IR - PERPUSTAKAAN UNIVERSITAS AIRLANGGA

B

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

SKRIPSI

Disusun oleh

Rahmadi Pratama Aritonang

071511233049

PROGRAM STUDI SARJANA ILMU HUBUNGAN INTERNASIONAL

DEPARTEMEN HUBUNGAN INTERNASIONAL

FAKULTAS ILMU SOSIAL DAN ILMU POLITIK

UNIVERSITAS AIRLANGGA

SEMESTER GENAP 2018/2019

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

SKRIPSI

Diajukan sebagai Salah Satu Syarat untuk Menyelesaikan Studi S-1
di Fakultas Ilmu Sosial dan Ilmu Politik
Universitas Airlangga

Disusun Oleh
Rahmadi Pratama Aritonang
071511233049

PROGRAM STUDI SARJANA ILMU HUBUNGAN INTERNASIONAL
DEPARTEMEN HUBUNGAN INTERNASIONAL
FAKULTAS ILMU SOSIAL DAN ILMU POLITIK
UNIVERSITAS AIRLANGGA
SEMESTER GENAP 2018/2019

HALAMAN PERSETUJUAN

Skripsi dengan judul:

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

Disusun oleh:

Rahmadi Pratama Aritonang
071511233049

Disetujui untuk diujikan di hadapan Komisi Penguji
Surabaya, 02 Juli 2019

Dosen Pembimbing,

I Basis Susilo Drs., MA
NIP. 19540808 198103 1 007

Mengetahui,
Ketua Departemen Hubungan Internasional,

M. Muttaqien, S.IP, MA, Ph.D
NIP. 19730130 199903 1 001

HALAMAN PENGESAHAN DEWAN PENGUJI

Skripsi ini telah dipertahankan di hadapan Komisi Penguji pada hari Kamis, 23 Mei 2019, pukul 13.00 WIB di Ruang Sidang Cakra Buana Catur Matra, Gedung C Fakultas Ilmu Sosial dan Ilmu Politik Universitas Airlangga Surabaya

Komisi Penguji

Ketua,

Hj.Lilik Salamah Dra., M.Si.
NIP. 195605071986012 001

Anggota I

DRS. Wahyudi Purnomo, M.Phill
NIP. 195609211988101 001

Anggota II

Sartika Soesilowati Dra.,MA., Ph.D
NIP. 196407301995122 001

HALAMAN PERNYATAAN TIDAK MELAKUKAN PLAGIAT

Bagian atau keseluruhan skripsi berjudul:

"Operasi Siber Ofensif Iran Terhadap Amerika Serikat, Israel dan Arab Saudi: Kepentingan dan Strategi Ofensif Siber Iran"

Ini tidak pernah diajukan untuk mendapatkan gelar akademis pada bidang studi dan/atau universitas lain dan tidak pernah dipublikasikan/ditulis oleh individu selain penyusun kecuali bila dituliskan dengan format kutipan dalam isi skripsi.

Surabaya, 02 Juli 2019

Rahmadi Pratama Aritonang

KATA PENGANTAR

Segala puji bagi Tuhan, karena atas limpah rahmat-Nya penulis dapat menyelesaikan skripsi ini. Skripsi ini merupakan persembahan penulis kepada almarhum Ayah dan juga mamaku tercinta, yakni Elfrida Yenika Saragi yang telah mendidik dan membesarkan penulis selama ini. Penulis juga mengucapkan banyak terima kasih atas dukungan dari keluarga penulis selama penulisan skripsi ini. Terima kasih juga pacarku tercinta Astrid yang sudah mendukung dan membantu penulis selama penelitian tugas akhir ini. Ucapan terima kasih juga penulis sampaikan kepada dosen-dosen dan staf Departemen Hubungan Internasional Universitas Airlangga yang telah membina penulis dengan ilmu-ilmu hingga dapat menyelesaikan skripsi ini; Pak Basis selaku pembimbing penulis, Bu Lilik, Bu Sartika, Pak Wahyudi, Bu Irma, Bu Ani, Mbak Ica, Mbak Indah, Mbak Citra, Mas Ari, Mbak Irfa, Mas Yunus, Mas Joko, Pak Joko, dan Pak Ajar. Penulis juga mengucapkan terima kasih kepada keluarga penulis dalam menjalani kehidupan selama 4 tahun ini, yaitu teman-teman penulis di HI 2015: Jason, Rezza, Martin, Kurnia, Alam, Maula, Rama, Anggia, Akbar, Zarrin, Rahmat Imawan, NRG, Abi dan teman-teman HI 15 yang hebat dan luar biasa lainnya. Terima kasih juga kepada teman-temanku di Dana Cita atas pengalaman berorganisasi bersama selama satu tahun belakangan ini: Halfie, Aldi, Rafika, Savira, Mbak Riyan, Pratama, Zhafirah, Hadit, dan Mail dari ITS. Terima kasih juga kepada teman-teman di IDN Media yang amat sangat mewarnai hidupku selama 6 bulan belakangan ini: Clara, Fide, Ida, Suci, Mich, Dyah, dan Cilla. Aku juga berterimah kasih kepada keluarga besar Rezza yang telah menjadi keluarga keduaku selama di Surabaya. Selain itu terima kasih kepada teman-teman penulis, yakni Natan dan Tio, atas pengalaman tidak terlupakannya.

ABSTRAK

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.

DAFTAR ISI

HALAMAN JUDUL i
HALAMAn JUDUL DALAM ii
LEMBER PERSETUJUAN iii
HALAMAN PENGESAHAN iv
HALAMAN PERNYATAAN TIDAK MELAKUKAN PLAGIAT v
KATA PENGANTAR vi
ABSTRAK vii
BAB I PENDAHULUAN 1
1.1 Latar Belakang Masalah 1
1.2 Rumusan Masalah 8
1.3 Tinjauan Pustaka 8
1.3.1 Budaya Strategis dan Tujuan Perang Siber 9
1.3.3 Kemampuan Operasi Siber Ofensif 10
1.3.2 Strategi Siber Ofensif Korea Utara 13
1.4 Kerangka Pemikiran 15
1.4.1 Biological Metaphors 16
1.4.2 Tingkatan Analisis Identitas Nasional 19
1.4.3 Tingkatan Analisis Individu 21
1.4.4 Strategi Deterrence Active 23
1.4.5 Strategi Siber Asimetris Korea Utara 26
1.5 Hipotesis Penelitian 28
I.6 Metode Penelitian 29
1.6.1 Defenisi dan Operasionalisasi Konsep 29
1.6.1.1 Operasi Siber Ofensif Iran 29
1.6.1.2 Mempertahankan Status Quo 30
1.6.1.3 Strategi Siber Ofensif Iran 31
1.6.2 Tipe Penelitian 31
1.6.3 Ruang Lingkup dan Jangkauan Penelitian 31
1.6.4 Teknik Pengumpulan Data 32

1.6.5 Teknik Analisis Data 32
1.6.6 Sistematika Penulisan 33
BAB II KEPENTINGAN ATAU TUJUAN DARI OPERASI SIBER OFENSIF IRAN 34
2.1 Identitas Nasional Sebagai Alasan Iran untuk Mempertahankan Status Quo 34
2.2 Kebijakan Politik Khamenei: Kepentingan Operasi Siber Ofensif Iran..... 41
BAB III STRATEGI SIBER OFENSIF IRAN 46
3.1 Strategi Siber Asimetris Iran: Fokus Terhadap Operasi Siber Ofensif Skala Kecil dan Sedang 46
3.2 Strategi Siber Deterrence Active Iran: Fokus Terhadap Serangan Siber Skala Kecil dan Sedang..... 54
3.2.1 Deklarasi Peringatan yang Harus Keras dan Jelas..... 56
3.2.2 Kredibilitas untuk Melakukan Serangan Balasan..... 60
3.2.3 Mampu Memproduksi Ketakutan dan Melakukan Tindakan Penalti 63
3.2.4 Perhitungan Biaya dengan Manfaat Ketika Melakukan Serangan 66
BAB IV KESIMPULAN 69
DAFTAR PUSTAKA 75

DAFTAR TABEL

Tabel 1	Operasi Siber Ofensif Iran Terhadap AS, Israel, dan Arab Saudi	3
Tabel 2	Atribut Strategi Pencegahan	25
Tabel 3	Spektrum Skala Operasi Siber Ofensif	49
Tabel 4	Kelompok-Kelompok Peretas yang Berhubungan dengan Iran	54

DAFTAR SINGKATAN

DDoS	:	Distributed Denial-of-Service
AIPAC	:	Islamic Revolutionary Guard Corps
IRGC	:	Islamic Revolutionary Guard Corps
DNI	:	Direktur Intelijen Nasional
APT	:	Advance Persistent Threat
HBO	:	Home Box Office

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

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. Siber ofensif

dari Tiongkok sebagian besarnya berusaha untuk mengambil dan mensabotase informasi-informasi penting negara lain. Sedangkan siber ofensif dari Rusia hanya berfokus pada serangan siber yang fungsinya mengambil informasi-informasi penting. Adapun pada dasarnya, semua negara pada umumnya memiliki satu kesamaan, yakni berusaha menyembunyikan kalau mereka adalah pelaku penyerangan siber. Di lain sisi, peretas Iran berusaha melakukan hal yang jauh lebih berbeda dari kebanyakan negara lain. Iran berfokus pada operasi siber ofensif 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 saat ini, yakni Amerika Serikat, Israel, dan Arab Saudi (Rattray, 2018: 3-8). Hasil penelitian MalCrawler 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.

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*

Berdasarkan tabel satu, operasi siber ofensif Iran pertama yang paling fenomenal dikenal dengan kode operasi Ababil. Gelombang operasi ini dimulai dari Desember 2011 dan berlanjut hingga pertengahan 2013. Pada saat itu, sebuah kelompok yang menamakan dirinya *Izz ad-Din al-Qassam Cyber Fighters* atau dikenal juga dengan *Qassam Cyber Fighters* mengumumkan bahwa mereka merupakan aktor dibalik aksi serangan siber dalam bentuk *Distributed denial-of-service* (DDoS) terhadap 46 bank dan sistem keuangan termasuk *Bank of America, Wells Fargo, JPMorgan Chase, dan New York Stock Exchange*. Serangan yang

terjadi hanya dalam hitungan menit, selama sepuluh bulan pertama dan kemudian meningkat menjadi hampir setiap minggu. Lalu hasilnya pada tanggal 18 September 2012, *Izz ad-Din al-Qassam Cyber Fighters* diketahui berhasil menyerang perangkat lunak ribuan situs web sektor keuangan Amerika Serikat. Iran juga berhasil mencegah ratusan ribu individu dan pebisnis untuk mengakses akun online mereka, dan karena hal ini kemudian layanan online keuangan Amerika Serikat tersebut nonaktif (Disegi, 2016: 6). Lebih lanjut dengan metode yang tidak jauh berbeda, Iran kemudian secara berkala melancarkan serangan sibernya dengan target yang masih sama, yakni sektor keuangan Amerika Serikat. Akan tetapi berbagai serangan siber tersebut nyatanya gagal, sampai akhirnya pada bulan Juli 2013, yakni pada gelombang serangan siber Ababil mereka yang keempat, Iran kembali berhasil melakukan serangan siber yang cukup merusak. Operasi Ababil keempat ini mengunci ratusan ribu pelanggan perbankan untuk jangka waktu yang lama dan mengakibatkan puluhan juta dolar biaya untuk memulihkannya (Anderson dan Karim, 2018: 30).

Adapun, operasi siber ofensif yang paling sering digunakan oleh Iran bukanlah DDoS, namun *spearphishing* pada email pribadi dan akun media sosial karyawan pemerintah AS, Israel, dan Arab Saudi. Adapun serangan dalam bentuk ini sendiri berbeda dengan DDoS. Pada bentuk *spearphishing*, serangan siber dilakukan dengan mensabotase email atau akun media sosisal tertentu. 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 negara atau bahkan individu itu sendiri. Adapun *spearphishing* ini mudah dilakukan karena akun pribadi cenderung tidak memuat informasi rahasia pemerintah, sehingga memiliki keamanan yang jauh lebih lemah, namun disisi lainnya tetap memiliki fungsi yang sangat penting. Dikarenakan sering mengandung informasi yang berguna seperti materi pribadi dan jejak komunikasi profesional. Misalnya, Iran berusaha untuk menyerang akun email pribadi anggota khusus AS selama negosiasi nuklir. Demikian pula, setelah pemilihan presiden AS 2016, Iran pada saat itu menargetkan mantan staf anggota Kongres partai Republik, pendukung Donald Trump, dan organisasi media konservatif. Adapun Teheran cenderung menargetkan personil dan lembaga pemerintah asing yang memiliki kaitan pekerjaan dengan Iran, sebagai contoh orang-orang di Amerika Serikat atau Eropa yang bekerja pada televisi *Voice of America* dan Radio Farda. Uniknya disini, sebenarnya sebagian spionase akun-akun ini tidak hanya mengandalkan serangan siber. Namun disini, Iran juga merampas akun-akun tadi secara paksa. Dimana mereka 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. Adapun karena hal tersebut, baru-baru ini kampanye *spearphishing* ini malah menghadirkan kritik yang jauh lebih banyak dibandingkan operasi Ababil di Kongres AS. Sementara sanksi baru telah dipertimbangkan, seiringan dengan fakta sulitnya AS menangani *spearphishing* ini (Anderson dan Karim, 2018: 30-32).

Selain Amerika Serikat, Arab Saudi juga menjadi korban dari operasi siber ofensif Iran. Salah satu serangan paling terkenal terjadi pada tanggal 15 Agustus 2012 oleh Iran terhadap 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 dengan DDoS, menyebabkan kerusakan puluhan hingga ratusan juta dolar hilang sebagai konsekuensinya. Serangan itu mengganggu sebagian besar proses bisnis Aramco, termasuk manajemen pasokan, pengiriman, dan manajemen kontraknya dengan cara menghapus data di tiga perempat komputer perusahaan Aramco dan mengganti data dengan gambar bendera orang Amerika yang terbakar. Butuh waktu sekitar lima bulan untuk membuat seluruh organisasi kembali menggunakan akses internet (Anderson dan Karim, 2018: 32-34). Serangan kedua yang paling fenomenal adalah ketika serangan Shamoon yang digunakan dalam insiden Aramco muncul kembali pada November 2016 hingga Januari 2017 dalam bentuk yang diperbarui (diberi label sebagai Shamoon 2 oleh peneliti). Shamoon 2 ini menghancurkan database milik pemerintah dan sektor swasta, termasuk Otoritas Umum Penerbangan Sipil, Departemen Tenaga Kerja, Bank Sentral Saudi, dan perusahaan ekstraksi sumber daya alam. Shamoon 2 juga berisi hal-hal terkait konflik Yaman dan gambar para korban dengan gambar anak pengungsi Suriah yang tewas, yakni Alan Kurdi (Disegi, 2016: 7).

Lebih jauh, salah satu kebijakan utama luar negeri Iran adalah Iran menjadi penentang eksistensi Israel dan pendukung untuk kelompok militan anti-Israel, seperti Hizbullah, Hamas, dan Jihad Islam Palestina. Meskipun demikian, dalam prosesnya Teheran jauh dari kata berhasil dalam menargetkan lembaga-lembaga Israel dalam strategi siber ofensifnya. Bahkan jika dibandingkan, operasi siber ofensif Iran di Amerika Serikat dan kawasan Eropa masih jauh lebih sukses. Dalam dokumen keamanan Israel, yang berhasil didokumentasikan oleh para peneliti, setidaknya ada 54 upaya serangan siber yang telah dilancarkan oleh Iran kepada Israel. Salah satunya selama konflik antara Israel dan Gaza pada musim panas 2014 dengan kode operasi *Protective Edge*. Pihak berwenang Israel mengklaim bahwa infrastruktur Pasukan Pertahanan Israel ditargetkan oleh serangan DDoS yang diluncurkan oleh berbagai pihak, termasuk Teheran. Serangan DDoS ini memiliki sistem dan kekuatan yang sama dengan serangan DDoS sebelumnya, termasuk taktik yang digunakan untuk melawan Amerika Serikat dan negara-negara Eropa. Meskipun dengan rekam jejak keberhasilan yang memukau dari serangan DDoS milik Iran, kemampuan Teheran untuk menimbulkan kerusakan berarti pada Israel melalui operasi siber ofensif tersebut sejauh ini sangat terbatas. Adapun mengingat kegagalan-kegagalan tersebut, Teheran telah dipaksa untuk fokus pada serangan siber yang memiliki potensi kerusakan fisik kecil. Teheran telah terlibat dalam upaya *spearphishing* terhadap lembaga akademis, pejabat keamanan nasional, diplomat, anggota Knesset, dan perusahaan kedirgantaraan Israel. Demikian pula, Iran secara umum telah menciptakan serangan siber yang sama persis dengan milik *American Israel*

Public Affairs Committee (AIPAC) dan telah menargetkan karyawan dari organisasi Yahudi liberal dan konservatif di Amerika Serikat, Israel dan di tempat lain (Anderson dan Karim, 2018: 34-35). 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.

1.2 Rumusan Masalah

Dari penjabaran latar belakang tersebut diperoleh pertanyaan penelitian berupa : 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?

1.3 Tinjauan Pustaka

Dalam tinjauan litelatur ini, peneliti mendapat kesulitan dalam menemukan litelatur-litelatur yang relavan dengan topik pembahasan penelitian. Hal tersebut dikarenakan keterbatasan sumber yang membahas mengenai tujuan dan strategi operasi siber ofensif yang dimiliki oleh sebuah negara. Meskipun demikian, dari sumber litelatur tersebut, peneliti berupaya mengkolaborasikannya sehingga

mampu mengarah pada kerangka pemikiran dengan menunjukkan tujuan dan strategi operasi siber ofensif yang dimiliki oleh berbagai negara didasarkan beberapa aspek.

1.3.1 Budaya Strategis dan Tujuan Perang Siber

Litelatur pertama yang peneliti tinjau yakni, *Strategic Culture and Cyberwarfare Strategies: Four case studies* oleh Gregory Rattray tahun 2018. Litelatur pertama ini mengkaji bagaimana budaya strategis mempengaruhi cara Rusia, Cina, Iran, dan Korea Utara membuat konsep, memahami, dan bertindak dalam dunia maya. Adapun litelatur ini juga menginformasikan kemampuan yang saat ini dimiliki keempat negara tersebut, pengembangan operasi siber ofensifnya, dan bagaimana mereka berencana untuk menggunakannya. Adapun budaya strategis yang digunakan adalah sejarah, geografi, politik, ekonomi, agama dan filsafat yang membentuk identitas suatu negara dan menciptakan respons keamanan nasional yang terstruktur secara konsisten digunakan untuk memungkinkan pemahaman yang lebih luas dan lebih dalam dari strategi siber ofensif masing-masing negara (Rattray, 2018)

Pada tulisannya dia menjelaskan bahwa budaya strategis Cina biasanya digambarkan dengan paradigma Konfusianisme dan Mencian yang menjunjung tinggi moral dalam segala hal dan paradigma *Parabellum* yang mengutamakan kekerasan sebagai sebuah solusi paling efektif. Keduanya seringkali bertentangan satu sama lain, namun dapat dikatakan bahwa kehadiran dunia maya menciptakan kendaraan baru yang mampu mendukung kedua paradigma budaya tersebut. Dalam hal ini, sebagai konsekuensi kedua budaya strategis tersebut, strategi siber

ofensif Tiongkok lebih difokuskan pada spionase, pencurian kekayaan intelektual, dan dominasi informasi. Hal ini karena sesuai dengan paradigma Konfusianisme dan Mencian yang menjunjung tinggi moral dalam segala hal, Tiongkok dalam strategi perang sibernya perlu menghindari kekerasan yang berkelanjutan. Akan tetapi disisi lainnya tetap menjunjung tinggi paradigma *Parabellum* yang menganggap kekerasan sebagai sebuah solusi paling efektif. Lalu dalam kasus ini, spionase, pencurian kekayaan intelektual, dan dominasi informasi dianggap sebagai sebuah bentuk kekerasan yang cocok karena sangat efektif untuk mencapai kepentinganya (Rattray, 2018: 24).

Lebih jauh dalam litelatur ini juga dijelaskan bahwa strategi perang siber Tiongkok saat ini juga terkait dengan permasalahan internasional yang dimiliki. Sebagai contoh terkait dengan inisiatif OBOR, lalu juga terkait dengan perselisihan di Tiongkok Selatan, konflik dengan Taiwan, perang dagang dengan Amerika Serikat. Di sisi lain, permasalahan-permasalahan Tiongkok tersebut juga dapat menjadi acuan tentang bagaimana kedepannya strategi perang siber Tiongkok diarahkan. Sebagai contoh semisal perang dagang dengan Amerika Serikat semakin meningkat, maka mungkin saja hal ini akan mempengaruhi pengambilan keputusan Tiongkok ketika mempertimbangkan serangan siber yang dapat berdampak secara negatif mempengaruhi atau berpotensi merusak infrastruktur ekonomi penting AS (Rattray, 2018: 35).

1.3.3 Kemampuan Operasi Siber Ofensif

Litelatur ketiga, yang peneliti ambil adalah *Cyber War: The Next Threat to National Security And What To Do About It* oleh Richard Clarke dan Robert

Knake tahun 2010. Litelatur ini berusaha mengkaji tentang kemampuan siber pada umumnya. Lebih lanjut, Richard A. Clarke yang merupakan seorang pakar keamanan komputer ternama dan sekalian seorang professor di *Harvard University* menjelaskan bahwa di era ini ada dua alasan kenapa kehadiran dunia maya ini sangat mempengaruhi konflik dan perang. Alasannya pertama adalah dunia maya dapat digunakan dengan mudah dan tanpa resiko yang besar. Salah satu permasalahan utama pada isu ini ada pada sistem dunia maya saat ini yang penggunaanya susah untuk dapat dikenali dan dikendalikan dengan mudah. Tidak adanya alat untuk mengindetifikasi pelaku penyerangan secara spesifik, serta ketiadaan hukum atau aturan yang cukup kuat. Secara tidak lansung hal ini membuat negara-negara dunia kesusahan untuk menghukum pelaku yang melakukan serangan siber. Terutama ketika serangan siber tersebut melibatkan sebuah negara, karena faktanya sebagian besar hukum siber sampai saat ini hanya berfokus pada kejahatan siber yang dilakukan oleh invidu atau kelompok organisasi tertentu. Selain itu tantangan besar lainnya bagi para profesional keamanan militer dan dimensi siber adalah bahwa serangan yang datang tidak dapat diprediksi, dan sekali lagi strategi pencegahan saat ini cenderung hanya efektif untuk memfasilitasi kejahatan siber yang dilakukan oleh sebuah invidu atau kelompok organisasi dan bukan sebuah negara (Rid dan McBurney, 2012).

Alasan kedua, menurutnya dunia maya mampu untuk menimbulkan kerusakan kolateral yang serius pada sebuah negara. Pada era dimana internet menjadi sebuah kebutuhan, sebagian besar aspek penting dalam kehidupan, baik pada aspek publik dan privat dikendalikan oleh internet. Sehingga jika suatu

negara terkena serangan siber, maka yang akan terkena dampaknya bukan cuman tentara atau perangkat militer sebuah negara, akan tetapi juga akan menjadi ancaman terhadap lumpuhnya sistem operasional negara dan juga menimbulkan korban sipil yang disebabkan oleh serangan siber. 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). Lebih buruk lagi adalah manipulasi opini publik dan hasil pemilihan yang tidak terlihat dengan menggunakan alat digital seperti iklan bertarget dan pemalsuan yang dalam rekaman dan video yang secara realistis dapat memanipulasi melalui kecerdasan buatan demi tujuan politik tertentu.

Dari ketiga litelatur yang berbeda tersebut, peneliti menggunakan litelatur pertama, yakni *Strategic Culture and Cyberwarfare Strategies: Four case studies* oleh Gregory Rattray tahun 2018. Hal ini karena litelatur pertama ini menjelaskan bagaimana tingkatan analisis diaplikasikan dalam kasus perang siber. Selain itu litelatur ini juga memberikan peneliti informasi yang berhubungan dengan topik tulisan penelitian, yakni dalam mengkaji tujuan operasi siber ofensif Iran terhadap situasi konfliktualnya melalui tingkatan analisis budaya strategis dan identitas suatu negara. Peneliti juga menggunakan litelatur kedua yang berjudul *North Korea's Cyber Operations* oleh Jenny Jun tahun 2018. Litelatur ini berusaha mengkaji tentang kemampuan dan strategi siber Korea Utara. Pada tulisannya ia mengatakan bahwa Korea Utara ini telah melakukan berbagai macam serangan

siber yang merusak. Terkait hal ini, menurut mereka secara historis Korea Utara telah mengandalkan berbagai strategi yang asimetris untuk menghindari kebuntuan militer konvensional. Adapun strategi dan kemampuan asimetris ini, peneliti implementasikan pada kasus tulisan ini, yang mana disini eksistensi dunia maya menjadi cara baru bagi Iran untuk mengeksploitasi kerentanan AS, Israel, dan Arab Saudi pada intensitas yang relatif rendah untuk mengganggu kedamaian atau status quo pada konflik tanpa khawatir kalau perang militer konvensional akan terjadi. Sebagai pelengkap penelitian ini, peneliti juga menggunakan litelatur ketiga untuk membantu menjelaskan hal-hal yang terkait dengan kepentingan dan strategi siber ofensif Iran.

1.3.2 Strategi Siber Ofensif Korea Utara

Litelatur kedua yang peneliti ambil berjudul *North Korea's Cyber Operations* oleh Jenny Jun tahun 2018. Litelatur ini berusaha mengkaji tentang kemampuan siber Korea Utara. Dalam tulisannya ia mengatakan bahwa Korea Utara ini telah melakukan berbagai macam serangan siber yang merusak. Sebagai contoh serangan siber terhadap *Sony Pictures Entertainment* tahun 2014 dan serangan terhadap bank dan agen media hiburan di Korea Selatan tahun 2013. Adapun serangan-serangan ini yang kemudian menimbulkan pertanyaan penting dalam tulisannya. Dalam tulisannya ia menanyakan tentang mengapa Korea Utara melakukan serangan-serangan ini, bagaimana Korea Utara dapat meluncurkan serangan-serangan ini, dan apa implikasinya bagi strategi dan kebijakan AS. Laporan ini berupaya menjawab pertanyaan-pertanyaan ini dengan pandangan *top-down* mengenai motivasi Korea Utara, serta struktur organisasi pemerintah

dan militernya. Ini juga memberikan analisis tentang bagaimana faktor-faktor ini mempengaruhi perilaku Korea Utara di dunia maya (Jun, 2018).

Lebih lanjut dalam tulisannya, dipaparkan bahwa pemahaman tentang strategi politik dan militer Korea Utara yang ada diperlukan untuk menilai strategi siber ofensif Korea Utara. Hal ini sehubungan dengan operasi siber ofensif yang harus dianggap sebagai perpanjangan dari strategi nasional sebuah negara. Dalam konteks ini menurut mereka, secara historis Korea Utara telah mengandalkan berbagai strategi yang asimetris untuk menghindari kebuntuan militer konvensional. Eksistensi dunia maya menjadi cara baru bagi Korea Utara untuk mengeksploitasi kerentanan AS dan Korea Selatan pada intensitas yang relatif rendah untuk mengganggu kedamaian atau status quo pada konflik tanpa khawatir kalau perang militer konvensional akan terjadi. Unsur terpenting dari strategi siber asimetris ini, Korea Utara tidak akan pernah melakukan serangan siber yang benar-benar merusak Amerika Serikat ataupun sekutu-sekutunya. Sebaliknya Korea Utara hanya akan berfokus pada serangan siber yang dampak kerusakannya kecil, namun disatu sisi tetap efektif. Hal ini dilakukan untuk menghidari kemungkinan terjadinya perang dengan Amerika Serikat dan sekutunya. Adapun meski strategi Korea Utara selalu berada pada intensitas rendah atau asimetris, dan mungkin tidak mengakibatkan kerusakan atau korban yang luas, tetapi serangan siber yang dilakukan sebenarnya juga berguna sebagai alat untuk menyampaikan ancaman kepada lawannya. Dalam hal ini Korea Utara menurut mereka secara rutin menyerang Amerika Serikat dan sekutunya demi tujuan untuk memberikan peringatan bahwa meski tidak dapat menghancurkan atau

mengalahkan lawan-lawannya, Korea Utara masih sanggup untuk menimbulkan kerusakan yang berarti bagi mereka melalui serangan siber. Dalam litelatur ini juga dipaparkan, serangan siber selain terbukti efektif sebagai sebuah perantara untuk merusak musuh, serangan siber nyatanya juga tidak terikat oleh hukum dan norma yang ada, sehingga membuat sulit Amerika Serikat dan sekutunya kesulitan mengatasi serangan siber Korea Utara. Dimana dengan kata lain, jika tidak ada serangan siber yang benar-benar dapat mengancam eksistensi Amerika Serikat dan sekutunya, dan juga tidak ada norma dan hukum yang benar-banar berfungsi untuk mengatasi serangan siber, maka secara logika tidak ada alasan bagi AS dan serkutunya untuk berperang dengan Korea Utara. Sebaliknya Amerika Serikat seharusnya atau secara terpaksa harus mengambil alternatif lain yang tidak menimbulkan kerusakan lebih dipihak mereka dan salah satunya adalah dengan memberikan subsidi pangan atau ekonomi yang menjadi kebutuhan atau tuntutan Korea Utara selama ini untuk dapat *survive* (Jun, 2018: 4-7).

1.4 Kerangka Pemikiran

Berdasarkan tinjauan pustaka dari berbagai litelatur yang telah peneliti paparkan di atas, peneliti menyimpulkan bahwa untuk menjawab pertanyaan rumusan masalah, maka perlu diketahui faktor pendorong dan faktor aksi. Akan tetapi sebelum itu, perlu diketahui dulu sifat dasar dunia maya, hal ini demi menggambarkan tampilan operasi siber ofensif Iran selama ini.

1.4.1 *Biological Metaphors*

Pemikiran pertama yang peneliti gunakan, berfungsi untuk mengetahui bagaimana sebenarnya aturan atau setidaknya hal-hal yang harus diperhatikan negara ketika berniat memanfaatkan dunia maya sewaktu konflik. Lalu juga kapabilitas dan kekurangan kemampuan siber Iran. Dalam hal ini, kerangka pemikiran pertama yang peneliti angkat adalah *biological metaphors*. *Biological metaphors* ini dipopulerkan oleh Sean Lawson (2012) yang merupakan seorang Asisten Profesor di Departemen Komunikasi di Universitas Utah. Menurutnya perang biologis dan bioterorisme adalah analogi yang paling tepat untuk menggambarkan dan menanggapi sikap negara dalam memutuskan strategi perang dan keamanan siber yang dimilikinya. Sean Lawson (2012) mengatakan bahwa melakukan serangan siber pada sebuah negara memiliki kelemahan yang mencolok dengan *bio-weapon*. Dalam hal ini dia mengutip perkataan dari Nixon pada tahun 1969 yang mengatakan bahwa "biological weapons were naturally resistant to the strategic aims of mutual deterrence and should be abandoned". Jika merujuk pada operasi siber ofensif maka dapat dilihat bahwa berdasarkan kerangka pemikiran ini, serangan siber seringkali tidak cocok dengan strategi dan kepentingan nasional suatu negara sewaktu konflik dan karena hal itu operasi siber ofensif dalam intesitas atau skala yang sangat merusak seringkali dipinggirkan.

Alasannya menurut Lawson (2012), program virus komputer memiliki efek dari serangan biologis yang tidak dapat diprediksi. Jika serangan biologis menurutnya terlalu responsif terhadap kondisi iklim dan lingkungan yang tidak

menentu, sehingga tidak peduli dengan batas-batas nasional dan cenderung menjadi bumerang bagi mereka yang menggunakannya. Maka tidak jauh berbeda dengan serangan siber yang penggunaanya tidak dapat dikendalikan dengan baik, sehingga sulit untuk mempertahankan batas antara sipil dan lingkungan militer, teman dan musuh, di sini dan di sana. Sebagai contoh hal ini dapat dilihat dari serangan virus Stuxnet. Stuxnet merupakan serangan siber yang disinyalir berhasil diciptakan oleh Amerika Serikat dan Israel pada tahun 2010. Stuxnet sampai saat ini juga dianggap merupakan salah satu serangan siber paling kontroversial di abad ke-21. Semakin hebatnya serangan Stuxnet itu mampu menonaktifkan pengayaan uranium nuklir Iran waktu itu. Karena hal tersebut, Iran kemudian terpaksa menghentikan operasi Natanz beberapa saat untuk mencegah kerusakan lebih besar sembari mencari penyebabnya. Cara kerja virus ini adalah dengan membuka lalu menutup katup yang memasok gas heksafluorida ke centrifuges, tanpa sepengetahuan operator yang mengoperasikannya. Akibat serangan ini, Iran mengalami banyak kerugian yang secara tidak lansung memaksa negara ini untuk berbenah di sektor kekuatan siber.

Pada dasarnya meski sukses memberhentikan pengadaan uranium nuklir Iran saat itu, kehadiran virus Stuxnet pada dasarnya bukan tanpa kekurangan. Virus Stuxnet ini penggunaannya tidak dapat dibatasi oleh negara pengembang, yakni Amerika Serikat dan Israel. Dimana karena hal itu, pada saat itu virus Stuxnet tidak hanya menyasar perangkat yang dituju, namun juga berbagai perangkat lain di Iran dan beberapa perangkat negara lainnya. Selain itu, meski efek penggunaan dari serangan siber ini dapat menimbulkan kerusakan kolateral yang serius pada

sebuah negara, sifatnya sebenarnya hanya dapat menunda, atau dengan kata lain Stuxnet tidak lebih dari hanya memberikan kerusakan sesaat saat konflik. Hal ini dapat dilihat dari jumlah uranium nuklir Iran yang saat ini bahkan telah mencapai jumlah sepuluh kali lipat sebelum serangan Stuxnet ini dilakukan. Adapun karena hal itu, seperti halnya serangan biologis, penggunaan Stuxnet ini dapat menjadi boomerang, karena serangan biologis dan serangan siber nyatanya meningalkan jejak dan jejak tersebut dapat menghasilkan teknologi baru bagi musuh yang telah diserang. Sampel dari "patogen" (biologis atau digital) dapat dikumpulkan, dianalisis, dimateraikan lebih lanjut, atau digunakan untuk membuat penawarnya. Bahkan ketika serangan mencapai target yang dituju, seringkali kekuatan untuk menyerang tadi tidak hanya dimiliki oleh negara yang diserang, tetapi juga untuk pihak ketiga. Dengan demikian, kode Stuxnet sekarang tersedia untuk diunduh di Internet oleh kelompok negara dan non-negara. Lalu kode Stuxnet yang bentuknya dapat menimbulkan kerusakan kolateral yang serius terhadap Iran ini pada dasarnya dapat kemudian digunakan terhadap Israel dan AS. Dengan Stuxnet, tampaknya Israel dan Amerika Serikat telah mempromosikan apa yang ingin dihindari dalam kasus perang biologis, yaitu penyebaran mode peperangan yang baru dan sulit dikendalikan ke aktor negara dan non-negara (Lawson, 2012).

Dengan bantuan penggunaan *biological metaphors* ini, peneliti menemukan bahwa berdasarkan penggambaran bagaimana perang biologis dan bioterorisme bekerja, penggunaan serangan siber pada sebuah negara memiliki kelemahan yang mencolok dengan bio weapon. Dalam hal ini, virus biologis dan virus siber penggunaanya tidak dapat dikendalikan dengan baik, sehingga sulit untuk

mempertahankan batas antara sipil dan lingkungan militer, teman dan musuh, di sini dan di sana. Selain itu, seperti halnya serangan biologis, penggunaan serangan siber dapat menjadi boomerang, karena penyerangan dengan dengan serangan biologis dan serangan siber nyatanya meningalkan jejak dan jejak tersebut dapat menghasilkan teknologi baru bagi musuh yang telah diserang.

1.4.2 Tingkatan Analisis Identitas Nasional

Sebagaimana yang dipaparkan oleh Anne L. Clunan (2009:3), pada dasarnya identitas nasional suatu negara dapat menentukan kepentingan nasional yang mana kemudian akan menjadi patokan pembuatan kebijakan luar negeri bagi negara itu sendiri. Dengan memahami identitas nasional, pembuat keputusan akan lebih mudah mengidentifikasi kekuatan dan kepentingan negaranya hingga potensi, bahkan ancaman sesungguhnya yang sedang dihadapi negaranya. Berdasarkan tinjauan pustaka, penarikan tingkatan analisis harus dimulai dari sejarah politik luar negeri dan militer negara tersebut. Sehingga dengan kata lain penjelasan identitas nasional Iran terkait sejarah politik luar negeri dan militer negara tersebut, secara tidak lansung akan ikut menjelaskan kebijakan atau pengambilan keputusan Iran terkait operasi siber ofensifnya terhadap Amerika Serikat, Israel, Arab Saudi. Adapun meski identitas nasional harus ditarik dari sisi sejarah atau pengalaman masa lampau, menurut pandangan konstruktivisme aspirasional, identintitas nasional juga harus mempertimbangkan masa sekarang. Hal ini karena pada beberapa sisi tertentu, identitas yang dimiliki sebuah negara berubah atau setidaknya mengalami transformasi.

Adapun identitas nasional dapat dilihat dari segi internal maupun eksternal. Dilihat dari segi internal, identitas nasional yang kemudian menjadi kepentingan nasional ini tidak terbentuk dengan sendirinya, namun muncul karena adanya interaksi antara struktur sosial dan peranan manusia sebagai agen. Dengan kata lain ada proses yang melibatkan aktor-aktor tertentu yang memegang kekuasaan, agar identitas ini ada lalu kemudian diterima menjadi kepentingan nasional. Sementara itu dari faktor eksternal, identitas nasional menyangkut mengenai pandangan negara lain terhadap suatu negara. Dalam hal ini, pandangan masyarakat internasional diyakini dapat menjadi sebuah cara untuk melihat identitas nasional negara lain (Clunan, 2009:23). Adapun baik itu dari segi internal maupun eksternal, identitas nasional seringkali dipersepsikan berdasarkan kesamaan-kesamaan tertentu dari segi objektif, seperti geografis, ekologis, dan demografis. Lalu subjektif, yaitu faktor historis, sosial, politik, dan kebudayaan (Suryo, 2002).

Lebih jauh, Hudson (2014) mengemukakan tentang beberapa metode dalam menganalisis identitas nasional dan budaya terkait kebijakan luar negeri. Metode pertama yang dia tawarkan adalah dengan melakukan investigasi kultural. Metode ini meliputi analisis identitas nasional berdasarkan sejarah negara tersebut. Lalu, kemudian dikaitkan dengan faktor internal atau eksternal negara tersebut. Dengan kata lain, bisa dilihat dari bagaimana masyarakat negara itu menyepakati sejarah tersebut sebagai identitas nasional, yang mana dalam hal ini dapat dari internal atau elit politik negara tersebut atau bahkan dari persepsi masyarakat internasional atau faktor eksternal. Metode kedua yang ditawarkannya adalah *hearing of*

congressional committees. Metode ini dilakukan dengan mengumpulkan dan menganalisis pernyataan-pernyataan yang disampaikan oleh para elit politik negara yang membuat keputusan. Pernyatan-pernyataan yang disampaikan oleh pejabat tinggi negara itu pun dapat diperoleh melalui pidato maupun wawancara (Hudson, 2014:119).

1.4.3 Tingkatan Analisis Individu

Fokus penelitian menggunakan tingkatan analisis individu berpusat pada manusia sebagai aktor pengambil keputusan sebuah negara, yang mana oleh karena itu dibutuhkan pemahaman mengenai faktor-faktor yang mempengaruhi pengambilan kebijakan seorang individu. Dalam hal ini, perlu diketahui bahwa Individu yang dimaksud dalam tingkatan analisis ini adalah pemimpin atau pembuat kebijakan dalam suatu negara, sehingga analisis tingkatan 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 tingkatan individu melihat bahwa pemimpin dalam merumuskan dan memutuskan suatu kebijakan pasti selalu didasarkan pada kepentingan nasional negaranya (Neack, 2008). Adapun fokusnya terletak pada bagaimana pemimpin atau individu yang mengambil keputusan ini membuat dan mengimplementasikan kepentingan nasional ke dalam bentuk kebijakan negara yang ia pimpin, persepsi dan mispersepsi apa yang dimiliki, cara interaksi individu tersebut dengan kelompok kecil hingga teratas, dan sebagainya (Neack 2008, 10).

Hal ini sesuai dengan pendapat Breuning (2007), yakni penelitian tingkatan analisis individu harus dimulai melalui karakteristik pribadi dari seorang pemimpin meliputi cara berpikir (kapabilitas) maupun persepsi dalam menghadapi isu turut mempengaruhi proses pembuatan kebijakan luar negeri. Adapun perlu dipastikan terlebih dahulu kecocokan model pengambilan kebijakan yang terpusat pada elit petinggi negara dengan isu yang ada, agar dapat menggunakan peringkat analisis individu. Dalam kasus Iran, sosok *supreme leader*, yakni Ali Khamenei dapat menjadi acuan yang begitu jelas untuk mengkaji kebijakan 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. Lebih lanjut, pada dasarnya, Breuning (2007, 45) membagi tiga strategi atau metode yang dapat digunakan untuk menganalisis tingkatan analisis individu, yaitu *presidential character, operational code, dan leadership traits analysis*. Metode *presidential character* lebih mengarah pada analisis karakter presiden atau pemimpin negara tersebut. Dengan metode ini akan dilihat apakah sosok pemimpin ini aktif atau pasif dalam mengeluarkan kebijakan luar negerinya. Metode kedua, yakni *operational code* lebih berusaha untuk menganalisa apa yang sedang dipikirkan oleh pemimpin negara tersebut. Terakhir, yakni *leadership traits analysis* adalah metode peringkat analisis individu, yang berfokus pada penelitian bertujuan untuk menganalisa kemampuan individu dalam kehidupan politik negaranya, terutama dalam menangani isu-isu politik luar negeri. Pendekatan *leadership trait analysis*

ini lebih berfokus pada kehidupan politik pemimpin, yang mana cerminan dari kehidupan politik tersebut tertuang dalam sisi kualitatif dan interpretasi akan pidato maupun tulisan komentar informal dalam sebuah wawancara (Breuning 2007, 38).

1.4.4 Strategi *Deterrence Active*

Selanjutnya, kerangka pemikiran keempat adalah strategi *deterrence active*. Peneliti menggunakan kerangka pemikiran ini untuk menggambarkan salah satu fungsi serangan siber, yakni untuk mencegah perang konvesional. Dalam bukunya *Cyber Deterrence* dan *Cyber War*, Martin Libicki memaparkan dua jenis *deterrence,* yakni *deterrence passive* (kemampuan untuk menggagalkan serangan) dan *deterrence active* (ancaman pembalasan). Adapun dalam kasus ini, peneliti menggunakan konsep *deterrence active*. Dari perspektif dunia maya, *deterrence active* merujuk pada tindakan yang diambil untuk mengamankan jaringan siber dari serangan dengan cara mengancam akan melakukan balas dendam atau semacam respons 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.* Berdasarkan sejarah, senjata nuklir merupakan senjata pemusnah massal terkuat yang pernah diciptakan, hal ini terlihat dari perannya sewaktu perang dunia kedua. 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 akan terjadi pada perang nuklir, karena disamping tidak akan ada yang bisa menebak 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. Dalam hal ini nuklir diasumsikan sebagai kekuatan tersebut, sehingga menimbulkan asumsi bahwa ketika sebuah negara menyerang negara lain yang juga punya senjata nuklir, maka ia akan mendapat balasan senjata nuklir juga. Adapun karena keyakinan dan ketakutan tersebut, negara-negara yang biasanya sama-sama memiliki kekuatan nuklir, akan menolak untuk berperang satu sama lain. Hal ini dikarenakan bahaya nuklir itu sendiri yang pada akhirnya akan 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 serangan 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 serangan nuklir, serangan siber dapat digunakan 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 serangan. 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. Lebih jauh, McKenzie (2017: 3) memaparkan tujuh atribut yang mengarah pada strategi *deterrence* yang sukses.

Tabel 2 : Atribut Strategi Pencegahan

Deterrence attribute	Definition
Interest	A state employs a deterrence strategy to protect an interest.
Deterrent declaration	To keep adversaries from attacking the interest, a state makes a deterrent declaration: Do not do this, or else that will happen. This is any adversary action that threatens the interest, and that includes either denial measures, penalty measures, or both.
Credibility	Credibility is the attacker's calculation of the defender's capability and intent to carry out the deterrent declaration. For other states to take a deterrent declaration seriously, the declaration must be credible and believable.
Fear	If a potential adversary fears the denial or penalty measures, that actor is less likely to take an undesirable action.
Denial measures (passive measures)	Denial is the defensive aspect of deterrence and consists of prevention and futility. Deterrence by prevention means that if an attack is launched, the defensive measures will disrupt the attack to keep it from succeeding. Deterrence by futility means that even if an attack breaches defenses, it will not have its desired effect on the target.
Penalty measures (active measures)	Penalty is the offensive aspect of deterrence and consists of retaliation. Classical deterrence theory demands that penalty measures be certain, severe, and immediate.
Cost-benefit calculation	What are the benefits and costs of action versus the benefits and costs of restraint?

Sumber: *Timothy M. McKenzie*

Jika melihat tabel dua tersebut, ketujuh atribut yang diperlukan adalah kepentingan yang harus dilindungi, deklarasi pencegahan atau peringatan yang harus keras dan jelas, kredibilitas untuk melakukan serangan balasan, memproduksi ketakutan, tindakan pencegahan dampak terburuk, tindakan penalti ketika telah diserang, dan perhitungan biaya dengan manfaat ketika akan melakukan serangan. Berdasarkan ketujuh atribut tersebut, peneliti mengakaitkannya dengan jejak serangan siber ke Amerika Serikat, Israel dan Iran. Hal ini demi tujuan untuk melihat kesesuain operasi siber ofensif Iran dengan strategi *deterrence active*.

1.4.5 Strategi Siber Asimetris Korea Utara

Kerangka pemikiran terakhir adalah strategi siber asimetris Korea Utara. Peneliti menggunakan kerangka pemikiran ini untuk menggambarkan salah satu strategi siber ofensif yang dapat digunakan sebuah negara untuk memproleh keuntungan dari pemanfaatan dunia maya dalam sebuah konflik. Pada dasarnya strategi asimetris tidak hanya terikat pada operasi siber ofensif, namun juga mencakup senjata nuklir, senjata konvensional seperti artileri dan dengan cara-cara lainnya yang pada dasarnya memanfaatkan kerentanan atau kelemahan lawan. Adapun Korea Utara semakin mengandalkan strategi militer asimetris selama beberapa tahun terakhir, sebagian besar dari senjata nuklir. Akan tetapi hal ini semakin sulit untuk dilakukan di masa ini, karena tekanan dan kritikan secara luas oleh komunitas internasional dan dibentuknya aturan-aturan khusus mengenai kepemilikan nuklir Korea Utara. Sehingga dalam hal ini, serangan siber menjadi salah satu opsi paling masuk akal untuk mengeksploitasi kerentanan dari negara-

negara lain. Serangan Siber dalam konteks ini secara efektif menggantikan atau, setidaknya, menambah kemampuan provokatif yang ada karena sifatnya yang sulit untuk dilacak dan dibalas baik dari aspek hukum atau serangan siber lainnya. Serta efek merusak yang tidak jauh berbeda dengan senjata nuklir, tetapi dengan biaya yang relatif rendah dan risiko operasional yang jauh lebih kecil dari senjata nuklir. Kejahatan, spionase, sabotase, dan paksaan semua dapat dilakukan melalui dimensi siber, dengan pelatihan dan infrastruktur yang tepat. Dimensi siber memiliki kemampuan untuk mengganggu atau menghancurkan satu atau lebih elemen yang terdapat pada dunia maya, termasuk informasi, perangkat lunak, dan infrastruktur fisik (Jun, 2018: 4-7).

Aspek penting dalam strategi siber asimetris Korea Utara ini adalah penggunaan atau pemanfaatan dimensi siber pada saat masa damai atau status quo di suatu konflik. Status quo di suatu konflik disini merujuk pada suatu kondisi konflik dimana aktor-aktor yang terlibat melalukan penangguhan permusuhan atau gencatan senjata untuk jangka waktu tertentu, guna melakukan suatu pekerjaan yang tidak boleh diganggu. Merujuk pada strategi asimetris, strategi ini ditujukan sebagai media bagi Korea Utara untuk menggantikan perang konvensional yang berpotensi merusak masa damai disuatu konflik. Operasi siber ofensif layaknya yang dilakukan oleh Korea Utara ini penting dilakukan bukan demi memenangkan konflik, tetapi untuk melemahkan kemauan musuh untuk melakukan perang konvensional dengan gangguan, kehancuran, kelelahan, atau paksaan. Untuk kekuatan militer yang lebih lemah seperti Korea Utara, mengandalkan strategi siber asimetris untuk melawan kekuatan konvensional

musuh adalah pilihan yang sangat tepat. Hal ini karena selain operasi siber ofensif relatif hemat dari segi biaya dan juga memiliki risiko kegagalan yang lebih rendah, serangan siber juga sangat efektif untuk mengeksploitasi kerentanan musuh yang signifikan. Mereka dapat digunakan sebagai paksaan atau sebagai bagian dari operasi ofensif yang lebih besar (Jun, 2018).

Peneliti menggunakan kerangka teori pertama untuk menjelaskan kemampuan dan batasan operasi siber ofensif yang digunakan oleh Iran. Adapun berdasarkan kemampuan dan kelemahan ini, peneliti menggunakannya sebagai sebuah landasan untuk menjawab tujuan dan strategi siber ofensif Iran. Lebih lanjut, melalui kerangka pemikiran kedua dan ketiga, peneliti mengakaji tujuan atau kepentingan nasional Iran terkait serangkaian serangan siber yang dilakukan negara ini dari tahun 2010 sampai 2018. Berdasarkan tujuan ini, peneliti mengunakan kerangka teori keempat dan kelima untuk mengkaji strategi operasi siber ofensif Iran. Dalam hal ini, kerangka pemikiran keempat dapat menggambarkan salah satu fungsi serangan siber, yakni untuk menakut-nakuti ketiga negara tersebut. Sedangkan kerangka pemikiran kelima, memberitahu bahwa serangan siber dapat digunakan sebagai alat untuk membantu negara yang lebih lemah dalam melakukan perang asimetris.

1.5 Hipotesis Penelitian

Peneliti melihat bahwa strategi operasi siber ofensif Iran saat ini dilakukan bukan demi memenangkan konflik, tetapi tujuannya adalah untuk melemahkan kemauan musuh dalam melakukan perang konvensional dan mempertahankan

status quo dengan menganggu, menghancurkan, meletihkan, atau memaksa. Iran dalam situasi konfliktualnya juga menggunakan strategi yang sama dengan Korea Utara, yakni strategi siber asimetris. Strategi ini ditujukan sebagai media bagi Iran untuk menggantikan perang konvensional yang berpotensi merusak masa damai disuatu konflik. Hal ini karena perang konvensional hanya akan membuat Iran mengalami kekalahan. Sehingga dengan begitu, akan jauh lebih baik menggunakan serangan siber dalam skala kecil yang sifatnya asimetris. Akan tetapi meskipun begitu, potensi bahwa Iran akan menggunakan serangan siber skala besar tidak bisa dihindarkan begitu saja, terutama dalam situasi terdesak. Adapun menurut peneliti, hal ini dengan cerdas dimanfaatkan oleh Iran menggunakan strategi *deterrence active* dengan tujuan untuk menimbulkan keyakinan dan ketakutan yang sama pada perang nuklir, yakni bahwa Iran akan menyerang dengan kekuatan yang sama atau bahkan lebih besar jika ada negara yang mengancam esksistensi negaranya.

1.6 Metode Penelitian

1.6.1 Defenisi dan Operasionalisasi Konsep

1.6.1.1 Operasi Siber Ofensif Iran

Australian Strategic Policy Institute (n,d) mendefinisikan operasi siber ofensif sebagai operasi yang dilakukan untuk mendapatkan kepentingan tertentu dengan memanipulasi, menyangkal, mengganggu, menurunkan, atau menghancurkan komputer, sistem informasi atau jaringan yang ditargetkan. Berdasarkan hal ini, maka dapat dilihat bahwa semua operasi siber ofensif Iran

kepada Amerika Serikat, Israel, dan Arab Saudi ditujukan demi kepentingan nasional tertentu yang ingin dicapai Iran.

1.6.1.2 Mempertahankan Status Quo

Secara definisi, menurut Badan Pengembangan Bahasa dan Perbukuan (n.d), status quo berasal dari bahasa Latin, yang mana artinya adalah 'keadaan tetap sebagai-mana keadaan sekarang atau sebagaimana keadaan sebelumnya'. Jadi, mempertahankan status quo berarti mempertahankan keadaan sekarang yang tetap seperti keadaan sebelumnya. Dalam penelitian ini, mempertahankan status quo dengan gangguan, kehancuran, kelelahan, atau paksaan penting dilakukan oleh Iran karena negara ini pada akhirnya tidak atau masih belum dapat mengakomodasi kepentingan nasional yang telah dibentuk oleh elit politik negara ini sebagai identitas nasional, yaitu negara yang kuat, pemimpin yang dominan, kemampuan militer yang kuat, dan menjadi pemain penting dalam struktur dunia. Sehingga pada akhirnya, Iran terjebak pada sebuah situasi dimana Iran tidak dapat menyerah karena identitas nasional sebagai negara kuat dan yang merupakan pihak yang benar telah tertanam sejak lama. Lalu di satu sisi, Iran juga tidak dapat berperang secara diplomatik dan berperang secara konvensional, sebab negaranya sendiri tidak memiliki kapabilitas untuk menang. Adapun hal ini dapat diamati dari analisis kebijakan *supreme leader,* yakni Ali Khamenei. Dalam hal ini, Khamenei yang sudah berulang kali menggunakan kemampuan ofensif yang hanya bertujuan melukai dan melemahkan niat lawannya untuk melakukan perang konvesional. Sebagai contoh, Iran lebih memilih mengembangkan rudal balistik

antar benua, alih-alih mengembangkan angkatan udara konvensional yang kemampuan merusaknya lebih kecil.

1.6.1.3 Strategi Siber Ofensif Iran

Secara sederhana, menurut Kamus Besar Bahasa Indonesia (KBBI), strategi adalah ilmu dan seni menggunakan semua sumber daya bangsa untuk melaksanakan kebijaksanaan tertentu dalam perang dan damai. Merujuk pada hal ini, siber merupakan sumber daya bangsa yang digunakan dalam strategi Iran untuk mendapatkan kepentingannya, yakni mempertahankan status quo. Adapun strategi tersebut adalah, strategi siber asimetris Korea Utara dan strategi siber *deterrence active*. Dalam hal ini, yang menjadi faktor kunci strategi siber asimetris adalah merusak untuk mengurangi niat lawan untuk berperang. Sedangkan dalam strategi *deterrence active*, penggunaan ancaman dan melakukan pembalasan menjadi faktor utama yang digunakan Iran untuk mencapai kepentigan dari operasi ofensif siber Iran selama ini.

1.6.2 Tipe Penelitian

Berdasarkan kerangka pemikiran dan rumusan masalah yang diajukan, tipe penelitian yang digunakan adalah eksplanatif yang bertujuan untuk menjelaskan fenomena dan menjelaskan kepentingan dan strategi Iran dalam melakukan operasi siber ofensif terhadap AS, Israel, dan Arab Saudi.

1.6.3 Ruang Lingkup dan Jangkauan Penelitian

Ruang lingkup penelitian ini mencakup berbagai jenis operasi siber ofensif yang dilakukan oleh Iran kepada Amerika Serikat, Israel, dan Arab Saudi dari tahun 2010 sampai 2018. Hal ini karena Iran aktif melakukan operasi siber ofensif

pasca serangan virus Stuxnet tahun 2010 yang merupakan serangan siber terakhir yang ditujukan untuk merusak infrastruktur negaranya. Pasca serangan ini, Iran mulai melakukan berbenah diberbagai sektor siber, termasuk melakukan operasi siber ofensif pertama ke Amerika Serikat di tahun 2010. Meskipun begitu, peneliti disini tidak menutup kemungkinan untuk memasukkan data-data penelitian sebelum tahun 2010 jika memiliki kaitan dengan topik pembahasan penelitian.

1.6.4 Teknik Pengumpulan Data

Metode pengumpulan data yang digunakan adalah dengan studi literatur dokumen primer maupun sekunder. Sumber primer yang dimaksud adalah pernyataan resmi dari pemerintah Iran yang dikumpulkan melalui situs resmi kantor berita resmi Iran, pidato serta peryataan dari *supreme leader* dan penjabat resmi pemerintahan Iran lainnya. Sumber sekunder berasal dari artikel, buku, jurnal ilmiah, data statistik, artikel online, dan berita online yang tidak bersumber dari pemerintah Iran, namun yang mempunyai korelasi terhadap identifikasi permasalahan yang diangkat dalam topik penelitian ini.

1.6.5 Teknik Analisis Data

Dalam membuktikan hipotesis dan menjawab rumusan masalah, peneliti menggunakan teknik analisis kualitatif. Teknik ini menekankan kepada interpretasi peneliti dengan data dari sumber-sumber yang telah dikumpulkan. Analisis interpretasi tersebut kemudian akan disusun sebagai hasil penelitian yang menjelaskan seperti apa kepentingan dan strategi operasi siber ofensif Iran terhadap AS, Israel, dan Arab Saudi.

1.6.6 Sistematika Penulisan

Penelitian ini terbagi menjadi empat bagian. Bagian pertama terdiri dari pendahuluan yang mencakup latar belakang masalah, rumusan masalah, tujuan penelitian, tinjauan pustaka, kerangka teori, hipotesis dan metodologi penelitian. Bagian kedua dan ketiga berisi tentang karakteristik sasaran penelitian dalam bentuk deskripsi atau narasi. Lalu berisi tentang jawaban pertanyaan penelitian sebagaimana yang dirumuskan dan menguji hipotesis yang telah peneliti sebutkan sebelumnya, dengan menggunakan teknik analisis kualitatif pada tataran level empiris variabel identitas nasional, level analisis individu dan analisis kebijakan peran siber yang telah dilakukan oleh Iran sebagai langkah strategis terkait konflik yang sedang dialaminya. Adapun pada bagian kedua, penelitian ini terdiri dari analisa dan interpretasi data terkait tujuan dan kepentingan dari operasi siber ofensif Iran. Tujuan dari deskripsi ini agar pembaca mendapatkan gambaran yang jelas tentang kenapa Iran harus menggunakan strategi siber ofensif itu dan kenapa serangan siber dalam bentuk itu dilakukan. Sedangkan dibagian ketiga penelitian ini, peneliti menganalisa dan melakukan interpretasi data terkait strategi siber ofensif Iran. Peneliti menggunakan analisa dan interpretasi data bab dua penelitian ini dan menghubungkannya dengan strategi siber ofensif yang kemungkinan digunakan oleh Iran, yakni strategi siber ofensif asimetris Korea Utara, dan strategi *deterrence active* nuklir yang kemungkinan dapat menggambarkan strategi siber ofensif Iran saat ini. Terakhir, bagian keempat berisi tentang kesimpulan, yang mana mencakup temuan-temuan pokok sebagai jawaban pertanyaan penelitian dan juga temuan-temuan berupa proposisi, teori dan atau penajaman konsep-konsep baru.

BAB II

KEPENTINGAN ATAU TUJUAN

DARI OPERASI SIBER OFENSIF IRAN

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. Pada dasarnya dalam mengetahui kepentingan Iran tersebut, peneliti menggunakan dua tingkatan analisis, yakni identitas nasional dan individu.

2.1 Identitas Nasional Sebagai Alasan Iran untuk Mempertahankan Status Quo

Sebagaimana yang dipaparkan oleh Anne L. Clunan (2009:3), pada dasarnya identitas nasional suatu negara dapat menentukan kepentingan nasional yang mana kemudian akan menjadi patokan pembuatan kebijakan luar negeri bagi

negara itu sendiri. Dengan memahami identitas nasional, pembuat keputusan akan lebih mudah mengidentifikasi kekuatan dan kepentingan negaranya hingga potensi, bahkan ancaman sesungguhnya yang sedang dihadapi negaranya. Seperti yang telah peneliti paparkan sebelumnya, penarikan tingkatan analisis Iran dalam penelitian ini harus dimulai dari sejarah politik luar negeri dan militer negara tersebut. Sehingga dengan kata lain penjelasan identitas nasional Iran terkait sejarah politik luar negeri dan militer negara tersebut, secara tidak lansung akan ikut menjelaskan kebijakan atau pengambilan keputusan Iran terkait operasi siber ofensifnya terhadap Amerika Serikat, Israel, Arab Saudi. Hal ini dilakukan karena serangan siber sendiri merupakan perpanjangan dari strategi nasional sebuah negara. Terlebih lagi data mengenai atribut perang siber atau bahkan keamanan dan pertahanan siber Iran tidak pernah dipublikasikan secara resmi sepanjang sejarah negara ini.

Lebih jauh, Hudson (2014) mengemukakan tentang beberapa metode dalam menganalisis identitas nasional dan budaya terkait kebijakan luar negeri. Metode pertama yang dia tawarkan adalah dengan melakukan investigasi kultural. Metode ini meliputi analisis identitas nasional berdasarkan sejarah negara tersebut. Lalu, kemudian dikaitkan dengan faktor internal atau eksternal negara tersebut. Dengan kata lain, bisa dilihat dari bagaimana masyarakat negara itu menyepakati sejarah tersebut sebagai identitas nasional, yang mana dalam hal ini dapat diliat dari internal atau elit politik negara tersebut atau bahkan dari persepsi masyarakat internasional atau faktor eksternal (Hudson, 2014:119). Berhubungan dengan hal ini, dilihat dari sisi sejarah politik luar negeri dan militer Iran, identitas nasional

negara ini adalah negara yang kuat, pemimpin yang dominan, kemampuan militer yang kuat, dan sebagai pemain penting dalam struktur dunia. Hal ini tidak terlepas dari sejarah negara ini yang pernah menjadi pusat peradaban utama dan kekuatan regional hegemonik di masa lampau. Sebagai contoh sejarah panjang peradaban dan kekaisaran Persia yang manyoritas penduduknya adalah orang Iran. Adapun semangat ini dibangkitkan kembali di era ini, dimana Iran ingin sekali lagi menjadi kekuatan regional hegemonik di kawasan Timur Tengah. Terlihat dari kebijakan luar negeri Iran dan kegiatan militernya secara umum, dan kegiatan perang siber khususnya yang banyak diantaranya menargetkan musuh-musuh regionalnya, seperti negara-negara Teluk Arab. Selain itu, perannya yang dianggap sebagai pemimpin "Sumbu Perlawanan" (ke Israel) telah menyalurkan kebijakan luar negeri Iran dan kegiatan militernya yang agresif terhadap AS dan sekutu Barat di wilayah tersebut.

Lebih lanjut, identitas nasional yang kemudian menjadi kepentingan nasional ini tidak terbentuk dengan sendirinya, namun muncul karena adanya interaksi antara struktur sosial dan peranan manusia sebagai agen. Dengan kata lain ada proses yang melibatkan aktor-aktor tertentu yang memegang kekuasaan, agar identitas ini ada, lalu kemudian diterima menjadi kepentingan nasional. Iran dalam kasus ini menggunakan sejarah historis, budaya, dan karakteristik negaranya menjadi identitas nasional. Lalu kemudian mengangkatnya ke masyarakat bahwa mereka adalah korban, dan pada akhirnya menggunakannya sebagai justifikasi untuk memulai konflik dengan AS, Israel, dan Arab Saudi. Hal ini dapat dibuktikan dari metode keduanya Hudson (2014: 119). Metode kedua

yang ditawarkannya adalah *hearing of congressional committees*. Metode ini dilakukan dengan mengumpulkan dan menganalisis pernyataan-pernyataan yang disampaikan oleh para elit politik negara yang membuat keputusan. Pernyatan-pernyataan yang disampaikan oleh pejabat tinggi negara itu pun dapat diperoleh melalui pidato maupun wawancara. Sebagai contoh hal ini dapat dilihat dari argumen *supreme leade*r Iran pertama, yakni Ayatollah Ruhollah Khomeini yang mendeklarasikan bahwa budaya barat dan ide-ide barat sebagai sesuatu yang buruk dan menakutkan. Hal ini dapat dikutip dari artikel yang dipublikasikan oleh *The New York Times* pada 7 Oktober 1979. Artikel ini memuat wawancara Oriana Fallaci, jurnalis Italia yang terkenal karena wawancara provokatifnya dengan para pemimpin dunia dan salah satunya adalah Ayatollah Ruhollah Khomeini. 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 mendungkung 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 mereka 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 yang 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 konteks 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. Adapun fenomena-fenomena tersebut sekali lagi terjadi sebagai akibat dari sanksi ekonomi terhadap Iran yang ditujukan untuk menekan Iran dan pengaruhnya di bidang ekonomi di kawasan Timur Tengah (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 pilihanya 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.

2.2 Kebijakan Politik Khamenei: Kepentingan Operasi Siber Ofensif Iran

Hasil analisis identitas nasional sejalan dengan tingkatan analisis individu yang menunjukkan bahwa keputusan Iran untuk menggunakan serangan siber ofensif tidak terlepas dari fakta bahwa Iran ingin mempertahankan status quo dan menghindari perang konvensional dengan menggunakan serangan siber asimetris yang mereka punya. 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). Terutama dalam kasus Iran, sosok *supreme leader*, yakni 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. Dengan kata lain, meskipun Ali Khamenei tidak membuat keputusan nasional sendiri, tidak ada keputusan Iran yang dapat diambil tanpa persetujuannya. Seorang *supreme leader* di Iran memiliki kekuasaan yang tidak dapat diganggu gugat, sebagian besar kebijakan penting Iran diputuskan olehnya dan lembaga lainnya bergerak sesuai arahanya. Dimana karena hal itu peneliti yakin bahwa kebijakan siber Iran selama ini juga menjadi bagian dari keputusannya Ali Khamenei (Sadjadpour, 2010).

Lebih lanjut, pada dasarnya, Breuning (2007, 45) membagi tiga strategi atau metode yang dapat digunakan untuk menganalisis tingkatan analisis individu, yaitu *presidential character, operational code, dan leadership traits analysis*. Pada tulisan ini, peneliti memilih untuk menggunakan metode *leadership traits analysis*. Metode ini adalah peringkat analisis individu, yang berfokus pada penelitian bertujuan untuk menganalisa kemampuan individu dalam kehidupan politik negaranya, terutama dalam menangani isu-isu politik luar negeri. Pendekatan *leadership trait analysis* ini lebih berfokus pada kehidupan politik

pemimpin, yang mana cerminan dari kehidupan politik tersebut tertuang dalam sisi kualitatif dan interpretasi akan pidato maupun tulisan komentar informal dalam sebuah wawancara (Breuning 2007, 38). Seperti yang telah peneliti paparkan sebelumnya, penarikan tingkatan analisis Iran dalam penelitian ini harus dimulai dari sejarah politik luar negeri dan militer negara tersebut. Sehingga perlu diketahui terlebih dahulu kebijakan *supreme leader* Iran dalam menangani isu-isu politik luar negeri dan militer negaranya.

Ketergantungan Iran pada status quo ditengah konflik yang sedang dialaminya telah dibentuk sejak lama. Berdasarkan sejarahnya, Iran dibawah pemerintahannya Ali Khamenei sudah berulang kali menggunakan kemampuan ofensif yang hanya bertujuan melukai dan melemahkan niat lawannya untuk melakukan perang konvesional. Adapun hal ini dapat dilihat pada contoh kasus dimana Iran membeli sistem senjata konvensional yang pada dasarnya tujuannya hanya untuk mengeksploitasi kerentanan lawan-lawan regionalnya. Adapun langkah ini diambil sebagai hasil dari sanksi Amerika Serikat, sehingga Iran tidak mendapatkan teknologi senjata konvensional yang canggih, seperti lawan regionalnya Arab Saudi. Sebagai contoh, Iran lebih memilih mengembangkan rudal balistik antar benua, alih-alih mengembangkan angkatan udara konvensional yang kemampuan merusaknya lebih kecil. Lalu, alih-alih mengembangkan kemampuan angkatan laut tradisional yang kuat, seperti kepemilikan kapal-kapal perang besar, Iran untuk menghemat pengeluaran militer lebih memilih untuk mengandalkan kawanan speedboat kecil yang cepat menyerang. Alih-alih pasukan darat konvensional yang pada dasarnya membutuhkan pendanaan yang banyak,

meliputi gaji bulanan, tunjangan, dan biaya-biaya lainnya. Iran lebih memilih untuk membangun proksi teroris seperti Hizbullah dan *Islamic Revolutionary Guard Corps* (IRGC), yang pada dasarnya tidak memerlukan berbagai hak yang sama dengan pasukan darat konvensional. Adapun aplikasi kemampuan asimetris dalam strategi militer Iran juga dapat dilihat dari strategi Iran yang saat ini berfokus pada kemampuan 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 (Fixler & Cilluffo, 2018: 8-10).

Lebih lanjut, interpretasi tulisan Ali Khamenei juga dapat menjadi salah satu landasan yang memperlihatkan keputusan Iran untuk mempertahankan status quo pada konflik. Salah satu tulisan yang peneliti ambil adalah cuitan 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.

Berhubungan dengan operasi siber ofensif Iran, Direktur Intelijen Nasional (DNI) James Clapper menjelaskan bahwa Iran juga memandang program siber sebagai salah satu dari banyak alat untuk melakukan pembalasan asimetris tetapi proporsional terhadap musuh politik. Departemen Luar Negeri AS menyimpulkan, "Iran dibawah otoritas Ali Khamenei telah mengembangkan kemampuan dunia maya dengan maksud untuk mengawasi dan menyabot musuh-musuhnya, merusak norma-norma internasional dan mengancam stabilitas internasional (Fixler & Cilluffo, 2018: 10). Sebagai contoh kasus pada Februari 2014, *CEO Las Vegas Sands Corporation Sheldon*, yakni Adelson menyarankan agar Amerika Serikat menjatuhkan bom nuklir di padang pasir Iran untuk meyakinkan Republik Islam untuk melepaskan ambisi nuklirnya sendiri. Tidak lama berselang itu, para peretas dari Iran menembus sistem perusahaan Adelson. Serangan itu menyebabkan komputer menjadi *flat-line*, membuat e-mail perusahaan tidak aktif, dan melumpuhkan ponsel atau platform operasi bisnis lainnya yang terkait dengan perusahaan senilai $14 miliar ini. Adelson juga diperkirakan rugi $ 40 juta sebagai akibat dari kerusakan materil yang diterima. Lalu dibutuhkan seminggu penuh untuk memulihkan jaringan perusahaan itu (Disegi, 2016: 7).

BAB III

STRATEGI SIBER OFENSIF IRAN

Berdasarkan kedua tingkatan analisis sebelumnya, yakni identitas nasional dan individu, bagi Iran damai dan perang bukanlah pilihan dan sama halnya dengan melanjutkan politik luar negeri dan kebijakan militer yang agresif kepada ketiga negara lainnya. Sehingga pada akhirnya, peneliti 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. Terkait hal ini, peneliti berpendapat bahwa serangan siber menjadi salah satu opsi yang digunakan oleh Iran untuk menjaga status quo di situasi konflik tersebut dan mencegah terjadinya perang konvensional di masa depan. Dalam memperkuat opini ini, peneliti akan memaparkan strategi siber ofensif Iran, yang mana pada dasarnya dapat memfasilitasi kepentingan atau tujuan negaranya, yakni menjaga status quo dan menghindarkan dirinya terlibat perang konvensional yang pada situasi ini tidak mungkin Iran menangkan. Adapun dua teori yang menurut peneliti dapat memfasilitasi kepentingan siber ofensif Iran, adalah strategi siber asimetris milik Korea Utara dan strategi *deference active*.

3.1 Strategi Siber Asimetris Iran: Fokus Terhadap Operasi Siber Ofensif Skala Kecil dan Sedang

Strategi pertama adalah strategi perang siber asimetris. Pada dasarnya strategi siber asimetris bertujuan untuk mencegah terjadinya perang konvesional, yang

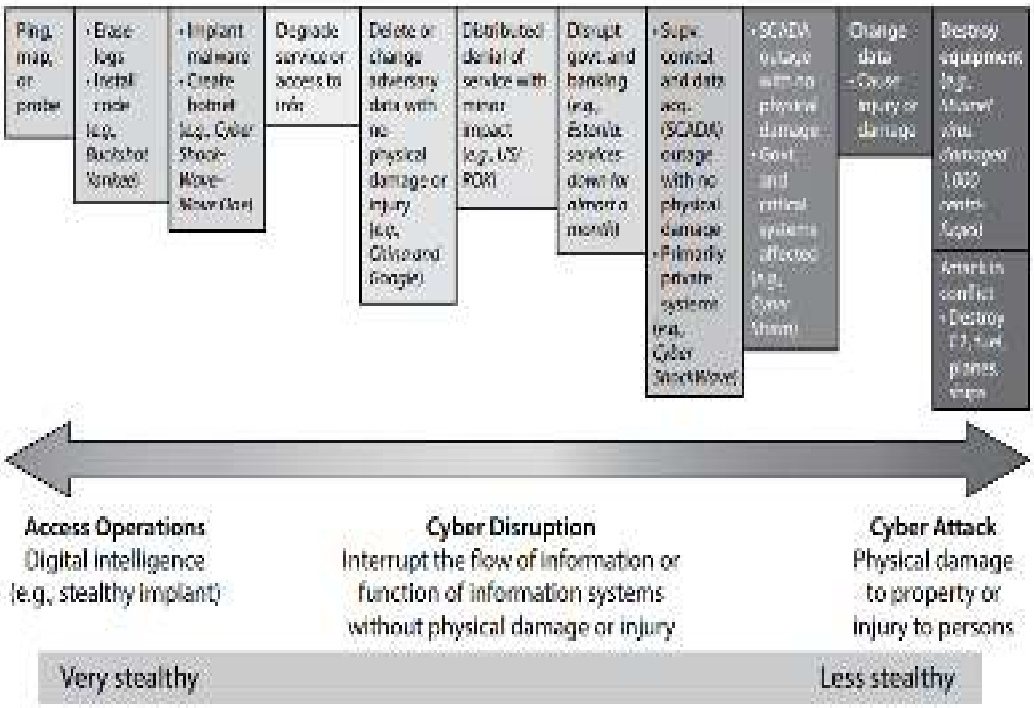
mana karena itu strategi ini sangat cocok dengan asumsi peneliti bahwa Iran ini punya tujuan untuk mempertahankan stasus quo pada konfliknya dengan ketiga negara lainnya melalui operasi siber ofensif. Pada dasarnya strategi ini dapat digunakan menggunakan senjata nuklir, senjata konvensional seperti artileri dan dengan cara-cara lainnya yang memanfaatkan kerentanan atau kelemahan lawan. 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 aktor lain yang lebih kuat (Fixler & Cilluffo, 2018: 8-10).

Adapun serangan asimetris yang biasanya menggunakan senjata nuklir dan senjata konvensional akhir-akhir ini semakin sulit untuk diaplikasikan sebagai media dari strategi asimetris, karena tekanan dan kritikan secara luas oleh komunitas internasional dan dibentuknya aturan-aturan khusus mengenai penggunaan senjata nuklir dan senjata-senjata konvesional. Dimana karena itu, Iran mulai berinvestasi dalam kemampuan militer asimetris untuk digunakan di

luar wilayah militer konvesional. Dalam hal inilah penggunaan operasi siber ofensif menjadi salah satu media utama dalam menerapkan strategi perang asimetris. Hal ini karena operasi siber ofensif memiliki keunggulan untuk melukai pihak lawan tanpa harus takut terkena ancaman yang sebanding atau dengan kata lain tanpa takut akan bayangan dimulainya perang konvesional. Pada dasarnya, kemampuan ini memungkinkan Iran untuk melawan Amerika Serikat, Israel dan Arab Saudi tanpa pernah benar-benar melawan ketiga negara tersebut (Fixler & Cilluffo, 2018: 10).

Berhubungan dengan strategi siber asimetris milik Korea Utara, 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. Untuk detailnya dapat melihat tabel dibawah ini:

Tabel 3 : Spektrum Skala Operasi Siber Ofensif



Sumber : *Timothy M. McKenzie*

Adapun dalam teori 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 (Fixler & Cilluffo, 2018: 10). Serangan Siber dalam konteks *Access Operations* sampai *Cyber Disruption* secara efektif menggantikan atau, setidaknya, menambah kemampuan provokatif yang ada karena sifatnya yang lebih sulit untuk dilacak dan dibalas dari aspek

hukum dibandingkan dengan tingkatan *cyber attack* yang lebih terbuka. Sehingga meninggalkan celah untuk dibalas secara hukum atau regulasi yang berlaku. Selain itu, memiliki efek asimetris yang tidak jauh berbeda dengan senjata nuklir, tetapi dengan biaya yang relatif rendah dan risiko operasional yang jauh lebih kecil dari senjata nuklir (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 pertama keuntungan finansial. Hal ini dapat dilihat dari banyaknya serangan dalam bentuk DDoS terhadap sektor keuangan ketiga negara tersebut. Salah satunya adalah serangan siber yang mengatasnamakan dirinya *Izz ad-Din al-Qassam Cyber Fighters* atau dikenal juga dengan *Qassam Cyber Fighters*. Operasi siber ofensif ini dilakukan dalam bentuk DDoS terhadap sektor keuangan Amerika Serikat. Cara kerja Serangan DDoS ini ditujukan untuk meyibukkan jaringan karena menerima jutaan paket data tiap detiknya. Lebih lanjut dengan metode yang tidak jauh berbeda, Iran kemudian secara berkala melancarkan serangan sibernya dengan target yang masih sama, yakni sektor keuangan Amerika Serikat. Akan tetapi berbagai serangan siber tersebut nyatanya gagal, sampai akhirnya pada bulan Juli 2013, yakni pada percobaan serangan siber mereka yang keempat, Iran kembali berhasil melakukan serangan siber yang cukup merusak di bidang keuangan. Pada operasi yang diberi kode ababil ini mengunci ratusan ribu pelanggan perbankan dari akun-akun untuk jangka waktu yang lama dan mengakibatkan puluhan juta dolar biaya untuk

memulihkannya (Anderson, 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).

Fokus strategi kedua adalah sebagai upaya untuk penambangan data. Adapun data disini merujuk pada sabotase dan spionase informasi. Salah satu metode favorit Iran adalah upaya *spearphishing* pada email pribadi dan akun media sosial karyawan pemerintah AS. Serangan dalam bentuk ini sendiri berbeda dengan DDoS. Pada bentuk *spearphishing*, serangan siber dilakukan dengan mensabotase email atau akun media sosial tertentu. Dimana kemudian melalui email dan akun media sosial tersebut. Iran akan mengirimkan pesan-pesan kepada pihak tertentu yang bertujuan untuk menipu atau mengelabui penerima pesan agar melakukan semacam tindakan yang akan menguntungkan Iran, termasuk membagi infromasi rahasia. Adapun *spearphishing* ini mudah dilakukan karena akun pribadi cenderung tidak memuat informasi rahasia pemerintah, sehingga akan memiliki keamanan yang jauh lebih lemah, namun disisi lainnya tetap memiliki fungsi yang sangat penting. Dikarenakan sering mengandung informasi yang berguna seperti materi pribadi dan jejak komunikasi profesional. Adapun Teheran cenderung

menargetkan personil dan lembaga pemerintah asing yang memiliki kaitan pekerjaan dengan Iran, sebagai contoh orang-orang di Amerika Serikat atau Eropa yang bekerja pada televisi *Voice of America* dan Radio Farda. Uniknya 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 mereka 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, 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. Menurut *Kaspersky Lab* dan *Seculert* (sebuah perusahaan keamanan Israel yang menemukan malware Mahdi pertama kali), perangkat lunak 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, 2018). Contoh upaya *spearphishing* lainnya dapat dilihat terhadap lembaga akademis, pejabat keamanan nasional, diplomat,

anggota Knesset, dan perusahaan kedirgantaraan Israel. Demikian pula, Iran secara umum telah menciptakan domain jahat yang telah meniru milik AIPAC dan telah menargetkan data para karyawan dari organisasi Yahudi liberal dan konservatif di Amerika Serikat, Israel dan di tempat lain (Anderson, 2018). Adapun secara global, Iran juga memfokuskan upayanya pada operasi spionase yang bertujuan untuk mengumpulkan data untuk mempengaruhi opini publik melalui propaganda.

Berhubungan dengan pembahasan strategi asimetris, maka dapat dilihat bahwa hanya dengan beberapa buah komputer dan akses internet, Iran dapat menimbulkan kerusakan yang sama efeknya dengan senjata nuklir atau senjata konvesional, yakni melemahkan kemauan musuh untuk melakukan perang konvensional dengan gangguan, kehancuran, kelelahan, atau paksaan. Adapun strategi asimetris ini tidak bertentangan dengan pola operasi siber ofensif Iran selama ini, hal ini karena strategi ini memang harus dilakukan melalui serangan siber skala kecil dan sedang atau disebut juga dengan *Access Operations* sampai *Cyber Disruption*. Hal ini 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 aktor negara menggunakan serangan siber dalam skala besar atau *cyber attack*, maka itu berarti negara tesebut telah siap untuk melakukan perang habis-habisan atau *total war*. Mengingat aktor yang melakukan penyerangan sudah harus siap akan konseskuensi yang mungkin diterima, baik

dari aktor-aktor internasional lainnya, atau mendapat serangan balasan dari negara yang diserang.

3.2 Strategi Siber *Deterrence Active* Iran: Fokus Terhadap Serangan Siber Skala Kecil dan Sedang

Strategi kedua yang peneliti gunakan adalah strategi *deterrence active*. Peneliti menggunakan kerangka pemikiran ini untuk menggambarkan salah satu fungsi serangan siber, yakni mengancam untuk menangkal adanya serangan. Dari perspektif dunia maya, *deterrence active* merujuk pada tindakan yang diambil negara untuk mengamankan dirinya dari serangan negara lain dengan ancaman balas dendam atau respons 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*. Berdasarkan sejarah, senjata nuklir merupakan senjata pemusnah massal terkuat yang pernah diciptakan, hal ini terlihat dari perannya sewaktu perang dunia kedua. 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 akan 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 ia akan mendapat balasan senjata nuklir juga. Adapun karena keyakinan dan ketakutan tersebut, negara-negara yang biasanya sama-sama memiliki kekuatan nuklir, akan menolak untuk berperang satu sama lain. Hal ini dikarenakan bahaya nuklir itu sendiri yang pada akhirnya akan 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.

Lebih jauh, McKenzie (2017: 3) memaparkan tujuh atribut yang diperlukan pada strategi *deterrence* yang sukses. Jika melihat ketuju atribut tersebut, selain kepentingan yang harus dilindungi ada lima atribut yang diperlukan merujuk pada *deterrence active*. Kelimanya adalah deklarasi pencegahan atau peringatan yang harus keras dan jelas, kredibilitas untuk melakukan serangan balasan, memproduksi ketakutan, tindakan penalti ketika telah diserang, dan perhitungan biaya dengan manfaat ketika akan melaukan serangan. Berdasarkan kelima atribut tersebut, peneliti mengakaitkannya dengan jejak serangan siber Iran ke AS, Israel dan Arab Saudi. Hal ini demi tujuan untuk melihat apakah strategi *deterrence active* memang menjadi rujukan operasi siber ofensif siber Iran selama ini dan kalau memang benar, seperti apa Iran melaksanakannya.

3.2.1 Deklarasi Peringatan yang Harus Keras dan Jelas

Pada perang dunia dingin, Amerika Serikat dan Uni Soviet sama-sama memberikan peringatan yang jelas bahwa kedua negara tidak akan menahan diri semisal salah satu negara berniat menyerang menggunakan nuklir. Kedua negara

siap untuk menggunakan senjata nuklirnya, meski itu artinya kehancuran kedua negara atau bahkan kehancuran dunia. Hal ini pada dasarnya tidak jauh berbeda dengan strategi *deterrence active* lainnya. Strategi ini memang mengharuskan deklarasi peringatan yang keras dan jelas, bahwa akan ada konsekuensi jika negara lain berusaha untuk mengganggu kedaulatan atau keamanan negara tersebut. Iran dalam kasus perang siber dengan AS, Israel, dan Arab Saudi pada dasarnya tidak jauh berbeda. Iran perlu untuk mendeklarasikan peringatan yang keras dan jelas jika memang menjadikan strategi ini sebagai rujukan. Adapun terkait ini, meski Iran tidak mendeklarasikan kapabilitas sibernya seperti mereka mendeklarisikan kekuatan nulirnya atau bahkan Iran menolak tuduhan sebagai pelaku penyerangan siber. Menurut perusahaan keamanan komputer MalCrawler, Iran dengan sengaja mempertunjukkan bahwa negaranya adalah pelaku sekalian ancaman siber di era ini dengan mengeksploitasi pertahanan siber musuh-musuhnya untuk mendatangkan kerusakan yang lebih besar di masa depan (Rattray, 2018, 3-8). Bukti mengungkapkan bahwa rezim Iran dan Islam IRGC mensponsori berbagai operasi siber ofensif yang berasal dari Iran semenjak terkena Virus Stuxnet, yang dilaporkan dilakukan oleh AS dan Israel.

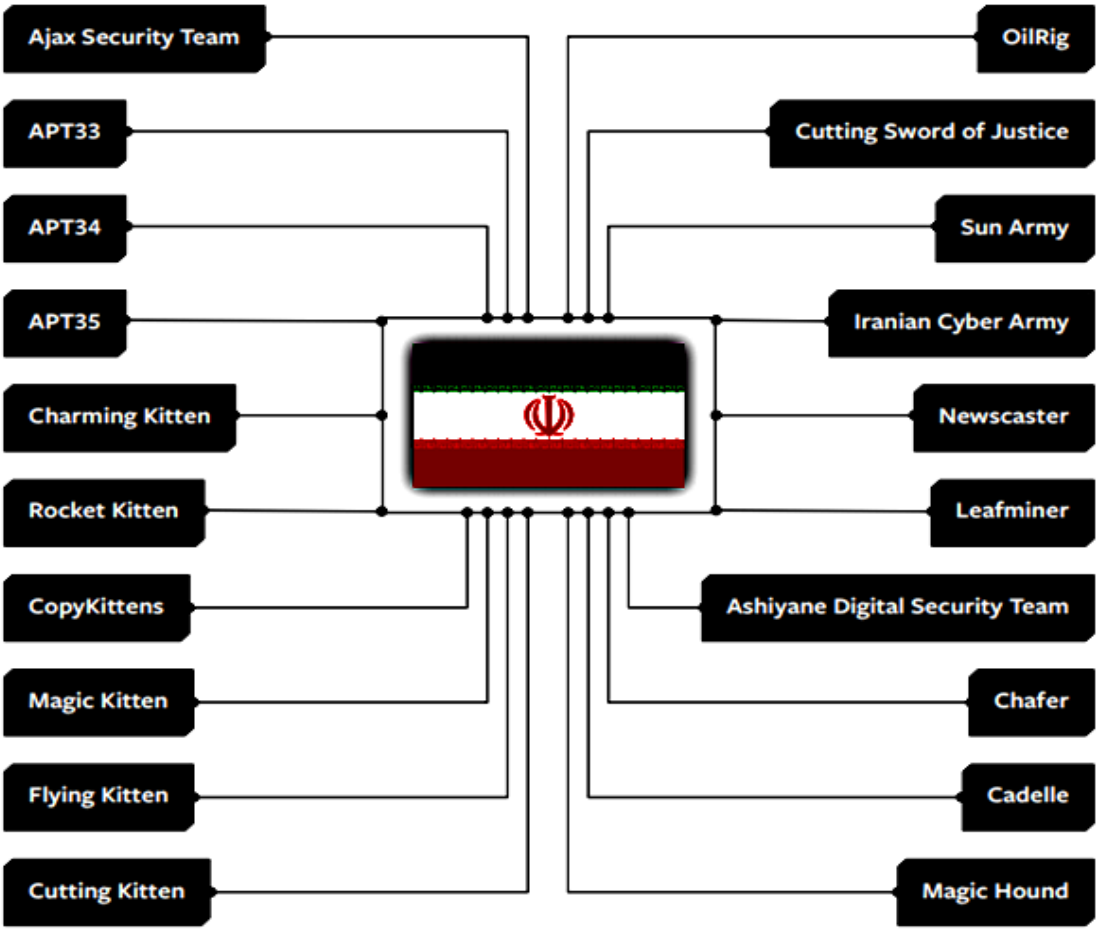
Salah satu bukti yang dipaparkan oleh MalCrawler adalah dari segi infrastruktur atau jaringan siber yang digunakan. Pada kasus serangan siber dari negara lain, sperti Tiongkok dan Rusia, infrastruktur atau jaringan siber yang digunakan kelompok atau individu dari kedua negara itu ketika melakukan operasi siber ofensif cenderung dinamis atau berubah-ubah dan karena hal itu identifikasi pelaku ancaman dunia maya sulit untuk dilakukan. Dalam hal ini, negara pelaku

penyerangan siber selalu mengganti atau mengaburkan kode atau letak jaringan siber yang digunakan, dengan tujuan agar tidak ketahuan bahwa negaranya adalah pelaku serangan siber. Akan tetapi berbeda dengan kasus penyerangan siber yang berasal dari Iran, dimana banyak serangan siber berasal dari infrastruktur atau jaringan siber yang sama. Padahal, di satu sisi serangan siber tersebut dilakukan oleh kelompok penyerangan siber yang berbeda. Sebagai contoh, para peneliti pada awalnya mengidentifikasi dua kelompok peretas yang diberi label "Flying Kitten" dan "Rocket Kitten" pada 2013 dan 2014. Kedua kelompok peretas tersebut pada awalnya menggunakan infrastruktur atau jaringan siber yang berbeda. Akan tetapi, pada 2015 di waktu yang berbeda, para peneliti mencatat dua kelompok tersebut menggunakan model operasi yang sama dan berbagi nama domain yang sama. Sehingga membuat para peneliti menyimpulkan bahwa kondisi itu hanya terjadi jika negara asal penyerangan siber mengijinkan atau mendukung serangan siber yang dilakukan oleh kedua kelompok peretas tersebut (Fixler & Cilluffo, 2018: 10-15).

Bukti lain bahwa Iran mensponsori berbagai operasi siber ofensif yang berasal dari Iran dapat dilihat dari bagaimana kelompok-kelompok ini sering menggunakan alat *malware* yang tersedia untuk umum. Misalnya, serangan Shamoon 2 pada 2016-2017 terhadap Arab Saudi yang memiliki karakteristik yang sama dengan serangan label APT33, yakni dalam hal penentuan penggunaan *Advance Persistent Threat* (APT). Dalam kasus ini, Shamoon 2 dan APT33 menggunakan nama-nama orang terkemuka yang sama untuk mendapatkan akses illegal ke suatu jaringan dan menetap disana tanpa terdekteksi untuk waktu yang

lama sembari melakukan pencurian data (Fixler & Cilluffo, 2018: 10-15). Adapun berdasarkan dua metode ini maka terlihat jelas bahwa ada sekumpulan kelompok peretas Iran yang saling terkait satu sama lain dan dicurigai berhubungan dengan Iran. Beberapa kelompok terkemuka tersebut adalah sebagai berikut:

Tabel 4 : Kelompok-Kelompok Peretas yang Berhubungan dengan Iran



Sumber: *Annie Fixler and Frank Cilluffo*

Lebih lanjut, bukti lain bahwa Iran yang merupakan sponsor dari kelompok-kelompok tersebut dapat dilihat dari pernyataan pers Departemen Kehakiman AS. Pada bulan Maret 2016, Departemen Kehakiman membuka dakwaan terhadap tujuh orang yang bertanggung jawab atas serangan DDoS yang didistribusikan

pada lembaga keuangan AS antara 2011 dan 2013. Departemen Kehakiman juga menuduh salah satu peretas yang telah menyusup sistem kontrol bendungan di New York pada bulan Agustus dan September 2013. Berdasarkan pernyataan pers Departemen Kehakiman para pelaku penyerangan siber di dua peristiwa tersebut mengaku bahwa perusahaan yang mempekerjakan mereka itu disponsori oleh Iran. Dua tahun kemudian, pada tahun 2018, Departemen Kehakiman juga menyatakan bahwa orang-orang yang bertanggung jawab atas penyusupan komputer di ratusan universitas AS dan lusinan perusahaan AS, bergerak atas nama Iran. Bahkan dakwaan 2017, terkait kasus akses tidak sah ke sistem komputer HBO dan upaya pemerasan terhadap perusahaan tersebut mencatat bahwa tertuduh sebelumnya bekerja atas nama militer Iran untuk melakukan serangan jaringan komputer yang menargetkan sistem militer, sistem perangkat lunak nuklir, dan infrastruktur Israel (Fixler & Cilluffo, 2018: 10-15).

3.2.2 Kredibilitas untuk Melakukan Serangan Balasan

Pada dasarnya tidak ada dokumentasi mengenai kredibilitas operasi siber ofensif Iran, Iran sendiri tidak pernah mempublikasi kemampuan atau strategi sibernya secara resmi. Dimana karena hal itu, Peneliti kesulitan untuk mengkaitkan argumen peneliti dengan fakta yang ada. Akan tetapi satu hal yang pasti, ancaman serangan siber Iran itu nyata, dan Iran terbukti secara sengaja menunjukkan bahwa dirinya adalah ancaman siber. Dikaitkan dengan jejak serangan siber tersebut dan kerangka teori pertama yang peneliti gunakan, peneliti meyimpulkan bahwa ada satu pengetahuan yang diketahui oleh semua negara, yakni kemampuan siber Iran tidak kalah hebatnya dengan kemampuan siber

negara kuat lainnya**.** Adapun untuk menjelaskan hal ini, peneliti menggunakan *biological metaphors.* Lawson (2012) memaparkan teori bahwa perang biologis dan bioterorisme adalah analogi yang paling tepat untuk menggambarkan serangan siber. Program serangan siber memiliki efek yang sama dengan serangan biologis, yaitu tidak dapat dikendalikan penyebarannya dan pengembangannya. Sehingga teknologi serangan siber dan biologis dapat dengan mudah dimiliki negara lain. Sebagai contoh hal ini dapat dilihat dari serangan virus Stuxnet. Pada dasarnya meski sukses memberhentikan pengadaan uranium nuklir Iran saat itu, virus Stuxnet penggunaannya tidak dapat dibatasi oleh negara pengembang, yakni Amerika Serikat dan Israel. Seperti halnya serangan biologis, penggunaan stuxnet ini dapat meningalkan jejak dan jejak tersebut dapat menghasilkan teknologi baru bagi musuh yang telah diserang. Sampel dari "patogen" (biologis atau digital) dapat dikumpulkan, dianalisis, dimateraikan lebih lanjut, atau digunakan untuk membuat penawarnya. Lalu dengan kata lain, kode Stuxnet yang bentuknya dapat menimbulkan kerusakan kolateral yang serius terhadap Iran ini pada dasarnya dapat kemudian digunakan kembali terhadap Israel dan Amerika (Lawson, 2012).

Dihubungkan dengan kredibilitas Iran untuk melakukan serangan balasan, ada efek positif dari serangan siber virus Stuxnet ini bagi Iran. Salah satunya adalah mendorong kemampuan siber Iran ini untuk berkembang. Hal ini sebagai akibat dari virus siber yang menurut Lawson (2012) sama seperti virus biologis, yakni meningalkan jejak dan jejak tersebut dapat menghasilkan teknologi baru. Dengan kata lain, meski belum pernah menggunakan serangan siber dalam skala besar, kemampuan serangan siber Iran secara teori setidaknya saat ini memiliki

kapabilitas yang cukup besar, mengingat virus Stuxnet termasuk serangan siber skala besar atau jenis serangan yang memiliki kapabilitas untuk melukai infrastruktur, properti, dan nyawa manusia.

Sebagai contoh untuk mendukung argumen bahwa Iran memiliki kemampuan siber yang telah digunakan kepada mereka, dapat dilihat dari operasi siber ofensif Iran terhadap salah satu perusahaan milik negara Arab Saudi, yakni Saudi Aramco selama liburan Idul Fitri Muslim, tepatnya tanggal 15 Agustus 2012 dan serangan serupa terhadap Perusahaan RasGas Qatar dua minggu kemudian. 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. Adapun kelebihan utama Shamoon adalah kemampuannya yang dapat menyebar dari mesin yang terinfeksi ke komputer lain di jaringan. Setelah sistem terinfeksi, virus terus menyusun daftar file dari lokasi tertentu pada sistem, mengunggahnya ke penyerang, dan menghapusnya. Akhirnya virus menimpa *master boot record* komputer yang terinfeksi, membuatnya tidak dapat digunakan. Selain itu Shamoon juga terkenal karena di setiap serangannya selalu disertai dengan gambar bendera Amerika Serikat yang terbakar, setelah komputer-komputer tersebut selesai diretas. Disinilah dapat dilihat bahwa Iran telah meniru atau menggunakan serangan siber yang tidak lain adalah serangan siber yang dilakukan kepadanya, yakni malware Flame yang telah menargetkan Iran pada April 2012 dan kemudian diperbaruhi oleh Iran. Hal ini mengingat banyaknya kesamaan diantara keduanya, salah satunya adalah keduanya meretas data yang tersimpan,

lalu setelah itu menghancurkannya sebagai metode sabotase. Flame sendiri disinyalir berupa virus yang tidak hanya menyasar perangkat industri tetapi juga tokoh pebisnis dan univeristas di Iran. Flame ini sifanya tidak berbeda dengan Shamoon karena pada dasarnya Flame tidak merusak atau membahayakan suatu sistem tertentu, namun lebih kepada mendapatkan data dan mensabotase data dengan cara melakukan mata-mata, seperti menyadap audio, merekam ketikan keyboard mengambil *screenshot*, mencegat email, lalu mengambil data dari bluetooth dari komputer yang telah terinfeksi (Morton & Grace, 2018).

Contoh lainnya dapat dilhat dari serangan Shamoon yang digunakan dalam insiden Aramco muncul berulang-ulang. Salah satunya saat Shamoon muncul kembali dalam bentuk yang diperbarui (diberi label sebagai Shamoon 2 oleh peneliti). Pada November 2016 hingga Januari 2017, Shamoon 2 berhasil menghancurkan *database* dan file milik pemerintah dan sektor swasta, termasuk Otoritas Umum Penerbangan Sipil, Departemen Tenaga Kerja, Bank Sentral Saudi, dan perusahaan ekstraksi sumber daya alam. Shamoon 2 berisi referensi ke Yaman dan hard drive para korban dengan gambar anak pengungsi Suriah yang tewas, yakni Alan Kurdi. Adapun dari cara Shamoon 2 ini bekerja kita dapat mengetahui bahwa sekali lagi serangan itu merupakan virus yang sama dengan malware Flame (Morton & Grace, 2018).

3.2.3 Mampu Memproduksi Ketakutan dan Melakukan Tindakan Penalti

Secara kapabilitas Iran pada dasarnya memang dapat melakukan serangan balasan dalam melakukan strategi *deterrence active*. Hal ini setidaknya dapat dilakukan melalui Virus Stuxnet yang telah dimiliki oleh Iran. Melalui Virus

Stuxnet Iran dapat mengancam teknologi nuklir milik AS, Israel, dan Arab Saudi. Akan tetapi dalam perspektif siber, Iran tidak dapat selalu menggunakan kemampuan itu. Hal ini terjadi karena pengguna serangan siber dalam skala besar pada dasarnya akan ikut merugi juga dan karena hal itu ada baiknya menggunakan serangan siber dalam skala kecil. Adapun hal ini tidak terlepas dari jejak serangan siber yang dapat dilacak, dan diteliti untuk memberikan teknologi baru bagi musuh jika diserang dengan serangan siber. Jadi dengan kata lain jika Iran melakukan serangan siber skala besar, maka konsekuensinya serangan siber tersebut tidak dapat digunakan lagi untuk seterusnya. Dimana karena itu ada baiknya Iran untuk menyimpan serangan siber dalam skala besar sebagai pilihan terakhir, ketika eksistensi Iran terancam.

Peneliti pada dasarnya melihat bahwa Iran menggunakan strategi siber *deterrence active* yang berbeda dengan metode senjata nuklir memberikan ancaman dan ketakutan. Strategi siber *deterrence active* Iran lebih kepada memberikan ketakutan atau keyakinan bahwa musuhnya akan merugi dengan mengandalkan serangan siber dalam skala kecil dan sedang. Salah satu cara untuk menimbulkan ketakutan tersebut adalah dengan terus menerus melakukan serangan siber skala kecil dan sedang kepada ketiga negara yang menjadi musuhnya, sebagai respon terhadap suatu kebijakan yang merugikan Iran. Meski tidak sebesar pada senjata nuklir, operasi siber ofensif Iran yang terus menerus kepada ketiga negara lainnya setidaknya terbukti berhasil menimbulkan ketakutan atau keyakinan terhadap lawannya. Hal ini terbukti dari argumen Perdana Menteri Israel, yakni Benjamin Netanyahu juga menyebut bahwa Iran secara teratur telah

mengancam Israel melalui serangan siber terhadap negaranya setiap harinya. Arab Saudi melalui Menteri Luar Negerinya, yakni Adel Al-Jubeir juga 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).

Selain rutin melakukan operasi siber ofensif lansung kepada ketiga negara lainnya menggunakan serangan siber skala kecil dan sedang, Iran dalam kasus ini juga menggunakannya ke negara lain yang memiliki kaitan dengan lawan-lawannya. Sebagai contoh hal ini dapat dilihat dari serangan siber Shamoon yang menurut para akademisi bisa saja menjadi indikasi bahwa Iran mungkin tidak selalu dapat membela diri terhadap kemampuan siber yang lebih maju, tetapi Iran masih dapat memberlakukan serangan balasan yang cukup besar terhadap sekutu-sekutu Amerika Serikat. Dengan kata lain serangan Shamoon ini dapat dikatakan juga sebagai operasi siber ofensif yang berfungsi sebagai media untuk membalas dendam. Hal ini berhubungan juga dengan aksi-aksi rahasia oleh aktor-aktor asing yang menargetkan infrastruktur nuklir dan minyak Iran (Anderson, 2018).

Adapun perlu diketahui bahwa meski dapat menimbulkan ketakutan, strategi *deterrence* yang telah dimoditifikasi Iran ini terbukti tidak seefektif senjata nuklir, yang mana sukses merendahkan niat lawat untuk berperang dengan cara menimbulkan keyakinan dan ketakutan bahwa akan ada kemungkinan Iran akan menyerang dengan kekuatan yang sama atau bahkan lebih besar jika eksistensi negara itu sedang terancam. Hal ini sesuai dengan fungsi dan kemampuan dari serangan siber skala kecil dan sedang yang pada dasarnya tidak akan

menimbulkan kerusakan kolateral yang berdampak pada eksistensi negara lainnya. Salah satu pemanfaatan strategi siber *deterrence active* Iran dapat dilihat dari adanya ancaman Iran terhadap bisnis milik keluarga dan kerabat Presiden Trump, sebagai respon terhadap pernyataan baru-baru ini yang dibuat oleh Presiden Trump terkait destabilisasi Iran di wilayah tersebut. Pada prosesnya, ancaman ini terbukti gagal dan destabilisasi Iran dibawah pemerintahan Presiden Trump tetap dilakukan (Fixler & Cilluffo, 2018).

3.2.4 Perhitungan Biaya dengan Manfaat Ketika Melakukan Serangan

Pada akhirnya, strategi *deterrence active* melalui serangan siber mungkin memang berhasil memberikan ketakutan terhadap lawan-lawannya. Dari segi kapabilitas Iran pada dasarnya memang dapat melakukan serangan balasan dalam melakukan strategi *deterrence active*. Hal ini setidaknya dapat dilakukan melalui Virus Stuxnet atau serangan siber dalam skala besar lainnya yang telah dimiliki oleh Iran. Akan tetapi dalam perspektif siber, Iran tidak dapat selalu menggunakan kemampuan itu. Hal ini tidak terlepas dari jejak siber yang dapat dilacak, dan diteliti untuk memberikan teknologi baru bagi musuh jika diserang dengan serangan siber. Jadi dengan kata lain jika Iran melakukan serangan siber skala besar, maka konsekuensinya serangan siber tersebut tidak dapat digunakan lagi untuk seterusnya. Dimana karena itu, menurut peneliti Iran lebih memilih untuk menyimpan serangan siber dalam skala besar sebagai pilihan terakhir, ketika eksistensi Iran terancam. Adapun, strategi siber *deterrence* Iran lebih kepada memberikan ketakutan atau keyakinan bahwa musuhnya akan merugi dengan mengandalkan serangan siber dalam skala kecil dan sedang secara terus

menerus kepada ketiga negara yang menjadi musuhnya, sebagai respon terhadap suatu kebijakan yang merugikan Iran (Lawson, 2012).

Akan tetapi, strategi ini tidak terbukti seefektif strategi *deterrence active* nuklir. Hal ini sesuai dengan fungsi dan kemampuan dari serangan siber skala kecil dan sedang yang pada dasarnya tidak akan menimbulkan kerusakan kolateral yang berdampak pada eksistensi negara lainnya. Jadi dengan kata lain peringatan ancaman dengan serangan siber skala kecil dan sedang versi Iran ini cenderung gagal karena negara lain tidak begitu khawatir terhadap ancaman yang ditawarkan Iran. Dikaitkan dengan perhitungan biaya dan manfaat ketika melakukan operasi siber ofensif selama ini, maka dapat dilihat bahwa meski tidak sebaik serangan nuklir. Serangan siber Iran dalam skala kecil dan sedang ini tidak memberikan Iran kerugian yang sebanyak serangan siber skala besar, yang mana dapat membahayakan eksistensi Iran karena jejak siber tidak dapat pernah hilang dan karena itu dapat dikaji dan digandakan oleh negara yang terkena serangan siber. Sehingga dalam kasus ini, langkah Iran yang hanya bergantung dengan serangan siber dalam skala kecil dan sedang, yang mana tidak memberikan Iran kerugian yang banyak, karena meski dapat digandakan oleh negara penerima serangan siber Iran. Serangan siber dalam skala kecil dan sedang tidak akan membahayakan eksistensi Iran di masa depan (Lawson, 2012).

Adapun dari hal ini dapat disimpulkan bahwa efek dari strategi siber *deterrence active* ini tidak jauh berbeda dengan strategi siber asimetris. Dimana keduanya berpotensi untuk mencegah terjadinya perang konvensional yang kemungkinan besar akan berakhir dengan kekalahan Iran dan menjagah status quo

selama mungkin dengan ketiga negara yang menjadi lawannya. Jika dalam strategi siber asimetris, yang menjadi faktor kuncinya adalah merusak untuk mengurangi niat lawan untuk berperang. Maka berbeda dengan strategi *deterrence active*, yang pada dasarnya mencegah terjadinya perang konvensional dengan cara mengancam dan menyakinkan pihak lawan bahwa Iran juga dapat menimbulkan penderitaan dan kerugian jika ketiga negara lainnya mencoba untuk menyerang Iran (Lawson, 2012).

BAB IV

KESIMPULAN

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 Iran sendiri tidak pernah mengemukakan strategi perang, pertahanan dan keamanan siber negaranya. Akan tetapi, meski tidak pernah memaparkan secara lansung strategi siber ofensifnya, Iran banyak dikaitkan dengan berbagai operasi siber ofensif yang terjadi kepada ketiga negara tersebut. Berhubungan dengan hal ini, peneliti melalui tingkatan analisis identitas nasional dari segi sejarah politik luar negeri dan militer negara tersebut menemukan bahwa kepentingan atau tujuan Iran dalam melakukan berbagai operasi siber ofensif, tidak terlepas dari fakta bahwa negara ini berusaha untuk menjaga agar status quo konflik dapat bertahan selama mungkin dengan ketiga negara lainnya, mengingat perang diplomatik dan perang konvensional bukanlah pilihan yang logis bagi Iran.

Hal ini sendiri terkait dengan identitas nasional 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. Akan tetapi, pada prosesnya sepanjang sejarah konfliknya dengan ketiga negara tersebut, Iran telah mengalami berbagai situasi dimana negara ini tidak mungkin untuk

memenangkan konflik dengan perang konvensional dan negosiasi. Sebagai hasilnya perdamaian atau menyerah bukan pilihan logis bagi Iran, mengingat yang membentuk dan mempergunakan identitas nasional sebagai negara yang kuat dan negara yang benar dalam konflik ini adalah pemerintah Iran sendiri. Pada akhirnya, Iran sampai pada sebuah kesimpulan bahwa Iran perlu mengambil kebijakan untuk menetapkan status quo karena dengan begitu Iran dapat terlepas dari bahaya perang konvensional dan perang diplomasi yang kemungkinan besar membuat Iran kalah.

Adapun tujuan Iran untuk menjaga status quo pada konfliknya juga terlihat dari hasil tingkatan analisis individu Iran. Berhubungan dengan tingkatan analisis ini, peneliti menggunakan sosok *supreme leader*, yakni Ali Khamenei dan pendekatan *leadership trait analysis,* yang mana bertujuan untuk menganalisa kemampuan Khamenei dalam kehidupan politik negaranya, terutama dalam menangani isu-isu politik luar negeri. 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. Hal ini juga dapat disimpulkan dari cuitan *twitter* Khamenei, yang mana dia memaparkan bahwa penyelesaian konflik melalui perang dan negosiasi bukanlah pilihan Iran. Sebaliknya Khamenei saat ini ingin agar status quo dalam konflik ini tetap bertahan.

Lebih lanjut, 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 milik Korea Utara dan strategi *deference active.* Strategi perang siber asimetris Korea Utara ini tidak bertentangan dengan pola operasi siber ofensif Iran selama ini. Hal ini karena strategi ini memang harus dilakukan melalui serangan siber 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 atau *total war.* Mengingat aktor yang melakukan penyerangan sudah harus siap akan konseskuensi yang mungkin diterima, baik dari aktor-aktor internasional lainnya, atau mendapat serangan balasan dari negara yang diserang. Adapun penerapan strategi siber asimetris yang berdasarkan operasi siber ofensif skala kecil dan sedang ini hanya berfokus kepada 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 Serika secara berulang-ulang. Contoh lainnya dapat dilihat dari serangan siber *spearpishing* yang telah dilakukan berulang-ulang sejak tahun 2011 sampai sekarang ini, dengan target utamanya termasuk Amerika Serikat, Israel, dan Arab Saudi.

Strategi siber ofensif Iran selanjutnya adalah strategi *deterrence active*. Kesimpulan peneliti terhadap strategi ini adalah strategi *deterrence active* siber memang berhasil memberikan ketakutan terhadap lawan-lawannya. Namun strategi ini tidak terbukti seefektif strategi *deterrence* nuklir, karena Iran tidak dapat selalu 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. Dimana karena itu, Iran 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 akan membahayakan eksistensi Iran di masa depan.

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.

Dari pembahasan-pembahasan di atas, dapat disimpulkan bahwa hipotesis peneliti terkait kepentingan operasi siber ofensif Iran terhadap konfliknya dengan Amerika Serikat, Israel, Arab Saudi adalah benar, yakni untuk melemahkan kemauan musuh dan mengancam musuh untuk melakukan perang konvensional dengan gangguan, kehancuran, kelelahan, atau paksaan. Salah satu strategi yang digunakan oleh Iran juga 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, menjanjikan 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

Buku dan Artikel dalam Buku:

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.

Hudson, V. M. (2014). *Foreign Policy Analysis, Classic and Contemporary Theory, Rowman & Littlefield*; Ch.4.

McKenzie, T. M. (2017). *Is Cyber Deterrence Possible. Air Force Research Institute.*

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

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

Jurnal Ilmiah:

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

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.*

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

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

Suryo, J. (2002). Pembentukan Identitas Nasional. Makalah Seminar Terbatas Pengembangan Wawasan tentang *Civic Education*.

Artikel dan Berita Online:

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

Disegi, Jonathan. (2016). *The Evolution of Iranian Cyber Warfare* [online]. Dalam https://www.academia.edu/30359761/The_Evolution_of_Iranian_Cyber_War

Morton, K, F & Grace, David. 2018. *A case study on Stuxnet and Flame Malware* [Online]. Dalam http://vixra.org/pdf/1209.0040v1.pdf. [Diakses 30 Maret 2018].

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;

Situs Pemerintah:

Australian Strategic Policy Institute. (n.d.). *Defining offensive cyber capabilities.* [online]. Dalam https://www.aspi.org.au/report/defining-offensive-cyber-capabilities [Diakses pada 13 Maret 2019].

Badan Pengembangan Bahasa dan Perbukuan. (n.d.). Status Quo, Klarifikasi, Kondusif, Modus Operandi, Dan Provokator. Diakses [online] pada 13 Maret 2019, melalui http://badanbahasa.kemdikbud.go.id/lamanbahasa/petunjuk_praktis/608

Kamus Besar Bahasa Indonesia. "strategi". Diakses [online] pada 12 November 2018 melalui https://kbbi.web.id/ strategi.