BAB III
DILEMA KEAMANAN SIBER ANTARA AMERIKA SERIKAT DAN IRAN

Baik Amerika Serikat dan Iran sama-sama menghadapi dilema keamanan sibernya masing-masing. Dalam menghadapi dilema keamanan siber, masing-masing negara memiliki kebijakannya demi menjaga keamanan infrastruktur digitalnya. Proses pengambilan kebijakan-kebijakan tersebut dibuat dengan harus memperhatikan beberapa faktor agar menjadi efektif. Ada pula beberapa determinan yang dapat digunakan oleh negara agar dapat mengambil kebijakan yang tepat sehingga konflik dapat dihindari karena terjadinya kesalah pahaman antar negara.

A. Dilema Keamanan Siber Amerika Serikat Dan Iran

Baik Amerika Serikat maupun Iran sama-sama layak diperhitungkan keberadaannya di kancah dunia internasional. Baik dari segi kekuatan politiknya, pertahanan dan keamanannya, maupun kemajuan teknologi informasinya. Tak ayal, kedua negara tersebut sejak masa pasca revolusi Iran hingga sekarang selalu bersifat kontra dan bermusuhan satu sama lain.

Seperti yang telah disebutkan dalam kerangka teori dilema keamanan siber diatas, dilema ini muncul akibat adanya upaya negara untuk meningkatkan dan menjaga keamanan infrastruktur digital yang mereka miliki. Infrastruktur digital adalah penting karena hal tersebut berisi kekuatan sekaligus kelemahan serta kepentingan-kepentingan suatu negara, yang mana jika diketahui oleh musuh, maka keamanan nasional negara tersebut akan terancam.

Berdasarkan eksplanasi teori tersebut, maka dilema keamanan siber yang dimiliki oleh Amerika Serikat dan Iran berada pada tingkat yang tinggi. Keduanya memiliki infrastruktur digital yang canggih. Masing-masing dalam upaya mencapai kepentinganya, saling menyerang infrastruktur digitalnya satu sama lain. Berbeda dengan perang konvensional, seperti yang telah dinyatakan dalam kerangka teori sebelumnya, perang siber ini membawa frekuensi konflik antara kedua negara tersebut semakin meningkat. Melalui berbagai metode dan sarana, kedua negara saling mengacaukan dan menyerang sektor ekonomi dan teknologi komunikasi.

Berdasarkan pembagian kapabilitas untuk menjaga keamanan infrastruktur digital menurut Richard A. Clarke dan Robert K. Knake, berikut adalah aplikasi determinan terhadap Amerika Serikat dan Iran.

Tabel 3. 1 Perbandingan Kapabilitas Amerika Serikat dan Iran (Richard A. Clarke, 2010)

Negara	*Cyber Offense*[1]	*Cyber Dependence*[2]	*Cyber Defense*[1]	Total[3]
AS	9	2	4	15
Iran	4	5	3	12

1. Rentang skala 10, dengan 10 sebagai tingkat terkuat.
2. Rentang skala 10, dengan 10 sebagai tingkat ketergantungan terendah
3. Rentang skala 30, dengan 30 sebagai tingkat yang paling rentan

1. Determinan Kapabilitas Keamanan Infrastruktur Digital Amerika Serikat

Pada tabel diatas, Amerika Serikat mendapat predikat negara dengan kapabilitas ofensif yang kuat. Mengingat

banyaknya anggaran negara yang dialokasikan kepada sektor militer, termasuk teknologi siber, memang bukanlah sesuatu yang aneh jika kekuatan ofensifnya kuat. Amerika Serikat masih berada di urutan pertama dalam bidang pertahanan. Ia mendapat PowerIndex rating sebanyak 0.0857, dimana dengan rating 0.0000 adalah nilai paling sempurna. (Global Fire Power, 2017)

Sedangkan untuk kapabilitas defensif, Amerika Serikat mendapat predikat sedang. Hal ini sesuai dengan fakta bahwa kekuatan defensif Amerika Serikat sangat lemah dan rentan untuk mendapat serangan siber dari musuh. Tercatat dalam kurun waktu 12 bulan, Amerika Serikat telah mengalami serangan siber sebanyak 245 kali (periode Oktober 2013 sampai September 2014) yang menargetkan sektor industri energi dan manufaktur kritikalnya.

Sejak September 2012, Amerika Serikat mengalami beberapa kali serangan siber. Salah satunya adalah kasus pembajakan 46 institusi maupun perusahaan yang bergerak disektor finansial, salah satunya adalah JPMorgan Chase, Bank of America, CitiGroup, HSBC, AT&T, dan lain sebagainya. James Lewis, seorang staf ahli keamanan komputerisasi di Pusat Strategis Internasional di New York, mengatakan bahwa ia yakin adalah Iran yang menjadi dalang dari serangan ini. Tak lama setelah itu, muncul sebuah kelompok dengan sebutan Kelompok Izzuddin Al-Qasam *Cyber Fighters* yang mengaku bahwa merekalah pelaku aksi pembajakan itu. Namun, ada banyak pihak yang yakin bahwa kelompok ini merupakan upaya untuk menutupi keterlibatan Iran dalam aksi pembajakan tersebut. Metode yang digunakan oleh para penyerang ialah dengan menginfeksi pusat data untuk pelayanan dengan mengelabui sistem komputasi melalui virus dengan jenis "*cloud*". Amerika Serikat juga menemukan bahwa para penyerang tersebut juga menggunakan metode *distributed denial of service* (DDoS). Metode ini merupakan metode pembajakan yang tidak terlalu

canggih. Dengan metode DDoS, jaringan komputer akan dibanjiri dengan lalu lintas data yang sangat tinggi secara mendadak dan terus menerus sehingga sistem akan dengan mudah dikelabui.

Jenderal William Shelton, seorang pejabat senior di Angkatan Udara Amerika Serikat juga menyatakan bahwa Angkatan Udara Amerika Serikat sedang berada dalam proses penguatan. Sekitar 1000 sumber daya manusia ditambah untuk memperkuat sistem defensif sibernya. Akan tetapi, meskipun mengingat situasi kondisi finansial di Washington, para pimpinan tertinggi Angkatan Udara Amerika Serikat berharap mereka bisa mendapat anggaran dana yang lebih banyak lagi agar benar-benar bisa menghadang semua serangan siber di masa mendatang.

Untuk kapabilitas dependensinya, Amerika Serikat memiliki tingkat dependensi yang tinggi terhadap teknologi siber. Amerika Serikat bergantung penuh pada teknologi siber untuk dapat menjalankan semua manufakturnya. Sehingga, jika terjadi serangan siber yang tidak dapat ditanggulangi, maka Amerika Serikat akan mendapat dampak dalam jumlah besar yang tidak hanya menargetkan pada informasi negara akan tetapi juga aktifitas di negara tersebut akan lumpuh. Kelumpuhan tersebut tentu akan berdampak ke semua sektor, termasuk juga ekonomi. Sebuah bendungan di Rye Brook, New York yaitu Bowman Avenue Dam juga ikut dibajak bersamaan dengan pembajakan 46 institusi dan perusahaan yang bergerak di sektor finansial. Akan tetapi, pada saat itu, sistem pembuka pintu bendungan sedang tidak tersambung dengan sistem jaringan siber untuk sementara, dikarenakan sedang ada aktifitas perawatan infrastruktur rutin disana.

2. Determinan Kapabilitas Keamanan Infrastruktur Digital Iran

Iran memiliki kapabilitas yang seimbang, baik secara ofensif maupun defensif. Meskipun seimbang, tingkat kapabilitasnya masih tergolong rendah dan rentan. Akan tetapi, pasca revolusi Iran terjadi, pemerintahnya gencar meningkatkan kekuatan siber.

Pemerintah Iran giat mengembangkan dan menguatkan kekuatan siber mereka. Akan tetapi, perkembangan teknologi siber yang dilakukan lebih condong kepada kekuatan defensif ketimbang kekuatan ofensif. Berdasarkan fakta, Iran berhasil beberapa kali menahan serangan-serangan maupun aksi spionase yang dilakukan oleh Amerika Serikat terhadapnya.

Sedangkan untuk kapabilitas dependensinya terhadap teknologi siber adalah baik. Iran masih mandiri dan tidak mengandalkan teknologi siber sepenuhnya untuk menjalankan dan mengontrol semua aktifitas manufakturnya. Hal ini membuat resiko yang diterima oleh Iran jika tidak berhasil membendung serangan siber yang diluncurkan kepadanya semakin diminimalisir. Dampak dari serangan tersebut tidak akan berpengaruh secara signifikan terhadap beberapa sektor kritikal di negaranya.

B. Faktor-Faktor Pengambilan Kebijakan Dalam Dilema Keamanan Siber

Dalam merumuskan kebijakan yang harus diambil ketika berada dalam situasi dilema keaman siber, ada beberapa faktor yang harus diperhatikan oleh si pembuat kebijakan. ((N.M, 2012)

Pertama, si pengambil kebijakan harus memerhatikan kemampuan sumber daya teknologi informasi yang ia miliki apakah mendukung atau tidak mendukung dalam pelaksanaannya. Jika sumber daya tidak mendukung, maka

keamanan siber akan terancam dari serangan-serangan yang ditujukan kepadanya. *Kedua*, tingkat kesiapan doktrin siber juga harus diperhatikan. Doktrin siber merupakan aspek fundamental dalam menyusun rencana dan strategi. Dalam menjaga keamanan siber, doktrin siber haruslah dalam keadaan siap dan disesuaikan dengan kemampuan sumber daya yang dimiliki oleh pihak pembuat kebijakan. *Ketiga*, selain doktrin awal, si pengambil kebijakan harus menyediakan strategi dan aturan pendukung lainnya. Hal ini bermanfaat dalam menjamin implementasi keamanan siber dari serangan pihak lawan agar tetap berjalan. *Keempat*, dalam menentukan dan merumuskan kebijakan, si pembuat kebijakan harus menelaah segala aspek yang memengaruhi kebijakan. Aspek tersebut dapat berasal dari internal maupun eksternal.