BAB I

PENDAHULUAN

1.1. Latar Belakang

Sun Tzu menyatakan fakta bahwa bentuk peperangan terbaik adalah mengalahkan musuh tanpa melawannya: *"One hundred victories in one hundred battles is not the most skillful. Seizing the enemy without fighting is the most skillful"* (Tzu, 2007). Kutipan tersebut seolah cukup menjelaskan bahwa kemenangan dapat dicapai melalui cara-cara yang lebih cerdas, efektif, dan tidak selalu melibatkan pertempuran terbuka. Dalam konteks hubungan internasional, menghindari konfrontasi langsung dapat menjadi pendekatan yang lebih bijaksana. Perang siber menjadi salah satu alternatif strategis untuk menghindari eskalasi konflik yang dapat berakibat buruk.

Seiring dengan berkembangnya ilmu pengetahuan dan teknologi dewasa ini perlahan menggeser pemahaman akan kekuatan *(power)* dan kedaulatan *(sovereignty)* suatu negara (Saputera, 2015). Kemajuan teknologi akibat revolusi industri yang telah memasuki era industri 4.0, atau dikenal dengan istilah *the Internet of Things* (IoT) telah mentransformasikan dunia nyata menjadi terdigitalisasi yang memungkinkan manusia tidak dibatasi oleh adanya ruang, waktu, dan jarak serta membuat pekerjaan menjadi lebih efektif dan efisien. Tidak hanya mampu menghasilkan berbagai macam produk canggih yang dapat membantu manusia *(artificial intelligence)*, dan kemudahan analisis informasi dalam *Big Data*, akan tetapi turut melahirkan the *Age of Disruption* yang dapat menciptakan berbagai macam bentuk ancaman siber *(cyber threats*) terhadap keamanan *(national security)* dan kedaulatan negara (Munirathinam, 2020b).

Keberadaan internet sebagai salah satu produk dari perkembangan teknologi saat ini membuat seluruh lapisan di dunia semakin terhubung dalam sinergi *the Power of One*. Era *the Power of One* telah mengantar aktor-aktor, baik individu, *non-state actors* (teroris, *hacktivists*), dan *nation states* untuk memanfaatkan informasi sebagai alat pengembangan dominasi dan pengaruhnya dalam percaturan politik global (Jajodia et al., 2015). Ketersediaan informasi yang luas dan bersifat *cross-borders* menyebabkan tidak adanya individu, perusahaan, bahkan negara sekalipun yang memiliki otoritas penuh terhadap internet. Dengan demikian, adanya konflik kepentingan serta penggunaan teknologi, informasi, dan komunikasi secara destruktif memicu terjadinya peperangan siber berbasis informasi (*Information Warfare* atau *Cyber Warfare*) yang mulanya peperangan tradisional diterapkan secara *real space* kini mulai beralih ke ranah *cyber space* (Czosseck & Geers, 2009; Jajodia et al., 2015).

Cyber Warfare digadang-gadang sebagai salah satu ancaman signifikan di abad ke-21. Hal ini dikarenakan kemampuan *Information Technology* (IT) yang dapat menyentuh segala aspek dan mendorong pola-pola baru dalam interaksi hubungan internasional. *Warfare* di era digital telah mengubah motif, bentuk, sasaran, aktor, sponsor, dan alat atau senjata perang (Andress et al., 2013). Selama ini perang konvensional hanya berfokus pada sumber daya yang terbatas dan bersifat membangun kekuatan militer yang dikendalikan oleh negara, namun yang terjadi saat ini individu dapat dengan mudah memanfaatkan teknologi untuk bersaing dalam skala global. Dunia virtual memungkinkan individu maupun *criminal group* untuk menciptakan virus, *malware,* dan menyembunyikan identitas mereka ketika menjalankan operasinya sehingga pemerintah kesulitan untuk melacaknya. Selain itu, proses persebaran dan pengaruh informasi, hak milik terhadap akses informasi, jaringan interkoneksi di media sosial, data pribadi konsumen, dan sistem yang menggerakkan *critical infrastructures* kini semakin menjadi perhatian negara (Andress et al., 2013). Sehingga, dapat ditarik benang merah bahwa ancaman siber tidak berbeda atau sama berbahayanya dengan ancaman militer lainnya.

Jika ditarik garis mundur, perjalanan hubungan penuh gejolak antara Amerika Serikat dan Iran dilihat dari sisi historis memang kerap memancing perhatian dunia. Memasuki tahun 2000-an tensi keduanya memanas karena adanya spekulasi Iran sedang membangun fasilitas pengayaan uranium dan George W. Bush memunculkan istilah *'axis of evil'* bersanding dengan Irak dan Korea Utara yang diduga tengah mengembangkan *Weapon of Mass Destruction*. 11 September 2001, merupakan kejadian paling memukul Amerika Serikat setelah aksi serangan terorisme menewaskan total 2.996 korban jiwa dan meruntuhkan dua menara kembar, yakni gedung *World Trade Center* dan *Pentagon* (History, 2019). *War on Terrorism* adalah bentuk respon Amerika Serikat pasca serangan 9/11 yang mulai menitikberatkan kebijakan luar negeri dan mendorong masyarakat internasional untuk memerangi segala tindakan terorisme (Chossudovsky, 2005).

Aksi saling balas antara dua kubu Amerika Serikat dan Iran pasca peristiwa 9/11 nampaknya berbuntut panjang. Situasi ini semakin diperkeruh oleh Amerika Serikat setelah meluncurkan serangan virus Stuxnet tahun 2010 yang menargetkan fasilitas nuklir Iran, sehingga memicu adanya retaliasi *tit for tat* (Cunningham, 2020b). Dalam *Game Theory,* strategi *tit for tat* digunakan untuk menggambarkan relasi timbal balik antara kedua belah pihak berdasarkan pada hubungan sebab-akibat (kausalitas) (Springer, 2015). Apabila salah satu pihak melakukan pengkhianatan, kecurangan, dan melanggar perjanjian atau kesepakatan kerjasama, maka pihak yang lain akan melakukan hal serupa. Hal ini dapat tercermin dari perjalanan hubungan antara kedua negara. Ketika Amerika Serikat bersikap kooperatif, maka Iran akan melunak dan menerima tawaran untuk bekerjasama. Sebaliknya, ketika Amerika Serikat 'mencederai' Iran, maka Iran akan membalas dengan perbuatan yang setimpal.

Kompleksnya hubungan Amerika Serikat dan Iran yang kerap mengalami pasang surut, membuat peneliti merasa topik ini menarik untuk diteliti. Terlebih, di balik berbagai serangan saling berbalas antara Amerika Serikat dan Iran terdapat faktor-faktor yang tidak lepas dari adanya intrik politik. Eskalasi konflik kedua negara semakin meningkat setelah terbunuhnya petinggi militer pasukan Quds,

Jenderal Qasem Soleimani (The Guardian, 2020). Serangan tersebut dikomando langsung atas perintah Presiden Trump menggunakan pesawat nirawak atau *drone* MQ-9 Reaper nyaris tak bersuara yang membawa misil Hellfire H9X. Dilansir dari *Cambridge University Press*, keberadaan Soleimani di Bandara Internasional Baghdad diamati oleh *drone* canggih yang memiliki sensor sensitif terhadap waktu dan mampu menembakkan rudal tepat pada target sasaran (Cambridge University Press, 2020). Trump, dalam pidato di kediamannya Mar-A-Lago Florida menyatakan alasan pembunuhan terhadap Jenderal Soleimani dikarenakan ingin melindungi Amerika dan dunia dari teror yang mengguncang Timur Tengah selama 20 tahun terakhir. Soleimani disebut-sebut sebagai orang yang harus bertanggungjawab atas kematian warga sipil Amerika dan sedang merencanakan serangan terhadap diplomat serta personel militer Amerika. Maka tindakan itu harus segera dihentikan untuk mengakhiri perang.

Akibatnya, pada 4 Januari 2020 *DHS's National Terrorism Advisory System* merilis buletin, yang menetapkan Iran sebagai *"State Sponsor of Terrorism"* karena secara aktif terlibat dalam serangkaian tindakan kekerasan dan mematikan yang mengancam *national security* Amerika Serikat. Lebih lanjut, dalam peringatan tersebut Amerika Serikat menetapkan *Islamic Revolutionary Guard Corps (IRGC)* sebagai organisasi teroris karena keterlibatan langsungnya dalam perencanaan kegiatan terorisme (Department of Homeland Security, 2020). Pasca tewasnya Soleimani, dunia dibuat geger dengan ramainya tagar *#WorldWarThree* dan *#HardRevenge* di media sosial yang bermunculan. Bahkan, banyak pihak meramalkan perang berskala besar akan terjadi. Sebagaimana yang diketahui Iran sudah belasan tahun membangun pengaruhnya di beberapa negara Timur Tengah, seperti Lebanon, Yaman, Suriah, hingga Irak. Hal ini membuat khawatir dunia apabila Iran akan mengibarkan bendera perlawanan bersama dengan para sekutunya.

Namun, peneliti memiliki pandangan lain. Mengingat dalam kondisi saat ini, Iran dan Amerika Serikat masih cukup 'waras' bahwa perang skala masif hanya akan membawa kerugian. Berbagai pencarian terdahulu sudah dilakukan guna

memahami *Cyber Warfare* antara Amerika Serikat dan Iran. Namun, peneliti tidak menemukan penelitian dengan judul atau sudut pandang yang mirip dengan peneliti. Meskipun demikian, peneliti tetap melakukan tinjauan pustaka sebagai sumber referensi untuk memperkaya pemahaman selama penelitian ini dilakukan. Beberapa dari studi terdahulu yang peneliti temukan adalah sebagai berikut:

Pertama, Miko Aditiya Suharto (2015) dari jurnalnya yang berjudul Analisis Yuridis Mengenai *Cyber Attack* dalam *Cyber Warfare* Berdasarkan Hukum Humaniter Internasional menjelaskan *cyber Attack* yang dilakukan AS terhadap Iran tergolong intervensi terhadap kedaulatan negara Iran. Dan alasan AS tidak sesuai dengan prinsip hukum humaniter internasional yakni: *non-use act of force* dan *non-intervention.* Meninjau proposal penelitian yang disusun oleh peneliti, maka jurnal ini memiliki kesamaan yaitu disebutkan bahwa salah satu *cyber attack* yang dilancarkan oleh Iran, Stuxnet dikategorikan sebagai *cyber weapon* dalam peperangan siber. Namun adapun perbedaannya, jurnal ini membahas serangan *cyber* AS terhadap program nuklir Iran dan mencari konsep *cyber attack* melalui definisi serangan konvensional lalu dianalisis dengan instrumen hukum yang ada.

Kedua, skripsi yang ditulis oleh Ary Melysa (2016) Mahasiswi Hubungan Internasional Universitas Diponegoro berjudul Analisis Penggunaan *Offensive Cyber Operations* Menghadapi Ancaman Nuklir Iran. Penelitian ini menjelaskan Amerika Serikat menggunakan *Offensive Cyber Operations* karena hadirnya beberapa keunggulan jika dibandingkan dengan *conventional military operations.* 1) Anonimitas, 2) Praktis dari segi jarak, biaya, dan risiko, 3) Mudah untuk dioperasikan, dan 4) Mudah dalam proses politik dan birokrasi. Berdasarkan tinjauan peneliti, terdapat kesamaan pembahasan menggunakan kerangka pemikiran *Offensive Realism*. Namun di samping itu, terdapat perbedaan peneliti dalam proposal penelitian ini mengambil sudut pandang Iran yang berusaha membangun *cyber power* untuk mengimbangi kekuatan Amerika Serikat.

Ketiga, Ralph Peter Martins (2018) dalam jurnalnya berjudul *Punching above their digital weight: Why Iran is developing cyberwarfare capabilities far beyond*

expectations memaparkan latar belakang Iran membangun kapasitas *cyberwarfare* berdasarkan proyeksi kekuatan, upaya perlindungan berdasarkan prinsip Revolusi Iran, dan respon terhadap agresi Barat serta nasionalisme Iran. Adapun kesamaan tulisan ini dengan proposal penelitian peneliti adalah melakukan analisis terhadap kapabilitas *Cyber Warfare* Iran. Di sisi lain, terdapat perbedaan di mana dalam tulisan Martins hanya terfokus satu arah pada satu negara, yakni Iran tanpa adanya keterlibatan dengan negara atau *non-state actors,* misalnya AS dan IRGC.

Keempat, hasil temuan Agustina Intan Prahawati (2020) dalam skripsinya berjudul Kebijakan *Cyber Security* Iran dalam Menghadapi Ancaman *Cyber Warfare* dijelaskan bahwa Iran memiliki kapabilitas nuklir yang patut diperhitungkan, namun seiring perkembangan teknologi informasi Iran menerima serangkaian *malware* berbahaya. *Malware* ini bertujuan untuk memperlambat pengayaan uranium Iran yang membahayakan bagi Israel dan Amerika Serikat. Maka dari itu, Iran menerapkan kebijakan sekuritisasi untuk menangkal serangan siber. Melalui analisa peneliti, kesamaan tulisan ini adalah membahas mengenai *Cyber Warfare* antara Iran dan Amerika Serikat. Namun, yang menjadi pembeda adalah Prahawati menggunakan perspektif *Cyber Security,* sedangkan peneliti menggunakan sudut pandang konsep *Cyber Warfare.*

Berdasarkan *literature review* diatas, secara umum argumen yang dibangun dalam kajian akademik terdahulu lebih meninjau pada sudut pandang hukum maupun sekuritisasi dalam menganalisis *Cyber Warfare* antara Amerika Serikat dan Iran. Walaupun demikian, kajian-kajian terdahulu terkait *Cyber Warfare* masih terbilang minim, topiknya beragam, dan memiliki ciri masing-masing. Hanya saja yang disayangkan topik-topik yang relevan cenderung berputar pada upaya pertahanan maupun perlindungan apabila terjadi serangan siber. Riset terdahulu tidak menawarkan faktor yang menjadi *underlying process* perilaku Iran. Alih-alih menyatakan perang terbuka sebagai respon atas tindakan AS, justru Iran mewujudkan dalam bentuk lain, yakni retaliasi *Tit-for-Tat* dalam ruang siber.

Dengan demikian, peneliti mencoba menggunakan kerangka pemikiran Neo-Realisme dalam Realisme Ofensif untuk meninjau berbagai macam faktor, analisis komparasi kapabilitas, strategi, instrumen, motif, tujuan, taktik yang digunakan, dan mengidentifikasi secara mendalam relasi aktor yang terlibat beserta potensi dampak yang ditimbulkan pada penerapan konsep *Cyber Warfare.* Di mana pasca terbunuhnya Jenderal Qasem Soleimani, Iran melakukan balas dendam tidak dengan perang fisik namun memanfaatkan kecanggihan teknologi yang diwujudkan dalam *Cyber Warfare*. Hal ini sekaligus mematahkan asumsi tradisional bahwa perang hanya dapat terjadi secara *real space* dengan penggunaan kekuatan militer. Faktor lain turut dipengaruhi oleh keberadaan *non-state actor,* yakni *terrorism group* di Iran dalam upaya menyebarkan idenya sebagai hegemoni regional.

1.2. Rumusan Masalah

Berangkat dari *problem driven research,* peneliti mengajukan pertanyaan penelitian **"Mengapa Iran mewujudkan serangan balas dendam dalam bentuk *'Cyber Warfare'* ke Amerika Serikat?"**

1.3. Tujuan Penelitian

Penelitian ini secara umum bertujuan untuk menjelaskan hubungan historis dan mengidentifikasi perilaku ofensif Iran terhadap AS pasca peristiwa 9/11 hingga sekarang, mengetahui faktor-faktor penyebab dan mengungkap alasan Iran melakukan retaliasi siber terhadap Amerika, dan mengkaji secara mendalam motif, instrumen, serta tujuan keamanan yang diterapkan kedua negara dalam *Cyber Warfare* untuk membangun dan mengelaborasi teori berdasarkan kenyataan sehingga menjadi penjelasan yang lengkap.

1.4. Manfaat Penelitian

Dari penelitian yang dilakukan oleh peneliti, maka manfaat yang akan diberikan antara lain:

1.4.1. Manfaat Teoritis

Penelitian ini berupaya menambah wawasan dan rujukan dalam ilmu pengetahuan khususnya Ilmu Hubungan Internasional, serta menambah wawasan terkait implementasi konfliktual dan persaingan antarnegara berdasarkan perspektif Neo-Realisme dan konsep *Cyber Warfare*.

1.4.2. Manfaat Akademis

Penelitian ini berupaya memberikan kontribusi ilmiah berupa penjelasan faktor kausal *Cyber Warfare* yang telah mengubah persepsi perang konvensional dan mulai beralih ke aspek nirmiliter terkait strategi, instrumen, motif, serta tujuan keamanan yang diterapkan kedua negara AS dan Iran dalam menghadapi *cyber attack*. Lebih jauh lagi, diharapkan dapat memberikan kontribusi dan menjadi sumber referensi lebih bagi perkembangan Studi Siber dan Politik Internasional.

1.4.3. Manfaat Praktis

Penelitian ini sekiranya dapat menjadi peluang untuk memberikan *new insights* terkait rekomendasi kebijakan penyelesaian konflik yang dapat diterapkan di masyarakat dan mampu mengidentifikasi konfrontasi antarnegara yang motifnya bersifat *intangible*.

1.5. Kerangka Pemikiran

Untuk menjawab pertanyaan penelitian, maka peneliti akan menggunakan teori Neorealisme dan konsep *Cyber Warfare* yang nantinya akan dijadikan sebagai pegangan penelitian.

1.5.1. Neo-Realisme

Dalam tulisannya yang berjudul *Theory of International Politics,* Kenneth Waltz (1979) memaparkan ketika negara-negara berada dalam sistem yang anarki maka negara-negara tersebut harus bersiap menghadapi segala situasi karena natur dari negara adalah negara yang berperang *(the nature of the state is a state of war)*. Ini bukan berarti bahwa perang pasti terjadi tapi ketika suatu negara menggunakan *force* atau tidak, perang sewaktu-waktu bisa terjadi (Waltz, 1979). Aliran neorealisme bertujuan untuk menjawab faktor penyebab terjadinya perang. Waltz melihat realisme klasik terlalu menekankan pada *human nature* yang jahat dan *animus dominandi* sebagaimana ambisi negara mengejar kekuasaan menjadi penyebab perang. Sedangkan asumsi dasar dari neorealisme adalah perang terjadi karena adanya struktur internasional, yakni berupa tekanan struktur *(structural constraint)* dari sistem internasional yang anarki. Neorealisme melihat secara *outside looking in* yang mana berbeda dengan realisme klasik *inside looking out.* Waltz menjabarkan struktur sebagai *'ordering principle'* yang merupakan aturan main dalam tatanan internasional. Level analisis dalam neorealisme meninjau pada struktur sebagai level analisis *'third image'*, level domestik sebagai *'second image'*, dan individu dalam posisi *'first image'.* Perubahan dalam politik internasional ditentukan oleh faktor distribusi kapabilitas, hal ini berkaitan dengan kemampuan ekonomi dan kekuatan militer (Waltz, 1979).

Sebagaimana dijelaskan oleh Kenneth Waltz kunci gagasan Neo-Realisme adalah sebagai berikut: 1) Sistem internasional anarki, tidak ada otoritas tertinggi atau terpusat yang dapat memaksakan hukum pada setiap negara; 2) Negara akan

bertindak dengan basis *self-help* dengan maksud untuk bertahan ketika menjalin interaksi dengan negara lain; 3) Struktur hanya akan berganti ketika negara dengan kekuatan besar memiliki intensi untuk mengubah struktur, atau negara yang lemah akan menyeimbangkan kekuatan mereka sebagai upaya bertahan diri. Dan terkadang disebut sebagai distribusi kekuatan, ketika negara memerhatikan keamanan nasionalnya, maka ia berusaha untuk memaksimalkan *relative power.* Dalam konteks sistem internasional yang anarkis, negara cenderung berinteraksi seperti bola biliar yang saling berbenturan. Hal ini dikarenakan anarki *'the only game in town'* sehingga perilaku negara mengarah pada *"like unit"* atau seragam. Neorealisme menegaskan bahwa negara terlepas dari tingkat kemakmuran, geografi, jumlah penduduk, kemampuan militer, maupun bentuk pemerintahannya bukan berjuang meraih kekuasaan *(struggle for power)*, melainkan memiliki orientasi yang sama dalam mencari keamanan *(security seeking under anarchy).* Negara besar menentukan pengaruh yang lebih besar dalam konstelasi politik internasional, sementara negara kecil memiliki pengaruh yang lebih kecil (Burchill et al., 2013; Jackson & SØrensen, 2013).

Prinsip *self-help* adalah prinsip paling penting dalam sistem anarki. Dengan adanya *self-help* dalam sistem anarki maka setiap negara yang ada akan berusaha untuk berbuat sesuatu yang berkaitan dengan proteksi negaranya. Dalam *self-help* juga akan terlihat sampai sejauh mana sebuah negara dapat bertahan dalam sistem tersebut. Ketika negara mampu bertahan dengan situasi anarki yang ada, ini akan berpengaruh kepada perilaku negara. Selain itu elemen lain dalam sistem anarki adalah *power* dan proses *struggling*. Negara-negara dalam sistem anarki bertindak demi kepentingan mereka dan tak jarang menggunakan *force* untuk mendapatkan kepentingannya (Waltz, 1979).

Waltz menuliskan bahwa hal yang dapat membuat sistem anarki stabil adalah *balance of power*. *Balance of power* adalah kondisi untuk mempertahankan stabilitas sistem yang ada (dalam hal ini adalah sistem yang anarki) tanpa harus merusak keberagaman elemen atau unit (negara) dalam sistem itu sendiri. *Balance of power*, menurut Waltz, dapat terjadi dikarenakan dua hal: karena sistem itu

adalah sistem yang anarki dan negara-negara dalam sistem tersebut ingin *survive*. Dengan demikian, negara-negara dalam sistem anarki akan berusaha bertahan dalam sistem ini demi terciptanya kondisi *balance of power*. Ada dua jenis sarana *(means)* bagi negara untuk mencapai kondisi *balance of power: internal balancing* (seperti meningkatkan kapabilitas/kemampuan ekonominya, meningkatkan kekuatan militer, atau mengembangkan sejumlah strategi) dan *external balancing* (seperti misalnya memperkuat dan memperbesar aliansi untuk melemahkan lawan).

Adanya *balance of power* membuat ekspektasi bahwa perilaku negara akan disesuaikan dengan *balance forming*. Ketika dihadapkan pada ancaman-ancaman yang datang dari luar, maka negara dapat memilih untuk melakukan *balancing* atau *bandwagoning*. *Balancing* adalah situasi dimana negara-negara dalam sistem akan berusaha untuk membentuk koalisi demi menghadapi ancaman tersebut untuk mempertahankan *status quo.* Ketika dalam koalisi *balancing* ini ada satu negara yang lebih mendominasi, maka negara lain akan memilih opsi *bandwagoning* daripada harus melanjutkan koalisi tersebut. Sedangkan, *bandwagoning* memiliki pengertian menjajarkan dengan lawan, yang mana dimaksudkan negara-negara lemah akan bersekutu dengan negara *rising power* untuk *spoils of victory.* Yang sebenarnya harus menjadi perhatian negara-negara yang ada dalam sistem adalah bukan untuk memaksimalkan *power* tetapi untuk mempertahankan posisinya dalam sistem tersebut (Burchill et al., 2013). Hal ini tidak terlepas dari upaya negara dalam memperbesar kekuasaan dapat berisiko bagi negara itu sendiri. Iklim internasional yang kompetitif membuat negara menghadapi ketidakpastian mengenai dampak dari perluasan kekuasaan, seperti meningkatnya persenjataan dan konflik. Maka dalam rangka mencapai keamanan, negara lebih memprioritaskan kepentingan keamanan daripada kepentingan kekuasaan (Taliaferro, 2000).

Dalam tulisannya yang berjudul *The Origins of War in Neorealist Theory*, Waltz menjelaskan bahwa ada dua "faktor kembar" dalam sistem anarki yang dapat menyebabkan kompetisi dan konflik. Kedua "faktor kembar" itu adalah: 1) Karena negara berada dalam tatanan anarki dan negara harus mengamankan negaranya; dan 2) Karena adanya ancaman atau sesuatu yang berpotensi sebagai ancaman yang

mengancam keamanan negaranya (Burchill et al., 2013). Negara mulai mengidentifikasi hal-hal yang mengancam negara dan jika mereka memiliki *power* tertentu maka mereka akan coba menangkal hal-hal yang mengancam negaranya tersebut. Setiap negara akan melakukan usaha-usaha tertentu untuk mengamankan negaranya. Secara kolektif, negara-negara dapat memilih untuk melakukan aliansi atau justru melakukan perlombaan persenjataan *(arms race)* (Waltz, 1979).

Negara-negara dalam sistem anarki juga harus bersiap menghadapi keadaan *security dilemma*, yaitu keadaan ketika baik itu meningkatnya atau melemahnya keamanan suatu negara akan berpengaruh terhadap negara lainnya. Di lain sisi, keadaan ini bisa berpotensi mendorong negara-negara yang ada untuk membentuk satu aliansi jika ditemukan kesamaan kepentingan di antara negara-negara ini, misalnya karena kekhawatiran atau ketakutan bersama terhadap satu atau beberapa negara (Jackson & SØrensen, 2013).

Beberapa argumen besar di negara Barat akan *'perpetual peace'* nampaknya sedang diagung-agungkan. Saat ini negara-negara sedang memasuki dunia kecil akan kemungkinan bahwa negara akan terlibat dalam perang. Berseberangan dengan perspektif liberal, realis lebih pesimis ketika memandang politik internasional. Meskipun sepakat bahwa dunia yang damai merupakan hal *favourable* namun tidak dapat menutup kemungkinan akan terjadi persaingan antarnegara. Waltz, memperkenalkan *'defensive realism'* dan Mersheimer *'offensive realism'* yang sama-sama merupakan teori struktural politik internasional, tetapi yang menjadi pembeda adalah realisme defensif lebih berfokus pada upaya untuk menjaga *balance of power*, sedangkan dalam realisme ofensif negara akan cenderung agresif dengan melakukan apapun yang dapat dilakukan sehingga dapat memaksimalkan *relative power* dengan cara hegemoni sebagai tujuan utama. Negara dengan kekuatan besar justru berpotensi takut terhadap satu sama lain karena saling memandang curiga dan khawatir perang akan terjadi. Dasar dari ketakutan ini adalah karena negara dapat sewaktu-waktu menyerang dengan motif dan tujuan tertentu. Meskipun negara dapat menjalin mitra aliansi dengan negara lain, tetapi hal ini hanya bersifat sementara (Ripsman et al., 2016).

Dalam penelitian ini, peneliti mencoba menemukan alasan mengapa AS dan Iran meskipun dua negara dengan kekuatan besar memilih untuk mentransformasikan persaingan mereka kedalam bentuk baru yakni *Cyber Warfare,* bukan adu senjata militer. Selanjutnya, melihat dari sisi historis hubungan AS dan Iran yang tidak pernah akur, muncul spekulasi peneliti apa sebenarnya motivasi Iran dalam memberikan respon terhadap serangan siber yang dilancarkan oleh AS. Peneliti menduga, adanya struktur internasional yang anarki memaksa negara-negara yang terancam oleh kekuatan negara besar untuk menyelamatkan diri demi keamanan nasional mereka berbasis *self-help*. Salah satu caranya adalah dengan meningkatkan kapabilitas agar tercipta *balance of power*. Iran sebagai negara yang khawatir akan serangan siber AS yang mampu melumpuhkan *critical infrastructures* pasca peristiwa Stuxnet, mulai mengembangkan kekuatannya dengan menerapkan *balancing* dan *bandwagoning*. *Balancing* berusaha menyeimbangkan ancaman siber yang ditujukan AS, dan *bandwagoning* ketika Iran berusaha menjalin aliansi dengan negara lain. Maka dari itu negara akan saling berbagi informasi untuk mempromosikan keamanan.

Terlihat pula AS berusaha mendominasi sistem internasional; hegemoni sebagai tujuan akhir. AS khawatir apabila tidak merespon akan muncul *asymmetric warfare* atau perang dengan skala lebih kompleks lagi, yakni *hybrid warfare.* Serangan balasan Iran *(Tit-for-Tat)* merupakan strategi *defensive realism* yang digunakan Iran untuk melindungi kepentingan nasional di sistem internasional.

1.5.2. *Cyber Warfare*

Menurut (Nye, 2012) ancaman siber terbagi menjadi empat kategori, yang didasarkan pada pembedaan dengan siapa mereka berasosiasi (aktor negara atau aktor non-negara). *Cyber war* dan *cyber espionage* diinisiasi dan disponsori oleh negara, sementara *cyber crime* dan *cyber terrorism* diinisiasi dan disponsori oleh aktor non-negara (teroris dan kriminal). *Cyber threats* dapat bermanifestasi dalam banyak cara termasuk *cyber attacks,* seperti *syntactic attacks* (virus, *malware*,

worms, *trojan horses*), *phishing, cross-site scripting, SQL injection, backdoors, Distributed Denial of Service* (DDoS), dan serangan teroris melalui komunikasi elektronik (Yager et al., 2015).

Definisi *Cyber Warfare* di dalam buku *Cyber Warfare Building the Scientific Foundation* (Jajodia et al., 2015), bahwasanya serangan dunia maya bergantung pada aktor, motivasi, target dan tindakan yang dapat pula disebut sebagai *cyber terrorism*, *cybercrime*, atau *cyber activism*. Terdapat empat mode konflik memengaruhi politik internasional di bidang siber, yaitu: 1) Perang media sosial yang memengaruhi politik internal negara dan menyebabkan pemberontakan sosial yang menyebabkan perubahan politik, 2) Perang strategis dengan menyebabkan kerusakan bagi musuh dan sumber daya alam, misalnya spionase industri dan mengembangkan alat agar dapat mematikan aktivitas permusuhan, misalnya infrastruktur pada kekuasaan, komunikasi, media, dan internet, 3) Pertarungan ideologi dimana organisasi yang bersifat fundamental menggunakan internet untuk menyebarluaskan ideologi mereka dan merekrut anggota dari negara lain untuk memenuhi tujuan mereka, 4) Perang yang dipelopori oleh warga negara yang secara langsung menyerang warga negara lain dan institusi sebagai bagian dari konflik yang lebih besar. Jaringan *critical infrastructure* untuk saat ini merupakan target utama bagi serangan siber karena sistem komando dan kontrol pemerintahan dan juga sistem senjata terhubung dalam *Global Information Grid* (GIG) atau perangkat *chips* (Winterfeld & Andress, 2013). Pesawat digunakan sebagai *router* untuk menerima dan mengirim informasi penargetan. Pertahanan terhadap udara dan *artillery* dipandu oleh sistem komputer dan menembakkan amunisi berdasarkan *Global Positioning System* (GPS). *The Intelligence Surveillance and Reconnaissance* (ISR) *systems* mengumpulkan banyak informasi dan menyaring data-data penting.

Adanya *Cyber Warfare* telah menyebabkan perubahan yang disebut sebagai *Electronic Warfare, Information Superiority, Information Dominance, Network Centric Warfare, Information Warfare Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance* (C4ISR) *Hyperwar,*

Netwar, dan *Third Wave Warfare*. Selain itu, siber juga berhubungan langsung dengan *drone* (kendaraan tak berawak) atau UAV (*Unmanned Aerial Vehicles)*, *nanotechnology*, *robotics*, dan bioteknologi. Siber dibangun diatas infrastruktur fisik namun yang membuat unik karena memiliki komponen virtual (Carr, 2009).

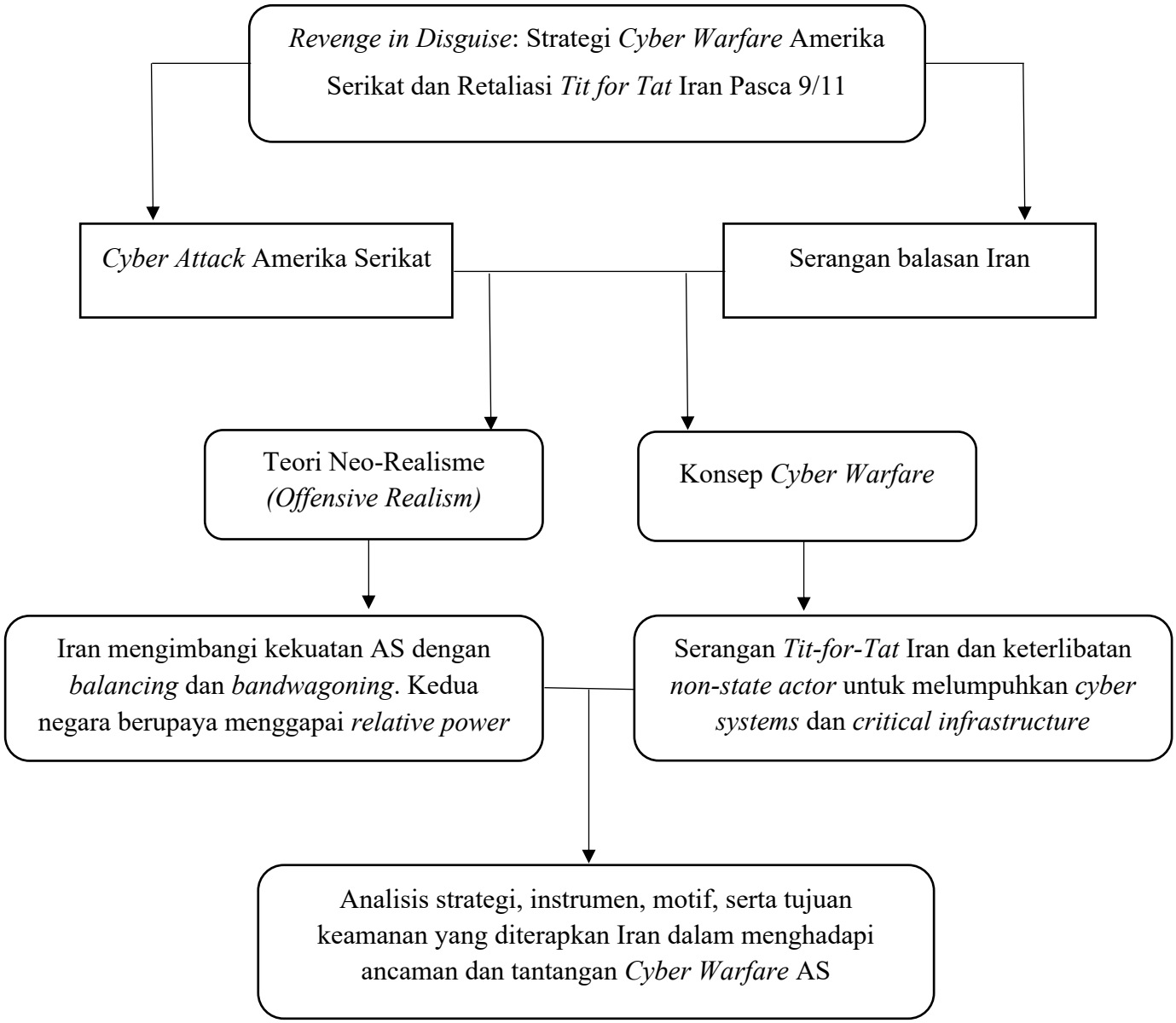
Cyber Warfare dapat diartikan sebagai perang di dalam *cyberspace*, namun penyerangannya berbeda dengan perang konvensional. Media utama yang digunakan adalah komputer dan internet. Objek yang diserang bukanlah fisik, seperti wilayah teritorial, geografis, melainkan objek dalam *cyberspace* yang dikuasai oleh suatu negara. Sehingga dapat ditarik kesimpulan, bahwa *Cyber Warfare* merupakan perang yang dilakukan dalam ruang maya. Karakteristik utama dalam *Cyber Warfare* adalah penggunaan *cyber weapon* yang berkaitan dengan *cyber systems*. Objek yang diserang di dalam *Cyber Warfare* adalah sebuah *cyber systems* yang berkenaan langsung dengan pemerintahan negara di dalam negara yakni *cyber infrastructure*. Dalam Tallin Manual disebutkan bahwa *cyber infrastructure* memiliki pengertian *"a physical or virtual system and assets under jurisdiction of a state that are so vital that their incapacitation or destruction may debilitate a State's security, economy, public health or safety, or the environment."* (Mazanec & Bradley, 2015)

Dari beberapa contoh diatas, dapat dilihat bahwa lumpuhnya aktivitas pemerintahan yang berbasis komputer dan internet dalam *Cyber Warfare* menyebabkan sulit untuk menentukan pelaku *Cyber Warfare*. Sulit untuk benar-benar membuktikan bahwa pelaku tindakan kejahatan *Cyber Warfare* adalah negara (Rosenzweig, 2013a).

Sehingga menurut penjelasan diatas dapat dirinci sebagai berikut:

1. Subjek: negara atau *hacker group (non-state actor)*
2. Objek yang diserang: *cyber systems* dan *cyber infrastructure*
3. Metode: *Cyber Attack* tertentu
4. Sarana: *Cyber Weapon*
5. Motif: mendapat akses terhadap *cyber infrastructure* negara lawan

1.6. Skema Kerangka Berpikir



1.7. Argumen Penelitian

Setelah insiden *Stuxnet* dan terbunuhnya Jenderal Qasem Soleimani, kekhawatiran akan serangan siber yang mampu memberikan dampak signifikan membuat Iran berada dalam bayang ancaman negara adidaya AS. Kendati dalam sistem internasional yang anarki; dilihat dari dunia yang tidak pasti kapan terjadinya perang, negara selalu siap siaga dalam mengembangkan kapabilitas agar tercipta *balance of power*. Peneliti menduga negara-negara yang merasa terancam oleh kekuatan negara besar berupaya menyelamatkan diri demi keamanan nasional berbasis *self-help*. Iran mencari alternatif lain untuk menghindari perang fisik serta memanfaatkan teknologi canggih dengan biaya lebih murah dan efektif. *Cyberwarfare* dimaksudkan untuk menggapai *relative power* dalam meredam ancaman *cyberattack* AS dengan cara memiliki kekuatan yang lebih unggul. Maka dari itu, Iran berusaha *climbing to the top* menerapkan *balancing* dan *bandwagoning*. Serangan balasan Iran *(Tit-for-Tat)* merupakan strategi *offensive realism* yang digunakan Iran untuk memperluas kekuasaannya menjadi hegemon di kawasan dibantu oleh kehadiran kelompok teroris sebagai aktor non-negara.

1.8. Operasionalisasi Konsep

1.8.1. Definisi Konseptual

1.8.1.1. Ruang Siber *(Cyberspace)*

> Dunia maya merupakan ruang halusinatif, tidak berbentuk, dan bersifat *virtual* yang terhubung dalam komputer, jaringan internet, *router, server* dan bagian elemen lain dalam prasarana internet. Aktivitas berselancar di internet, menonton video, mengunduh foto, mengirim pesan melalui suatu *platform,* dan mengunggah status di media sosial terjadi dalam ruang siber (Springer, 2015). Dalam

cyberspace, tidak ada negara sekalipun yang memiliki otoritas terhadap internet.

1.8.1.2. Serangan Siber *(Cyberattack)*

Cyberattack merupakan serangan yang dilakukan dalam ranah dunia maya untuk mencapai suatu tujuan. Sifatnya ofensif dengan menyerang sistem informasi komputer, infrastruktur, jaringan komputer, maupun perangkat komputer sebagai target sasaran. Misalnya, *ransomware, DDoS attack,* dan *malware* (Winterfeld & Andress, 2013).

1.8.1.3. *Tit-for-Tat*

Tit-for-Tat merupakan sebuah strategi berdasarkan pada konsep pembalasan dan untung-rugi. Konsep ini diperkenalkan ketika menghadapi situasi dilema *(Prisoner's Dilemma).* Dalam strategi ini, negara akan bersikap kooperatif apabila rekannya pernah membantu, sebaliknya akan berkhianat apabila pernah dicurangi (Cunningham, 2020b) .

1.8.2. Definisi Operasional

1.8.2.1. Ruang Siber *(Cyberspace)*

Dalam penelitian ini, keberadaan ruang maya untuk memfasilitasi persaingan dan konflik yang dimanfaatkan oleh AS dan Iran dalam perang berbasis siber akibat adanya konflik kepentingan serta penggunaan teknologi, komunikasi, dan informasi secara destruktif. Ketersediaan data yang luas, sifatnya *cross-border,* dan kemudahan akses membuka peluang bagi Iran untuk mencapai *relative power* dengan keterlibatan *non-state actors* untuk

melumpuhkan *critical infrastructures* dan *cyber systems* pihak lawan (Mazanec & Bradley, 2015).

1.8.2.2. Serangan Siber (*Cyberattack)*

Peneliti akan berfokus pada serangan siber yang dilakukan oleh kedua negara, AS dan Iran yang menargetkan infrastruktur kritis seperti rumah sakit, institusi perbankan, sistem transportasi yang langsung terhubung dengan sistem kontrol terpusat *Global Information Grid* (GIG) dan perangkat *chips.* Media utama komputer, internet, dan *removable devices* dapat menjadi perantara untuk mentransfer *virus, malware, ransomware* untuk menghancurkan data penting atau memperoleh kepentingan militer dan bisnis. Hal ini didapati dari serangan AS kepada Iran seperti Stuxnet, yang kemudian Iran turut merespon dengan melancarkan serangan balasan dalam *Operation Cleaver dan Ababil.*

1.8.2.3. *Tit-for-tat*

Dalam analisis ini, Iran melakukan balas dendam terhadap AS dengan melakukan serangan balasan berbasis teknologi dengan cara *hacktivism* dan rekayasa sosial yang melibatkan *terrorism group,* untuk spionase, mencuri *intellectual property,* dan data penting AS. Selain itu, pembajakan akun resmi media sosial pemerintahan untuk menyebarkan propaganda anti-Amerika yang lebih lanjut akan dibahas dalam bab berikutnya (Whyte & Mazanec, 2019).

1.9. Metodologi Penelitian

Penelitian ini dibuat guna membantu menambah pemahaman mengenai hakikat dari *Cyber Warfare* yang telah mengubah persepsi perang konvensional dan mulai beralih ke aspek nirmiliter. Lebih jauh lagi, diharapkan dapat memberikan kontribusi lebih bagi perkembangan Studi Siber dan Politik Internasional. Metode penelitian yang digunakan adalah eksplanatif-kualitatif dengan pengujian studi kasus secara rinci. Adapun penelitian ini menggunakan konsep *Cyber Warfare* mengutamakan penggunaan teknologi dengan teknik dan taktik untuk menyerang dan mencapai kepentingan suatu negara yang dapat memangkas biaya perang, tidak memakan korban jiwa, relatif murah, sulit untuk melacak identitas pengirim serangan siber karena seringkali menggunakan *proxy* dari negara lain. Namun, memiliki potensi besar untuk menghilangkan, bahkan merusak sistem data dan informasi, infrastruktur publik, dan gangguan kegiatan militer yang merugikan ekonomi negara. *Tit for Tat Strategy* menjelaskan dinamika hubungan AS-Iran yang sempat mesra dan kini memanas.

1.9.1. Metode Penelitian

Penelitian ini dilakukan dengan metode eksplanatif, yaitu metode untuk mengidentifikasi faktor-faktor penyebab dan mencari penjelasan dari suatu fenomena maupun perilaku antarnegara yang berhubungan dengan sebab-akibat. Tujuan metode eksplanatif adalah membuktikan adanya hubungan kausal antara dua atau beberapa variabel yang berbeda. Di tahap akhir penulisan ini, peneliti berfokus pada penemuan fakta-fakta sebab akibat mengenai hubungan historis AS-Iran sebagaimana adanya hingga saat ini, dan motif aksi saling berbalas yang dilayangkan kedua belah pihak, untuk dikaitkan dengan konsep *Cyber Warfare*.

1.9.2. Jenis Penelitian

Selanjutnya, peneliti menggunakan jenis pendekatan kualitatif atau disebut sebagai pendekatan naturalistik karena penelitiannya dilakukan pada kondisi yang alamiah tanpa ada rekayasa dari peneliti (Sugiyono, 2007, hal. 8). Pendekatan kualitatif berusaha untuk mendapatkan gambaran dan penjelasan dari permasalahan sosial yang dipilih (Moleong, 2007), bukan untuk mengkaji kekuatan antar variabel seperti pendekatan kuantitatif. Dalam mengkaji permasalahan sosial, penelitian ini mengambil satu studi kasus, yaitu *Cyberwarfare* antara kedua negara AS dan Iran. Studi kasus adalah kegiatan dimana peneliti menggali sebuah kesatuan atau fenomena tunggal yang dibatasi oleh waktu dan aktivitas tertentu dengan menggunakan informasi rinci yang diperoleh dari berbagai prosedur pengumpulan data (Creswell, 1994)(Neuman, 2014).

Melalui penjelasan di atas maka dapat disimpulkan bahwa dalam penelitian ini, peneliti berusaha memperoleh gambaran dan penjelasan lebih lanjut mengenai dimensi strategi, taktik, instrumen, motif, dan tujuan perang dalam ranah *cyberspace* melalui studi kasus *Cyberwarfare* AS-Iran.

1.9.3. Teknik Pengumpulan Data

Dalam melakukan penelitian mengenai *Cyber Warfare* melalui studi kasus Konflik AS-Iran, peneliti menganalisis dengan menggunakan data sekunder yang diperoleh melalui studi literatur dengan kajian kepustakaan yang meliputi buku, jurnal internasional, *research and government report*s, *think-tanks,* dokumentasi dan berita dari media massa yang diakses melalui internet maupun perpustakaan secara langsung. Penelitian ini menggunakan sumber-sumber buku dan

artikel jurnal terkait dengan teori Neo-Realisme, konsep *Cyber Warfare*, dan sumber yang mendukung analisis studi kasus konflik AS-Iran dalam perang maya. Beberapa sumber spesifik menjadi rujukan peneliti, salah satunya situs resmi pemerintah, yakni US *Department of Defense,* US *Department of Homeland Security,* US *Cyber Command, Iranian Supreme National Security Council,* dan *Iranian Ministry of Communications and Information Technology.* Peneliti mengklasifikasikan organisasi, seperti RAND *Corporation, Brookings Institution,* dan *Center for Strategic and Internasional Studies* (CSIS) sebagai *think-tanks* yang memberikan studi dan analisis tentang perang siber dan hubungan internasional. Dalam memahami perang siber antara AS dan Iran, peneliti berusaha menggali *online databases* yang diperoleh dari *Scopus, Google Scholar,* JSTOR, dan *Science Direct* diantaranya *Internasional Security, Journal of Strategic Studies,* dan *Survival: Global Politics and Strategy.* Peneliti serta memanfaatkan publikasi jurnalisme seperti *The New York Times, The Wall Street Journal, Reuters, BBC,* dan sumber lainnya yang memiliki kredibilitas tinggi dan terpercaya.

Untuk menjawab rumusan masalah "Mengapa Iran mewujudkan serangan balas dendam dalam bentuk *'Cyber Warfare'* ke Amerika Serikat?" Peneliti akan terlebih dahulu mencoba mengumpulkan informasi mengenai konsep *Cyber Warfare* dalam hubungan internasional untuk memperoleh pemahaman agar dapat menemukan faktor kausal (sebab-akibat) beserta strategi, instrumen, motif, dan tujuan AS-Iran dibalik aksi perang saling berbalas di ruang maya. Pada akhirnya, tahapan-tahapan diatas akan memberikan penjelasan alasan Iran melakukan serangan balasan ke AS dalam bentuk perang siber.

1.9.4. Teknik Analisis Data

Peneliti menggunakan teknik analisis data menggunakan metode penelusuran hubungan kausal atau metode kongruen, di mana peneliti dalam prosesnya melakukan pencocokan data dan teori yang sebangun melalui studi kasus. Metode ini berangkat dari teori dan berusaha menjawab rumusan masalah kausalitas dengan pertanyaan 'mengapa' untuk menganalisa pemikiran dari teori tersebut yang memprediksi atau menjelaskan hasil dari kasus tertentu (George & Bennett, 2005, p. 301). Pertama, peneliti memastikan variabel independen yang lalu dianalisis apakah prediksi atau ekspektasi penelitian sudah sesuai dengan variabel dependen, sehingga dalam proses ini tidak semua data terbilang relevan dan dapat disajikan. Maka dari itu, perlu adanya filter menggunakan teori (Mills et al, 2010, p. 63). Metode penelitian ini digunakan karena peneliti berupaya untuk membuktikan kesesuaian antara teori dengan motif dari peristiwa yang digunakan sebagai studi kasus penelitian. Dengan penggunaan metode kongruen, peneliti berfokus pada hubungan antara variabel dependen dengan variabel independen atau korelasi antara X dan Y, di mana penelitian akan berawal dari analisis variabel independen melalui kerangka pemikiran Neo-Realisme yang akan menentukan penyebab peristiwa dan pada akhirnya menghasilkan akibat dari peristiwa pada penelitian.

Peneliti berusaha mengumpulkan sekumpulan pengamatan yang beragam berdasarkan pada tiap kasus dan kemampuan dalam merefleksikan hubungan antara pengamatan empiris dan konsep abstrak. Melalui pendekatan ini, variabel dependen dan independen dioperasionalkan menggunakan indikator ganda dengan triangulasi. Peneliti menggunakan studi kasus untuk memberikan bukti empiris terhadap kekuatan relatif dan signifikansi penjelasan dari satu teori dibandingkan teori lainnya. Pada subtipe pertama, teori positivis dan

realis hanya berupaya memverifikasi atau menyangkal teori melalui pengujian empiris. Sedangkan, dalam teori divergen menempatkan adanya pertentangan teori satu sama lain dalam upaya untuk menentukan teori mana yang terbaik dan paling cocok dengan studi kasus yang diangkat. Asumsi ini menyiratkan bahwa teori tidak hanya memberikan dasar penjelasan yang komprehensif tetapi juga sebagai tujuan inovasi konseptual dan praktis (Blatter & Haverland, 2012).

Peneliti menyoroti negara-negara yang lemah cenderung mengalami kekalahan militer apabila berusaha melawan negara besar. Negara dalam sistem internasional dapat tertekan dengan lingkungan sekitarnya atau tindakannya cenderung diatur dan dibatasi. Dengan demikian, dalam sistem internasional yang anarki, Iran selalu merasa berada dalam bayang ancaman AS sebagai negara adidaya. Adanya rasa takut ini membuat Iran terdorong untuk berperilaku mengarah pada *balance of power* dan memanfaatkan penggunaan teknologi sebagai alat untuk perang. Sehingga dalam rangka mencapai *balance of power,* Iran terus melancarkan serangan balasan untuk bertahan diri dan membangun kekuatan dengan strategi *offensive realism* pada perang siber.

Dalam menarik kesimpulan, sejak awal peneliti berusaha untuk mengamati pola, tema, hubungan, hipotesis, dan fakta-fakta empiris perang siber yang terjadi antara AS dan Iran dengan menggunakan bingkai pemikiran Neo-Realisme dan konsep *Cyber Warfare* untuk dituangkan ke dalam kesimpulan yang sifatnya masih tentatif. Artinya, seiring peneliti menemukan dan memverifikasi data yang baru, kesimpulan yang awalnya masih goyah juga akan senantiasa diperbaiki dan diverifikasi dengan data baru tersebut, hingga pada akhir penelitian peneliti memperoleh kesimpulan.

1.10. Sistematika Penelitian

Penelitian ini terdiri dari empat bab. Bab I merupakan bagian pendahuluan yang memberikan gambaran secara umum terkait penelitian yang dilakukan dengan memaparkan latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, kerangka konseptual, hipotesis, metodologi penelitian, dan sistematika penulisan.

Bab II merupakan bagian pembahasan gambaran umum *Cyberwarfare,* perkembangan sejarah dan dinamika, serta linimasa perang maya AS-Iran pasca 9/11 hingga saat ini. Selanjutnya, akan dilengkapi dengan pembahasan ancaman dan tantangan yang melekat dalam *Cyberwarfare.*

Bab III merupakan bagian pembahasan yang lebih mendalam dan analisis terkait distribusi kekuatan, pengembangan strategi, instrumen, motif, serta tujuan keamanan yang diterapkan dan Iran dalam menghadapi *cyberattack* AS. Selanjutnya akan dilengkapi dengan analisis komparasi kapabilitas, taktik yang digunakan, dan mengidentifikasi secara mendalam relasi aktor yang terlibat beserta potensi dampak yang ditimbulkan dengan menerapkan konsep *Cyberwarfare.*

Bab IV merupakan bab penutup yang berisi kesimpulan dan saran, agar penelitian ini sebaiknya dilanjutkan oleh peneliti lain di masa depan. Kesimpulan pada Bab IV berfungsi untuk menegaskan temuan penelitian dan membuktikan apakah hasil penelitian sejalan dengan dugaan awal peneliti. Saran pada Bab IV berisi kekurangan dan evaluasi dari penelitian ini. Diharapkan, kekurangan tersebut dapat diperbaiki oleh peneliti selanjutnya.