BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan yang dapat diambil dalam menjawab rumusan masalah dari kepentingan siber ofensif Iran terhadap Arab Saudi dalam kasus virus *Shamoon* tahun 2012. Pertama, 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. Kemudian, tidak ada klaim resmi dari Iran atas serangan siber terhadap Saudi Aramco.

Kerusakan atas masuknya perangkat lunak berbahaya Malware jenis virus *Shamoon* yang di program untuk merusak sistem keamanan Saudi Aramco, telah merusak 30.000 komputer yang memutus jaringan komunikasi internal perusahaan. *Shamoon* yang merupakan sebuah *Boot Virus* berhasil menyerang melalui *Hard Drive* dan telah menghancurkan data acak dari Saudi Aramco. Kemudian, siber ofensif terhadap Saudi Aramco tahun 2012 telah merusak lapisan ruang maya dari Arab Saudi yaitu, lapisan fisik dan lapisan logika, namun Arab Saudi memiliki

kapabilitas dalam pengendalian *Cyberpower* dengan menguasai lapisan informasi dan pengguna internet di seluruh dunia. Disamping itu, penggunaan kelompok peretas Iran yakni *Cutting Sword of Justice* yang merupakan eksekutor memiliki peran penting, tidak hanya merusak komputer Saudi Aramco, melainkan telah berhasil mencuri data acak penting yang langsung dapat terhubung dengan komputer peretas.

Kedua, Iran melihat bahwa kepentingan nasional mengenai keamanan siber merupakan sebuah strategi yang memiliki aspek kerahasiaan, integritas dan ketersediaan. Bentuk strategi yang muncul dalam dilihat dari pola *Proxy War* dan serangan siber asimetris. Hal ini yang mengakibatkan pola dari strategi siber Iran cenderung tidak terorganisir secara jelas, namun bukan berarti berbagai kelompok yang tergabung dalam kekuatan siber Iran tidak dapat melakukan serangan berdasarkan atas kepentingan negara.

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 terutama Arab Saudi dalam mencapai eksistensi kekuatan siber di Timur Tengah.

Ketegangan atas dinamika Iran dikawasan Timur Tengah ditujukan bagi berbagai aktivitas Iran yang terus mendorong berbagai kelompok teroris di Timur

Tengah khususnya kelompok yang mengancam rezim diktator. Berangkat dari pengaruhnya yang begitu besar di Timur Tengah, Iran telah berhasil membangun kekuatan siber. Siber ofensif Iran ditujukan sebagai kebangkitan atas kekuatan regional untuk melawan pengaruh Amerika Serikat khususnya bagi sekutunya yaitu Arab Saudi. Iran dinilai dan berpotensi sebagai kekuatan regional yang dapat memberikan ancaman atas beberapa negara di Timur Tengah dan dunia internasional, karena dapat membangun kapabilitas sibernya untuk melawan musuh regional atas kepemimpinan Iran di kawasan Timur Tengah.

Ketiga, dalam melihat dampak serangan siber Iran dengan menggunakan virus *Shamoon,* tidak ada kecaman serius atas tindakan serangan siber tahun 2012. Hal ini dapat dilihat dari hubungan Iran dan Arab Saudi yang pada dasarnya konfliktual. Serangan siber atas infrastruktur vital Arab Saudi telah memberikan pukulan atas kerentanan keamanan Saudi Aramco. 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.

Serangan virus *Shamoon* mengharuskan Saudi Aramco untuk memutuskan jaringan komunikasi internal dan menghentikan sementara jaringan internet Saudi Aramco. 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.

Selanjutnya, 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. Namun, setelah serangan tersebut Arab Saudi telah mengembangkan sistem pertahanan siber yang cukup besar anggarannya untuk melindungi berbagai infrastruktur viral negara.

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*. Kondisi negara di kawasan Timur Tengah memanas kembali ketika setelah serangan terhadap Saudi Aramco, terjadi serangan siber pada tahun 2016, yang menyerang Arab Saudi dengan serangan *Shamoon* 2. 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 terhadap Saudi Aramco membuka berbagai pandangan atas ancaman nyata dari kerentanan dunia maya. Kerentanan dunia maya dapat menjadi ruang bagi para peretas siber untuk melakukan serangan baik atas dasar kepentingan maupun hanya untuk menguji keahlian dalam dunia maya. Perlindungan atas infrastruktur vital menjadi penting, ketika dampak yang ditimbulkan dapat mengancam keamanan nasional.

Ketahanan siber dalam kerangka nasional memberikan acuan atau dasar penting bagi membangun keamanan siber. Meskipun, kerentanan akan tindak kejahatan siber masih dapat terjadi, melihat sifat dunia maya yang abstrak. Investasi keamanan dunia maya yang dilakukan Arab Saudi, perlu mengedepankan berbagai kekuatan nasional, hal ini karena ketergantungan Arab Saudi terhadap sistem keamanan Amerika Serikat. Dalam perjalannya, setelah adanya serangan siber ofensif Iran terhadap Saudi Aramco, memberikan berbagai kesempatan bagi pembangunan keamanan nasional, baik dalam upaya keamanan siber ofensif maupun defensif yang dapat di adopsi dari Iran maupun Arab Saudi, sebagai pelajaran penting bagi negara di dunia untuk membangun keamanan sibernya.

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.