BAB I
PENDAHULUAN

A. Latar Belakang Masalah

Amerika Serikat adalah negara adidaya yang memiliki kekuatan politik, ekonomi, dan militer yang baik. Selain itu, Amerika Serikat sangat mengkhawatirkan kekuatan pertahanan dan esksitensinya di kancah internasional. Pemerintah Amerika Serikat percaya bahwa melalui *power*, negaranya dapat mengontrol dunia. Dengan demikian, keamanan nasional dapat sangat terjamin. Keamanan nasional merupakan sebuah sistem yang akan menciptakan rasa aman, dalam konteks ini ialah rasa aman yang disediakan oleh negara bagi warga negaranya. Hal ini merupakan kunci penting dalam semua aspek yang mempengaruhi keberlangsungan suatu negara. Oleh karena itu, Amerika Serikat gencar mengembangkan kekuatan pertahanannya hingga bahkan menghabiskan begitu banyak anggaran negara hanya untuk memiliki senjata yang terbaru dan terkuat. Pada tahun 2017, diperkirakan bahwa Amerika Serikat menghabiskan anggaran negara sebanyak US$ 587.8 milyar untuk dialokasikan ke sektor militer. (Global Fire Power, 2017)

Pada era saat ini, perang antar negara tidak lagi berupa perang konvensional. Dimana melalui perang konvensional, perang melibatkan penggunaan persenjataan dan komponen ide untuk berperang yang mencakup pemikiran doktrinal, struktur organisasi, regulasi penyerangan. (Azizah, 2013) Era modern ini, perang siber sangat diminati dan bahkan setiap negara menganggap bahwa mereka masing-masing harus memiliki teknologi yang mendukung perang siber. Hal ini dikarenakan melalui perang siber, kerugian dan kehancuran fisik tidak akan terlalu tampak. Perang konvensional juga

memicu reaksi protes dunia internasional karena akan memakan korban jiwa dalam jumlah banyak. Akan tetapi, bukan tidak mungkin, perang siber akan jauh lebih berbahaya dan memakan kerugian dalam jumlah yang lebih besar dibanding perang konvensional. Perang siber akan lebih memudahkan penggunanya untuk mengacaukan manufaktur-manufaktur negara lawan. Melalui siber, musuh dapat meledakkan rudal atau pipa gas, mengacaukan sistem nuklir, bahkan melumpuhkan aktifitas ekonomi suatu negara.

Amerika Serikat pun tak luput ikut mengembangkan teknologi siber ini dengan tempo cepat. Dalam waktu singkat, mereka telah memperoleh sistem teknologi canggih yang digunakan untuk mencapai kepentingan nasionalnya. Yang melatar belakangi percepatan perkembangan teknologi sibernya adalah Amerika Serikat rentan terhadap serangan siber. Dalam kurung 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 kritikal, seperti sumber daya listrik, gas, komunikasi, dan lainnya. (Alhabsyi, 2016)

Sejak pasca revolusi Iran terjadi, hubungan antara Amerika Serikat dan Iran kian memburuk. Kedua negara masing-masing memiliki peran dan posisi yang kuat. Akibatnya, hubungan buruk tersebut membawa dampak yang signifikan baik secara bilateral maupun internasional. Situasi tersebut juga mendorong Amerika Serikat untuk aktif membuat kebijakan-kebijakan yang sifatnya anti Iran. Iran yang notabene merupakan negara terkuat di Timur Tengah, merasa terancam dengan semua kebijakan tersebut. Ditambah lagi, Iran yang juga aktif memperkuat posisinya dengan mengembangkan nuklir buatannya sendiri merasa bahwa nuklirnya akan terancam gagal berkembang. Oleh karena itulah, ada berbagai fenomena perang siber tercipta. Baik dari Amerika Serikat maupun Iran sama-sama melancarkan

serangan siber dan menunjukkan kekuatan antara satu sama lain.

Dengan situasi dan kondisi tersebut, Amerika Serikat pun menyusun rangkaian strategi yang terencana dalam aktifitas perang sibernya dengan Iran. Strategi Amerika Serikat diwujudkan dalam berbagai bentuk serangan dan dalam berbagai bentuk sarana pula. Namun, berbagai serangan yang sifatnya internal maupun eksternal tidak membuat goyah pemerintah Iran untuk terus bertahan dan mengumpulkan kekuatan.

B. Rumusan Masalah

Berdasarkan latar belakang masalah diatas, maka saya akan membahas mengenai rumusan masalah tentang "Bagaimana strategi Amerika Serikat dalam perang siber dengan Iran pada tahun 2010-2016?"

C. Kerangka Pemikiran

1. Teori Dilema Keamanan Siber (*Cybersecurity Dilemma*)

Setiap negara pada zaman globalisasi ini pasti memiliki teknologi sibernya sendiri. Dengan adanya teknologi ini, setiap negara memiliki kekuatan perlindungan dari ancaman-ancaman eksternal yang dapat menginterupsi keamanan nasionalnya. Teknologi ini juga tak luput memunculkan persoalan baru yang pasti dihadapi oleh semua negara di dunia. Persoalan tersebut ialah dilema keamanan siber (*cybersecurity dilemma*).

Dilema keamanan siber adalah sebuah kondisi dimana tiap negara memiliki pilihan untuk memutuskan kebijakannya sendiri dalam rangka untuk merespon masalah keamanan sibernya dengan satu atau lebih negara lain. Dilema ini muncul akibat adanya upaya negara untuk meningkatkan

keamanan dari infrastruktur digital. Menimbang dari propertinya yang berupa digital, tipe dilema keamanan siber ini akan lebih sulit dihadapi daripada tipe dilema keamanan (*security dilemma*). Berbeda dengan dilema keamanan, suatu negara akan kebingungan dalam mengidentifikasi tujuan musuh dalam teknologi sibernya. Apabila negara salah mengidentifikasi tujuannya, permasalahan yang akan timbul akan menjadi pelik dan rumit dan berpotensi menyebabkan terjadinya perang antar negara tersebut. Akan tetapi, tiap negara dapat menghadapi kesulitan tersebut dengan membentuk sebuah kerjasama bilateral maupun multilateral dengan tujuan mengumpulkan kekuatan dari masing-masing negara.

Kekuatan yang dimiliki oleh semua negara di dunia pun tidaklah sama kuatnya. Negara lemah dapat saling bekerjasama dengan mengeluarkan biaya yang relatif tergolong lebih rendah. Misalnya pada saat berhadapan dengan negara yang memiliki industri pertahanan maju seperti Amerika Serikat, maka potensi kegagalan saat serangan siber dilancarkan akan tinggi. Oleh karena itu, jika negara lemah ingin menjalin kerjasama siber, negara tersebut harus memiliki infrastruktur digital atau ekonomi yang piawai dan sama dengan negara yang lebih kuat. Karena jika tidak, hubungan kerjasama siber yang diharapkan akan terjadi secara timbal balik tidak akan lagi efektif. Demikian juga, dengan adanya mode perang siber ini, frekuensi terjadinya konflik secara keseluruhan akan meningkat. Hal ini dikarenakan perang siber cenderung mengacaukan secara paksa sektor-sektor ekonomi maupun komunikasi saja. Hal ini berbeda dengan perang konvensional yang lebih cenderung untuk menjatuhkan korban jiwa. Perang siber berarti adalah suatu sarana untuk meningkatkan keamanan nasional dan potensi untuk mengintimidasi negara lain tanpa menanggung resiko yang sama seperti perang konvensional. Banyak negara yang ragu untuk mencapai kepentingan politiknya lewat cara-cara

konvensional, sehingga perang siber ini adalah suatu cara alternatif yang sangat atraktif bagi negara-negara untuk menciptakan konflik demi kepentingannya masing-masing.

Keamanan infrastruktur digital suatu negara dapat terjaga melalui dua bentuk kapabilitas, yakni ofensif dan defensif. Menurut Nicholas C. Rueter, terdapat dua determinan yang perlu diperhatikan dalam dilema keamanan siber ini, yakni (Rueter, 2011):

a. *The Offense-Defense Balance*

Setiap negara yang ingin menjalin bentuk kerjasama siber dengan negara lain harus memperhatikan apakah aktifitas ofensif dan defensif memiliki keuntungan dalam perang siber yang mereka jalankan. Tidak seperti perang kinetik (*kinetic warfare*) yang sifatnya masih konvensional sehingga membutuhkan area sebagai medan perang, ketiadaan medan dalam perang siber akan meningkatkan kemunculan serangan-serangan tak terduga yang menargetkan sistem jaringan yang lemah.

Hal ini menimbulkan dilema bagi sebuah negara dalam memilih untuk lebih mengembangkan sistem ofensif atau defensif. Selain itu, sistem kapabilitas defensif dinilai lebih tidak efektif. Sebuah penelitian oleh *National Research Council*, menyatakan bahwa "*cyber-attack is easier, faster, and cheaper than cyber-defense*," karena "*effective defense must be successful against all attacks, whereas an attacker need succeed only once*". (National Research Council, 1999) Berdasarkan penelitian tersebut, suatu negara lebih disarankan untuk fokus mengembangkan kekuatan defensif ketimbang ofensif. Dengan kekuatan defensif, keamanan infrastruktur digital suatu negara akan lebih aman sehingga secara otomatis keamanan nasional juga akan terjaga pula.

b. *Offense-Defense Differentiation*

Menurut Nicholas C. Rueter, kemungkinan kerjasama antar negara dalam perang siber akan terjadi jika negara dapat membedakan kebijakan, program, maupun senjata siber dari

kapabilitas ofensif atau defensifnya. Dengan kemampuan pembedaan dalam mengidentifikasi kebijakan, program maupun senjata tersebut, suatu negara akan lebih matang dalam menentukan respon yang tepat. Ketepatan respon yang diambil akan menghindarkan negara tersebut dari resiko konflik yang akan berujung kepada aktifitas perang siber. Selain itu, aktifitas ofensif dan defensif sama-sama dijalankan melalui sarana dan *platform* yang sifatnya tidak mengancam. Inilah yang menjadi tantangan bagi negara-negara untuk menghadapi masalah akan adanya kesulitan dalam mengontrol kekuatan siber.

Jika negara ingin mengetahui sebuah senjata siber bersifat ofensif atau defensif, maka negara tersebut harus terlebih dulu mengidentifikasi senjata dari sumbernya. Sebagai contoh, dalam kasus nuklir. Negara akan kesulitan menentukan kapabilitasnya, apakah nuklir yang dikembangkan oleh pihak oposisi bertujuan sebagai sumber energi atau sebagai sebuah senjata. Apabila diidentifikasi sebagai sebuah senjata, maka selanjutnya negara akan menghadapi kesulitan dalam mengidentifikasi apakah nuklir tersebut memiliki kapabilitas ofensif ataupun defensif. Pasalnya, kedua kapabilitas tersebut sama-sama dijalankan melalui sarana dengan mekanisme yang sama. Oleh karenanya, batas antara keduanya sangat tidak jelas. (Bain, 2010) Sehingga sebuah senjata destruktif hanya akan dapat diketahui kapabilitasnya setelah senjata tersebut digunakan.

Selain kapabilitas ofensif dan defensif, ada satu kapabilitas lainnya yang harus dijadikan sebagai determinan juga. Richard A. Clarke dan Robert K. Knake, dalam bukunya yang berjudul "*Cyber War: The Next Threat to National Security and What To Do About It*", menyebutkan bahwa determinan atau parameter kapabilitas terdiri atas tiga, yaitu kapabilitas ofensif, defensif, dan dependensi. Kapabilitas dependensi adalah kemampuan sebuah negara untuk tidak bergantung secara penuh dengan teknologi siber. Hal

dimaksud disini ialah kemandirian manufaktur dan sektor energi.

2. Konsep Perang Siber (*Cyber Warfare*)

Perang (*war*) telah menjadi bagian yang tidak terpisahkan dari sejarah peradaban manusia. Pengalaman perang yang dirasakan oleh ras manusia telah membawa banyak pemahaman yang digunakan untuk menurunkan persentase kemungkinan terjadinya perang. Banyak institusi internasional, perjanjian internasional sampai sistem peradilan kriminal perang dibentuk hanya untuk mendukung terciptanya perdamaian dunia. Akan tetapi, adanya arus globalisasi yang deras sehingga keharusan untuk melek akan IPTEK tidak terelakkan. Dengan ini, terciptalah suatu perang non-konvensional yang digunakan negara-negara untuk mengganti sistem perang konvensional yang sebelumnya dilarang oleh dunia internasional. Perang non-konvensional ini membutuhkan biaya dalam jumlah besar.

Perang digital atau teknologi informasi inilah yang disebut sebagai perang siber. Sampai saat ini, para ahli dan akademisi belum membuat kesepakatan tentang definisi perang siber itu sendiri. Pada umumnya, perang siber merupakan salah satu bentuk ancaman yang ditimbulkan oleh karena adanya digitalisasi atau dunia maya. Dunia maya adalah objek yang tidak memiliki batas, posisi, dan arah. Berbeda dengan daratan, lautan, ruang, spectrum elektromagnetik, dunia maya bukanlah bagian dari alam dan tidak akan eksis tanpa adanya teknologi informasi yang dikembangkan sejak beberapa dekade yang lalu.

Lior Tabansky mengungkap ada beberapa tindakan penggunaan dunia maya yang dapat diklasifikasikan sebagai sebuah perang siber, yakni (Tabansky, 2011):

a. Serangan yang ditargetkan kepada rakyat sipil dan menimbulkan kerusakan secara fisik.

b. Kekacauan yang disebabkan oleh serangan terhadap informasi infrastruktur penting milik nasional dan menimbulkan kerusakan secara fisik.
c. Kekacauan yang disebabkan oleh serangan yang menargetkan basis militer didalam wilayah kedaulatan negara lain.
d. Kekacauan yang disebabkan oleh serangan yang menargetkan basis militer diluar wilayah kedaulatan negara lain.
e. Penempatan alat serang yang tidak aktif dan yang akan aktif, misalnya *Trojan horse* atau bom yang sewaktu-waktu akan aktif menyerang.
f. Aktifitas kriminal, proyek pengintaian.
g. Penggunaan senjata dual use: perkumpulan intelijen, penyelidikan terhadap kelemahan akan keamanan, percobaan invansi.
h. Pelaksanaan sebuah media kampanye propaganda, penyalahgunaan dan perusakan situs (aset informasi) resmi.

Selain itu Lior Tabansky juga menambahkan bahwa ada kesulitan dalam menentukan perang siber karena hal ini tidaklah sama seperti konsep serangan, pertahananan, maupun kekerasan dalam dunia maya. Dalam proses penentuan suatu tindakan tergolong kedalam perang siber, maka ada beberapa substansi yang harus dilihat:

a. Sumber yang berhubungan dengan organisasi dan geografis: apakah tindakan tersebut dipelopori oleh sebuah negara atau tidak.
b. Hasil: dapatkah serangan tersebut menimbulkan kerusakan, dan apakah secara nyata dapat menimbulkan kerusakan dan korban?
c. Tingkat kompleksitas: apakah serangan tersebut memerlukan perencanaan yang kompleks dan terkoordinasi?

Konsep perang siber diatas memiliki banyak relevansi dengan kasus perang siber yang terjadi antara Amerika Serikat dan Iran. Ditinjau dari substansi yang dikemukakan oleh Lior Tabansky, tindakan Amerika Serikat tergolong ke dalam perang siber. Serangan tersebut mutlak dipelopori oleh sebuah negara, yaitu Amerika Serikat. Kerusakan yang disebabkan oleh serangan tersebut juga menimbulkan kerusakan yang nyata dan menjatuhkan korban jiwa. Selain itu, tingkat kompleksitas serangan ini tinggi dilihat dari perencanaan yang kompleks yang dilakukan oleh Amerika Serikat melalui CIA.

Ditinjau dari klasifikasi perang siber oleh Lior Tabanksy, perang siber ini juga memiliki relevansi dengan konsep diatas sebagai berikut. *Pertama*, serangan yang berupa sabotase terhadap sistem nuklir Iran ini ditujukan kepada rakyat sipil, dalam kasus ini yakni para ilmuwan dan pekerja yang bekerja di fasilitas nuklir Iran. *Kedua*, kekacauan yang ditimbulkan menyerang infrastruktur yang diklaim oleh Iran adalah penting yaitu sistem nuklirnya. Adalah penting karena Iran menggunakan nuklir sebagai energi alternatif pengganti bahan bakar fosil. *Ketiga*, tindakan Amerika Serikat adalah aktifitas kriminal karena terlebih dulu melakukan aksi spionase atau pengintaian terhadap fasilitas nuklir Iran.

Keempat, Amerika Serikat juga melakukan penyelidikan terhadap kelemahan keamanan fasilitas nuklir Iran dengan menempatkan mata-mata dan memanfaatkan kelemahan tersebut sebagai akses untuk menyabotase sistem. *Kelima*, serangan tersebut dilakukan dengan menempatkan alat serang siber yang sewaktu-waktu akan aktif yakni melalui *Stuxnet worm* ke dalam sistem. *Keenam*, selain melalui *Stuxnet worm*, Amerika Serikat juga banyak melakukan propaganda melalui media massa dan institusi internasional dengan menekankan kepada masyarakat internasional bahwa fasilitas nuklir yang dimiliki Iran adalah berbahaya.

D. Hipotesa

Amerika Serikat memanfaatkan strategi dalam perang siber dengan Iran pada tahun 2010 sampai 2016 dengan cara:

1. Pelaksanaan propaganda melalui media dan institusi internasional dengan tujuan untuk menyebarkan stigma-stigma negatif tentang Iran.
2. Pelaksanaan aksi spionase dan sabotase terhadap sektor politik dan fasilitas nuklir Iran secara terencana.
3. Penempatan senjata siber ke dalam sistem nuklir milik Iran dengan tujuan agar menghambat perkembangan nuklir Iran.

E. Jangkauan Penelitian

Dengan maksud agar penelitian menjadi lebih fokus, maka penulis menetapkan jangkauan penelitian adalah pada tahun 2010 hingga 2016. Alasan pemilihan jangkauan penelitian tersebut adalah sebagai berikut. Pada tahun 2010, Amerika Serikat mulai aktif melakukan strategi perang siber dengan Iran. Kemudian, tercatat strategi Amerika Serikat baru terlaksana sampai pada tahun 2016. Meskipun baru terlaksana hingga tahun 2016, strategi perang siber oleh Amerika Serikat tetap berlanjut. Penulis bermasud agar tetap menjaga data penelitian berdasarkan kejadian atau fenomena yang sudah terjadi dan validitasnya terbukti. Akan tetapi, penelitian ini terbuka untuk data di luar jangkauan waktu yang telah ditetapkan selama masih memiliki relevansi dan tetap mendukung penelitian.

F. Tujuan Penelitian

Adapun tujuan penulisan skripsi ini yaitu:

1. Untuk mengetahui dinamika hubungan antara Amerika Serikat dan Iran.

2. Untuk mengetahui dilema keamanan siber yang tengah terjadi antara Amerika Serikat dan Iran.
3. Untuk mengetahui strategi Amerika Serikat dalam perang siber dengan Iran.

G. Metode Penelitian

1. Metode Pengumpulan Data

Skripsi ini menggunakan metode pengumpulan data yang sifatnya sekunder. Hal ini berarti skripsi ini menggunakan sumber yang bersifat kepustakaan (*library research*) yang berbentuk data tertulis dan data digital. Sumber data tertulis berasal dari literatur, jurnal dan surat kabar. Sedangkan sumber data digital berasal dari jurnal online, berita dan artikel yang valid serta dapat dipertanggungjawabkan.

2. Metode Analisis Data

Skripsi ini menggunakan metode analisis data yang sifatnya kualitatif, dimana data diambil dalam berbentuk eksplanasi. Dengan teknik kualitatif, analisis data akan akurat dengan membuat relasi dan mengembangkan data sesuai dengan teori yang relevan.

H. Sistematika Penulisan

Skripsi ini terdiri dari 5 bab. Adapun sistematika penulisan dapat dirumuskan sebagai berikut:

BAB I memaparkan tentang struktur konstruksi skripsi secara keseluruhan yaitu; latar belakang masalah, rumusan masalah, kerangka pemikiran, hipotesa, tujuan penelitian, metode penelitian dan sistematika penulisan.

BAB II memaparkan tentang dinamika hubungan antara Amerika Serikat dan Iran. Hubungan yang dimaksud adalah

hubungan dalam politik dan keamanan hingga kebijakan-kebijakan yang dibuat oleh masing-masing negara untuk merespon isu-isu internasional.

BAB III memaparkan tentang dilema keamanan siber yang terjadi antara Amerika Serikat dan Iran. Pada bab ini, akan dijelaskan tentang faktor-faktor yang perlu diperhatikan oleh kedua negara dalam proses pengambilan kebijakan masing-masing untuk merespon situasi perang siber yang tengah terjadi.

BAB IV memaparkan tentang strategi yang digunakan oleh Amerika Serikat dalam perang siber dengan Iran. Pada bab ini, akan dijelaskan tahapan strategi yang direncanakan oleh Amerika Serikat mulai dari bidang *high politic*, ekonomi, militer, hingga senjata siber melalui berbagai macam sarana pula.

BAB V memaparkan tentang kesimpulan dari pembahasan pada bab-bab sebelumnya dan penanda sebagai akhir penulisan skripsi ini.