OPERASI SIBER OFENSIF IRAN TERHADAP AMERIKA SERIKAT, ISRAEL DAN ARAB SAUDI: KEPENTINGAN DAN STRATEGI SIBER OFENSIF IRAN

Rahmadi Pratama Aritonang Departemen Hubungan
Internasional Fakultas Ilmu Sosial dan Ilmu Politik, Universitas
Airlangga E-mail: rahmadiaritonang@gmail.com

Penelitian ini bertujuan untuk memahami kepentingan dan strategi siber ofensif yang diaplikasikan oleh Iran, terhadap ketiga negara yang telah menjadi musuh utamanya selama ini, yakni Amerika Serikat, Israel, dan Arab Saudi. Hal ini peneliti lakukan karena peretas Iran berusaha melakukan hal yang berbeda dari kebanyakan pola operasi siber ofensif negara lain, yakni dengan sengaja mempertunjukkan bahwa negaranya adalah pelaku sekalian ancaman siber di era ini dengan melakukan serangkaian operasi siber ofensif dari tahun 2010 sampai dengan 2018. Hasil penelitian menunjukkan bahwa berdasarkan tingkatan analisis identitas nasional dari segi sejarah politik luar negeri dan militer negara tersebut, kepentingan Iran adalah untuk melemahkan kemauan musuh dalam melakukan perang konvensional dengan menganggu, menghancurkan, meletihkan, atau memaksa. Adapun hal ini juga dapat dilihat dengan tingkatan analisis individu Iran, yakni Ali Khamenei dan pendekatan analisis sifat kepemimpinan, yang mana bertujuan untuk menganalisa kemampuan Khamenei dalam kehidupan politik negaranya, terutama dalam menangani isu-isu politik luar negeri. Lebih lanjut, penelitian ini juga menunjukkan bahwa tujuan dari serangkaian operasi siber ofensif Iran dapat diakomodasi dengan strategi siber asimetris yang digunakan Korea Utara dan strategi pencegahan aktif.

Kata-kata kunci: Iran, Operasi Siber Ofensif, Kepentingan Iran, Strategi Siber Asimetris, Strategi Pencegahan Aktif

Pendahuluan

Penggunaan teknologi yang menghendaki interkonektivitas melahirkan dunia maya yang perannya vital bagi kehidupan manusia saat ini. Dewasa ini eksistensi dunia maya membuat manusia dapat berkomunikasi satu sama lain dengan jauh lebih mudah, dunia maya juga membantu manusia untuk mengakses berbagai jenis informasi, menikmati media hiburan baru seperti game online, dan bahkan membantu perkerjaan manusia dari ruang privat sampai publik, seperti pengoperasian infrastruktur negara. Seiringan dengan hal tersebut, kehadiran dunia maya secara tidak lansung membuat struktur perang dan pertahanan yang hanya bergantung pada elemen-elemen fisik saja

seperti, tentara, pesawat, nuklir, dan lain sebagainya kurang relavan. Dalam hal ini dunia maya menjadi tempat baru bagi aktor internasional untuk berkonflik, karena peran dunia maya yang telah melewati kedaulatan dan keamanan negara yang berdasarkan empat matra yakni darat, laut, udara, dan luar angkasa (Rid & McBurney, 2012).

Lebih lanjut, pada tahun 2016 perusahaan keamanan komputer industri terkenal, yakni MalCrawler melakukan sebuah percobaan terkait pemanfaatan dunia maya dalam konflik. Perusahaan ini menciptakan sebuah sistem atau perangkat di dunia maya yang memiliki fungsi untuk menjebak berbagai macam operasi siber ofensif. Berdasarkan penelitiannya, perusahaan ini menyimpulkan bahwa operasi siber ofensif dari tiap negara memiliki pola berbeda. Namun pada umumnya memiliki satu kesamaan, yakni berusaha menyembunyikan kalau mereka adalah pelaku penyerangan siber. Akan tetapi yang paling unik adalah operasi siber ofensif dari para peretas Iran yang bertujuan untuk menunjukkan kalau Iran adalah pelaku sekalian ancaman siber ofensif dengan menimbulkan kerusakan sebanyak mungkin kepada negara-negara lain, terutama kepada tiga negara yang menjadi musuh utamanya, yakni Amerika Serikat, Israel, dan Arab Saudi (Rattray, 2018: 3-8). Hasil penelitian MalCrawler ini dapat dilihat data serangan dunia maya Iran selama satu dekade terakhir. Berdasarkan tabel dibawah ini, Iran terbukti melakukan atau mendukung berbagai macam operasi siber ofensif yang berasal dari negaranya ke berbagai pertahanan jaringan dunia maya musuh-musuhnya (Anderson dan Karim, 2018).

Tabel 1: Operasi Siber Ofensif Iran Terhadap AS, Israel, dan Arab Saudi

No	Keterangan	Kode Serangan	Pelaku	Bentuk Serangan	Target	Tujuan
1	Pertama Kali digunakan pada 2011 dan berlanjut hingga pertengahan 2013.	Ababil	Izz ad-Din al-Qassam Cyber Fighters	DDoS	Amerika Serikat	Merusak sektor keuangan Amerika Serikat
2	Mulai digunakan sejak 2010 dan diperkirakan akan selalu digunakan oleh Iran. Mahdi telah digunakan sejak Desember 2011	Mayoritas Tidak Memiliki Nama Mahdi	Tidak Diketahui	Spearphishing	Amerika Serikat Israel Arab Saudi	Mengambil dan Mensabotase Informasi
3	Gelombang Serangan Pertama terjadi pada 15 Agustus 2012 Gelombang kedua terjadi pada November 2016 hingga Januari 2017.	Shamoon	Cutting Sword of Justice	DDoS	Arab Saudi	Merusak sistem keuangan Saudi Aramco dan Perusahaan RasGas Qatar. Menghancurkan database dan file milik pemerintah dan sektor swasta.
4	Setidaknya 54 upaya operasi siber ofensif dalam bentuk ini Ditemukan Pada musim panas 2014	Protective Edge		DDoS	Israel	Menyerang infrastruktur Pasukan Pertahanan Israel

Sumber: ***Collin Anderson and Karim Sadjadpour***

Lebih jauh, serangan-serangan siber Iran inilah yang merupakan alasan utama mengapa peneliti tertarik meneliti permasalahan ini. Dari berbagai serangan kepada ketiga negara tersebut dapat

dilihat bahwa Iran melakukan operasi siber ofensif yang fokusnya adalah untuk menimbulkan kerusakan sebanyak mungkin kepada negara lain. Dengan kata lain, berbeda dengan negara lain yang menutupi operasi siber ofensifnya ke berbagai negara, Iran dengan sengaja mempertunjukkan bahwa negaranya adalah pelaku sekalian ancaman siber di era ini (Anderson dan Karim, 2018). Adapun karena itu, penelitian ini memfokuskan pada pertayaan penelitian mengenai apa kepentingan dan strategi siber ofensif Iran dalam melakukan serangkaian operasi siber ofensif yang mempertunjukan bahwa Iran adalah pelaku penyerangan siber terhadap Amerika Serikat, Israel, dan Arab Saudi.

Kepentingan Nasional Atau Tujuan Dari Operasi Siber Ofensif Iran Berdasarkan Identitas Nasional

Sebagai sebuah negara, kepentingan nasional dalam ilmu hubungan internasional selalu digunakan sebagai idikator untuk menjelaskan prilaku atau kebijakan luar negeri sebuah negara. Seringkali kepentingan nasional ini juga dapat menjadi sebuah rujukan para akademisi untuk menganalisis strategi negara dalam melakukan perang. Hal ini karena kepentingan nasional sendiri memiliki fungsi penting yaitu sebagai tuntunan negara atau pembuat kebijakan untuk melakukan kebijakan luar negeri atau strategi negara yang berorientasi untuk mendapatkan kepentingan nasionalnya. Serangan-serangan siber Iran dalam kurun waktu tersebut terhadap Amerika Serikat, Israel, dan Arab Saudi pada dasarnya juga begitu. Operasi siber ofensif Iran selama kurang lebih delapan tahun itu pasti dilakukan atas dasar tujuan atau kepentingan nasional tertentu yang ingin dicapai Iran (Clunan, 2009: 3).

Pada dasarnya kepentingan Iran tersebut dapat dilihat dari tingkatan analisis identitas nasional. Berdasarkan jejak historis, peneliti menyimpulkan bahwa identitas nasional Iran adalah sebagai

negara kuat dan merupakan pihak yang benar dalam konfliknya, yang mana identitas ini telah diangkat oleh aktor-aktor yang memegang kekuasaan di Iran sejak pemerintahan *supreme leader* pertama Iran, yakni Ayatollah Ruhollah Khomeini. Adapun identitas nasional Iran itu kemudian dapat dilihat dari pernyataan-pernyataan yang disampaikan oleh para elit politik negara yang membuat keputusan. Sebagai contoh hal ini dapat dilihat dari argumen *supreme leade*r Iran pertama. Hal ini dikutip dari artikel yang dipublikasikan oleh *The New York Times* pada 7 Oktober 1979. Dalam menjawab salah satu pertayaan wawancaranya, pemimpin tertinggi Iran pertama ini mengatakan:

> Ayatollah Ruhollah Khomeini: "We are afraid of your ideas and of your customs. Which means that we fear you politically and socially and we want this to be our country. We do not want you to interfere anymore in our politics and our economy, in our habits, our affairs. And from now on, we will go against anyone who tries to interfere — from the right or from the left, from here or from there. And now that's enough."

Dari perkataan Khomeini tersebut dapat disimpulkan bahwa melalui pemimpin tertinggi pertamanya yang berperan sebagai agen atau aktor tertentu yang memegang kekuasaan Iran sudah dari awal menggunakan sejarah historis, budaya, dan karakteristik negaranya menjadi identitas nasional. Lalu Khomeini yang berperan sebagai agen pemegang kekuasaan pertama di Iran mengklaim secara sepihak bahwa masyarakat Iran secara keseluruhan menyakini ide-ide barat sebagai sesuatu yang menakutkan dalam segala bidang, termasuk, sosial, ekonomi dan politik. Oleh karena itu, Khomeini mengatakan bahwa seluruh masyarakat Iran akan melawan pihak manapun yang mencoba menggangu nilai-nilai identitas nasional Iran. Hal tersebut dapat menjadi pendukung argumen peneliti bahwa konflik negara ini dengan AS, Israel, dan Arab Saudi terjadi tidak terlepas karena Khomeini yang merupakan agen pemegang kekuasaan memposisikan Iran dari awal sebagai korban karena negara lain berusaha untuk merusak negaranya dengan

menggunakan ide-ide budaya mereka dan karena itu perang yang terjadi sekarang sebagai bagian dari pembelaan Iran untuk melindungi dirinya (Nytimes, 1996).

Adapun jika dilihat dari sisi sejarah politik luar negeri dan militer Iran, identitas nasional sebagai negara yang kuat, pemimpin yang dominan, kemampuan militer yang kuat, dan sebagai pemain penting dalam struktur dunia juga dapat dilihat dari aktor-aktor tertentu dalam negara Iran yang mengangkat identitas tersebut. Beberapa diantaranya adalah argumen dari Presiden Iran saat ini, yakni Hassan Rouhani dan Mayor Jenderal Qassem Soleimani.

> Hassan Rouhani: "America should know that peace with Iran is the mother of all peace, and war with Iran is the mother of all wars."
> Qassem Soleimani: "If you begin the war, we will end the war. You know that this war will destroy all your capabilities."

Dari argumen Rouhani dan Soleimani tersebut dapat dilihat bahwa secara tidak lansung Iran berusaha menunjukkan bahwa Iran adalah negara kuat, yang mana jika perang konvensional dengan AS terjadi, maka menurut Iran yang akan memenangkan perang tersebut. Sebaliknya AS akan menderita kerugian yang sangat besar. Adapun dari sini dapat dilihat bahwa ada interaksi antara struktur sosial dan peranan manusia sebagai agen. Dengan kata lain melalui aktor-aktor yang memegang kekuasaan, yakni Presiden dan Mayor Jenderal, pemerintah Iran berusaha mengangkat identitas nasional dari sisi sejarah politik luar negeri dan militer bahwa Iran adalah negara yang kuat. Dalam hal ini, negara pada tingkatan *super power* sendiri akan hancur jika berhadapan dengan Iran (BBC, 2018).

Lebih jauh lagi, identitas nasional Iran inilah yang membuat Iran melakukan serangan siber kepada ketiga negara yang menjadi musuhnya. Hal ini terjadi, ketika Iran pada akhirnya tidak atau masih belum dapat mengakomodasi kepentingan nasional untuk menjadi negara yang kuat, pemimpin yang dominan, kemampuan militer yang kuat, dan sebagai pemain penting dalam struktur dunia,

meski telah mendapat persetujuan dari publiknya untuk melakukan konflik. Berdasarkan hal ini, Iran telah mengalami koflik puluhan tahun dengan ketiga negara tersebut. Lalu hasilnya, meski Iran dewasa ini masih sangat berambisi untuk menjadi negara hegemoni kawasan Timur Tengah dan mengembalikan kejayaan masa lampau, perlu diketahui kalau sepanjang sejarah konfliknya dengan ketiga negara tersebut, Iran telah mengalami berbagai situasi yang bahkan mengancam eksistensinya. Sebagai contoh, Iran pada 2018 kemarin dikenai sangsi ekonomi oleh Amerika Serikat dan Israel. Dampaknya pada bulan Januari kemarin, demonstrasi di banyak kota di seluruh pelosok negara Iran terjadi. Ribuan orang dikabarkan tertangkap dan sedikitnya 20 orang meninggal. Demonstrasi ini terjadi sehubungan dengan naiknya harga pangan, standar kehidupan memburuk, dan jumlah pengangguran meningkat. Para demonstran meminta Ali Khamenei, yakni *supreme leader* Iran saat ini untuk mundur dari jabatannya (BBC, 2018).

Di sisi lain, memaksa untuk melanjutkan politik luar negeri dan kebijakan militer yang agresif, seperti melakukan perang konvensional juga bukanlah pilihan untuk mengalahkan ketiga negara lainnya saat ini. Mengingat tidak ada jaminan Iran akan memenangkan perang konvensional, apalagi persenjataan Iran dan jumlah tentara yang aktif masih kalah baik dari kualitas dan kuantitas. Sehingga pada akhirnya, ketika menjadi jelas bahwa Iran sedang mengalami kesulitan karena berkonflik dengan ketiga negara tersebut dan tidak dapat secara konvensional mengalahkan mereka, Iran sampai pada sebuah kesimpulan bahwa Iran perlu mengambil kebijakan untuk menetapkan status quo dan kalau perlu menjaga agar status quo ini dapat bertahan selama mungkin dengan ketiga negara lainnya, mengingat perang diplomatik dan perang konvensional bukanlah pilihan yang logis bagi Iran. Perlu diketahui bahwa damai atau *win-win solution* juga bukan pilihan logis bagi Iran, mengingat yang membentuk dan mempergunakan identitas nasional adalah pemerintah Iran sendiri sejak Ayatollah Ruhollah Khomeini berkuasa. Adapun, berdasarkan

argumen Presiden Iran saat ini, yakni Hassan Rouhani dan Mayor Jenderal Qassem Soleimani di atas, dapat dilihat juga kalau Iran tidak ingin melanjutkan perang dengan negara manapun, terutama dengan Amerika Serikat. Dimana karena itu, keduanya memperingatkan bahwa Iran adalah negara kuat, yang mana jika perang konvensional dengan Amerika Serikat terjadi, maka menurut mereka Iran yang akan memenangkan perang tersebut atau setidaknya AS akan menderita kerugian yang sangat besar. Merujuk pada hal ini, peneliti berpendapat bahwa operasi siber ofensif menjadi salah satu opsi yang digunakan oleh Iran untuk menjaga status quo di situasi konflik tersebut dan mencegah terjadinya potensi perang konvensional di masa depan.

Kebijakan Politik Khamenei Sebagai Kepentingan Operasi Siber Ofensif Iran

Adapun tujuan Iran untuk menjaga status quo pada konfliknya juga terlihat dari hasil tingkatan analisis individu Iran. Terlebih dahulu, perlu diketahui bahwa Individu yang dimaksud dalam tingkatan analisis ini adalah pemimpin atau pembuat kebijakan dalam suatu negara, sehingga analisis level individu berfokus pada individu pemimpin. Hal ini dikarenakan pemimpin adalah sosok penting dalam pengambilan keputusan. Keputusan yang telah diambil oleh pemimpin tidak saja dianggap sebagai representasi dirinya sendiri, melainkan juga dianggap sebagai representasi negaranya. Dengan kata lain, analisis level individu melihat bahwa pemimpin dalam merumuskan dan memutuskan suatu kebijakan pasti selalu didasarkan pada kepentingan nasional negaranya (Neack, 2008: 10). Berhubungan dengan tingkatan analisis ini, peneliti menggunakan sosok *supreme leader*, yakni Ali Khamenei. Menurut penulis Ali Khamenei dapat menjadi acuan yang begitu jelas untuk mengkaji kebijakan operasi siber ofensif Iran yang agresif dan terbuka. *Supreme leader* atau disebut juga dengan pemimpin tertinggi revolusi Islam adalah kepala negara, sekaligus pemegang otoritas politik dan agama tertinggi di Iran. Presiden, Militer, kepolisian, kehakiman,

dan bahkan media berada dibawah pengaruh Ali Khamenei. Seorang *supreme leader* juga yang menentukan keputusan akhir terkait ekonomi, lingkungan, pendidikan, perencanaan nasional dan kebijakan luat negeri. Ali Khamenei juga dapat membuat keputusan akhir tentang jumlah transparansi dalam pemilu, memberhentikan dan mengembalikan kabinet yang ditunjuk sebagai presiden (Sadjadpour, 2010).

Berhubungan dengan tingkatan analisis ini, peneliti menggunakan pendekatan *leadership trait analysis*, yang mana bertujuan untuk menganalisa kemampuan Khamenei dalam kehidupan politik negaranya, terutama dalam menangani isu-isu politik luar negeri (Breuning. 2007). Berdasarkan sejarahnya, Iran dibawah pemerintahannya Khamenei sudah berulang kali menggunakan kemampuan ofensif yang hanya bertujuan melukai dan melemahkan niat lawannya untuk melakukan perang konvensional demi mengatasi situasi konflik yang meningkat. Adapun aplikasi kemampuan asimetris dalam strategi militer Iran yang berfokus untuk mengembangkan kemampuan senjata nuklir, melakukan kegiatan teroris di seluruh dunia, mengancam dengan serangan rudal, dan menyandera pasar minyak global dengan mengancam akan menutup Selat Hormuz yang merupakan jalur air vital bagi perdagangan minyak global adalah beberapa cara yang dilakukan Khamenei untuk melukai dan melemahkan niat lawannya untuk melakukan perang konvensional demi mengatasi situasi konflik yang meningkat (Fixler & Cilluffo, 2018: 8-10). Hal ini juga dapat disimpulkan dari interpretasi tulisan Ali Khamenei di twitter Ali Khamenei, yakni pada tanggal 13 Agt 2018 Ali Khamenei mengatakan bahwa:

> "Recently, U.S. officials have been talking blatantly about us. Beside sanctions, they are talking about war and negotiations. In this regard, let me say a few words to the people: there will be no war, nor will we negotiate with the U.S."

Perkataan Ali Khamenei dapat menunjukkan bahwa Amerika Serikat terkait situasi konfliktual ini, kemungkinan memberikan pilihan kepada Iran, yakni perang atau mengakui kekalahannya.

Melalui respon Ali Khamenei di Twiter, dapat dilihat juga bahwa penyelesaian konflik melalui perang dan negosiasi bukanlah pilihan Iran, yang mana karena itu Ali Khamenei menyebutkan pada akun resmi Twiternya bahwa tidak ada perang atau negosiasi dengan Amerika Serikat. Sebaliknya Ali Khamenei saat ini ingin agar situasi quo dalam konflik ini tetap bertahan, setidaknya sampai negosiasi atau perang dapat menguntungkan Iran.

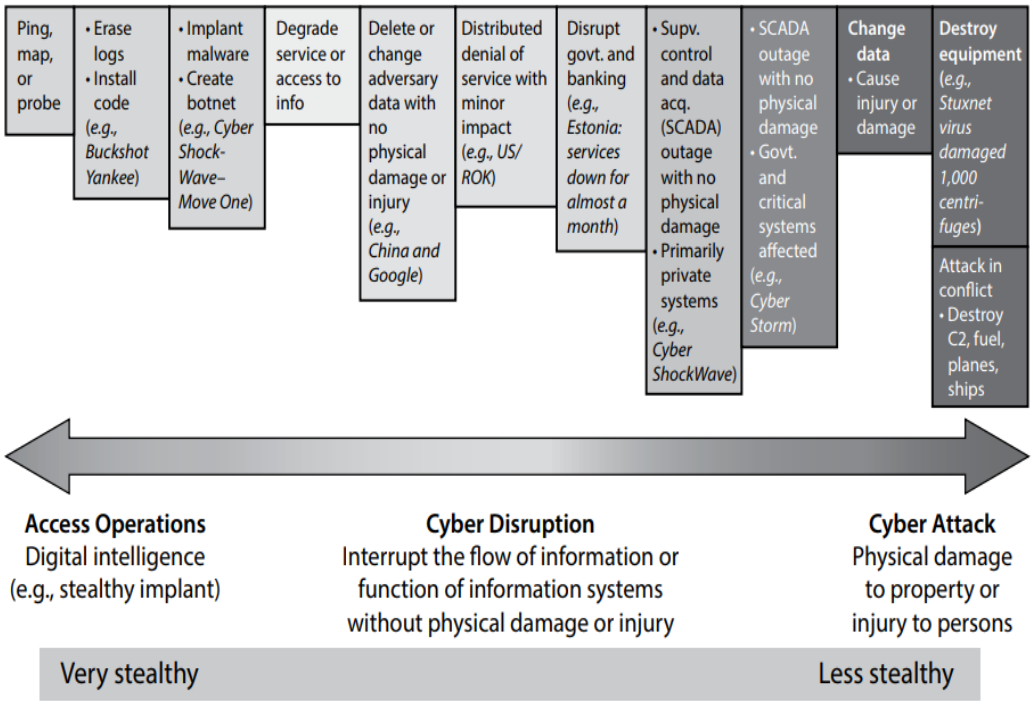
Strategi Siber Ofensif Iran: Strategi Siber Asimetris

Berdasarkan hasil dari penggunaan kedua tingkatan analisis sebelumnya, yakni identitas nasional dan individu, peneliti menggunakan dua strategi yang menurut peneliti dapat memfasilitasi kepentingan siber ofensif Iran. Kedua strategi tersebut adalah strategi siber asimetris dan strategi *deference active*. Seperti yang telah peneliti paparkan sebelumnya, Iran dalam menangani isu-isu politik luar negeri dan militer negaranya menggunakan kemampuan asimetris. Pengaplikasian kemampuan asimetris dalam strategi militer Iran dapat dilihat dari strategi Iran yang saat ini berfokus pada kemampuan untuk mengembangkan kemampuan senjata nuklir, melakukan kegiatan teroris di seluruh dunia, mengancam serangan rudal, dan menyandera pasar minyak global dengan mengancam akan menutup Selat Hormuz, dan lain sebagainya. Strategi asimetris ini penting dilakukan bukan demi memenangkan konflik, tetapi untuk melemahkan kemauan musuh untuk melakukan perang konvensional dengan gangguan, kehancuran, kelelahan, atau paksaan. Dimana karena itu, strategi asimetris biasanya digunakan oleh aktor yang lebih lemah terhadap kelemahan aktor lain yang lebih kuat (Jun, 2018).

Berhubungan dengan strategi siber asimetris, operasi siber ofensif harus dilakukan dalam dalam skala kecil atau sedang. Dengan kata lain operasi siber ofensif hanya perlu dilakukan dari *Access Operations* sampai *Cyber Disruption*, yakni kerusakan operasi siber ofensif yang hanya berfokus

pada kerusakan informasi dan sistem keuangan negara atau perusahaan yang berhubungan dengan negara tersebut (McKenzie, 2017). Untuk detailnya dapat melihat tabel dibawah ini:

Tabel 2 : Spektrum Skala Operasi Siber Ofensif



Sumber : *Timothy M. McKenzie*

Adapun dalam strategi siber asimetris ini, operasi siber ofensif dalam sekala besar atau *cyber attack* (serangan siber yang merusak properti dan melukai manusia) tidak perlu dilakukan, hal ini karena dari awal tujuannya asimetris bukanlah memulai *total war* atau menghancurkan pihak lawan, namun kemudian hanya ditujukan untuk mengekspoitasi kerentanan dari negara-negara lain agar negara tersebut tidak mau atau ragu untuk memulai perang konvensional dengan negara pengguna serangan siber dalam skala kecil dan sedang. Hal ini juga sesuai dengan fakta bahwa serangan siber pada bentuk yang dapat menimbulkan kerusakan kolateral yang serius pada sebuah negara bukan lagi melukai negara tersebut, namun menghancurkan negara tersebut. Sama seperti

nuklir, jika sebuah negara melakukan serangan nuklir, maka itu berarti negara tersebut telah siap untuk melakukan perang habis-habisan. Dalam hal ini aktor yang melakukan serangan yang dapat menimbulkan kerusakan kolateral sudah harus siap terhadap konsekuensi yang mungkin diterima, baik dari aktor-aktor internasional lainnya, atau mendapat serangan balasan dari negara yang diserang (McKenzie, 2017: 5).

Adapun hal inilah yang dilakukan oleh Iran dalam rentang waktu 2010-2018. Dalam rentang waktu itu, operasi siber ofensif Iran hanya dilakukan menggunakan jenis serangan dalam skala kecil dan sedang. Serangan dalam skala kecil dan sedang ini difokuskan pada dua hal, yakni kerusakan finansial dan pencurian serta sabotase informasi. Sebagai contoh hal ini dapat dari serangan siber *Qassam Cyber Fighters* dalam bentuk DDOS terhadap sektor-sektor keuangan Amerika Serikat secara berulang-ulang dengan kode Ababil. Serangan siber ini mengunci ratusan ribu pelanggan perbankan dari akun-akun untuk jangka waktu yang lama dan mengakibatkan puluhan juta dolar biaya untuk memulihkannya (Anderson dan Karim, 2018). Contoh lainnya adalah salah satu serangan paling terkenal Iran terhadap salah satu perusahaan Arab Saudi, yakni Saudi Aramco selama liburan Idul Fitri Muslim dan serangan serupa terhadap Perusahaan RasGas Qatar dua minggu kemudian. Kelompok yang mengaku bertanggung jawab adalah *Cutting Sword of Justice*. Terkait hal ini, dalam serangan yang dikenal dengan kode Shamoon, puluhan ribu komputer Saudi Aramco dan Perusahaan RasGas Qatar diserang, menyebabkan kerusakan puluhan hingga ratusan juta dollar hilang sebagai konsekuensinya (Fixler & Cilluffo, 2018).

Contoh pencurian serta sabotase informasi dapat dilihat dari serangan siber *spearpishing* yang telah dilakukan berulang-ulang sejak tahun 2011 sampai sekarang ini, dengan target utamanya email pribadi dan akun media sosial karyawan pemerintah Amerika Serikat, Israel, dan Arab Saudi. Dimana kemudian melalui email dan akun media sosial tersebut, Iran mengirimkan pesan-

pesan kepada pihak tertentu yang bertujuan untuk menipu atau mengelabui penerima pesan agar melakukan semacam tindakan yang menguntungkan Iran, termasuk membagi informasi rahasia. Adapun disini, sebenarnya sebagian spionase dan sabotase akun-akun ini tidak hanya mengandalkan serangan siber. Namun disini Iran juga merampas akun-akun tadi secara paksa. Dimana Iran mulai dengan menangkap pegawai-pegawai (kebetulan sedang berada di Iran) yang memiliki kaitan dengan bidang-bidang tadi secara lansung, lalu mengambil kendali akun media sosialnya (Anderson dan Karim, 2018). Salah satu serangan siber *spearphishing* Iran yang paling sukses dan sering dilakukan adalah serangan Mahdi. Mahdi adalah *malware* komputer yang awalnya ditemukan pada Februari 2012 dan dilaporkan pada bulan Juli tahun itu. Mahdi ini telah digunakan oleh Iran untuk spionase dunia maya sejak Desember 2011. Menginfeksi setidaknya 800 komputer di Iran, negara-negara Timur Tengah lainnya, dan negara-negara aliansi Amerika Serikat. Negara-negara dan entitas-entitas yang ditargetkan adalah perusahaan minyak, lembaga *think tank* AS, lembaga pemerintah, perusahaan rekayasa, lembaga keuangan, dan akademisi. Beberapa negara kawasan Eropa juga telah memberikan bukti adanya operasi Mahdi Iran dalam dakwaan dan laporan keamanan. Salah satunya adalah Jerman, yang mana atas kejadian ini, pemerintah Jerman menyebut Iran sebagai ancaman sumber baru spionase dunia maya (Anderson dan Karim, 2018).

Strategi Siber Ofensif Iran: Strategi Siber *Deference Active*

Strategi siber ofensif Iran selanjutnya adalah strategi *deterrence active*. *Deterrence active* merujuk pada tindakan yang diambil negara untuk mengamankan dirinya dari serangan negara lain dengan ancaman balas dendam atau respon yang tidak diinginkan negara lain jika menyerang. Dihubungkan dengan contoh, senjata nuklir dan dampak yang dimiliki senjata nuklir dapat menjadi

rujukan untuk menjelaskan *deterrence active*. Menurut Waltz dalam tulisannya yang berjudul *Nuclear Myths and Political Realities,* ia memaparkan bahwa senjata nuklir yang sangat merusak tersebut menimbulkan ketakutan akan perang, yang mana hal ini tidak terjadi pada perang konvensional yang ia nilai menawarkan keuntungan secara politik dan ekonomi jika menang. Namun hal tersebut tidak terjadi pada perang nuklir, karena disamping tidak akan ada yang tau siapa yang akan menang, perang nuklir pada dasarnya tidak akan memberikan keuntungan apapun bagi negara manapun, termasuk negara pemenang perang sekalipun. Lebih lanjut dalam strategi *deterrence active* ini, ada sebuah keyakinan dan ketakutan bahwa akan ada kemungkinan negara lain akan meyerang dengan kekuatan yang sama atau bahkan lebih besar, ketika kita menyerang mereka (Waltz, K, 1990). Dalam hal ini nuklir diasumsikan sebagai kekuatan tersebut, sehingga menimbulkan asumsi bahwa ketika sebuah negara menyerang negara lain yang juga punya senjata nuklir, maka negara itu akan mendapat balasan senjata nuklir juga. Adapun karena keyakinan dan ketakutan tersebut, negara-negara yang biasanya sama-sama memiliki kekuatan nuklir, menolak untuk berperang satu sama lain. Hal ini dikarenakan bahaya nuklir itu sendiri yang pada akhirnya sangat merugikan negara itu sendiri jika diserang dengan nuklir. Hal ini terbukti saat perang dingin, yang mana saat itu baik Uni Soviet maupun Amerika Serikat tidak berani untuk berperang satu sama lain secara lansung, karena adanya ketakutan akan bahaya dari senjata nuklir itu sendiri (Waltz, K, 1990).

Terkait pemikiran itu, maka dapat dilihat bahwa hal ini juga relavan dengan serangan siber. Clarke memaparkan bahwa beberapa hal yang dapat disebabkan oleh serangan siber adalah meledaknya kilang dan pipa minyak, menimbulkan kekacauan pada sistem keuangan, saluran komunikasi mati, arsip-arsip kenegaraan dicuri, rusaknya sistem keamanan militer, tergelincirnya kereta api, jatunya pesawat terbang, dan lepas kendalinya satelit (Clarke, 2010). Jika membandingkannya dengan

senjata nuklir, maka dapat dikatakan bahwa serangan siber tidak kalah berbahayanya, karena keduanya pada dasarnya mampu untuk menimbulkan kerusakan fatal pada sebuah perang. Terlebih lagi sedikit unggul dibandingkan senjata nuklir, serangan siber dapat dilakukan dengan mudah dan tanpa resiko yang yang besar karena tidak adanya alat untuk mengindetifikasi pelaku penyerangan secara spesifik, serta ketiadaan hukum atau aturan yang cukup kuat. Adapun dihubungkan dengan strategi *deterrence active*, maka dapat disimpulkan jikalau dilihat dari segi ancaman kerusakan yang dapat ditimbulkan masing-masing senjata. Serangan siber juga dapat menimbulkan efek *deterrence active* yang sama, yaitu menimbulkan keyakinan dan ketakutan bahwa akan ada kemungkinan negara lain akan menyerang dengan kekuatan yang sama atau bahkan lebih besar jika eksistensi negara itu sedang terancam (Clarke, 2010).

Lebih jauh, meski strategi *deterrence active* siber memang berhasil memberikan ketakutan terhadap lawan-lawannya. Namun strategi ini tidak terbukti seefektif strategi *deterrence* nuklir, karena Iran tidak dapat menggunakan serangan siber dalam skala besar yang dapat menimbulkan ketakutan dan kerusakan yang sama dengan serangan nuklir. Hal ini tidak terlepas dari jejak siber yang dapat dilacak, dan diteliti untuk memberikan teknologi baru bagi musuh jika diserang dengan serangan siber (Lawson, 2012). Dimana karena itu, Iran lebih bergantung terhadap serangan siber dalam skala kecil dan sedang, yang mana ternyata bukan ketakutan akan kehancuran seperti yang dapat dilakukan melalui serangan nuklir yang muncul, namun hanya ketakutan terkait dengan kerugian yang mungkin diperoleh jika menyerang Iran.

Akan tetapi dikaitkan dengan perhitungan biaya dan manfaat ketika melakukan operasi siber ofensif selama ini, maka dapat dilihat bahwa meski tidak sebaik serangan nuklir. Operasi siber ofensif Iran dalam skala kecil dan sedang ini tidak memberikan Iran kerugian yang sebanyak serangan siber skala besar. Hal ini karena meski dapat digandakan oleh negara penerima serangan

siber Iran, serangan siber dalam skala kecil dan sedang tidak membahayakan eksistensi Iran di masa depan (McKenzie, 2017). Adapun, serangan siber dalam skala kecil dan sedang yang dilakukan secara berulang-ulang nyatanya setidaknya terbukti berhasil menimbulkan ketakutan atau keyakinan terhadap beberapa lawannya. Terbukti dari argumen Arab Saudi melalui Menteri Luar Negerinya, yakni Adel Al-Jubeir yang menyebut Iran sebagai negara yang berbahaya dalam hal serangan siber, sembari mengatakan bahwa negaranya telah berulangkali diancam oleh negara yang dianggap sebagai musuh tersebut (Fixler & Cilluffo, 2018).

Kesimpulan

Dari pembahasan-pembahasan di atas, dapat disimpulkan bahwa berdasarkan analisis identitas nasional dan analisis individu Iran, kepentingan operasi siber ofensif Iran terhadap konfliknya dengan Amerika Serikat, Israel, Arab Saudi adalah untuk mengancam musuh agar tidak melakukan perang konvensional dan menjaga status quo di situasi konflik tersebut. Salah satu strategi yang digunakan oleh Iran adalah strategi asimetris. Strategi ini ditujukan sebagai media untuk melemahkan kemauan musuh untuk berperang dengan cara menyerang kelemahan musuh-musuhnya dengan serangan siber skala kecil dan sedang terhadap sistem finansial dan informasi ketiga negara lainnya. Adapun, peneliti juga menyimpulkan bahwa Iran juga menggunakan strategi *deterrence active* sebagai landasan operasi siber ofensifnya. Iran dalam hal ini mengunakan strategi *deterrence active* untuk melemahkan kemauan musuh-musuhnya dengan cara mengancam, menyakinkan dan melakukan serangan balasan sebesar-besarnya jika negaranya diserang atau dilukai oleh negara lain. Akan tetapi perlu diketahui bahwa ternyata Iran belum menggunakan atau memang pada dasarnya tidak dapat selalu bergantung dengan serangan siber dalam skala besar yang dapat menimbulkan kerusakan dan ketakutan yang sama dengan serangan

nuklir. Sebab sifat dasar serangan siber yang dapat diteliti dan digandakan oleh musuh yang terkena serangan siber, sehingga cenderung tidak efektif digunakan dalam perang sesungguhnya. Oleh karena itu, Iran lebih berfokus pada serangan siber skala kecil dan sedang yang pada dasarnya tidak begitu efektif dalam menjaga status quo dalam konflik, sebab tidak menimbulkan ketakutan yang sebesar serangan nuklir.

Daftar Pustaka

Anderson, Collin dan Karim, Sadjadpour. 2018. *Iran's Cyber Threat: Espionage, Sabotage, Revenge*.

BBC News. 2018. "Setelah demo besar antipemerintah di Iran, sulit memastikan apa yang akan terjadi namun rakyat sudah bersuara". Diakses [online] pada 15 Januari 2019, melalui https://www.bbc.com/indonesia/dunia-42604143

Breuning, M. (2007). *Foreign Policy Analysis: A Comparative Introduction*. New York: Palgrave MacMillan Ch.2-3.

Cilluffo, A. F. (2018). *Evolving Menace Iran's Use of Cyber-Enabled Economic Warfare*.

Clarke, R. a. (2010). *Cyber War: The Next Threat to National Security and What To Do About It.*

Clunan, A. L. (2019). *The Social Construction of Russia's Resurgence: Aspirations, Identity, and Security Interests. Baltimore: Maryland: The Johns Hopkins University Press*, Ch.1 & 2.

Jenny Jun, S. L. (2018). *North Korea's Cyber Operations. Central for Strategic International Studies Korea Chair*.

Lawson, S. (2012). *Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States. the University of Illinois at Chicago University Library*

Neack, L. (2008). *The New Foreign Policy: Power Seeking in a Globalized Era. Plymouth: Rowman & Littlefield Publishers*. Ch.2 & 3.

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

Rid, Thomas & McBurney, Peter. 2012. *Cyber-Weapons. The RUSI Journal*.

Sadjadpour, Karim. 2010. *The Supreme Leader* [Online]. Dalam http://iranprimer.usip.org/resource/supreme-leader. [Diakses 30 Maret 2018].

The New York Times. 2016. *"An Interview With Khomeini"*. Diakses [online] pada 11 Januari 2019 melalui https://www.nytimes.com/1979/10/07/archives/an-interview-with-khomeini.html;

Waltz, K. (1990). *Nuclear Myths and Political Realities. The American Political Science Review*, 84 (3):731-745.