharapkan (Kamiński, 2020). Perbedaan artikel tersebut dengan tulisan diatas terletak pada pembahasannya. Artikel tersebut membahas tentang latar belakang politik yang bertujuan untuk menghambat pengembangan nuklir Iran dengan melibatkan badan intelijen Amerika Serikat dan Israel, sedangkan tulisan ini membahas mengenai hasil dari konsekuensi virut Stuxnet yang berpengaruh terhadap kemajuan pengayaan fasilitas nuklir Iran.



Bahan kajian keenam, diambil dari artikel yang ditulis oleh Emir Hadžikadunić pada tahun 2014 berjudul *“Understanding Iranian Foreign Policy- The Case of Iranian Nuclear Program”* (Hadžikadunić, 2014). Artikel ini mendiskusikan orientasi kebijakan program nuklir Iran yang dilihat dari 3 kepemimpinan presiden terakhir Iran yaitu Mohammad Khatami, Mahmoud Ahmadinejad dan Hassan Rouhani dalam menyelesaikan permasalahan dengan komunitas internasional dalam kemajuan program nuklirnya. Penelitian ini tidak akan lengkap bila tidak dilihat dari kepemimpinan Ali Khamenei yang mempunyai kekuatan otoritas tertinggi. Perbedaan artikel tersebut terhadap tulisan ini terletak pada studi kasus. Artikel ini menjelaskan tentang bagaimana ekspektasi kebijakan nuklir terhadap kebijakan nuklir yang konsisten dalam memperjelas kekuatan yang mendominasi di Timur Tengah. Penulis menjadikan artikel tersebut sebagai acuan karena keputusan kebijakan luar negeri tentang nuklir Iran dan hubungannya dengan teori hubungan internasional dalam mengidentifikasi kebijakan luar negeri siapa yang paling dominan dan paling efektif dalam memajukan peningkatan program nuklir di Iran khususnya wilayah Natanz.

Berikutnya, artikel ketujuh ditulis pada tahun 2019 oleh Kiki Mikail dan Achmad Fathoni yang berjudul *“Program Pengembangan Nuklir Iran dan Pengaruhnya terhadap Masyarakat Iran ( 1957-2006 M )”* (Mikail, 2019). Artikel ini mendiskusikan mengenai pengembangan program nuklir Iran yang menimbulkan konflik dan respon negative dari dunia barat. Selain itu didalam artikel ini membahas tentang sejarah munculnya program nuklir Iran dan dinamika yang dihadapi Iran dalam pengembangan kebijakannya dan respon dari Timur Tengah serta negara barat terhadap keputusan yang diambil Iran tersebut.

Penulis menjadikan artikel tersebut sebagai acuan karena ingin melihat bagaimana dampak yang muncul terkait dengan hubungan antara Iran dengan Amerika Serikat. Selain itu pula Iran harus menerima konsekuensi yang ditimbulkan akibat kebijakannya yaitu sanksi embargo internasional yang mengakibatkan terhambatnya ekspor minyak dan gas yang dimiliki Iran. Perbedaan artikel tersebut dengan tulisan ini terletak pada pembahasannya. Artikel ini mengkaji bagaimana perkembangan dinamika program nuklir Iran yang berdampak ke berbagai bidang seperti dampak ekonomi, politik, sosial budaya dan termasuk pengembangan nuklir

Iran sendiri dikarenakan sanksi yang diberikan dengan menyegel beberapa program nuklir Iran yang salah satunya berada di wilayah Natanz, sedangkan tulisan ini membahas mengenai kebijakan Ahmadinejad terkait program nuklir Iran yang berdampak kepada penyerangan program nuklir Iran yang berada di wilayah Natanz.

Selanjutnya, bahan kajian kedelapan ditulis oleh Christopher J. Eberle pada tahun 2013 yang berjudul "*Just War and Cyber War*" (Eberle, 2013). Dalam artikel ini membahas bagaimana serangan dunia maya dikatakan sebagai perang siber serta faktor yang mendukung serangan tersebut dikategorikan sebagai perang. Untuk menentukan apakah serangan dunia maya menimbulkan perang maka harus memiliki pemahaman yang jelas mengenai persyaratan perang. Hal ini membantu untuk menjelaskan apakah serangan sutyxnet dikategorikan sebagai perang siber atau sebaliknya. Penulis menjadikan artikel ini sebagai acuan karena virus Stuxnet tidak berdampak kepada jumlah korban yang jatuh. Hal ini mendukung bahwa dampak dari virus ini tidak berdampak langsung terhadap masyarakat. Virus Stuxnet berdampak kepada ekonomi yang diberikan serangan dunia maya kepada Iran. Perbedaan tulisan ini dengan artikel tersebut berada pada pembahasannya, artikel tersebut mendiskusikan mengenai penyebab dan hal yang dikategorikan sebagai sebuah perang siber, sedangkan tulisan ini mendiskusikan Stuxnet sebagai dampak berjalannya program nuklir diluar pengawasan IAEA.

Artikel yang digunakan untuk kajian kesembilan ditulis oleh Gustri Erni Putri pada tahun 2016 yang berjudul "*Pandangan Politik Mahmoud Ahmadinejad Studi Kasus : Hubungan Iran-Amerika Serikat (2005-2009)*" (Putri, 2016). Artikel ini menjelaskan tentang kepemimpinan Mahmoud Ahmadinejad dengan keputusannya yang berpengaruh terhadap hubungan antara Iran dengan Amerika Serikat. Faktor kepemimpinan Ahmadinejad yang memulai kembali program nuklir Iran pada tahun 2005 dan mencari dukungan serta kekuatan dari negara lain membuat Amerika menentang kebijakan ini. Dalam hal ini Ahmadinejad tetap kokoh terhadap keputusannya dan bersikap lebih keras terhadap perundingan-perundingan dengan negara Eropa demi membela harga diri Iran dan program nuklirnya. Diantara artikel diatas dengan penelitian ini memiliki perbedaan pada fokus pembahasannya. Artikel diatas lebih fokus membahas tentang kebijakan

politik Ahmadinejad dalam menentukan masa depan program nuklir Iran yang mempengaruhi hubungan antara Iran dan Amerika Serikat. Sebagai pemimpin Iran, Ahmadinejad mempunyai kekuasaan untuk membawa arah kebijakan Iran. Kebijakan ini akan menjadi kuat dengan dukungan dari pejabat nasional yang akan menguatkan kedudukan Ahmadinejad. Cara radikal yang sering diambil Ahmadinejad dalam mencapai tujuan politiknya akan menyulitkan Iran untuk mempunyai hubungan yang baik khususnya terhadap Amerika Serikat.

Kajian yang terakhir merupakan artikel yang berjudul “*Assembling Cyber Security : The Politics and Materiality of Technical Malware Reports and the case of Stuxnet*” yang ditulis oleh Iare Stevens pada tahun 2019 (Stevens, 2019). Artikel ini berfokus bagaimana peran besar Symantec dalam mendeteksi adanya virus Stuxnet yang menyerang program nuklir Iran. Symantec sendiri merupakan perusahaan pencipta perangkat lunak yang diciptakan oleh Amerika Serikat. Symantec sendiri menjadi kontroversi karena diyakini tujuan Symantec diciptakan untuk mencapai tujuan politik Amerika. Penulis menjadikan jurnal ini sebagai acuan karena Iran perlu menjadikan Symantec sebagai salah satu contoh nyata dalam mendukung kemajuan siber di Iran. Jika pemerintah Iran membuat perusahaan pendeteksi virus yang sama, maka akan sangat membantu Iran dalam melihat ancaman dimasa depan yang akan mengganggu stabilitas dan keamanan regional Iran.

## **I.2 Rumusan Masalah**

Tindakan Iran yang tetap mengembangkan program nuklir nya dan juga sikap nya yang terus menolak resolusi dan tidak mengikuti keinginan dunia terkait penghentian program nuklir yang dikembangkan Mahmoud Ahmadinejad pada tahun 2010 mendapatkan kecaman dari dunia internasional yang menganggap nuklir Iran merupakan ancaman bagi keamanan dan perdamaian dunia internasional. Amerika Serikat dan Israel yang memiliki kepentingan di kawasan Timur Tengah juga merasa bahwa tindakan Iran ini akan mengganggu kepentingan Amerika Serikat dan Israel di kawasan Timur Tengah. Karena kekhawatiran tersebut AS dan Israel membuat malware bernama Stuxnet untuk

melumpuhkan program nuklir Iran yang berada di Natanz. Malware ini diharapkan mampu menghancurkan program nuklir Iran secara permanen. Namun kenyataannya program nuklir Natanz hanya lumpuh sementara dan hanya mengalami gangguan yang kecil. Oleh karena itu penulis tertarik meneliti bagaimana dampak yang dihasilkan Stuxnet dalam Program Nuklir Iran di Natanz dengan pertanyaan masalah sebagai berikut : **“Bagaimana Implikasi Perang Siber antara Israel, Amerika Serikat, dan Iran melalui Olympic Game Operation terhadap kekuatan nuklir Iran di Timur Tengah?”**

### **I.3 Tujuan Penelitian**

Tujuan Penelitian ini adalah sebagai berikut :

- a. Mengetahui penyebab perang siber Stuxnet
- b. Mengetahui peran cyberwar dalam konflik
- c. Menjelaskan dampak dari malware Suxnet terhadap kekuatan Iran di Timur Tengah

### **I.4 Manfaat Penelitian**

#### **1. Manfaat Akademis**

Hasil dari penelitian ini diharapkan mampu untuk memberikan pemahaman dan pengetahuan untuk para pembaca mengenai akibat dari virus Stuxnet yang menyerang fasilitas nuklir di wilayah Natanz, Iran. Selain itu, dari hasil penelitian ini juga akan melihat bagaimana upaya Mahmoud Ahmadinejad sebagai pemimpin Iran pada masa itu dalam memulihkan kembali fasilitas dan upaya yang ditempuh untuk melindungi negaranya dari ancaman yang serupa.

#### **2. Manfaat Praktis**

Penelitian ini diharapkan dapat dijadikan acuan ataupun masukan terhadap negara ataupun lembaga siber dalam permasalahan penguatan keamanan nasional negara yang terlibat. Selain itu penulis ingin memberikan edukasi

serta kesadaran bagi masyarakat mengenai bahaya dari perang siber terhadap perdamaian dan keamanan baik dalam skala nasional maupun skala internasional.

## **I.5 Sistematika Penulisan**

Sistematika penulisan dalam tugas akhir adalah sebagai berikut :

### **BAB I PENDAHULUAN**

Pada bab ini penulis akan mendeskripsikan mengenai rangkaian peristiwa dan masalah yang difokuskan menjadi sebuah rumusan masalah ,tujuan,dan manfaat dari penelitian yang penulis ingin bahas.Dalam bagian latar belakang penulis menjelaskan mengenai gambaran besar mengenai cyber dan cyberwar.Lalu penulis menjelaskan secara umum permasalahan yang terjadi dalam kasus Stuxnet.

### **BAB II TINJAUAN PUSTAKA**

Penulis akan mendeskripsikan tentang pengertian,konsep dan teori yang relevan dengan kasus yang diangkat oleh penulis dalam penelitian ini.Penulis akan menjelaskan konsep serta teori yang relevan dengan masalah penelitian yang dianalisis oleh penulis.Hal ini bertujuan untuk memberikan bukti,riset,data dan fakta yang sebenar-benarnya.

### **BAB III METODOLOGI PENELITIAN**

Dalam bab ini penulis akan menjelaskan mengenai metode dan jenis penelitian yang akan digunakan dalam penelitian ini.Pada penelitian kali ini penulis menggunakan metode penelitian kualitatif.Penulis mengumpulkan data dengan wawancara dan literature review,data primer dan data sekunder yang mendukung penelitian yang akan penulis teliti.

### **BAB IV GAMBARAN UMUM OPERASI OLYMPIC GAME OPERATION**

Pada bab ini penulis akan menjelaskan mengenai gambaran umum mekanisme operasi olympic game operation

## **BAB V ANALISIS DAN DAMPAK VIRUS STUXNET TERHADAP KEKUATAN IRAN DI TIMUR TENGAH**

Bab ini akan menjelaskan dampak dari virus Stuxnet terhadap kekuatan Iran di Timur Tengah

## **BAB VI PENUTUP**

Berisi beberapa kesimpulan dan saran yang dapat ditarik dari hasil penelitian

## **DAFTAR PUSTAKA**