BAB I

PENDAHULUAN

1.1 Latar Belakang

Hubungan Internasional merupakan interaksi diantara aktor – aktor internasional. Aktor dalam hubungan internasional (HI) meliputi, negara, *International Non-Governmental Organization, International Organization*, perusahaan multinasional, dan bahkan individu dapat menjadi aktor dalam hubungan internasional. Selain itu, hubungan internasional memiliki ciri khas interdisipliner dalam menunjang keilmuannya. Menurut Darmayadi dkk (2015:25) menjelaskan hubungan internasional memuat berbagai perubahan – perubahan dalam sistem kenegaraan, perkembangan teknologi dan peran negara tidak hanya melibatkan dominasi negara barat namun melibatkan juga negara berkembang.

Dinamika internasional menjadi landasan dalam penentuan eksistensi hubungan internasional. Pendapat Yani (2010:2) kemunculan berbagai tren baru mengenai hubungan internasional dapat menimbulkan konsekuensi-konsekuensi baru bagi tatanan global. Berdasarkan pernyataan tersebut, ada dua aspek yang difokuskan sebagai isu dominan dalam hubungan internasional yakni perubahan aktor hubungan internasional dan konsep "*Power*".

Paska Perang Dingin perkembangan teknologi telah menjadi kebutuhan bagi kepentingan nasional khususnya dalam pertahanan dan keamanan. Dominasi dunia antara Blok Barat dan Blok Timur membuat persaingan teknologi semakin cepat.

Hal ini dijelaskan juga oleh Rachmat (2016:200-201) menyatakan bahwa teknologi dan industri pertahanan berkembang dengan sangat pesat pada masa Perang Dingin, terutama dengan terjadinya perlombaan senjata. Pada saat ini, teknologi berevolusi dengan berbagai kehidupan manusia. Kemampuan teknologi bahkan dapat menggantikan kinerja manusia dengan adanya komputer. (https://binus.ac.id/bandung/2019/12/perkembangan-teknologi-pada-perang-dingin-front-barat-dan-front-timur/ diakses 08/04/2020).

Kemajuan teknologi informasi dan komunikasi mengalami perkembangan pesat. Penggunaan teknologi yang digunakan oleh negara dioptimalkan dalam upaya memasuki fase atau era globalisasi di seluruh dunia. Globalisasi menjadi "Rumah Baru" dalam perkembangan teknologi informasi yang berkembang sekarang. Disamping itu, menimbulkan berbagai dampak di kehidupan masyarakat maupun negara, sehingga negara – negara bersaing untuk masuk dalam era digitalisasi dan industrialisasi global serta membentuk pola – pola baru dalam berinteraksi dengan negara di dunia internasional (Sodiki, 2005:4).

Evolusi pemanfaatan teknologi mengubah cara pandang negara – negara di dunia internasional. Situasi di berbagai aspek kehidupan seperti politik, sosial, keamanan secara otomatis berubah dan dihadapkan pada komputer dan internet. Kamus Besar Bahasa Indonesia menjelaskan internet adalah jaringan komunikasi elektronik yang menyatukan jaringan komputer dan fasilitas komputer yang telah diatur di seluruh dunia melalui telepon atau satelit. Internet berkembang dengan peluang dan tantangan yang akan memberi ruang baru yakni Ruang Maya atau

Cyberspace dalam pola interaksi negara, dalam memanfaatkannya untuk kerjasama maupun konflik (https://kbbi.web.id/internet diakses 22/04/2020).

Ruang maya atau *Cyberspace* sebagai ruang interaksi yang rumit dan sangat dinamis, karena penguasaan terhadap ruang maya tidak hanya dikendalikan oleh negara tetapi individu yang memiliki keahlian dalam pengatur ruang maya atau sibernya, sehingga menimbulkan perluasan dari makna *Power* yang berbeda, khususnya bagi hubungan internasional yang meliputi negara sebagai actor utama (Triwahyuni dan Wulandari, 2016:108)

Dinamika internasional memberikan berbagai kebaharuan, khususnya dalam dunia siber. Keamanan ruang maya mendapat prioritas karena melihat dampak buruk dari internet yang mengakibatkan negara harus memiliki pengaturan atas penggunaan internet negaranya (Triwahyuni dan Yani, 2018:2). Negara di seluruh dunia melakukan eksplorasi di dunia maya, sehingga mengakibatkan negara memiliki ketergantungan dengan siber sehingga menimbulkan kerentanan akan data kepentingan nasional dan keamanan negara.

Upaya tindak kejahatan dengan memanfaatkan teknologi di ruang maya disebut sebagai kejahatan siber atau *"Cybercrime".* Menurut *International Strategy for Cyberspace* dalam Triwahyuni (2020:50) Perkembangan kejahatan siber menjadi semakin luas dan beragam, dilihat dari target penyerangan atau jenis pola – pola serangan siber. Hal ini yang menimbulkan pentingnya untuk membangun lingkungan dunia maya yang memiliki norma sebagai tanggungjawab sebuah

negara atas tindakannya di dunia maya, hal ini dibentuk dalam upaya untuk menciptakan kekuasaan tertinggi dalam ruang maya.

Serangan siber menurut Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia (2014: 12) menjelaskan bahwa serangan siber merupakan segala bentuk perbuatan dengan dilakukan secara sengaja maupun tidak sengaja dengan motif dan tujuan yang ditujukan pada sistem elektronik penting suatu negara. Urgensi memahami serangan siber dijelaskan dalam Bendovschi (2015:25-26) mengatakan bahwa perlunya memahami serangan siber dalam berbagai bentuk seperti jenis serangan, karakteristik dan hasil yang akan dicapai, salah satunya yaitu *Malware*.

Malware atau *Malicious Software* yaitu serangan siber yang ditujukan pada jenis perangkat lunak berbahaya, digunakan oleh penyerang untuk membahayakan dan merusak integritas data, diantaranya yakni: Virus, *Worm, Trojan* dan lain-lain. Menurut Kementerian Pertahanan Republik Indonesia (2014:8), serangan *Malware* merupakan sebuah program yang dirancang untuk mengganggu operasi sistem komputer guna memperoleh keuntungan bahkan untuk kepentingan tertentu yang dioperasikan oleh penyerang.

Ancaman serangan siber melalui virus merupakan bagian dari sejarah kejahatan siber yang membuat beberapa negara di dunia mengalami berbagai masalah akibat serangan tersebut, salah satunya Iran. Serangan *Malware Stuxnet* terhadap Iran yang dilakukan oleh Amerika Serikat dan Israel ditujukan kepada Iran sebagai tindakan pencegahan atas pengembangan teknologi nuklir Iran (Suharto, 2015:9).

Implikasi dari ancaman dan serangan siber yang semakin rentan memberikan dasar pijakan bagi Republik Islam Iran atau Iran untuk mengembangkan eskalasi siber. Disamping itu hal ini menjadi penting bagi setiap negara, karena didasarkan pada penyesuaian atau adaptasi dari percepatan teknologi informasi akibat dari globalisasi dalam pertahanan siber yang akan terus berkembang dimasa depan (Soewardi, 2013:31).

Serangan siber dapat menjadi tolak ukur dari perubahan paradigma keamanan suatu negara, hal ini dilakukan oleh Iran. Serangan siber Amerika Serikat dan Israel menjadi titik balik dari kebangkitan siber Iran. *Worm Stuxnet* telah mengakibatkan komputer dalam pengayaan nuklir sekitar 980 sentrifugal Iran di Natanz rusak oleh *Malware* jenis *Worm* yang diberi nama *Stuxnet*. Hal ini menjadi motivasi Iran untuk melakukan berbagai serangan dunia maya terhadap bank-bank Amerika Serikat dan perusahaan minyak Saudi Aramco yang dimiliki oleh Arab Saudi (https://www.cato.org/publications/commentary/cyberwar-iran-wont-work-heres-why diakses 09/04/2020).

Kemajuan teknologi siber Iran mengalami percepatan setelah serangan *Stuxnet*. Kepentingan nasional Iran menjadi salah satu aspek dominan dalam pelaksanaan politik di kawasan Timur Tengah. Iran memiliki peran yang besar di kawasan bahkan dunia internasional. Menurut Rattray (2018:7) aspek utama dalam kebijakan nasional Iran yakni menjadi pemimpin utama dan mendominasi. Kemudian dirumuskan pada identitas budaya nasional untuk ambisi hegemonik dan didukung dengan organisasi militer kuat.

Meskipun aktivitas siber Iran tidak setara dengan negara yang memiliki kekuatan siber mapan, namun kapabilitas Iran dalam pengembangan siber telah dapat melakukan serangan-serangan siber ofensif kepada negara target penyerangan siber. Kondisi dalam negeri Iran tahun 2012 yang telah dijatuhkan sanksi internasional atas pengembangan senjata nuklir berdampak pada terpuruknya ekonomi Iran, namun tidak menghentikan langkah Iran untuk melakukan pelatihan militer dan perlindungan atas nuklir Iran dari serangan agresi asing Amerika Serikat dan sekutunya sebagai salah satu target serangan siber Iran (Pujayanti, 2012:6).

Serang siber Iran tahun 2012 menjadi peran penting Iran dalam kawasan karena telah berhasil meletakan kekuatan di Timur Tengah mengenai perimbangan kekuatan dan eksistensi Iran. Rattray (2018:7) menyatakan bahwa Iran sebagai salah satu peradaban besar dan memiliki kekuatan regional hegemonik telah terwujud dalam serangan siber Iran dan diantaranya telah menargetkan musuh regional. Kompetitor atau lawan Iran dikawasan Timur Tengah yakni Arab Saudi sebagai sekutu Amerika Serikat.

Kekuatan regional di Timur Tengah dikuasai oleh Iran dengan Arab Saudi. Ketegangan Iran dan Arab Saudi juga dapat dilihat dari persaingan hegemoni dan dualisme ideologi di kawasan Timur Tengah antara Sunni dan Syiah sebagai pemimpin Islam baik di kawasan maupun di dunia. Adanya salah satu kasus seorang akvitis perjuang kesetaraan Syiah di Arab Saudi di eksekusi karena diduga sebagai teroris di Riyadh, Arab Saudi. Dampak dari putusan atas eksekusi tersebut yaitu pemutusan hubungan diplomatik Iran dengan Arab Saudi

(https://www.cnnindonesia.com/internasional/20160105133321-120-102293/sejarah-panjang-perselisihan-arab-saudi-dan-iran diakses 09/04/2020). Dominasi kekuatan dan ideologi menambah situasi konfliktual Iran dan Arab Saudi. Disisi lain, perimbangan kekuatan di kawasan terus berlangsung dalam berbagai aspek kehidupan negara Iran dan Arab Saudi, khususnya mengenai keamanan siber.

Kemampuan siber Iran dalam menggunakan siber dengan memilih menggunakan strategi siber ofensif tidak hanya dilihat dari strategi yang dilakukan, tetapi aktor-aktor yang membantu dalam suksesi berbagai serangan siber terhadap target serangan Iran. Pengembangan siber Iran didukung oleh berbagai sumber daya manusia yang terampil dan juga menggunakan teknologi komputer canggih. Komponen penting seperti kelompok – kelompok dalam eksekusi serangan siber dan organisasi pemerintah bekerja sama untuk membentuk kemampuan siber Iran, kekuatan utama siber Iran dikendalikan oleh *Iran Cyber Army*.

Cybersecurity and Infrastructure Security Agency (CISA) berpendapat bahwa Korps Pengawal Revolusi Islam atau *Islamic Revolutionary Guard Corps* (IRGC) merupakan bagian penting sebagai kekuatan serangan siber Iran (https://www.us-cert.gov/ncas/alerts/aa20-006a diakses 22/04/2020). Sedangkan dalam perumusan target dan upaya membangun kekuatan masyarakat atau sipil ditujukan kepada Hossein Hamadani Brigadir Jenderal Korps Pengawal Revolusi Islam, telah melatih 1.500 *Basij* yakni Milisi Rakyat Iran yang dilatih sebagai "*Cyber War Commandoes* (Connell, 2014:7). Terbentuknya kekuatan siber Iran dilakukan dengan membentuk berbagai kelompok peretas komputer dalam melancarkan serangan terhadap target siber dan membentuk kekuatan siber Iran. Hal ini menjadi kekuatan besar bagi Iran

dalam menyerang berbagai target serangan siber dengan menggunakan kekuatannya dalam ruang maya.

Pada bulan Agustus tahun 2012, terjadi fenomena hubungan internasional, yaitu serangan siber yang dilakukan oleh Iran. Serangan siber yang dilakukan oleh Iran merupakan serangan dengan menggunakan strategi siber ofensif dan dipandang sebagai upaya untuk menciptakan konflik asimetris untuk mencapai kepentingan nasional Iran di Kawasan Timur Tengah. Serangan siber pada tahun 2012 diarahkan pada perusahaan kilang minyak Arab Saudi yakni Saudi Aramco, yang merupakan salah satu perusahaan yang berpegaruh sebagai pemasokan minyak terbesar dunia.

Saudi Aramco atau dengan nama resmi *Saudi Aramco Oil Company* adalah perusahaan penghasil dan pengekspor minyak dan menjadi salah satu perusahaan terbesar minyak dunia. Aramco merupakan kepanjangan dari *Arabian American Oil Company* sebagai sebuah perusahaan yang dengan standar *Co. of California* (Chevron), ketika memberikan konsesi terhadap minyak Arab Saudi. Ekspansi dari perusahaan Saudi Aramco memiliki mitra yang melingkupi berbagai kawasan di dunia diantaranya Amerika Serikat, Eropa, China, India, Jepang, Korea, Singapura dan Malaysia (https://www.saudiaramco.com/en/who-we-are/overview/our-history diakses 10/04/2020).

Pada tanggal 15 Agustus tahun 2012 pukul 11.00 waktu Arab Saudi, bertepatan dengan Hari Raya Idul Fitri. Hal ini terjadi pada saat semua pekerja perusahaan Saudi Aramco sedang berlibur merayakan hari besar Umat Islam. Temuan kerusakan yakni terjadi sebuah masalah pada sistem komputer internal dan

komunikasi internal perusahaan Saudi Aramco dengan menampilkan gambar bendera Amerika Serikat yang terbakar. Serangan siber tersebut dilakukan oleh Iran melalui kelompok peretas siber yakni *Cutting Sword of Justice* melalui *Malware* berjenis virus yang disebut "*Shamoon*" atau "*W32.Disstrack"* dengan memasukan virus berbahaya *Shamoon* oleh seseorang yang memiliki akses tertentu melalui *Hard Drive* yang dapat melakukan duplikasi dirinya sendiri sehingga menyebar ke sistem komputer dan merusak data internal sesuai dengan pemrograman awal virus tersebut.

Serangan siber terhadap Saudi Aramco yang dilakukan oleh kelompok peretas komputer Iran yakni *Cutting Sword of Justice* ditujukan terhadap objek vital Arab Saudi yakni Saudi Aramco sebagai salah satu perusahaan terbesar penghasil dan pengekspor minyak dunia dan sangat berpengaruh terhadap Arab Saudi. Respons awal dari perusahaan Saudi Aramco yakni menyebarkan informasi pada halamannya bahwa telah terjadi serangan siber terhadap Saudi Aramco dengan menggunakan virus *Shamoon*. Di sisi lain, dampak dari serangan siber tersebut telah merusak operasi komputer internal Saudi Aramco sebagai merusak terhadap lapisan fisik dan juga merusak terhadap lapisan logis dengan melakukan merusak data serta saluran komunikasi internal Saudi Aramco sehingga terjadi penutupan atau pemberhentian perusahaan Saudi Aramco, sebagai penggunaan siber Iran di ruang maya untuk menyerang objek vital Arab Saudi.

Asumsi penyerangan Saudi Aramco tahun 2012 diarahkan pada tindakan siber ofensif yang dilakukan Iran. Hal ini dijelaskan oleh Leon Panetta dalam Dan De Luce (2012) bahwa Amerika Serikat percaya Iran adalah aktor atau pelaku dari

serangan siber pada perusahaan minyak Arab Saudi yakni Saudi Aramco dan juga perusahaan gas Qatar pada tahun 2012 (https://phys.org/news/2012-10-iran-cyberattack-saudi-ex-official.html diakses 10/04/2020).

Selanjutnya, pendapat Alelyani dan Kumar (2018:43) menduga bahwa serangan siber tahun 2012 terhadap kilang minyak Arab Saudi yakni Saudi Aramco dilakukan oleh Iran. Penyerangan itu ditujukan pada produsen minyak terbesar didunia yakni Saudi Aramco dan mengakibatkan terhapusnya data dari 30.000 komputer di perusahaan Saudi Aramco.

Pendapat Abdullah Al-Saadan, Wakil Presiden Aramco menjelaskan bahwa peretas yang merusak sistem komputer Saudi Aramco berasal dari kelompok *Cutting Sword of Justice*, merupakan salah satu kelompok peretas dari Iran. Motif penyerang yang ditemukan bersifat politis yakni untuk mengakses komputer – komputer Saudi Aramco menggunakan virus *Shamoon* (https://www.reuters.com/article/saudi-attack/saudi-arabia-says-cyber-attack-aimed-to-disrupt-oil-gas-flow-idUSL5E8N91UE20121209 diakses 10/04/2020).

Meskipun beberapa kasus siber di dunia internasional dianggap tidak selesai, bahkan beberapa kasus siber yang telah diselidiki dan dilacak dengan menggunakan *Internet Protocol Address* atau *IP Address*, pelaku serangan baik individu atau negara tidak mengakui serangan siber tersebut. Selain itu, beberapa kejahatan siber yang dilakukan oleh organisasi pemerintah, kelompok kepentingan bahkan individu hanya mencoba untuk menguji keterampilannya dalam dunia maya.

Adapun masalah utama dalam penelitian ini ialah bagaimana serangan siber ofensif yang dilakukan Iran dapat dilakukan dalam upaya mencapai kepentingan nasional Iran terhadap Arab Saudi. Ekplorasi ruang maya yang dilakukan oleh Iran yakni telah merusak lapisan ruang maya Arab Saudi meliputi fisik dan logis. Aspek fisik dan logis yang diserang yakni telah merusak jalannya operasi sistem komputer internal dan memusak sistem komunikasi di perusahaan Saudi Aramco. Disamping itu, bagaimana virus *Shamoon* 2012 yang digunakan untuk meretas sistem komputer Saudi Aramco menjadi studi kasus dalam mencapai kepentingan nasional Iran. Konsep utama dalam masalah penelitian yakni mengenai siber ofensif Iran yang merupakan konsep abstrak, karena melihat dari target serangan dan pola serangan siber Iran yang digunakan yakni untuk mencapai kepentingan nasional dengan menggunakan virus *Shamoon* 2012 dengan menyerang perusahaan minyak Arab Saudi yaitu Saudi Aramco.

Latar belakang dari target siber ofensif Iran ditujukan pada Saudi Aramco sebagai perusahaan minyak terbesar di dunia. Disamping itu, Saudi Aramco merupakan perusahaan konsensi pembukaan tambang minyak bersama dengan Amerika Serikat. Hal ini beranjak dari situasi dan kondisi Iran yang ditekan oleh berbagai sanksi internasional baik dalam sektor ekonomi terutama dalam sektor sumber daya minyak. Penargetan terhadap Saudi Aramco disebabkan oleh pengalihan pelanggan atau mitra pemasok minyak yang pada awalnya bermitra dengan Iran, lalu beralih kepada Arab Saudi atas sanksi internasional terhadap Iran yang telah melumpuhkan sektor penting Iran yakni ekspor minyak bumi

(https://www.nytimes.com/2012/10/14/world/middleeast/us-suspects-iranians-were-behind-a-wave-of-cyberattacks.html diakses 26/04/2020).

Tujuan utama siber ofensif yang dilakukan Iran yakni sebagai upaya mencapai kepentingan hegemoni kawasan Timur Tengah, mempertahankan kekuatan regional sebagai wujud eksistensi Iran serta menjadi perimbangan kekuatan atas Arab Saudi sebagai sekutu Amerika Serikat di Timur Tengah. Kemudian, siber ofensif Iran ditujukan untuk mencapai kepentingan nasional, yakni melemahkan target musuh dan menghindari konflik terbuka. Menurut Forum Kajian Pertahanan Maritim menjelaskan bahwa unsur – unsur dalam kepentingan nasional secara umum yakni membela hak – hak, mempertahankan eksistensi, dan melaksanakan interaksi dan hubungan yang melibatkan negara tersebut. (http://www.fkpmar.org/national-interest-indonesia-and-the-development-of-the-defence-force/ diakses 22/04/2020).

Membela hak – hak atas Iran yakni mengacu pada hak Iran atas kemandirian, dan pengakuan perjuangan. Meskipun Irak dan Arab Saudi merupakan negara yang memilih untuk menggunakan strategi *Proxywar*, namun dalam upaya mencapai kepentingan Iran, salah satunya dengan menggunakan siber ofensif melalui *Malware* virus *Shamoon.*

Mempertahankan eksistensi mengarah pada pengakuan Iran untuk mempertahankan ideologi di kawasan di Timur Tengah. Dualisme Sunni dan Syiah di Timur Tengah mengakibatkan pecahnya kesatuan Islam. Iran dan Arab Saudi saling mencurigai diantara Sunni dan Syiah di negara masing-masing dan mencoba

mendominasi upaya hegemoni kawasan melalui ideologi. Selain itu, kepentingan untuk menjadi negara mandiri dalam interaksinya di dunia internasional, karena melihat Iran telah diberikan banyak sanksi atas keputusan dari kebijakan nasional Iran.

Penelitian yang serupa dengan penelitian yakni karya tulis akhir Rahmadi Pratama Aritonang (2019) dari Universitas Airlangga, berujudul Operasi Siber Ofensif Iran terhadap Amerika Serikat, Israel dan Arab Saudi: Kepentingan dan Strategi Siber Ofensif Iran. Penelitian ini menggunakan metode penelitian kualitatif. Dalam topik siber yang dijelaskan, strategi siber ofensif Iran ditujukan tidak hanya kepada Arab Saudi, tetapi diarahkan pada negara Amerika Serikat dan Israel. Tujuan dari penelitian ini untuk memahami strategi dan kepentingan siber Iran terhadap ketiga negara tersebut. Temuan dari penelitian ini bahwa strategi yang dilakukan oleh Iran menggunakan strategi asimetris dengan menunjukan bahwa Iran sebagai pelaku dari berbagai serangan siber terhadap negara – negara tersebut.

Penelitian karya tulis akhir yang dilakukan oleh Jodi Alif Iskandar (2019) dari Universitas Pertamina yang berjudul, Strategi Geopolitik Iran Untuk Mengimbangi Arab Saudi Melalui Perang Suriah. Penelitian ini menggunakan metode analisis kualitatif. Hasil penelitian menunjukan bahwa strategi Iran berhasil untuk menekan rivalitas dominasi dari Arab Saudi di Suriah dengan melakukan upaya persenjataan militer diplomasi-politik, dan ekonomi. Hal ini berkaitan dengan pengiriman pasukan untuk mempertahankan rezim di Suriah yang memiliki ideologi sama dengan Iran. Studi litelatur utama yang digunakan yakni dengan konsep *Balance Of Power* dan teori geopolitik.

Selanjutnya, penelitian yang dilakukan oleh Rizki Pratama Putra, Maryam Jamilah, Poppy Irawan dalam jurnal *Power In International Relation* (2020) mengenai Intervensi Militer Arab Saudi Terhadap Konflik Yaman Untuk Membendung Pengaruh Iran Di Timur Tengah. Penelitian ini menjelaskan bahwa dinamika hegemonik yang dilakukan oleh kedua negara di Yaman. Kepentingan nasioal Iran dalam melestarikan rezim Republik Islam dan memperluas pengaruhnya di kawasan melalui penyebaran ideologi politik dan peran media massa di Yaman, dengan menggunakan metode penelitian kualitatif.

Berdasarkan beberapa penelitian sebelumnya, diantaranya belum terdeskripsikan mengenai hubungan Iran dan Arab Saudi di era saat ini khususnya menggunakan serangan siber dengan menggunakan fokus khususnya mengenai masalah virus *Shamoon* 2012. Dalam beberapa penelitian belum tergambarkan dengan jelas berbagai kepentingan Iran terhadap Arab Saudi. Selain itu fokus penelitian yakni dengan memfokuskan pada virus *Shamoon* melalui studi kasus di tahun 2012. Kemudian, penggunaan teori mengenai siber ofensif dan defensif belum secara khusus digunakan di penelitian sebelumnya, karena penelitian sebelumnya menggunakan teori siber ofensif dari negara lain.

Alasan dalam pemilihan topik ini yakni temuan awal mengenai aktivitas siber Iran yang semakin berkembang, terutama siber ofensif Iran. Dengan melakukan penelusuran online maka ditemukan serangan siber terhadap Arab Saudi dalam kepentingan nasional Iran di kawasan Timur Tengah melalui kasus virus *Shamoon* 2012 yang merupakan serangan siber melalui penggunaan teknologi *Malware* untuk mengganggu bahkan merusak data sistem komputer di perusahaan Saudi Aramco.

Ketertarikan peneliti lainnya yakni strategi yang dilakukan Iran dengan menggunakan siber ofensif untuk menunjukan bahwa Iran adalah pelaku dalam berbagai serangan siber pada negara target serangan siber. Kemudian, masih sedikit diantaranya yang membahas mengenai fenomena siber di kawasan Timur Tengah. Hal ini yang mendorong peneliti untuk tertarik meneliti dengan judul "**Kepentingan Siber Ofensif Iran Terhadap Arab Saudi Dalam Kasus Virus *Shamoon* Tahun 2012".**

Implikasi keterkaitannya dalam studi Hubungan Internasional yaitu interaksi yang dilakukan oleh negara Iran dengan Arab Saudi sebagai landasan bagi studi antar aktor yang melewati batas-batas negara (Perwita dan Yani, 2006:4). Pola interaksi yang berupa serangan siber menjadi bagian dari studi keamanan internasional kontemporer yaitu keamanan siber khususnya mengenai siber ofensif guna mencapai kepentingan nasional melalui teknologi *Malware* jenis virus *Shamoon* di tahun 2012. Disamping itu mata kuliah yang memberikan sumbangan dalam daya dukung topik penelitian di Program Studi Ilmu Hubungan Internasional, Universitas Komputer Indonesia yakni;

1) Keamanan Siber, memberikan pemahaman mengenai keamanan baru dan konsep kejahatan baru dalam hubungan internasional dengan menggunakan teknologi yang menyerang komputer target serangan siber, yang menjadi fokus utama dalam penelitian ini.
2) Analisis Politik Luar Negeri memberikan pemahaman mengenai konsep penentuan, perencaan dan pelaksanaan kebijakan luar negeri suatu negara. Hal ini didasarkan pada perumusan kebijakan luar negeri Iran yang tidak

hanya dilihat dari aspek yang terlihat tetapi kekuatan yang tidak terlihat khususnya mengenai pengembangan kekuatan siber secara nyata telah meningkat.

3) Pengantar Hubungan Internasional, mengantarkan peneliti untuk memahami konsep dasar dari hubungan internasional khususnya yang terjadi diantara negara Iran dan Arab Saudi sebagai sebuah kajian ilmu mengenai dinamika internasional terutama mengenai konflik yang menggunakan serangan siber sebagai instrumennya.
4) Hubungan Internasional Timur Tengah memberikan sumbangan keilmuan mengenai dasar-dasar kajian negara Iran dan Arab Saudi. Kemudian mata kuliah Hubungan Internasional Timur Tengah memberikan gambaran dinamika konflik yang telah terjadi sebagai landasan dalam memahami latar belakang konflik Iran dan Arab Saudi.

1.2 Rumusan Masalah

1.2.1 Rumusan Masalah Mayor

Apa kepentingan Iran melakukan Siber Ofensif dengan menggunakan virus *Shamoon* kepada Arab Saudi pada tahun 2012?

1.2.2 Rumusan Masalah Minor

1. Bagaimana serangan siber ofensif Iran dengan menggunakan virus *Shamoon* tahun 2012 terhadap Arab Saudi?
2. Apa kepentingan Iran dalam menyerang perusahaan kilang minyak Arab Saudi?

3. Bagaimana Arab Saudi merespons serangan siber ofensif Iran?
4. Bagaimana hubungan Iran dan Arab Saudi paska serangan siber ofensif yang dilakukan Iran?

1.2.3 Pembatasan Masalah

Pembatasan masalah mengarah pada upaya siber ofensif melalui studi kasus virus *Shamoon* yang dilakukan oleh Iran untuk menyerang Arab Saudi. Implikasi dari virus *Shamoon* mengarah pada serangan siber ofensif Iran di tahun 2012 yang dilakukan oleh kelompok *Cutting Sword of Justice* sebagai upaya mencapai kepentingan nasional Iran. Penyerangan yang dilakukan mengarah pada pengayaan kilang minyak terbesar di dunia Saudi Aramco yang dimiliki oleh Arab Saudi.

1.3 Maksud dan Tujuan Penelitian

1.3.1 Maksud Penelitian

Maksud dari penelitian yaitu untuk mendapatkan informasi mengenai serangan siber ofensif yang dilakukan oleh Iran dengan menggunakan virus *Shamoon* untuk menyerang Arab Saudi dalam upaya mencapai kepentingan nasional Iran.

1.3.2 Tujuan Penelitian

Tujuan penelitian mengenai siber ofensif Iran terhadap Arab Saudi dalam kepentingan nasional dengan menggunakan virus *Shamoon* tahun 2012, yaitu:

1. Untuk mengetahui kepentingan nasional Iran dalam melakukan serangan siber ofensif terhadap Arab Saudi yakni Saudi Aramco.

2. Untuk mengetahui bagaimana virus *Shamoon* 2012 memberikan dampak terhadap infrastruktur minyak Arab Saudi yakni Saudi Aramco.
3. Untuk mengetahui bagaimana serangan siber Iran melalui virus *Shamoon* dilakukan terhadap Saudi Aramco sebagai objek vital Arab Saudi.

1.4 Kegunaan Penelitian

1.4.1 Kegunaan Teoretis

Kegunaan teoretis pada penelitian adalah untuk memperluas kajian mengenai siber ofensir Iran ataupun menambah rujukan mengenai siber ofensif Iran terhadap Arab Saudi dalam mencapai kepentingan nasional Iran melalui virus *Shamoon* tahun 2012.

1.4.2 Kegunaan Praktis

Kegunaan praktis dalam penelitian ini yakni ditujukan bagi peneliti sendiri sebagai khazanah keilmuan dan berguna bagi berbagai pengkaji, khususnya hubungan internasional mengenai berbagai data mengenai topik penelitian siber ofensif, konflik Timur Tengah dan kepentingan nasional suatu negara yang berbeda seperti Iran dan Arab Saudi.