Global Political Studies Journal
Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v4i2

Kepentingan Siber Ofensif Iran Terhadap Arab Saudi Dalam Kasus Virus *Shamoon* Tahun 2012

Ananty Hidayat[1]
[1]Bank Rakyat Indonesia
Jl. Prabu Geusan Ulun No.10 Regol Wetan, Kabupaten Sumedang, Indonesia

e-mail: [1]Anantyh2@gmail.com

Abstract

This study goals to determine the offensive cyber interests committed by Iran against the Saudi Arabian oil refinery, namely Saudi Aramco using the Shammon virus. In addition, finding meaning about the importance of the 2012 Shamoon Virus attack, motivated by the transfer of Iranian oil partners to Saudi Arabia over the economic embargo imposed on Iran in 2012 due to Iran's nuclear enrichment and Iranian cyberattacks aimed at Iran's existence and leadership in regional countries The Middle East is the essential for Iran's cyberattack to create a balance of power in the form of the phenomenon of international relations using cyber offensives.

The research method used is a qualitative method. Data collection techniques are carried out through literature studies and online data searches. Data triangulation technique is a technique used in analyzing research data.

The results of the study found that Iran's cyber offensive was not only aimed at resistance to the economic embargo imposed on Iran, but there were other interests aimed at the existence of Iranian cyber power causing a situation of tension and over the hegemony of the Middle East region. The conclusion from research related to Iran's cyber offensive against Saudi Arabia using the Shamoon virus is that the capabilities of cyber power can have a devastating impact on the vital infrastructure of Saudi Arabia. Vulnerability in cyberspace is used as a weapon in an effort to achieve national interests, especially for the Iranian state.

Keywords—*Iran, National Interest, Offensive Cyber, Shamoon Virus*

Abstrak

Penelitian ini bertujuan untuk mengetahui kepentingan siber ofensif yang dilakukan oleh Iran terhadap kilang minyak Arab Saudi yakni Saudi Aramco dengan menggunakan virus Shammon. Selain itu, menemukan makna mengenai kepentingan serangan Virus *Shamoon* Tahun 2012, dilatarbelakangi oleh pengalihan mitra minyak Iran ke Arab Saudi atas embargo ekonomi yang dijatuhkan kepada Iran tahun 2012 karena pengayaan nuklir Iran dan serangan siber Iran ditujukan atas eksistensi dan kepemimpinan Iran di negara - negara kawasan Timur Tengah menjadi landasan bagi serangan siber Iran untuk upaya menciptakan perimbangan kekuatan dalam bentuk fenomena hubungan internasional dengan menggunakan siber ofensif.

Metode penelitian yang digunakan adalah metode kualitatif. Teknik pengumpulan data dilakukan melalui studi pustaka. Teknik triangulasi data merupakan teknik yang digunakan dalam menganalisa data – data penelitian.

Hasil penelitian menemukan bahwa siber ofensif Iran tidak hanya ditujukan atas perlawanan terhadap embargo ekonomi yang dijatuhkan terhadap Iran, melainkan terdapat kepentingan lain yang ditujukan pada eksistensi kekuatan siber Iran menimbulkan situasi ketegangan dan atas hegemoni kawasan Timur Tengah. Kesimpulan dari penelitian terkait siber ofensif Iran terhadap Arab Saudi dengan menggunakan virus *Shamoon* yakni kapabilitas dari kekuatan siber dapat memberikan dampak kerusakan bagi infrastruktur vital Arab Saudi. Kerentanan diruang maya dimanfaatkan sebagai senjata dalam upaya mencapai kepentingan nasional, khususnya bagi negara Iran.

Katakunci—Iran, Kepentingan Nasional, Siber Ofensif, Virus *Shamoon*.

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v4i2

1. Pendahuluan

1.1 Latar Belakang

Hubungan Internasional merupakan interaksi diantara aktor – aktor internasional dan 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. Menurut pendapat Yani dalam Perpustakaan Universitas Padjajaran (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"*.

Selanjutnya, perkembangan hubungan 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, mengakibatkan negara memiliki ketergantungan dengan ruang siber sehingga menimbulkan kerentanan akan data kepentingan nasional dan keamanan negara. Pada akhirnya kerentanan dinilai sebagai upaya untuk menciptakan kestabilan keamanan yang mendorong tindak kejahatan dalam ruang siber.

Upaya tindakan 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. Salah satu bentuk atas tindak kejahatan siber yakni melalui *Malware.*

Menurut Kementerian Pertahanan Republik Indonesia, serangan *Malware* merupakan sebuah program yang dirancang untuk mengganggu operasi sistem komputer guna memperoleh keuntungan bahkan untuk kepentingan tertentu yang dioperasikan oleh penyerang. *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.

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). Disamping itu, *Stuxnet* menjadi titik dari pengembangan siber Iran.

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

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v4i2

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 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).

Pada bulan Agustus tahun 2012, terjadi fenomena hubungan internasional, yaitu serangan siber yang dilakukan oleh Iran. Serangan siber 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 *Flash Drive* yang dapat melakukan duplikasi dirinya sendiri sehingga menyebar ke sistem komputer dan merusak data internal sesuai dengan pemrograman awal virus tersebut.

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.

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

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v4i2

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. Kemudian, 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).

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 pada 26/04/2020).

Penelitian sebelumnya yang dapat menjadi acuan 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. 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 Arab Saudi, Amerika Serikat dan Israel.

Selanjutnya, karya tulis akhir Jodi Alif Iskandar (2019) dari Universitas Pertamina yang berjudul, Strategi Geopolitik Iran Untuk Mengimbangi Arab Saudi Melalui Perang Suriah. Hasil penelitian menunjukan bahwa strategi Iran berhasil

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v4i2

untuk menekan rivalitas dominasi dari Arab Saudi di Suriah dengan melakukan upaya persenjataan militer diplomasi-politik, dan ekonomi. Selain itu, Jurnal yang ditulis 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.

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 yang digumakan sebagai pembatasan penelitian. 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. 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

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

Rumusan masalah minor penelitian, diantaranya, yaitu:

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?

1.3 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.

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v4i2

2. Kajian Pustaka dan Kerangka Pemikiran

2.1 Kajian Pustaka

2.1.1 Hubungan Internasional

Perkembangannya hubungan internasional merupakan keilmuan baru mengenai politik internasional. Hubungan internasional lahir secara resmi pada masa paska Perang Dunia I dengan tujuan bahwa dunia setelah berakhirnya perang yang menimbulkan banyak korban di berbagai dunia dapat berhenti. Disamping itu, tujuan lainnya yakni memastikan interaksi diantara negara dapat berjalan dengan damai. Oleh karena itu, hubungan internasional secara nyata mempelajari interaksi diantara negara – negara bahkan dengan aktor non negara. Bahkan dinamika interaksinya meliputi berbagai kepentingan lainnya seperti kebudayaan, teknologi, ekonomi, dsb (Darmayadi, 2015:51-52).

Hubungan internasional menjadi populer melihat berbagai kecenderungan yang dinamis dari politik global. Hal ini mendorong skema bagi kemunculan hubungan internasional kontemporer yang diartikan sebagai interaksi mengenai fenomena sosial yang berhubungan dengan aspek politik, ideologi, hukum, ekonomi, budaya dan pertahan keamanan negara yang melintasi batas nasional suatu negara antara aktor-aktor yang lebih kompleks (Perwita dan Yani, 2006:8). Hal ini diimplikasikan terhadap Iran dan Arab Saudi.

Iran sebagai aktor hubungan internasional memiliki kapabilitas untuk melakukan interaksi baik dilihat dari upaya kerjasama ataupun konflik. Dinamika hubungan internasional memberikan peluang bagi bentuk interaksi Iran dengan menggunakan kekuatan siber ofensif. Interaksi yang terjadi antara Iran dengan Arab Saudi adalah bentuk konflik yang telah lama menjadi fenomena hubungan internasional di kawasan Timur Tengah. Untuk itu, dalam melihat fenomena ini, menggunakan tingkat analisa negara Iran dan Arab Saudi. Selain itu, hal ini ditujukan sebagai bentuk perjuangan kepentingan nasional Iran khususnya di kawasan Timur Tengah

2.1.2 *Cyber Space*

Ruang siber menjadi bagian penting dalam interaksi aktor – aktor hubungan internasional, khususnya negara yang memiliki kapabilitas lebih tinggi. Pendapat Aubrey Slaughter (2020) menjelaskan *Cyberspace* dapat dipahami secara luas sebagai lingkungan bersama dalam media komunikasi melalui perantara komputer yang mempresentasikan audio, visual dan kode khusus tertentu. Selain itu, ruang maya dibagi ke dalam dua aspek persfektif yaitu ruang maya dapat dilihat dari aspek spasial dan juga aspek sosial (https://lucian.uchicago.edu/blogs/mediatheory/keywords/cyberspace/ diakses 04/06/2020).

Selanjutnya, sifat dunia maya dapat dipahami melalui komponen pembentuknya yakni dibagi ke dalam lapisan utamanya yakni; Fisik, Sintaksis, dan Semantik. Lapisan fisik mengacu pada infrastruktur dasar yang mendukung transmisi, generasi, dan penyimpanan sinyal elektromagnetik, yaitu komputer, server, kabel. Lapisan sintaksis merupakan lapisan yang merujuk pada bagian dalam terdiri dari kode dan protokol dalam pengolahan data baik berupa transportasi, konstruksi dan manipulasi. Terakhir, lapisan semantik merupakan gabungan dari lapisan fisik dan sintaksis yang menekan pada makna atau proses atas kedua lapisan tersebut (Venables dkk., 2015).

Serangan siber ofensif Iran dengan menggunakan virus *Shamoon* berdampak pada aspek fisik komputer Saudi Aramco dan memutus jaringan komunikasi internal dalam aspek logis ruang maya. Penyerangan terhadap Saudi Aramco dilakukan oleh kelompok peretas komputer

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v4i2

Iran yaitu *Cutting Sword of Justice* yang merupakan orang – orang yang memiliki keahlian dalam mengoperasikan tujuan dan kepentingannya melalui virus *Shamoon.*

2.1.2.1 *Cyberpower* dalam *Cyber Space*

Konsep *Power* menurut K.J Holsti (2016:25-26) merupakan kapasitas atau kemampuan negara untuk mengendalikan negara lain yang dapat dilihat dalam empat bagian:

1. Power dalam persfektif Influence, merupakan alat guna mencapai tujuan
2. Power dalam memobilisasi sumber-sumber Power yang meliputi sumber fisik dan sumber mental yang dimiliki negara sebagai instrumen membuktikan atau menghukum negara lain
3. Power dalam persfektif Relation, yaitu menentukan keberhasilan suatu pihak lain apabila pihak tersebut mempunyai Power
4. Power dalam persfektif mengukur dilihat secara relatif bukan absolut, dengan membandingkan sumber-sumber kekuatan yang dimiliki oleh suatu negara dengan negara lain (https://repository.unikom.ac.id/32155/1/power.pdf diakses 03/06/2020).

Ruang maya yang bertambah mengakibatkan adanya perubahan dalam proses interaksi sekaligus memperluas makna *Power*, sehingga *Power* menjadi memudar. Ruang maya menjadi sarana baru dalam mencapai kepentingan yang kemudian dikenal dengan *Cyberpower* (Triwahyuni dan Yani, 2018:2). Kekuatan siber dalam ruang maya menurut Haaster (2016:14) terdiri dari berbagai kekuatan yang dapat mempengaruhi aktor – aktor negara dan aktor lainnya dalam menggunakan dunia maya, seperti komponen geografis, jaringan fisik, logis, dan siber persona.

Kekuatan siber Iran meskipun tidak simetris dengan negara lain, namun hal ini yang menjadi salah satu alasan Iran dalam mempercepat eskalasi kekuatan sibernya. Kerentanan akan serangan siber khususnya dari Amerika Serikat, Israel dan sekutunya di Timur Tengah yakni Arab Saudi memberikan ancaman untuk mencapai kepentingan nasional. Kelompok yang berperan penting dalam operasi siber Iran adalah Korps Pengawal Revolusi Iran, Basij, dan Passive Defense Organization (NPDO). Selain itu, dalam memperkuat Cyberpower Iran telah membentuk Dewan Tertinggi Dunia Maya atau Supreme Council of Cyberspace (https://www.csis.org/analysis/iran-and-cyber-power diakses 03/06/2020).

2.1.3 Politik Luar Negeri

Politik luar negeri menurut Perwita dan Yani (2006:47) politik luar negeri merupakan kebijaksanaan suatu negara guna mencapai kepentingan. Lebih luasnya, politik luar negeri adalah seperangkat formula yang merupakan nilai, arah dan sikap serta sasaran untuk memperjuangkan kepentingan nasional di dunia internasional.

Politik luar negeri Iran merupakan strategi, kerahasiaan, nilai yang tidak dapat didefinisikan secara jelas. Kebijakan luar negeri dibawah kepemimpinan Mahmoud Ahmadinejad membawa Iran ke dalam tekanan internasional yang semakin buruk. Upaya mempersenjatai diri menjadi bagian dalam nilai strategis untuk mengoptimalkan penggunaan teknologi dengan politik luar negeri Iran.

2.1.4 Kepentingan Nasional

Kepentingan nasional merupakan hal penting yang melekat pada kajian hubungan internasional. Kepentingan nasional secara umum merupakan upaya – upaya setiap negara untuk memenuhi kebutuhan nasionalnya melalui berbagai cara.

Urgensi dari kepentingan nasional merupakan tujuan vital atas dasar kebutuhan setiap negara. Menurut Perwita dan Yani (2006:35) menjelaskan

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v4i2

pentingnya kepentingan nasional sebagai upaya untuk memahami perilaku internasional dan dipersepsikan sebagai tujuan fundamental dan hasil akhir dalam mengarahkan pada kebijakan nasional suatu negara.

Menurut Burchill dalam Umar (2005:186-188) kepentingan nasional dalam persfektif realism berasumsi bahwa kepentingan nasional mutlak berasal dari negara. Dalam hal ini kepentingan nasional yang menjadi fokus terhadap Iran merupakan ambisi dalam pertarungan atau rivalitas Iran dengan Arab Saudi. Hal ini dilatarbelakangi oleh berbagai sanksi yang dijatuhkan atas Iran seperti pemberhentian ekspor minyak Iran sehingga mitra kerjasama minyak Iran beralih ke Arab Saudi.

Selanjutnya, bahwa Iran memiliki peran penting dalam kawasan, khususnya dalam eskalasi siber sebagai bentuk dalam konflik asimetris dan Proxy War yang dilakukan oleh kelompok *Islamic Revolutionary Guard Corps* (IRGC) dibawah kepemimpinan Iran untuk mencapai kepentingan nasionalnya di Timur Tengah dan dunia internasional.

2.1.5 Keamanan Internasional

Keamanan internasional merupakan kajian tradisional hubungan internasional. Keamanan dalam studi hubungan internasional menjadi bagian penting yang tidak bisa dilepaskan, hal ini berdasarkan pada temuan dari bidang keamanan yang melahirkan kajian – kajian baru dalam hubungan internasional.

Konsep keamanan menurut Budi Raharjo (2017:10) menjelaskan dalam keamanan terdapat bagian utama yakni perlindungan data atau informasi. Bagian dalam keamanan yang melindungi data yaitu *Security Triads* merupakan aspek yang terdiri dari kerahasiaan, ketersediaan, dan integritas. Disamping itu, pola atau siklus berjalannya data yang disebut sebagai *Security Life Cycle* berakar dari kesadaran akan melindungi asset informasi sebagai upaya dalam menciptakan keamanan.

Upaya dalam menjaga atau menciptakan keamanan nasional dalam kerentanan global saat ini bergeser menjadi keamanan data, ketika negara di seluruh dunia melakukan percepatan teknologi dan membentuk *Big Data* negara dalam ruang maya. Ketergantungan Arab Saudi terhadap teknologi dalam pengayaan minyak perusahaan Saudi Aramco menjadi ancaman ketika celah dapat ditemukan oleh penyerang siber Iran.

2.1.5.1 Ofensif Defensif Siber

Konsep mengenai ofensif -defensif siber secara praktik dan teori berbeda, hal ini berdasarkan atas variable – variable yang membentuk persepsi keamanan dengan menggunakan pola ofensif atau defensif.

Menurut Robert Jervis dalam Medvedev (2015:5) variable pertama ditentukan ketika situasi ketegangan dari negara lain dinilai sebagai ancaman atau mengancam. Hal ini mengasumsikan bahwa tindakan ofensif dan defensif ataupun keduanya digunakan sebagai upaya mempersenjatai negara dengan strategi politik dan kepentingan yang ingin dicapai oleh negara. Variabel kedua dalam ofensif - defensif yakni menitikberatkan pada kapabilitas yang mendukung akan tindakan ofensif atau defensif. Kapabilitas ini dinilai dari dominasi kemampuan, apabila memungkinkan untuk melakukan siber ofensif maka negara cenderung untuk melakukan serangan terlebih dahulu. Disamping itu, apabila dominasi kapabilitas pada tindakan defensif, maka tindakan diarahkan pada perang dan kerjasama.

Selanjutnya, menurut Smeets (2018:97-103) tindakan siber ofensif dapat memberikan beberapa kemungkinan yang dapat dipertimbangkan sebelum melakukan serangan siber terhadap negara lain.

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v4i2

Pertama, meminimalisir korban dan menekan biaya perang. Kedua, menciptakan pengaruh psikologis dengan memberikan kondisi seperti menakuti, penurunan kepercayaan yang dapat melemahkan musuh. Ketiga, mengefektifkan kemampuan militer khususnya dalam menciptakan senjata penyerangan dan strategi perang. Keempat, memberikan opsi keputusan terhadap pemimpin negara bagi tindakan siber.

Konsep ofensif siber Iran didasarkan atas kapabilitas siber Iran yang dapat melakukan serangan terlebih dahulu dan meminimalisir korban dari konflik terbuka. Kemudian penggunaan ofensif siber merupakan strategi konflik asimetris Iran terhadap Arab Saudi. Hal ini juga menjadi strategi Iran untuk menunjukan eksistensinya di Timur Tengah sebagai bentuk kepentingan nasional Iran.

2.1.5.2 Keamanan Siber

Keamanan siber pada perkembangannya dianggap sebagai dampak dari meningkatnya hubungan saling ketergantungan negara dengan keamanan ruang maya atau *Cyberspace.* Menurut Knapp (2009:1) keamanan siber atau *Cyber Security* adalah masalah yang dihadapi pengguna jaringan komputer dan administrator, khususnya terjadi pada sektor publik dan swasta. Kerentanan berasal dari masalah internet akibat lemahnya keamanan sistem komputer yang digunakan oleh penyerang sebagai titik celah bagi terjadinya kejahatan di ruang maya.

2.1.6 Kejahatan Siber

Kejahatan siber secara umum merupakan penggunaan teknologi siber untuk tujuan negatif. Pendapat Gema dalam *National Central Bureau* Interpol Indonesia (2013:2) memaparkan bahwa kejahatan siber memiliki karakteristik yang berbeda dari kejahatan konvensional, yakni:

1. Perbuatan atau tindakan yang dilakukan diruang maya secara ilegal
2. Tindakan kejahatan siber menggunakan peralatan atau perangkat yang terhubung melalui internet
3. Dampak dari serangan atau kejahatan siber dapat menimbulkan kerugian baik secara materil atau non materil seperti kebocoran kerahasiaan informasi, penurunan kapasitas data, uang bahkan martabat
4. Secara spesifik, pelaku yang melakukan tindak kejahatan siber merupakan seorang yang menguasai internet dan aplikasinya serta mampu mengorganisasikan sistem komputer dengan baik
5. Tindakan kejahatan siber diantaranya dilakukan tidak hanya dalam negara tetapi dapat melewati batas negara.

Tindak kejahatan Iran melalui siber ofensif terhadap perusahaan Saudi Aramco yang dimiliki oleh Arab Saudi merupakan bentuk kejahatan dalam pelanggaran sistem kerahasiaan data dalam sistem komputer. Pelaku dalam serangan merupakan kelompok terlatih dalam siber yakni *Cutting Sword of Justice,* secara konsep dan taktik telah menguasai dan mengorganisasikan komputer dengan baik.

2.1.6.1 Program Virus dalam *Malware*

Malware merupakan kepanjangan dari "*Malicious Software*" digambarkan sebagai perangkat lunak yang mencurigakan. Menurut Aycock (2006:11) menjelaskan beberapa metode operasi *Malware,* yaitu:

1. Mereplika dirinya sendiri secara aktif dengan menyebar dan membuat salinan baru atau melakukan duplikasi dirinya sendiri
2. Populasi dari penyebaran *Malware* menunjukan jumlah dalam hitungan angka dalam melakukan duplikasi *Malware* tersebut.
3. *Malware* parasite dalam eksekusinya memerlukan beberapa kode yang

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v4i2

harus dimasukan agar proses eksekusi dapat berlangsung.

Penggunaan *Malware* jenis virus oleh Iran digunakan untuk mencapai kepentingan nasional. Karakteristik dari virus yang dapat melakukan replika secara otomatis diarahkan pada merusak sistem komputer Saudi Aramco. Virus yang digunakan oleh Iran terhadap Arab Saudi yaitu *Shamoon* atau W32.Disstrack.

2.2 Kerangka Pemikiran

Hubungan Iran dan Arab Saudi merupakan sejarah panjang dalam persaingan hegemoni kawasan Timur Tengah. Konflik – konflik yang diciptakan oleh kedua negara tidak melibatkan secara langsung baik oleh Iran atau Arab Saudi, melainkan melalui pihak ketiga yang menjadi eksekutor atau penyerang terhadap Iran atau Arab Saudi. Perkembangan teknologi dan informasi menciptakan ketergantungan akan sebuah sistem yang terhubung secara daring, sehingga memberikan kerentanan atas keamanan nasional melalui serangan siber.

Keamanan yang menjadi dimensi penting bagi setiap negara berubah ketika setiap negara masuk dalam era globalisasi dan digitalisasi. Konsep keamanan tidak hanya melindungi kedaulatan dan garis batas negara, melainkan pada keamanan data nasional, infrastruktur kritis dan objek vital negara yang dapat berpotensi sebagai upaya tindak kejahatan di ruang maya. Eskalasi kapabilitas siber Iran mendorong Iran dalam upaya menyerang Arab Saudi melalui siber ofensif terhadap Saudi Aramco sebagai perusahaan kilang minyak Arab Saudi. Serangan siber ofensif Iran merupakan kebangkitan Iran dalam bidang keamanan siber dan menjadi perimbangan kekuatan Arab Saudi di Timur Tengah.

Siber ofensif Iran adalah bentuk kepentingan nasional Iran salah satunya dalam respons atas kondisi internal Iran akibat tekanan internasional khususnya embargo ekonomi sehingga harus menghentikan negara – negara untuk melakukan penghentian impor minyak dari Iran dan telah mengalihkan beberapa negara pengimpor minyak Iran kepada Arab Saudi yang memiliki perusahaan minyak terbesar di dunia yaitu Saudi Aramco.

Dampak penyerangan perusahaan minyak Saudi Aramco telah melemahkan sistem komputer internal dengan menampilkan gambar bendera Amerika Serikat terbakar dan menghapus data dari perusahaan Saudi Aramco sehingga menghentikan sementara operasi di perusahaan Saudi Aramco sebagai objek vital negara. Serangan siber terhadap Saudi Aramco, dilakukan oleh salah satu kelompok peretas siber Iran yakni Cutting Sword of Justice dengan menggunakan *Malware* jenis virus yaitu virus *Shamoon* atau "W32.Disstrack".

Respons setelah terjadinya siber ofensif Iran yakni Saudi Aramco memberikan pernyataan bahwa terjadi kerusakan atas sistem komputer yang diakibatkan oleh virus. Kemudian terusiknya perusahaan Aramco sebagai keamanan siber Arab Saudi memberikan pengaruh terhadap upaya untuk membangun teknologi pertahanan serangan siber dengan melakukan investasi dalam pembangunan terhadap sistem keamanan Saudi Aramco dan membangun keamanan nasional siber Arab Saudi.

3. Metode Penelitian

Metode penelitian yang digunakan yakni metode penelitian kualitatif dengan memfokuskan pada metode studi kasus terpancang, karena merujuk pada studi kasus terhadap siber ofensif Iran pada tahun 2012 terhadap kilang minyak Arab Saudi yakni Saudi Aramco dengan menggunakan virus *Shamoon* dengan eksekutor tantara siber Iran yakni kelompok *Cutting Sword of Justice.* Kemudian, teknik pengumpulan data yang mendukung penelitian menggunakan studi pustaka dengan

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v4i2

pengumpulan data melalui tulisan, artikel, jurnal, buku dan sumber relevan lainnya seperti dokumen. Selain itu, mengakses berbagai situs dan berita secara daring.

4. Hasil dan Pembahasan

4.1 Serangan Siber Ofensif Iran Terhadap Arab Saudi Melalui Virus *Shamoon* tahun 2012

Pada tanggal 15 Agustus 2012, pada waktu 11.00 waktu Arab Saudi. Seseorang yang memiliki kredensial untuk masuk ke dalam perusahaan Saudi Aramco telah menghubungkan *Flash Drive* pada komputer Saudi Aramco yang memiliki muatan sebuah *Malware* yang memiliki sifat perusak yaitu *Shamoon*. Muatan dalam *Malware* tersebut meliputi tiga komponen penting yang direncanakan sebagai bentuk serangan terorganisir, berikut merupakan rantai serangan virus *Shamoon*.

Klaim atas serangan siber terhadap Saudi Aramco oleh Cutting Sword of Justice merupakan pengakuan atas dengan ditujukan terhadap kilang minyak terbesar yaitu Saudi Aramco. Serangan siber terhadap kilang minyak adalah bentuk atas berbagai permasalahan di Timur Tengah mengenai negara Mesir, Bahrain, Suriah dan Yaman karena Arab Saudi telah menggunakan minyak untuk mendukung berbagai bentuk kejahatan di kawasan Timur Tengah. Tekanan internasional atas konflik Timur Tengah yang tidak berhenti telah menggerakan kelompok peretas di kawasan untuk melawan Arab Saudi yang menjadi sekutu Amerika Serikat di kawasan, yang secara langsung mendukung ketersediaan minyak mentah Amerika Serikat.

Serangan atas Aramco ditujukan terhadap kelompok peretas siber Iran. Asumsi ini difokuskan terhadap pernyataan Leon Pannetta (2012) bahwa serangan siber pada perusahaan minyak Saudi Aramco merupakan serangan yang dilakukan oleh Iran pada tahun 2012 (https://phys.org/news/2012-10-iran-cyberattack-saudi-ex-official.html diakses 24/08/2020).

Dalam menanggapi berbagai sanksi internasional dan keterlibatannya atas berbagai serangan di dunia maya khususnya dalam menyerang sumber daya untuk membangun kemampuan pertahanan dunia maya dengan menargetkan situs industri minyak mentah. Maka dari itu, Iran menyatakan tidak terlibat dalam upaya menyerangan industri minyak, Saudi Aramco pada tahun 2012 (https://www.iranfocus.com/en/iran-general-mainmenu-26/26834-iran-strengthened-cyber-capabilities-after-*Stuxnet*-us-general diakses 06/08/2020).

Selanjutnya, Iran menggunakan siber ofensif dengan teknologi dan peran tenaga ahli untuk menekan biaya operasional, karena siber ofensif memerlukan biaya yang tidak setinggi pengeluaran terhadap pertahanan siber dan juga melihat tingkat resiko yang lebih besar atas sanksi internasional maupun korban (Melysa, 2016: 217).

Dampak serangan siber terhadap Saudi Aramco yakni terganggunya lapisan ruang maya Saudi Aramco oleh virus *Shamoon*. Lapisan fisik telah merusak lebih dari 30.000 komputer yang telah terinfeksi oleh virus *Shamoon* dan tidak dapat melakukan Booting ulang sehingga komponen fisik dalam lapisan ruang maya yaitu komputer yang digunakan perusahaan dan sistem komputer yang tidak dapat dipulihkan. Kemudian, merusak lapisan logis, yaitu data penting Saudi Aramco. Serangan tersebut telah mematikan saluran komunikasi internal namun tidak menghentikan produksi minyak Saudi Aramco. Virus *Shamoon* tahun 2012 diidentifikasi sebagai bagian dari *Malware* yang menyerang Master Boot Record (MBR), kabel partisi, dan sebagian besar file dengan data acak, sehingga perangkat keras komputer tidak dapat digunakan kembali dan mengakibatkan situs website

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v4i2

www.aramco.com offline dalam masa isolasi (https://money.cnn.com/2015/08/05/technology/aramco-hack/ diakses 29/07/2020).

Menurut Anderson dan Sadjadpour dalam *Cyber Defense Project*, (2019: 15) kerugian atas dampak ekonomi mencapai 10 juta hingga 100 juta dollar. Meskipun perusahaan mengalami gangguan kerusakan sistem komputer pada Saudi Aramco dan pemberhentian sistem komunikasi internal terganggu, namun serangan siber Iran.

Kenaikan atas minyak mentah Arab Saudi dipengaruhi oleh beralihnya mitra minyak Iran akibat dari sanksi ekonomi atas eskalasi pengayaan Nuklir Iran. Produksi minyak Arab Saudi menurut *Annual Statistical Bulletin* OPEC atau *Organization of the Petroleum Exporting Countries* (2014:29) mencapai 9,763 (1000 barel/hari), dan mengalami peningkatan dari 2011 – 2012 sebanyak 452 (1000 barel/hari). Meskipun kerugian tidak berdampak terhadap secara langsung terhadap produksi minyak Arab Saudi, namun serangan terhadap Saudi Aramco telah menciptakan ketegangan keamanan siber di Timur Tengah, karena dampak atas serangan infrastruktur kritis Arab Saudi dapat ditembus melalui operasi siber ofensif Iran.

4.2.2 Kepentingan Nasional Iran Dalam Menyerang Kilang Minyak Arab Saudi

Sebelum serangan siber Iran terhadap Arab Saudi, pada tanggal 10 Agustus 2012 Presiden Barack Obama menandatangani undang-undang memperluas sanksi terhadap Iran. Undang-undang tersebut mencakup larangan penyediaan asuransi, reasuransi, dan layanan pengiriman lainnya ke entitas kapal yang terlibat. Kemudian Uni Eropa telah memperketat perdagangan dengan Iran terutama dalam ekspor minyak Iran (https://www.nti.org/learn/countries/iran/nuclear/ diakses 30/07/2020).

Arti penting Saudi Aramco bagi Amerika Serikat pada dasarnya dimulai dari perjanjian mengenai *Standard Oil of California* atau "Socal" yang membawa pada perizinan atas eksplorasi minyak di Arab Saudi (https://americas.aramco.com/en/who-we-are/about/our-history 24/08/2020). Kemudian, Amerika Serikat dan Arab Saudi telah membuat kesepakatan untuk membantu Saudi Aramco. Aspek – aspek yang termuat dalam perjanjian diantaranya pembangunan infrastruktur, pengembangan teknologi, transformasi digital Saudi Aramco (https://www.aramco.com/en/news-media/news/2017/mou-saudi-us-forum-2017 diakses 24/08/2020).

Ketergantungan atas Arab Saudi terhadap minyak memberikan tekanan, bahwa infrastruktur kritis khususnya kilang minyak penting untuk terus menanamkan kesadaran terhadap keamanan ruang maya. Optimalisasi dari kecanggihan teknologi tidak hanya memberikan berbagai kemudahan, seperti interkonetivitas dalam perusahaan Saudi Aramco, virtualitas data penting Saudi Aramco dan juga perluasan skala penyebaran informasi yang cepat telah tertanam pada Saudi Aramco, sehingga apabila terjadi ancaman terhadap Saudi Aramco dapat diartikan sebagai ancaman terhadap keamanan nasional Arab Saudi. Oleh karena itu, Arab Saudi menginvestasikan 33.000 tentara dan 5.000 penjaga, dalam mengamankan Saudi Aramco (Dehlawi dan Abokhodair, 2013:73).

Mitra minyak utama Iran yaitu China, menyetujui untuk menghentikan impor atas minyak mentah Iran. Hal ini penting untuk dilakukan karena China adalah mitra strategis Iran, dan untuk itu Amerika Serikat menekan sanksi atas Iran melalui pemberhentian impor minyak Iran. Namun, dalam perjalannya China tidak sepenuhnya mematuhi sanksi tersebut dan tetap China tetap melakukan pemasokan minyak dari

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v4i2

Iran (https://thediplomat.com/2020/05/us-sanctions-prompt-china-to-cut-most-iran-oil-supplies-officially-at-least/ diakses 24/08/2020). Dalam memahami hubungan Iran dan China dapat dilihat sebagai penanaman atas investasi sektor energi dan dijadikan sebagai jalan untuk masuknya berbagai perusahaan bara tatas sanksi internasional yang dijatuhkan terhadap Iran (Christiani, 2018:66).

India sebagai mitra minyak terbesar Iran setelah China mengambil langkah untuk menghentikan impor minyak dari dan mengalihkannya pada Arab Saudi. (https://economictimes.indiatimes.com/industry/energy/oil-gas/us-deadline-ends-india-stops-purchasing-iranian-oil/articleshow/69475495.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst diakses pada 24/08/2020). Menurut *Congressional Research Service* (2020:51) pengalihan mitra minyak Iran atas sanksi 2011-2015, mengakibatkan penjualan minyak mentah Iran turun dari 2,5 mbd tahun 2011 menjadi sekitar 1,1 mbd pada tahun 2014.

Dalam melihat serangan siber ofensif Iran terhadap Saudi Aramco merupakan sebuah kejahatan siber dengan menggunakan *Malware* berjenis virus, yaitu *Shamoon*. Penguasaan Iran terhadap ruang maya digunakan untuk menyerang sistem komputer Saudi Aramco yang memiliki interkonektivitas tinggi, khususnya dalam komunikasi internal perusahaan dan sistem komputer. Disamping itu, peran penting dari kelompok peretas siber sebagai eksekutor terhadap Saudi Aramco yaitu Cutting Sword of Justice. Serangan yang ditujukan bagi Saudi Aramco bukan hanya ditujukan bagi beralihnya mitra minyak Iran, klaim atas kelompok peretas Cutting Sword of Justice menyatakan atas tindakan protes terhadap penggunaan minyak untuk mendukung berbagai perang yang terjadi di Timur Tengah (https://pastebin.com/HqAgaQRj diakses 24/08/2020).

4.2.2.1 Eksistensi Siber Ofensif Iran Melalui Virus *Shamoon*

Revolusi Iran 1979 menjadi sejarah penting bagi Iran yang tidak akan pernah dilupakan, karena merupakan titik balik melepaskan pengaruh Barat sehingga telah mengakhiri program nuklir dengan Amerika Serikat. Hal ini menimbulkan fase baru bagi hubungan Iran dan Amerika Serikat dalam program nuklir. Tindakan Iran dalam menghentikan kerjasama dengan Amerika Serikat dinilai sebagai tindakan yang membahayakan karena dapat mengarah pada pengembangan senjata nuklir. Dorongan baik dari negara di Timur Tengah dan dunia internasional untuk melakukan sebuah pemeriksaan atau penyelidikan atas program nuklir Iran dilakukan oleh *International Atomic Energy Agency* atau IAEA. IAEA memberikan laporan bahwa tidak ada kegiatan pengembangkan nuklir yang mengarah pada pembuatan senjata nuklir. (https://edition.cnn.com/2013/11/07/world/meast/irans-nuclear-capabilities-fast-facts/index.html diakses pada 09/08/2020).

Pembangunan fasilitas nuklir dan pengayaan uranium Iran telah meluas hingga dibentuk fasilitas pengayaan nuklir di Natanz. Kekhawatiran timbul atas pesatnya pembangunan fasilitas nuklir. Pada tanggal 23 Desember 2006 Dewan Keamanan Perserikatan Bangsa – Bangsa menjatuhkan sanksi terhadap Iran karena tidak dapat menangguhkan program nuklirnya. Berdasarkan atas keputusan tersebut, Presiden Ahmadinejad berjanji untuk mengabaikan resolusi Dewan Keamanan PBB dan melanjutkan pengayaan, sehingga pada tahun 2012 menjadi puncak atas berbagai sanksi terhadap Iran, salah satunya yakni embargo penuh atas minyak Iran kepada Uni Eropa. Kemudian, keputusan Amerika Serikat secara sepihak memberikan ancaman

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v4i2

kepada Pemerintah Iran dan semua lembaga keuangan terkait dengan transaksi produk minyak bumi akan mengalami resiko yang berarti (https://www.nti.org/learn/countries/iran/nuclear/ diakses 29/07/2020).

Kesuksesan serangan siber di Timur Tengah seperti *Stuxnet*, Flame dan beberapa serangan siber lainnya merupakan inisiasi dari negara barat, namun Iran telah mengubah pandangan atas kapabilitas dari kekuatan siber. Dalam mengupayakan kemampuan siber, setiap negara dapat mengeskplorasi kemampuannya untuk mencapai kepentingan nasional, selain itu kekuatan siber dapat dijadikan senjata dalam mencari titik lemah atas target serangan siber. Serangan terhadap Saudi Aramco merupakan sebuah kejutan dari berbagai tekanan internasional melalui sanksi ekonomi yang melemahkan minyak Iran dan atas pengembangan nuklir Iran, namun Iran dapat membangun eskalasi kekuatan siber (https://www.iranfocus.com/en/iran-general-mainmenu-26/26834-iran-strengthened-cyber-capabilities-after-*Stuxnet*-us-general diakses 24/08/2020).

Setelah serangan siber ofensif Iran terhadap Saudi Aramco, Arab Saudi dan Amerika Serikat berupaya untuk memulihkan sistem komputer Saudi Aramco melalui Departemen Keamanan Dalam Negeri Amerika Serikat *atau United States Department of Homeland Security* (DHS). DHS dalam *Industrial Control System Cyber Emergency Response Team Monitor* (2012:1-2) menjelaskan dalam memulihkan serangan virus *Shamoon*, diperlukan mitigasi atas pemulihan sistem komputer Saudi Aramco, diantaranya ; 1) Menjalankan pencadangan bagi semua sistem kritis; 2) Isolasi jaringan kritis termasuk jaringan operasi dari sistem bisnis; 3) Menggunakan Anti-Virus yang terbaru; 4) Dalam pengaturan akses, perlu untuk menggunakan Virtual private Networks (VPNs) dan memastikan bahwa VPNs yang mengakses aman untuk sistem perusahaan, dan lain – lain.

Selanjutnya, serangan tersebut relevansi dari kepentingan yang ditujukan bagi kilang minyak Saudi Aramco, yaitu memberikan pengaruh bagi dunia internasional, bahwa Iran memiliki kapabilitas dalam bersaing dengan negara lain sebagai aktor hubungan internasional khususnya dalam siber ofensif. Pembangunan siber Iran telah meningkatkan kemampuan dunia maya, meskipun tidak berada dalam kekuatan utama, namun Iran berada di sebagian besar negara dengan kekuatan siber global, khususnya dalam strategi dan organisasi untuk perang dunia maya sebagai salah satu bentuk dari eksistensi siber khususnya di Timur Tengah (https://www.csis.org/analysis/iran-and-cyber-power diakses 24/08/2020).

4.2.2.2 Kepemimpinan di Kawasan Timur Tengah

Pemimpin Islam Ayatollah Sayyid Ali Khamenei meyakini bahwa Iran sebagai panutan bagi perubahan dikawasan dan hal ini mengancam Arab Saudi dan Amerika Serikat. Dalam menghentikan hegemoni kawasan Timur Tengah, Amerika Serikat dan Arab Saudi berupaya untuk menghentikan Iran sebelum membangkitkan negara lain di Timur Tengah dan membentuk kekuatan dengan membentuk kelompok kekuatan (https://www.leader.ir/en/content/8772/Enemies-fear-Iran's-leading-role-in-region diakses 30/07/2020).

Dalam kepemimpinan kawasan Timur Tengah, keamanan menjadi prioritas dalam melindungi kepentingan nasional. Ancaman akan serangan siber memberikan pengaruh besar bagi negara di Timur Tengah, yang ditandai dengan titik balik *Stuxnet* terhadap Iran. Iran telah memimpin dengan mengawali agresi sibernya melalui serangan berskala kecil, hingga berskala besar dengan menggunakan virus *Shamoon*.

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v4i2

Kapabilitas kekuatan siber Iran melalui siber ofensif telah memobilisasi sumber – sumber kekuatan sebagai instrumen untuk membuktikan dan menghukum negara Amerika Serikat dan sekutu di Timur Tengah atas berbagai sanksi internasional dan beralihnya mitra minyak Iran kepada Arab Saudi. maka dari itu, Iran menggunakan kekuatan dalam siber ofensif.

Iran ataupun Arab Saudi bukan merupakan dualisme dari kekuasaan regional, melainkan penguasaan akan peran pentingnya dalam pengaturan negara lain. Rivalitas akan kekuatan hegemoni Iran dan Arab Saudi tidak dibentuk untuk melakukan konflik terbuka, melainkan menanam berbagai permusuhan di negara lain sehingga persaingan hegemoni ini dapat dilihat sebagai upaya untuk mencapai perimbangan kekuatan dengan menciptakan berbagai perang secara tidak langsung atau Proxy War pada sebagian negara di Timur Tengah (https://mepc.org/saudi-arabias-foreign-policy diakses 30/07/2020).

Strategi Proxy War sering digunakan Iran dalam membantu negara ataupun sekutu di Timur Tengah. Konflik Timur Tengah yang berlarut tidak dapat diselesaikan dengan dominasi dari Arab Saudi, pada akhirnya perimbangan kekuatan ditunjukan oleh Iran untuk membentuk kekuatan dan melakukan serangkaian aktivitas yang menimbulkan distabilitas karena benturan kepentingan Iran dan Arab Saudi. hal ini mendorong berbagai upaya untuk menentang dominasi Arab Saudi yang merupakan sekutu Amerika Serikat, salah satunya upaya untuk menentang dominasi Arab Saudi dilakukan oleh kelompok peretas Iran yaitu Cutting Sword of Justice dengan klaim atas serangan terhadap infrastruktur kritis Arab Saudi melalui virus *Shamoon* dalam website Pastebin (Dehlawi dan Abokhodair, 2013:75)

4.2.3 Respons Arab Saudi Terhadap Siber Ofensif Iran

Pernyataan atas serangan siber ofensif Iran terhadap perusahaan kilang minyak Saudi Aramco dikeluarkan oleh *Ministry of Communications and Information Technology* Arab Saudi menyatakan pada Agustus 2012 terjadi kampanye atas serangan Virus *Shamoon* yang menargetkan Saudi Aramco. Virus ditujukan untuk merusak data dan merusak sistem komputer (https://www.mcit.gov.sa/en/media-center/news/89515 diakses 11/09/2020).

Paska serangan siber ofensif yang menyerang Arab Saudi, perusahaan kilang minyak Saudi Aramco memberikan konfirmasi mengenai serangan siber yang ditujukan pada perusahaan menggunakan sebuah virus yang menyerang terminal komputer internal. Sejalan dengan hal ini, beredar dalam sebuah klaim atas serangan terhadap Saudi Aramco merupakan serangan yang dilakukan oleh Cutting Sword of Justice yang dilakukan pada 15 Agustus 2012 dan mengakibatkan 30.000 komputer mengalami kerusakan (https://pastebin.com/HqAgaQRj diakses 23/08/2020).

Pernyataan dari Chief Executive Officer atau CEO Saudi Aramco yaitu, Khalid Al-Falih menjelaskan bahwa Saudi Aramco menjadi korban atas serangan siber, sehingga tindakan awal atas serangan tersebut, yakni dengan mematikan situs website perusahaan dan melakukan isolasi sistem sehingga virus tidak menyebar ke komponen produksi minyak Saudi Aramco (https://www.reuters.com/article/net-us-saudi-aramco-hacking/saudi-aramco-says-most-damage-from-computer-attack-fixed-idUSBRE87P0B020120826 diakses 23/08/2020). Selain itu, Kementerian Dalam Negeri Arab Saudi yang membantu dalam penyelidikan terhadap serangan siber virus *Shamoon*, tidak pernah dipublikasikan hasil penyelidikannya kepada publik, sehingga serangan siber

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v4i2

Saudi Aramco akan tetap dijaga kerahasiaannya (Meer, 2015: 3-4).

Pada tanggal 26 Agustus 2012 merupakan penyelesaian pemulihan perusahaan Saudi Aramco yang telah membersihkan semua terminal dan komputer terinfeksi virus *Shamoon*, sehingga dapat melanjutkan bisnis secara normal (Bronk dan Tikk, 2013:86).

Kekhawatiran atas serangan siber di masa depan mengakibatkan Arab Saudi melakukan manajemen ulang terhadap mitigasi ancaman serangan siber dan pembaharuan atas komponen – komponen keamanan terhadap infrastruktur kritis Saudi Aramco, salah satunya dengan memperkuat manajemen teknologi informasi dan berinvestasi dalam fasilitas keamanan Saudi Aramco.

Dalam memperkuat infrastruktur kritis, Arab Saudi memetakan perlindungan keamanan siber ditujukan terhadap Saudi Aramco sebagai objek vital negara atau infrastruktur kritis sehingga menimbulkan ketergantungan akan industri minyak sangat penting. Investasi sistem keamanan difokuskan pada membentuk perlindungan dengan menciptakan rasa aman terhadap keamanan data, fisik, aset perusahaan dari Saudi Aramco, hal di ini dukung oleh jaminan keamanan Amerika Serikat. Menurut Meer (2015:7) dalam serangan siber terhadap Saudi Aramco, Arab Saudi meminta bantuan terhadap Amerika Serikat melalui saluran diplomasi untuk melakukan analisa terkait virus *Shamoon* dan meminta untuk menghapus virus dari server atas serangan siber tahun 2012. Dalam hal ini, tidak ada pernyataan kebijakan luar negeri bagi Iran atas serangan siber ofensif yang menyerang Saudi Aramco tahun 2012. Bantuan atas Amerika Serikat ditujukan bagi dukungan bagi pemulihan infrastruktur kritis Saudi Aramco.

Setelah serangan siber pada tahun 2012, Arab Saudi meningkatkan investasi dibidang keamanan siber secara signifikan. Salah satunya dengan membentuk *National Information Security Strategy* (NISS), merupakan lembaga yang dibentuk dalam skala domestik untuk menciptakan kerangka dalam keamanan siber Arab Saudi khususnya dalam membangun keamanan siber terhadap infrastruktur kritis Arab Saudi (Hathaway dkk. 2017: 5-6).

Menurut *Virginia Economic Development Partnership's* (2014:6) Investasi keamanan siber Arab Saudi, ditujukan terhadap Amerika Serikat. Amerika Serikat dapat memberikan sumber daya dan pengadaan perusahaan pertahanan swasta atas nama Arab Saudi. Kemudian, besarnya investasi keamanan siber menjadikan Arab Saudi telah memberikan sumbangan 75% pengeluaran perangkat keras Timur Tengah.

Respon atas penguasaan ruang siber oleh Arab Saudi atas serangan *Shamoon* 2012, ditujukan bagi penguasaan arus informasi dan pengguna layanan internet. Kemampuan siber ofensif Iran dengan menggunakan Virus *Shamoon* telah merusak lapisan fisik dan logis dari keamanan siber, namun penguasaan atas lapisan informasi dan sosial dapat dikendalikan oleh Arab Saudi. Menurut Collier, ddk. (2013:469-470) lapisan informasi mencakup skema pengaturan risiko yang dapat dikendalikan atas dampak yang diterima dari serangan siber, sedangkan lapisan sosial merujuk pada kontrol sosial terhadap keamanan siber yang konsisten melalui pertimbangan sosial dan etika suatu negara.

Penguasaan lapisan keamanan siber informasi Arab Saudi pada serangan siber ofensif tahun 2012 menggunakan Virus *Shamoon* difokuskan pada skema pengendalian atas berbagai media informasi bahwa serangan siber terhadap Saudi Aramco dilakukan oleh Iran, sehingga media internasional mengarahkan kejahatan siber melalui *Shamoon* adalah serangan yang dilakukan oleh Iran. Kemudian, berbagai informasi rahasia mengenai kerusakan Saudi Aramco secara

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v4i2

lengkap tetap menjadi kerahasiaan. Selanjutnya, pengendalian terhadap lapisan sosial dilakukan oleh kelompok dengan mengawasi sumber arus informasi mengenai berbagai arus media yang menentang rezim, menghapus komentar yang merendahkan Arab Saudi dan secara umum mengwasi kontrol atas saluran media sosial yang sesuai dengan etika Kerajaan Arab Saudi, disebut sebagai "Troll Army" (https://www.inss.org.il/publication/how-prepared-is-saudi-arabia-for-a-cyber-war/ diakses 11/09/2020). Hal ini menekankan bahwa Cyber Power Arab Saudi dapat menekan berbagai kerusakan lapisan keamanan siber atas serangan siber ofensif terhadap Saudi Aramco pada tahun 2012.

4.2.4 Hubungan Iran dan Arab Saudi Paska Serangan Siber Ofensif Iran

Serangan siber Iran terhadap Arab Saudi telah memberikan ke khawatiran bagi negara lainnya untuk mengamankan infrastruktur kritis dalam menciptakan keamanan nasional, karena Iran telah berhasil menunjukan eksistensi dari kekuatan siber untuk menyerang infrastruktur vital Arab Saudi, Saudi Aramco.

Iran pada masa pemerintahannya Presiden Mahmoud Ahmadinejad telah meningkatkan intensitas atas berbagai konflik di Timur Tengah, khususnya mengenai dukungannya atas pemberontak yang mengancam terhadap negara – negara kecil. Sanksi internasional dan embargo ekonomi dapat efektif untuk melumpuhkan perekonomian Iran, namun tidak menghentikan Iran untuk melakukan berbagai tindakan atas kepentingan nasionalnya sebagai aktor dalam kawasan Timur Tengah dan dunia.

Setelah serangan siber terhadap kilang minyak Arab Saudi melalui *Proxy War* oleh *Cutting Sword of Justice*, ketegangan hubungan Arab Saudi dan Iran memasuki tahap dualisme kekuatan hegemoni kawasan Timur Tengah di Palestina, Irak, Libanon dan Afganistan (https://iranprimer.usip.org/blog/2016/jan/06/timeline-iran-saudi-relations diakses 22/08/2020).

Stabilitas Timur Tengah yang diciptakan atas pengaturan dari dualisme Iran dan Arab Saudi mengakibatkan instabilitas di kawasan. Meskipun Iran dan Arab Saudi tidak secara langsung menjalankan konflik terbuka melihat penguasaan pengaruh di kawasan yang besar, namun hal ini berdampak pada negara – negara dalam kawasan. Selain itu, sanksi internasional atas nuklir Iran menambah instabilitas di Timur Tengah, hal ini berpengaruh terhadap harga minyak mentah pada tahun 2012.

Kenaikan pada harga minyak mentah dunia menurut *Energy Information Administration* (2012) menjelaskan bahwa beberapa faktor yang mempengaruhi kenaikan harga minyak pada tahun 2012, diantaranya karena terganggunya pasokan dari negara – negara di Timur Tengah dan sanksi yang memberatkan Iran. Terganggunya pasokan minyak dari negara eksportir Timur Tengah diakibatkan oleh konflik – konflik di Timur Tengah yang berakibat pada penurunan produksi minyak. Selain itu, tekanan internasional atas Iran memberikan ancaman atas penutupan Selat Hormuz dan pengurangan ekspor minyak untuk menekan program nuklir, sehingga harga minyak pada tahun 2012 mencapai 111,67 dollar per barel. berada pada level tertinggi secara historis untuk tahun kedua berturut-turut (https://www.eia.gov/todayinenergy/detail.php?id=7630 diakses 23/08/2020).

Kekhawatiran negara – negara di Timur Tengah khususnya negara yang tergabung dalam *Gulf Cooperation Council* pasca serangan siber ofensif Iran dengan menggunakan virus *Shamoon* tahun 2012 telah memberikan dampak atas ancaman dari serangan siber lainnya terhadap infrastruktur kritis negara, hal ini

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v4i2

berlandaskan atas serangan Saudi Aramco yang mengindikasikan percepatan Perang Siber atau *Cyber Warfare* di Timur Tengah.

Temuan Cyber Warfare dikawasan Timur Tengah dapat dilihat setelah adanya berbagai serangan siber yang ditemukan di beberapa negara Timur Tengah. Menurut Segal dalam *German Marshall Fund* (2017:2) geopolitik siber di Timur Tengah terjadi pada Juni 2012, ketika Amerika Serikat dan Israel membocorkan serangan siber *Stuxnet*, yang disebut sebagai "Year Zero". Kemudian, beberapa serangan siber mulai diluncurkan oleh negara Iran dan Israel, sehingga negara di Timur Tengah lainnya mulai membangun kekuatan penuh siber.

Perlombaan atas senjata siber di Timur Tengah telah meningkat khususnya setelah serangan virus *Shamoon* tahun 2012 terhadap Saudi Aramco. Kemudian, pada tahun 2017 terjadi Krisis Qatar akibat serangan siber Uni Emirat Arab terhadap situs berita pemerintah Qatar. Kekhawatiran akan adanya *Cyber Warfare* yang lebih besar, maka dari itu salah satu upaya yang dilakukan negara GCC, yakni melakukan untuk bekerja sama dalam membangun keamanan siber dengan Amerika Serikat, Eropa, China dan Rusia (Alalwan et.al., 2013:35).

Selanjutnya, paska serangan Virus *Shamoon* tahun 2012, adanya indikasi atas gelombang kedua penyerangan dengan virus *Shamoon* 2 atau *Stonedrill*. Serangan *Shamoon* 2 ditargetkan terhadap organisasi Arab Saudi pada November 2016. *Shamoon* 2 secara umum memiliki kesamaan dengan *Shamoon* 2012 salah satunya serangan atas kode *Shamoon* 2 ditujukan untuk menghancurkan sistem komputer, berikut merupakan komponen yang terdapat dalam *Shamoon* tahun 2012 dan *Shamoon* 2.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Serangan siber terhadap Saudi Aramco merupakan serangan siber dengan menggunakan pola siber ofensif, hal ini dilakukan atas pertimbangan perang asimetris Iran yang berusaha untuk melawan sekutu Amerika Serikat dikawasan yakni Arab Saudi dengan mengembangkan kapabilitas yang tidak seimbang. Selain itu, siber ofensif terhadap Saudi Aramco tidak menimbulkan resiko ancaman korban jiwa yang perlu untuk diprioritaskan atas keamanan negara, melihat bahwa Iran telah dijatuhkan berbagai sanksi ekonomi internasional.

Iran melihat bahwa kepentingan nasional mengenai keamanan siber merupakan sebuah strategi yang memiliki aspek kerahasiaan, integritas dan ketersediaan. Kepentingan siber ofensif Iran terhadap Saudi Aramco ditujukan terhadap reaksi atas serangan *Stuxnet* yang telah menghancurkan instalasi pengayaan nuklir di Natanz. Kemudian, atas sanksi internasional yang dijatuhkan pada Iran karena dianggap telah mengancam stabilitas global atas program pembuatan senjata berteknologi nuklir, sehingga mitra minyak Iran telah beralih, diantaranya pada Arab Saudi. siber ofensif Iran telah mengancam keamanan sekutu Amerika Serikat yakni Arab Saudi dalam keamanan nasionalnya.

Dampak serangan siber Iran dengan menggunakan virus *Shamoon*, tidak ada kecaman serius atas tindakan serangan siber tahun 2012. Dalam menyelesaikan permasalahan tersebut, Arab Saudi bekerja sama dengan Amerika Serikat untuk melakukan berbagai pemulihan atas rusaknya komputer Saudi Aramco. Pemulihan dilakukan atas bantuan Amerika Serikat untuk menganalisa virus dan mengembalikan fungsi sistem komputer perusahaan Saudi Aramco.

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v4i2

Pernyataan resmi akan sebuah serangan ditujukan dengan menyebarkan informasi bahwa Saudi Aramco telah di serang oleh kelompok peretas *Cutting Sword of Justice.* Namun, serangan virus *Shamoon* diasumsikan sebagai masalah nasional tanpa harus adanya campur tangan internasional atau bahkan kebijakan luar negeri atas tindakan serangan siber Saudi Aramco.

Hubungan Iran dan Arab Saudi setelah serangan siber ofensif Iran, pada dasarnya tetap mengalami ketegangan dan permusuhan. Tindakan Arab Saudi yang memilih untuk menyelesaikan serangan siber ofensif menggunakan *Shamoon* melalui skema nasional, pada sebagian negara dinilai sebagai serangan yang tidak memiliki dampak besar. Serangan siber Iran tidak memberikan dampak yang besar khususnya mengenai perubahan harga minyak dunia, tetapi secara pasti telah memberikan kerusakan yang cukup besar yang disebabkan serangan siber menggunakan virus *Shamoon*.

Instabilitas keamanan dunia maya di Timur Tengah diarahkan pada Iran sebagai aktor atas berbagai serangan siber khususnya terhadap Arab Saudi. Disamping itu, Iran menolak atas tuduhan dibalik dari serangan siber tersebut. Dalam perjalanan hubungan Iran dan Arab Saudi hingga saat ini masih mengalami ketegangan khususnya bagi keamanan kawasan Timur Tengah.

5.2 Saran

Serangan siber Iran terhadap kilang minyak Arab Saudi memberikan pemahaman akan kerentanan ruang maya yang dapat digunakan sebagai senjata untuk kepentingan atau hanya menguji keahlian dalam ruang maya. Hal ini perlu difokuskan terhadap perlindungan kerentanan atas infrastruktur kritis dan objek vital negara yang dapat mengancam keamanan nasional.

Pembangunan keamanan siber penting untuk dilakukan melihat berbagai kemungkinan atas kerentanan ruang maya atas serangan terhadap Saudi Aramco tahun 2012. Ketergantungan ketahanan siber Arab Saudi memberikan kelemahan atas pembangunan ketahanan secara nasional.
Saran atas pengembangan kajian siber di Timur Tengah perlu di perluas, karena dapat memberikan persfektif baru dalam fenomena hubungan internasional di Timur Tengah. Selain itu, perlu adanya sebuah forum khusus bagi pengembangan siber dan analisa berbagai fenomena siber dunia, sehingga dapat memberikan pengetahuan dan pemahaman atas berbagai dinamika keamanan siber di dunia internasional.

Daftar Pustaka

Buku

Darmayadi, Andrias ddk. 2015. *Mengenal Studi Hubungan Internasional.* Bandung: Zavara

Perwita, Anak Agung Perwita dan Yani, Yanyan Mochamad. *Pengantar Ilmu Hubungan Internasional.* Bandung: PT Remaja Rosdakarya

Rahadjo, Budi. (2017). *Keamanan Informasi*. Bandung: PT Insan Infonesia,

Karya Tulis Ilmiah

Alalwan, N., Alzahrani, A., & Sarrab, M. (2013). Cybercrime Investigation Challenges for Gulf Cooperation Council Governments: A Survey. ICoFCS 2013, 33

Alelyani, S., & Kumar, H. (2018). Overview Of Cyberattack On Saudi Organizations.

Alif Iskandar, J. (2020). Strategi Geopolitik Iran Untuk Mengimbangi Arab Saudi Melalui Perang Saudi[skripsi].

Aritonang, R. P. (2019). Operasi Siber Ofensif Iran Terhadap Amerika Serikat, Israel Dan Arab Saudi: Kepentingan Dan Strategi Siber

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v4i2

Ofensif Iran[skripsi]. (Doctoral Dissertation, Universitas Airlangga

Aycock, J. (2006). *Computer Viruses And Malware (Vol. 22)*. Springer Science & Business Media.

Bronk, C., & Tikk-Ringas, E. (2013). Hack or attack? *Shamoon* and the Evolution of Cyber Conflict.

Christiani, A. (2018). Dukungan Tiongkok Terhadap Pengembangan Nuklir Di Iran Pada Masa Pemerintahan Hu Jintao. Global Political Studies Journal, 2(1), 56-71.

Collier, Z. A., Linkov, I., & Lambert, J. H. (2013). Four domains of cybersecurity: a risk-based systems approach to cyber decisions.

Dehlawi, Z., & Abokhodair, N. (2013, June). Saudi Arabia's response to cyber conflict: A case study of the *Shamoon* malware incident. In 2013 IEEE International Conference on Intelligence and Security Informatics (pp. 73-75). IEEE.

Hathaway, M., Spidalieri, F., & Alsowailm, F. (2017). Kingdom of Saudi Arabia Cyber Readiness at a Glance. Potomac Institute for Policy Studies.

Knapp, K. J. (2009). *Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions. United States of America: Information Science Reference*

Knapp, K. J. (2009). *Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions. United States of America: Information Science Reference*

Medvedev, S. A. (2015). Offense-Defense Theory Analysis Of Russian Cyber Capability. Naval Postgraduate School Monterey Ca.

Melysa, A., Putranti, I. R., & Dir, A. A. B. (2016). 23. Analisis Penggunaan Offensive Cyber Operations Menghadapi Ancaman Nuklir Iran. Journal of International Relations, 2(4), 213-220.

Pujayanti, A. (2012). Sanksi Ekonomi terhadap Iran dan Dampak Internasional nya. Info Singkat Hubungan Internasional, 4(4), 6.

Putra, R. P., Jamilah, M., & Irawan, P. (2020). Intervensi Militer Arab Saudi Terhadap Konflik Yaman Untuk Membendung Pengaruh Iran Di Timur Tengah. Jurnal Pir: Power In International Relations, 4(1), 76-100.

Rattray, Gregory. (2018). Strategic Culture and Cyberwarfare Strategic: Four Case Studies. SIPA Capstone Workshop.

Smeets, M. (2018). The Strategic Promise Of Offensive Cyber Operations. Strategic Studies Quarterly, 12(3), 90-113.

Suharto, M. A. (2015). Analisis Yuridis Mengenai Cyber Attack Dalam Cyber Warfare Berdasarkan Hukum Humaniter Internasional (Studi Kasus Cyber Attack Negara Amerika Serikat Terhadap Program Pengembangan Nuklir Negara Iran Pada Tahun 2009). Kumpulan Jurnal Mahasiswa Fakultas Hukum.

Triwahyuni, D. (2020, January). American Foreign Policy In Cyberspace. In International Conference On Business, Economic, Social Science, And Humanities–Humanities And Social Sciences Track (Icobest-Hss 2019) (Pp. 48-51). Atlantis Press.

Triwahyuni, D., & Wulandari, T. A. (2016). Strategi Keamanan Cyber Amerika Serikat. Jurnal Ilmu Politik dan Komunikasi Volume VI No.

Triwahyuni, D., & Yani, Y. M. (2018). Dampak Pembangunan Cyberpower Tiongkok Terhadap Kepentingan Amerika Serikat. Jurnal Ilmu Politik Dan Komunikasi Volume VIII No.1, 1-2.

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v4i2

Umar, A. R. M. (2015). The National Interest In International Relations Theory. Global South Review, 1(2), 185-190.

Van Haaster, J. (2016, May). Assessing cyber power. In 2016 8th International Conference on Cyber Conflict (CyCon) (pp. 7-21). IEEE.

Venables, A., Shaikh, S. A., & Shuttleworth, J. (2015, March). A Model for Characterizing Cyberpower. In International Conference on Critical Infrastructure Protection (pp. 3-16). Springer, Cham.

Dokumen

Congressional Research Service. 2020. Iranian Offensive Cyber Attack Capabilities

Cyber Defense Project. 2019. Hotspot Analysis: Iranian Cyber-Activities In The Context Of Regional Rivalries And International Tensions

German Marshall Fund. 2017. Cheap Havoc: How Cyber-Geopolitics Will Destabilize the Middle East

Industrial Control System Cyber Emergency Response Team Monitor. 2012. *Shamoon*

Kemhan. 2014. Pedoman Pertahanan Siber

NCB Interpol Indonesia. 2013. Cybercrime: Sebuah Fenomena Di Dunia Maya.

OPEC. 2014. Annual Statistical Bulletin

Perpustakaan Universitas Padjajaran. 2010. Dinamika Hubungan Internasional Dan Indonesia

UNIKOM. Power: Pemahaman Konsep Power Dalam Studi Hubungan Internasional

Virginia Economic Development Partnership's. 2014. Cyber Security Export Market: Saudi Arabia

Rujukan Elektronik

America Aramco._____. Diakses melalui https://americas.aramco.com/en/who-we-are/about/our-history [24/08/2020].

CNN. 2015. The inside story of the biggest hack in history. Diakses melalui (https://money.cnn.com/2015/08/05/technology/aramco-hack/ [29/07/2020].

CNN. 2020. Iran's Nuclear Capabilities Fast Facts. Diakses melalui https://edition.cnn.com/2013/11/07/world/meast/irans-nuclear-capabilities-fast-facts/index.html [09/08/2020].

CSIS. 2019. Iran and Cyber Power. Diakses melalui https://www.csis.org/analysis/iran-and-cyber-power [24/08/2020].

CSMT. 2020. Cyberspace. Diakses melalui https://lucian.uchicago.edu/blogs/mediatheory/keywords/cyberspace/ [04/06/2020].

EIA. 2012. Crude oil prices peaked early in 2012. Diakses melalui https://www.eia.gov/todayinenergy/detail.php?id=7630 [23/08/2020].

INSS. 2019. How Prepared is Saudi Arabia for a Cyber War?. Diakses melalui https://www.inss.org.il/publication/how-prepared-is-saudi-arabia-for-a-cyber-war/ [11/09/2020].

Iran Focus. 2013. Iran strengthened cyber capabilities after *Stuxnet*: U.S. general. Diakses melalui https://www.iranfocus.com/en/iran-general-mainmenu-26/26834-iran-strengthened-cyber-capabilities-after-*Stuxnet*-us-general [06/08/2020].

Iran Focus. 2013. Iran strengthened cyber capabilities after *Stuxnet*: U.S. general. Diakses melalui https://www.iranfocus.com/en/iran-general-mainmenu-26/26834-iran-strengthened-cyber-capabilities-after-*Stuxnet*-us-general [24/08/2020].

Iran Primer. 2019. Supreme National Security Council of Iran. Diakses

Volume 4 Nomor 2 Edisi Oktober 2020
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v4i2

melalui https://iranprimer.usip.org/blog/2019/apr/01/supreme-national-security-council-iran [03/08/2020].

Leader Iran. 2011. Enemies fear Iran's leading role in region. Diakses melalui https://www.leader.ir/en/content/8772/Enemies-fear-Iran's-leading-role-in-region [30/07/2020].

MEPC. 2020. Saudi Arabia's Foreign Policy. Diakses melalui https://mepc.org/saudi-arabias-foreign-policy [30/07/2020].

Ministry of Communications and Information Technology._____. Diakses melalui https://www.mcit.gov.sa/en/media-center/news/89515 [11/09/2020].

NTI. 2020. Iran. Diakses melalui https://www.nti.org/learn/countries/iran/nuclear/ [30/07/2020].

NTI. 2020. Nuclear. Diakses melalui https://www.nti.org/learn/countries/iran/nuclear/ [29/07/2020].

Nytimes. 2012. U.S. Suspects Iran Was Behind A Wave Of Cyberattacks. Diakses melalui https://www.nytimes.com/2012/10/14/world/middleeast/us-suspects-iranians-were-behind-a-wave-of-cyberattacks.html [26/04/2020].

Pastebin. 2012. Untitled. Diakses melalui https://pastebin.com/HqAgaQRj diakses [23/08/2020].

Phys. 2012. Us Thinks Iran Behind Cyberattack In Saudi: Ex-Official. Diakses melalui https://phys.org/news/2012-10-iran-cyberattack-saudi-ex-official.html [10/04/2020].

PHYS. 2012. US thinks Iran behind cyberattack in Saudi: ex-official. Diakses melalui https://phys.org/news/2012-10-iran-cyberattack-saudi-ex-official.html [24/08/2020].

Reuters. 2012. Saudi Aramco says most damage from computer attack fixed. Diakses melalui https://www.reuters.com/article/net-us-saudi-aramco-hacking/saudi-aramco-says-most-damage-from-computer-attack-fixed-idUSBRE87P0B020120826 [23/08/2020].

Saudi Aramco. 2017. Saudi Aramco signs agreements with American companies to promote bilateral trade and investment between Saudi Arabia and United States. Diakses melalui https://www.aramco.com/en/news-media/news/2017/mou-saudi-us-forum-2017 [24/08/2020].

Saudi Aramco. 2020. Our history. Diakses melalui https://www.saudiaramco.com/en/who-we-are/overview/our-history [10/04/2020].

The Diplomat. 2020. US Sanctions Prompt China to Cut Most Iran Oil Supplies, Officially at Least. Diakses melalui https://thediplomat.com/2020/05/us-sanctions-prompt-china-to-cut-most-iran-oil-supplies-officially-at-least/ [24/08/2020].

The Economic Times. 2019 .US deadline ends, India stops purchasing Iranian oil. Diakses melalui https://economictimes.indiatimes.com/industry/energy/oil-gas/us-deadline-ends-india-stops-purchasing-iranian-oil/articleshow/69475495.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst [24/08/2020].