BAB II

TINJAUAN PUSTAKA DAN KERANGKA PEMIKIRAN

2.1 Tinjauan Pustaka

2.1.1 Hubungan Internasional

Hubungan internasional merupakan studi politik yang dinamis. Cakupan dalam fenomena – fenomena internasional yang heterogen menjadi keunikan dalam setiap pakar keilmuan hubungan internasional untuk terus berkembang mengikuti dinamika dalam dimensi negara, kawasan bahkan global. Hal ini yang membentuk studi hubungan internasional harus dilengkapi dengan berbagai keilmuan lainnya, karena fenomena internasional tidak hanya ditelaah atau dikaji dengan satu persfektif , melainkan oleh berbagai keilmuan yang mendukung.

Dalam perkembangannya hubungan internasional merupakan keilmuan baru mengenai politik internasional. Hubungan internasional lahir secara resmi pada masa paska Perang Dunia Pertama dengan tujuan bahwa dunia setelah berakhirnya perang yang menimbulkan banyak korban di berbagai dunia dapat berhenti. Disamping itu, tujuan lainnya yakni memastikan interaksi diantara negara dapat berjalan dengan damai. Oleh karena itu, hubungan internasional secara nyata mempelajari interaksi diantara negara – negara bahkan dengan aktor non negara. Bahkan dinamika interaksinya meliputi berbagai kepentingan lainnya seperti kebudayaan, teknologi, ekonomi, dsb (Darmayadi, 2015:51-52).

Hubungan internasional merupakan studi yang kompleks, hal ini dapat dilihat dari aktor – aktor yang terlibat dalam tindakan internasional. Hal ini mendorong untuk penentuan tingkat analisa dari fenomena hubungan internasional. Berikut merupakan berbagai tingkat analisa dalam melihat perilaku aktor dalam hubungan internasional, yaitu:

1. Analisis tingkat sistem.

   Analisa pada tingkat sistem ditujukan terhadap sistem internasional yang dinamis, secara langsung mempengaruhi tindakan dan perilaku dari negara. Sistem internasional mencangkup pada kekuatan dari setiap negara.

2. Analisis tingkat negara

   Analisa pada tingkat negara menunjukan adanya ciri khusus yang dimiliki sebuah negara sehingga mempengaruhi tindakan dan perilaku dari negara tersebut. Analisa tingkat negara dapat dilihat dari tradisi sosial dan keagamaan serta warisan sejarah. Selain itu, faktor geografis dan ekonomi menjadi karakteristik bagi analisa tingkat negara.

3. Analisis tingkat organisasi

   Analisa tingkat organisasi berpendapat bahwa organisasi dapat mempengaruhi perilaku suatu negara bahkan terhadap kebijakan luar negeri. Dalam hal ini organisasi bukan merupakan negara, namun melihat pengaruhnya yang ditumbulkan akibat organisasi dalam negara tersebut.

4. Analisis tingkat individu

   Analisis tingkat individu memandang para pemimpin negara sebagai pengaruh terbesar kebijakan luar negeri.

(https://www.internationalrelationsedu.org/what-is-international-relations/ diakses 20/04/2020).

Goldstein dan Pevehouse (2014:13) mendefinisikan hubungan internasional secara sempit sebagai hubungan antar pemerintah dunia. Namun, ada ketentuan terkait mengenai aktor – aktor lain seperti perusahaan multinasional, organisasi internasional dan individu. Selain itu, ditandai dengan struktur yang mempengaruhinya yakni ekonomi, geografis, politik domestik dan budaya serta kelompok masyarakat. Hubungan internasional dapat berupa interaksi yang bersifat diplomatis dan juga perang.

Hikam (2014:4) menjelaskan bahwa diplomasi dan hubungan internasional tidak hanya sebagai upaya untuk mewujudkan perdamaian dunia, melainkan juga untuk memperjuangkan kepentingan nasional setiap negara. Dinamika masalah politik merupakan aspek dari lingkungan strategis global. Di sisi lain, beberapa aspek yakni sumber daya alam, energi, ekonomi, sosial dan diplomasi menjadi pertimbangan atas masalah dinamika internasional.

Hubungan internasional menjadi populer melihat berbagai kecenderungan yang dinamis dari politik global. Hal ini mendorong skema bagi kemunculan hubungan internasional kontemporer yang diartikan sebagai interaksi mengenai fenomena sosial yang berhubungan dengan aspek politik, ideologi, hukum, ekonomi, budaya dan pertahan keamanan negara yang melintasi batas nasional suatu negara antara aktor-aktor yang lebih kompleks (Perwita dan Yani, 2006:8).

Iran sebagai aktor hubungan internasional memiliki kapabilitas untuk melakukan interaksi baik dilihat dari upaya kerjasama ataupun konflik. Dinamika hubungan internasional memberikan peluang bagi bentuk interaksi Iran dengan menggunakan kekuatan siber ofensif. Interaksi yang terjadi antara Iran dengan Arab Saudi adalah bentuk konflik yang telah lama menjadi fenomena hubungan internasional di kawasan Timur Tengah. Untuk itu, dalam melihat fenomena ini, menggunakan tingkat analisa negara Iran dan Arab Saudi. Selain itu, hal ini ditujukan sebagai bentuk perjuangan kepentingan nasional Iran khususnya di kawasan Timur Tengah.

2.1.2 Konsep *Cyberspace*

Dinamika hubungan internasional memberikan berbagai perkembangan baru dalam menunjang analisa dari fenomena aktor – aktor hubungan internasional dalam memperjuangkan kepentingan nasional. Ruang siber atau ruang maya merupakan salah satu wilayah yang menjadi bagian penting selain ruang udara, ruang angkasa, laut dan juga darat. Ruang siber adalah sistem elektronik yang dapat diakses oleh pengguna komputer di seluruh dunia untuk saling berkomunikasi atau mengakses informasi dengan berbagai tujuan (https://dictionary.cambridge.org/dictionary/english/cyberspace diakses 04/06/2020).

National Institute of Standards and Technology (2012) menjelaskan bahwa ruang maya digambarkan dengan sebuah domain global dalam media informasi yang terdiri dari jaringan infrastruktur sistem informasi yakni komputer dan saling terhubung dan memiliki ketergantungan terhadap Internet, sistem komputer,

jaringan telekomunikasi yang dikendalikan oleh prosesor dan pengontrol yang tertanam dalam sistem komputer (https://csrc.nist.gov/glossary/term/cyberspace diakses 04/06/2020).

Ruang maya didefinisikan sebagai sebuah sistem elektronik dari jaringan komputer, yang ditafsirkan sebagai lingkungan tanpa batas. Ruang maya merupakan lingkungan komunikasi interaktif dan akses informasi bebas yang tersedia dalam internet. Disamping itu, ruang maya memberikan berbagai pilihan mengenai a) Menyediakan fiksi ilmiah dalam bentuk realitas virtual; b) Jaringan komputer global yang memfasilitasi komunikasi secara luas antara individu dan organisasi; c) dan, sebagai media elektronik dari jaringan komputer sehingga komunikasi dapat terhubung dengan internet (https://www.igi-global.com/dictionary/cybersecurity-new-challenge-information-society/6619 diakses 04/06/2020).

Lapisan ruang maya atau *Cyberspace* terdiri dari tiga lapisan berbeda tetapi memiliki kesatuan dan saling terhubung. Lapisan pertama yakni lapisan fisik terdiri dari komponen jaringan fisik dan fitur geografis. Kemudian, lapisan logis di representasikan sebagai data ketika mengalami pergerakan atau diam dalam lapisan fisik. Lapisan selanjutnya yakni lapisan siber persona terdiri dari representasi digital dari entitas yang berinteraksi satu sama lain dan dengan dua lapisan lainnya. (https://www.sbir.gov/node/1413495 diakses 03/06/2020).

Pendapat Aubrey Slaughter (2020) menjelaskan *Cyberspace* dapat dipahami secara luas sebagai lingkungan bersama dalam media komunikasi melalui perantara

komputer yang mempresentasikan audio, visual dan kode khusus tertentu. Selain itu, ruang maya dibagi ke dalam dua persfektif yaitu ruang maya dapat dilihat dari aspek spasial dan juga aspek sosial (https://lucian.uchicago.edu/blogs/mediatheory/keywords/cyberspace/ diakses 04/06/2020). Meskipun ruang maya merupakan konsep ruang yang memang masih banyak diperdebatkan terkait spasial dan aspek sosialnya, namun ruang maya memiliki karakteristik, diantaranya yaitu:

1. Interkonektivitas

   Interkonektivitas sebagai karakteristik untuk saling terhubung dan terkoneksi. Aspek fisik yang menjadi domain penting dalam mengeksplorasi ruang siber merupakan fondasi interkoneksi. Perusahaan dapat membuat beberapa sistem fisik dan interkoneksi tetapi tidak ada kepemilikan dunia maya sebagai kolektif, hal ini berlaku pada individu yang menggunakan ruang maya.

2. Virtualitas

   Aspek virtualitas ditujukan terhadap pemanfaatan bagian spektrum elektromagnetik yang terdapat pada aspek fisik yakni pada koneksi nirkabel komputer, namun pergerakan dalam karakteristik virtualitas tidak menekankan terhadap pergerakan fisiknya, melainkan virtualitas dari dunia maya yakni proses terjadinya sebuah dinamika dalam ruang maya. Intinya, ini jauh lebih mudah untuk melihat dan merasakan yang lain domain. Yang tidak terikat dan sifat virtual dari dunia maya memungkinkan tindakan

melaluinya, tapi bukan gerakan fisik didalamnya karena hanya meliputi informasi transfer.

3. Ekspansi

   Ekspansi merujuk pada perluasan skala ataupun tingkat penyebarannya. Hal ini berkaitan dengan perluasan informasi yang dilakukan dalam ruang maya, berkaitan dengan setiap tindakan yang dilakukan oleh pengguna ruang maya yang ditujukan terhadap pengguna ruang maya lain dengan melakukan perubahan pada ruang mayanya. Dinamika perkembangan dunia maya didorong oleh berbagai penelitian dan pengembangan industry sehingga menciptakan saling ketergantungan yang berdampak terhadap keamanan di ruang maya, khususnya mengenai jaminan keamanan negara, hal ini tentu berbeda dengan ekspansi di lingkungan darat, udara dan air.

4. Ketidakpastian

   Kombinasi interkonektivitas, virtualitas dan karakteristik ekspansi membuat dunia maya menjadi abstrak bahkan ambigu karena sulit dipahami secara fisik dan alami. Ambiguitas ruang maya merujuk pada pemahaman akan sifat ruang maya yang dinamis dan membingungkan, namun dalam memahami ketidakpastian ini, beberapa diantaranya memanfaatkan dunia maya dalam menyimpan informasi karena sifatnya yang sulit untuk dipahami, (Air Power Development Centre Bulletin, 2012:1-2).

Selanjutnya, dalam memahami sifat dunia maya dapat dipahami melalui komponen pembentuknya yakni dibagi ke dalam lapisan utamanya yakni; Fisik, Sintaksis, dan Semantik. Lapisan fisik mengacu pada infrastruktur dasar yang

mendukung transmisi, generasi, dan penyimpanan sinyal elektromagnetik, yaitu komputer, server, kabel. Lapisan sintaksis merupakan lapisan yang merujuk pada bagian dalam terdiri dari kode dan protokol dalam pengolahan data baik berupa transportasi, konstruksi dan manipulasi. Terakhir, lapisan semantik merupakan gabungan dari lapisan fisik dan sintaksis yang menekan pada makna atau proses atas kedua lapisan tersebut (Venables dkk., 2015:4).

Ruang maya atau *Cyberspace* memiliki lingkungan yang berbeda dengan lingkungan darat, air, udara dan ruang angkasa. Keunikan dari ruang maya yakni menghubungkan berbagai perangkat dengan teknologi dan juga internet yang membentuk sebuah kesatuan yang tidak dapat dipisahkan, lalu komponen fisik dari ruang maya yakni komputer dapat dimiliki oleh setiap orang di seluruh dunia untuk dihubungkan ke server dan terkoneksi dengan internet yang dapat bebas diakses oleh setiap individu, sehingga setiap orang dapat mengeksplorasi ruang maya. Sebaliknya, berbagai kemudahan dalam memasuki ruang maya terdapat kerentanan atas berbagai serangan karena rumitnya pemahaman dan pengawasan atas ruang maya secara global.

Lapisan – lapisan dan komponen ruang maya memiliki sensitivitas tertentu yang dapat dimanfaatkan sebagai potensi atau ancaman. Serangan siber Iran terhadap perusahaan Saudi Aramco dilakukan dengan memanfaatkan kerentanan ruang maya untuk menyebarkan pengaruhnya di Timur Tengah melalui operasi siber ofensif Iran dan juga untuk menyerang objek vital Arab Saudi yaitu Saudi Aramco yang memiliki sistem operasi terhubung dengan komputer dan internet sehingga

serangan Iran dapat berdampak karena ketergantungan perusahaan atas teknologi dan internet.

Serangan siber ofensif Iran dengan menggunakan virus *Shamoon* berdampak pada aspek fisik komputer Saudi Aramco dan memutus jaringan komunikasi internal dalam aspek logis ruang maya. Penyerangan terhadap Saudi Aramco dilakukan oleh kelompok peretas komputer Iran yaitu *Cutting Sword of Justice* yang merupakan orang – orang yang memiliki keahlian dalam mengoperasikan tujuan dan kepentingannya melalui virus *Shamoon* yang melakukan duplikasi di komputer internal Saudi Aramco dan dapat dikendalikan sesuai dengan keinginan dari penyerang yakni Iran melalui kelompok peretas komputernya.

2.1.2.1 *Cyberpower* Dalam *Cyberspace*

Hubungan internasional sebagai studi mengenai dinamika negara dalam melakukan interaksi di politik internasional telah berkembang. Interaksi negara sebagai bentuk interaksi sosial kompleks memberikan pengaruh bagi negara secara tunggal maupun global. Secara umum negara dapat memberikan pengaruh melalui *Power* nya untuk melakukan interaksi, sehingga interaksi tersebut dapat dikontrol oleh negara yang memiliki kekuatan lebih. Hal ini melihat bahwa kekuatan negara dapat dilihat secara relatif.

Konsep *Power* menurut K.J Holsti dalam Perpustakaan Univeristas Komputer Indonesia (2016:25-26) merupakan kapasitas atau kemampuan negara untuk mengendalikan negara lain yang dapat dilihat dalam empat bagian:

1. *Power* dalam persfektif *Influence*, merupakan alat guna mencapai tujuan

2. *Power* dalam memobilisasi sumber-sumber *Power* yang meliputi sumber fisik dan sumber mental yang dimiliki negara sebagai instrumen membuktikan atau menghukum negara lain
3. *Power* dalam persfektif *Relation*, yaitu menentukan keberhasilan suatu pihak lain apabila pihak tersebut mempunyai *Power*
4. *Power* dalam persfektif mengukur dilihat secara relatif bukan absolut, dengan membandingkan sumber-sumber kekuatan yang dimiliki oleh suatu negara dengan negara lain.

Kekuasaan atau *Power* menurut Toha (2012:102-103) adalah kemampuan seseorang atau sekelompok manusia untuk mempengaruhi tingkah laku seseorang atau kelompok lain sehingga selaras dengan harapan dan tujuan orang atau kelompok yang memiliki kekuasaan tersebut. Dalam mempersepsikan *Power* dalam sebuah entitas sosial seperti negara dapat dilihat dari tujuan atau kepentingan yang akan dicapai dalam upaya mengatur bahkan menekan negara lain sesuai dengan keinginan dari negara tersebut. Hal ini memerlukan strategi dan tujuan yang matang dalam menggunakan *Power* sebagai instrumen menghukum negara lain.

Perkembangan teknologi informasi dan komunikasi menambah berbagai fenomena dan interaksi negara dalam konteks hubungan internasional. Globalisasi dan pesatnya teknologi memberikan bagian penting bagi munculnya ruang siber sebagai tempat negara – negara untuk melakukan interaksi. Disamping itu, penggunaan ruang maya tidak hanya dapat dioptimalkan oleh negara dalam mencapai kepentingan nasional, juga dapat digunakan oleh individu yang dapat mendayagunakan ruang maya untuk perihal positif dalam penggunaan teknologi

bahkan dapat digunakan untuk hal negatif, maka dari itu perkembangan teknologi tidak hanya memberikan ruang maya atau *Cyberspace* tetapi memunculkan konsep *Cyberpower* dalam mengoptimalkan kekuasaan dalam ruang maya.

Ruang maya yang bertambah mengakibatkan adanya perubahan dalam proses interaksi sekaligus memperluas makna *Power*, sehingga *Power* menjadi memudar. Ruang maya menjadi sarana baru dalam mencapai kepentingan yang kemudian dikenal dengan *Cyberpower* (Triwahyuni dan Yani, 2018:2). Hal ini dijelaskan oleh Kuehl (2009:12) bahwa kemampuan dalam menggunakan *Cyberpower* digunakan untuk menciptakan keuntungan dan mempengaruhi berbagai fenomena di lingkungan operasional dalam instrumen kekuasaan. Dalam hal ini, *Cyberpower* dalam melihat kemampuan sebuah negara dapat dijadikan sebagai alat atau sarana untuk mencapai kepentingan nasional dalam memanfaatkan peluang dan potensi ruang maya. Selain itu, kekuatan siber suatu negara dapat memberikan keuntungan strategis yang dilakukan sebagai bagian instrumen dalam mencapai kepentingan negara.

Kerentanan dunia dan negara dalam pembangunan kekuatan siber atau *Cyberpower* tidak hanya ditujukan bagi negara lain, tetapi kekuatan siber dapat dibentuk oleh masyarakat bahkan individu yang dapat mengorganisir dan membangun kekuatan siber tanpa adanya kontrol dari negara. Apabila secara rasional masyarakat bergabung untuk membentuk kelompok dalam membangun *Cyberpower*, maka hal ini dapat menjadi ancaman bagi negara atau negara lain bahkan dapat dijadikan sebagai senjata untuk mencapai kepentingan negara.

Menurut Langner apabila masyarakat memiliki *Cyberpower* besar dan terlibat secara nyata dalam tindakan dunia maya, maka secara tidak langsung dapat mengancam negara lain, khususnya mengenai tindakan spionase, menjadi intelijen negara, menyabotase infrastruktur bahkan dapat mengganggu sebuah wacana politik dengan menggunakan siber (https://www.cirsd.org/en/horizons/horizons-autumn-2016--issue-no-8/cyber-power-an-emerging-factor-in-national-and-international-security diakses 03/06/2020).

Kekuatan siber dalam ruang maya menurut Haaster (2016:14) terdiri dari berbagai kekuatan yang dapat mempengaruhi aktor – aktor negara dan aktor lainnya dalam menggunakan dunia maya, seperti komponen geografis, jaringan fisik, logis, dan siber persona. Implikasi kekuatan siber dilihat dari penggunaan siber persona untuk tindak kejahatan siber yang digunakan oleh kelompok tertentu untuk menyebarkan pengaruhnya melalui tindakan siber ofensif yang merupakan komponen logis. Kemudian, pentingnya untuk memahami kekuatan siber secara fisik dalam membangun kontrol atas infrastruktur jaringan siber yaitu komponen fisik dari kekuatan siber yakni jaringan komputer yang luas dan kuat. Selain itu, dukungan peretas komputer menjadi penting dalam melancarkan serangan dan merealisasikan strategi untuk mencapai kepentingan nasional.

Iran merupakan negara yang menjadi target serangan siber dari negara lain, dalam hal ini Iran membentuk sumber daya kekuatan siber dengan mengoptimalkan *Cyberpower* dan instrumen internal Iran seperti; kelompok peretas Iran, penggunaan strategi yang tepat dan sesuai dengan kondisi Iran pada tahun 2012, khususnya dalam mencapai kepentingan Iran melalui siber ofensif.

Kekuatan siber Iran meskipun tidak simetris dengan negara lain, namun hal ini yang menjadi salah satu alasan Iran dalam mempercepat eskalasi kekuatan sibernya. Kerentanan akan serangan siber khususnya dari Amerika Serikat, Israel dan sekutunya di Timur Tengah yakni Arab Saudi memberikan ancaman untuk mencapai kepentingan nasional. Kelompok yang berperan penting dalam operasi siber Iran adalah Korps Pengawal Revolusi Iran, *Passive Defense Organization* (NPDO) dan *Basij*. Selain itu, dalam memperkuat *Cyberpower* Iran telah membentuk Dewan Tertinggi Dunia Maya atau *Supreme Council of Cyberspace.*

Kelompok utama dalam merumuskan bahkan melakukan operasi siber memiliki tugas yang berbeda. Korps Pengawal Revolusi Iran atau IRGC merupakan pasukan militer Iran yang menjadi eksekutor dalam serangan siber khususnya terhadap Amerika Serikat dan sekutunya yakni Arab Saudi. Dalam IRGC terdapat berbagai kelompok siber yang bermacam, sehingga dalam operasi serangan siber tidak hanya dilakukan oleh kelompok utama, tetapi dapat dilakukan oleh kelompok lain. *Basij* berperan sebagai kelompok paramiliter Iran yang membentuk kekuatan-kekuatan yang sulit untuk dihentikan, karena melibatkan masyarakat dengan berbagai massa dan dapat bersentuhan langsung dengan kelompok masyarakat lain. Selanjutnya, *Passive Defense Organization* sebagai kelompok yang menyiapkan dan memperhatikan mengenai berbagai infrastruktur siber Iran (https://www.csis.org/analysis/iran-and-cyber-power diakses 03/06/2020).

2.1.3 Politik Luar Negeri

Konsep politik luar negeri dalam hubungan internasional merupakan studi kompleks mengenai politik dan kebijakan. Secara umum dalam memahami politik

luar negeri dapat dilakukan dengan memisahkan politik dalam negeri atau "Internal" dan politik luar negeri "Eksternal". Menurut Perwita dan Yani (2006:47) politik luar negeri merupakan kebijaksanaan suatu negara guna mencapai kepentingan. Lebih luasnya, politik luar negeri adalah seperangkat formula yang merupakan nilai, arah dan sikap serta sasaran untuk memperjuangkan kepentingan nasional di dunia internasional.

Fenomena hubungan internasional dinilai sebagai proses dinamis dalam dunia internasional yang memberikan konsepsi baru khususnya dalam era globalisasi. Politik luar negeri atau *Foreign Policy* dinyatakan sebagai berbagai upaya yang dilakukan oleh negara terhadap negara lain yang dapat disebut sebagai politik luar negeri. Namun, dengan adanya interdependensi akibat dari globalisasi maka negara bukan satu – satunya kebijaksanaan bagi negara lain tanpa mengabaikan realitas bahwa politik luar negeri ditujukan terhadap organisasi internasional dan lembaga non pemerintah dalam kerangka skala internasional (Marolov, 2013: 237).

Politik luar negeri dapat diinterpretasikan dalam beberapa bagian, berikut merupakan bagian atau komponen dalam menginterpretasikan politik luar negeri, yaitu; 1) Komponen hasil atau "*The End"* yang ingin dicapai dalam upaya melakukan interaksi dengan negara lain; 2) komponen sarana atau cara *"The Way*" meliputi ide dan strategi dalam memajukan kepentingan nasional; 3) komponen makna "*The Means*" merupakan bagian dalam melihat kemampuan sumber daya yang dapat digunakan oleh suatu negara seperti ekonomi dan militer (As, 2018: 2).

Meskipun dalam politik luar negeri memiliki tingkat kompleksitas, namun politik luar negeri tetap memiliki fokus. Hal ini dijelaskan oleh Caporaso dkk dalam Spohr dan Silva (2017:2) merujuk pada kebijakan dan tindakan atau aksi dari negara diarahkan pada orientasi kondisi eksternal serta melewati batas yurisdiksi negara lain. Terutama penentuan fokus perlu melakukan penelusuran sumber – sumber dari politik luar negeri dan juga dampak atau konsekuensi yang timbul atas kebijakan luar negeri.

Politik luar negeri Iran merupakan strategi, kerahasiaan, nilai yang tidak dapat didefinisikan secara jelas. Namun, temuan mengenai siber ofensif iran yang diarahkan pada Saudi Aramco merupakan serangan siber yang didasarkan pada upaya mencapai kepentingan nasional. Kebijakan luar negeri dibawah kepemimpinan Mahmoud Ahmadinejad membawa Iran ke dalam tekanan internasional yang semakin buruk. Disadari bahwa dalam tindakan eksekusi siber ofensif iran terhadap Arab Saudi tidak dilakukan oleh pemerintah Iran secara langsung, melainkan dilakukan oleh kelompok peretas Iran yang disebut sebagai *Cutting Sword of Justice*. Upaya mempersenjatai diri menjadi bagian dalam nilai strategis untuk mengoptimalkan penggunaan teknologi dengan politik luar negeri Iran.

2.1.4 Kepentingan Nasional

Kepentingan nasional merupakan hal penting yang melekat pada kajian hubungan internasional. Kepentingan nasional secara umum merupakan upaya – upaya setiap negara untuk memenuhi kebutuhan nasionalnya melalui berbagai cara. Disadari bahwa, setiap negara tidak bisa secara mandiri tanpa memerlukan bantuan

dari negara terdekat, negara dalam kawasan bahkan bantuan negara di seluruh dunia.

Pola – pola untuk mencapai kepentingan nasional dapat berupa kerjasama yang dilakukan diantara negara atau aktor hubungan internasional, bahkan dalam mencapai kepentingan nasional dilakukan dengan menciptakan *Balance Of Power* atas dasar dari kepentingan nasional melalui strategi tertentu. Menurut Said menjelaskan kepentingan berperan sebagai sasaran yang akan dicapai, tanpa adanya sebuah kebijakan dari kepentingan nasional maka tidak akan pernah lahir strategi nasional (http://www.fkpmar.org/national-interests-theory-and-practice/ diakses 24/04/2020).

Kepentingan nasional dalam ungkapan bahasa Prancis yaitu *Raison d'État*, adalah ambisi dan tujuan negara, dalam kepentingan ekonomi, budaya dan militer. Konsep kepentingan nasional merupakan bagian penting bagi studi hubungan internasional dan juga sebagai dasar bagi negara dalam melakukan hubungan internasional (Bainus dan Rachman, 2018:109).

Urgensi dari kepentingan nasional merupakan tujuan vital atas dasar kebutuhan setiap negara. Menurut Perwita dan Yani (2006:35) menjelaskan pentingnya kepentingan nasional sebagai upaya untuk memahami perilaku internasional dan dipersepsikan sebagai tujuan fundamental dan hasil akhir dalam mengarahkan pada kebijakan nasional suatu negara.

Kepentingan nasional menurut Burchill dalam Umar (2005:186-188) membagi kepentingan nasional melalui berbagai persfektif hubungan internasional, diantaranya sebagai berikut:

1. Persfektif Realism. Realis berasumsi bahwa kepentingan nasional mutlak berasal dari negara. Kepentingan nasional harus dilihat dari kepentingan negara sebagai supremasi tertinggi yang berlandaskan atas kekuasaan paling tinggi. Keamanan negara merupakan kepentingan nasional yang menjadi konsentrasi penting.
2. Liberal Institusionalisme. Berasumsi bahwa kepentingan nasional tidak terletak dari kepentingan negara sebagai supremasi tertinggi, melainkan pada pasar dan stabilitas ekonomi suatu negara. Khususnya, stabilitas ekonomi dipusatkan sebagai upaya terciptanya aktivitas perekonomian yang damai atau tenang.
3. Marxisme. Asumsi marxisme dalam kepentingan nasional yakni melihat perjuangan kelas-kelas dalam tujuan ekonomi politik dan memiliki motif di balik kepentingannya.
4. Konstruktivisme. Konstruktivisme mengasumsikan kepentingan nasional merupakan konstruksi sosial dari kondisi atau fenomena yang terjadi secara nyata di masyarakat internasional. Hal ini menjelaskan bahwa kepentingan nasional dalam persfektif konstruktivisme yaitu negara tidak bersifat utuh. Selain itu, kepentingan nasional bertransformasi secara dinamis dan adaptif dengan struktur politik internasional.

5. English School. Asumsi yang dibangun English School mengenai kepentingan nasional sebagai eksistensi dari entitas lainnya. Bentuk – bentuk dari pengakuan atas entitas tersebut menjadi kepentingan nasional sebagai pembentuk masyarakat internasional yang stabil.

Kepentingan nasional yang menjadi fokus terhadap Iran merupakan ambisi dalam pertarungan atau rivalitas Iran dengan Arab Saudi. Kepentingan nasional adalah sasaran yang akan dicapai dalam penelitian ini menggunakan strategi siber terhadap objek penting yakni pengayaan minyak terbesar di dunia, Saudi Aramco. Hal ini dilatarbelakangi oleh berbagai sanksi yang dijatuhkan atas Iran seperti pemberhentian ekspor minyak Iran sehingga mitra kerjasama minyak Iran beralih ke Arab Saudi. Ambisi atau tujuan negara tidak hanya ditujukan bagi merusak atau terganggunya sistem komputer Saudi Aramco, lebih dari itu sebagai upaya untuk menunjukan bahwa Iran memiliki peran penting dalam kawasan, khususnya dalam eskalasi siber sebagai bentuk dalam konflik asimetris dan *Proxy War* yang dilakukan oleh kelompok *Islamic Revolutionary Guard Corps* (IRGC) dibawah kepemimpinan Iran untuk mencapai kepentingan nasionalnya di Timur Tengah dan dunia internasional.

2.1.5 Keamanan Internasional

2.1.5.1 Konsep Keamanan

Keamanan internasional merupakan kajian tradisional hubungan internasional. Keamanan dalam studi hubungan internasional menjadi bagian penting yang tidak bisa dilepaskan, hal ini berdasarkan pada temuan dari bidang keamanan yang melahirkan kajian - kajian baru meliputi keamanan manusia, keamanan ekonomi

bahkan keamanan data. Perkembangan keamanan yang dinamis membuka peluang bagi ditemukannya kajian keamanan yang lebih spesifik.

Menurut Buzan dalam Perwita (2008:4) konsep keamanan dalam hubungan internasional menjadi semakin luas, hal ini didasarkan pada makna konsep keamanan yaitu keamanan tidak hanya dalam aspek militer dan aktor negara, melainkan konsep keamanan juga meliputi aspek – aspek non militer serta aktivitas non-negara.

Konsep keamanan menurut Rahardjo (2017:10) menjelaskan dalam keamanan terdapat bagian utama yakni perlindungan data atau informasi. Bagian dalam keamanan yang melindungi data yaitu *Security Triads* merupakan aspek yang terdiri dari kerahasiaan, ketersediaan, dan integritas. Disamping itu, pola atau siklus berjalannya data yang disebut sebagai *Security Life Cycle* berakar dari kesadaran akan melindungi asset informasi sebagai upaya dalam menciptakan keamanan.

Keamanan secara umum meliputi berbagai aspek kehidupan, khususnya dalam mendukung studi hubungan internasional. Perdebatan mengenai konsep keamanan yang relevan menjadi bagian penting bagi perkembangan konsep – konsep hubungan internasional dan kajian strategis keamanan bagi semua negara. Disamping itu, keamanan tidak hanya dipandang sebagai bagian penting bagi negara, namun dalam persfektif hubungan internasional keamanan dapat berarti bagi semua aktor hubungan internasional, tidak hanya negara tetapi individu maupun organisasi internasional.

Menurut Wardoyo (2015) menjelaskan pemetaan dalam keamanan tidak hanya dilihat dari aktornya, tetapi menekankan pada pertanyaan mendasar untuk memahami konsep keamanan yaitu: 1) untuk siapa keamanan tersebut, 2) keamanan dari apa yang dimaksudkan, 3) bagaimana keamanan atau rasa aman dapat dicapai.

Keamanan pada era saat ini menjadi bagian penting dalam berbagai aspek dalam kenegaraan. Upaya dalam menjaga atau menciptakan keamanan nasional dalam kerentanan global saat ini bergeser menjadi keamanan data, ketika negara di seluruh dunia melakukan percepatan teknologi dan membentuk *Big Data* negara dalam ruang maya. Ketergantungan Arab Saudi terhadap teknologi dalam pengayaan minyak perusahaan Saudi Aramco menjadi ancaman ketika celah dapat ditemukan oleh penyerang siber Iran. Selain itu, Iran menggunakan siber sebagai upaya untuk meretas keamanan Arab Saudi. Hal ini menjadi sebuah upaya untuk meretas keamanan negara terhadap objek vital Arab Saudi.

2.1.5.2 Ofensif Defensif Siber

Definisi dari Ofensif adalah serangan. Suatu kondisi yang menyatakan akan melakukan tindakan militer atau dalam keadaan siaga untuk menghadapi musuh. (https://kbbi.web.id/ofensif diakses 24/04/2020). Konsep mengenai ofensif - defensif siber secara praktik dan teori berbeda, hal ini berdasarkan atas variable – variable yang membentuk persepsi keamanan dengan menggunakan pola ofensif atau defensif.

Menurut Robert Jervis dalam Medvedev (2015:5) variable pertama ditentukan ketika situasi ketegangan dari negara lain dinilai sebagai ancaman atau mengancam.

Hal ini mengasumsikan bahwa tindakan ofensif dan defensif ataupun keduanya digunakan sebagai upaya mempersenjatai negara dengan strategi politik dan kepentingan yang ingin dicapai oleh negara. Variabel kedua dalam ofensif - defensif yakni menitikberatkan pada kapabilitas yang mendukung akan tindakan ofensif atau defensif. Kapabilitas ini dinilai dari dominasi kemampuan, apabila memungkinkan untuk melakukan siber ofensif maka negara cenderung untuk melakukan serangan terlebih dahulu. Disamping itu, apabila dominasi kapabilitas pada tindakan defensif, maka tindakan diarahkan pada perang dan kerjasama.

Smeet dan Lin (2018: 58) menjelaskan bahwa tindakan siber ofensif merupakan kemampuan yang direncanakan guna mengakses jaringan komputer bahkan dirancang untuk merusak komputer dan juga membahayakan mahluk hidup serta material. Pola – pola yang dapat ditemukan dalam operasi ofensif dan defensif dapat diimplikasikan pada kondisi tindakan kejahatan pencurian konvensional. Pola serangan secara bertahap meliputi: pengintaian, intrusi, eskalasi hak istimewa dan pengiriman muatan.

Menurut Smeets (2018:97-103) tindakan siber ofensif dapat memberikan beberapa kemungkinan yang dapat dipertimbangkan sebelum melakukan serangan siber terhadap negara lain, yaitu:

1. Memberikan opsi keputusan

   Tindakan serangan siber atau *Cyber Offensive* dapat memberikan opsi bagi kepala negara atau pemimpin negara untuk menentukan keputusan baik

dalam upaya tindakan serangan balik atas siber ataupun keputusan yang bersifat politis terhadap negara lain.

2. Mengefektifkan kemampuan militer

   Penggunaan siber ofensif merupakan proses kompleks yang meliputi berbagai komponen yang terintegrasi. Siber ofensif dapat digunakan sebagai bentuk paksaan dan digunakan sebagai perang asimetris serta senjata untuk pemusnah musuh, tidak seperti senjata pemusnah massal. Siber ofensif menekankan pada integrasi kekuatan dan efektivitas dari kapabilitas penangkalan siber.

3. Menciptakan pengaruh psikologis

   Pengaruh psikologis dalam perang atau konflik merupakan tindakan yang dapat melemahkan musuh. Siber ofensif dikatakan dapat menciptakan pengaruh psikologis ketika negara lain menciptakan eskalasi teknologi siber, secara tidak langsung dapat memberikan dampak seperti menakuti, penurunan kepercayaan dan penghinaan. Dampak yang timbul dari serangan dapat memberikan pengaruh dengan lebih lembut terhadap musuh.

4. Meminimalisir korban

   Operasi siber yang bersifat ofensif dapat menekan korban manusia dan juga biaya perang. Seorang prajurit siber hanya duduk jauh dari target dan juga medan pertempuran dengan memperhitungkan pengembangan taktik atau strategi kemampuan siber. Hal ini didasarkan atas pandangan bahwa sulit memperkirakan prajurit dan juga individu yang menderita cedera akibat

serangan siber. Namun, yang harus diperhatikan adalah konsensus ketika penggunaan siber digunakan secara tidak bijaksana.

Lin dan Zegart (2019:6) berpendapat mengenai motif dari siber ofensif. Operasi siber ofensif secara strategis dapat digunakan di berbagai skenario dan tujuan. Skala dalam tujuan ofensif siber dilihat dari penggunaan jangka panjang dan pendek. Kapabilitas siber sebagai keamanan ditujukan bagi teknologi informasi lawan yang dikendalikan melalui jaringan atau sistem informasi.

Siber ofensif Iran merupakan kompleksitas dari berbagai konsep yang dijelaskan diatas. Implikasi konsep ofensif siber terhadap penelitian yakni memudahkan dalam interpretasi fenomena siber Iran. Selain itu, konsep ofensif dapat menjelaskan mengenai maksud atau tujuan atas penggunaan siber Iran, yakni tindakan serangan siber didasarkan atas kapabilitas siber Iran yang dapat melakukan serangan terlebih dahulu, berdasarkan atas meminimalisir korban dari konflik terbuka. Kemudian penggunaan ofensif siber merupakan strategi konflik asimetris Iran terhadap Arab Saudi. Hal ini juga menjadi strategi Iran untuk menunjukan eksistensinya di Timur Tengah sebagai bentuk kepentingan nasional Iran.

2.1.5.3 Keamanan Siber

Keamanan siber pada perkembangannya dianggap sebagai dampak dari meningkatnya hubungan saling ketergantungan negara dengan keamanan ruang maya atau *Cyberspace*. Globalisasi memberikan ruang baru dalam interaksi aktor-aktor hubungan internasional yang melihat upaya untuk memanfaatkan teknologi serta penguasaannya di ruang maya. Disamping itu, sifat dari dunia maya tidak

berwujud secara fisik memberikan tantangan dalam penggunaannya. Berdasarkan sifat fisiknya ruang maya maka tindakan atas pengendalian siber menjadi penting untuk dilakukan, melihat munculnya potensi dari kerentanan terhadap penyalahgunaan teknologi dalam dunia siber atau ruang maya.

Internet menjadi kunci dari pengorganisasian sistem komputer sehingga terhubung dengan ruang maya. Menurut Knapp (2009:1) keamanan siber atau *Cyber Security* adalah masalah yang dihadapi pengguna jaringan komputer dan administrator, khususnya terjadi pada sektor publik dan swasta. Kerentanan berasal dari masalah internet akibat lemahnya keamanan sistem komputer yang digunakan oleh penyerang sebagai titik celah bagi terjadinya kejahatan di ruang maya.

Menurut *International Telecommunications Union* (ITU) keamanan siber merupakan kumpulan alat, konsep keamanan, kebijakan, keamanan perlindungan, pendekatan manajemen risiko, pedoman, tindakan, pelatihan, praktik terbaik, jaminan, dan teknologi yang dapat digunakan guna melindungi lingkungan siber, organisasi dan aset pengguna yang terhubung dan disimpan di ruang siber (https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx diakses 26/04/2020).

Keamanan siber menjadi penting ketika kerentanan akan penggunaan dan interdependensi dari data yang disimpan di ruang maya. Disamping itu, pemanfaatan siber sebagai *Big Data*, sehingga penggunaan ruang maya sebagai kepentingan nasional dapat menjadi ancaman bagi negara lain. Keamanan siber dibangun agar pemanfaatan siber secara positif seperti membangun teknologi

perlindungan siber dalam upaya siber defensif, di sisi lain dapat digunakan untuk menciptakan senjata sebagai kekuatan nasional sebagai bentuk keamanan siber. Hal ini yang dibangun oleh Iran sebagai upaya untuk mencapai kepentingan nasional Iran melalui serangan siber terhadap kilang minyak Arab Saudi.

2.1.6 Kejahatan Siber

2.1.6.1 Tinjauan Umum Kejahatan Siber

Kejahatan siber secara umum merupakan penggunaan teknologi siber untuk tujuan negatif. *International Telecommunication Union* (2012:11) menjelaskan kejahatan siber atau kejahatan dunia maya dapat mencangkup berbagai tindakan kriminal. Namun, ada beberapa pendeketan yang dapat mengidentifikasi jenis pelanggaran siber, yaitu:

1. Pelanggaran terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem komputer
2. Pelanggaran terkait komputer
3. Pelanggaran terkait konten
4. Pelanggaran terkait hak cipta.

Gema dalam *National Central Bureau* Interpol Indonesia (2013:2) memaparkan bahwa kejahatan siber memiliki karakteristik yang berbeda dari kejahatan konvensional, berikut merupakan karakteristik dari kejahatan siber, yaitu:

1. Perbuatan atau tindakan yang dilakukan diruang maya secara ilegal
2. Tindakan kejahatan siber menggunakan peralatan atau perangkat yang terhubung melalui internet

3. Dampak dari serangan atau kejahatan siber dapat menimbulkan kerugian baik secara materil atau non materil seperti kebocoran kerahasiaan informasi, penurunan kapasitas data, uang bahkan martabat
4. Secara spesifik, pelaku yang melakukan tindak kejahatan siber merupakan seorang yang menguasai internet dan aplikasinya serta mampu mengorganisasikan sistem komputer dengan baik
5. Tindakan kejahatan siber diantaranya dilakukan tidak hanya dalam negara tetapi dapat melewati batas negara.

Dalam melihat klasifikasi utama dalam kejahatan siber, sasaran ditujukan kepada beberapa objek tertentu. Menurut Poonia (2014:2) menyatakan kejahatan siber memiliki empat kategori utama yaitu sebagai berikut :

1. Kejahatan terhadap individual, meliputi pencemaran nama baik, pencurian kartu kredit, pembajakan *software*, *hacking*, penyebaran isu sara dan lain – lain
2. Kejahatan terhadap properti orang lain merupakan kejahatan yang ditujukan atas merusak data terhadap orang lain, seperti kejahatan kekayaan intelektual
3. Kejahatan terhadap organisasi meliputi kejahatan terhadap pelayanan publik bahkan tindakan terorisme yang dapat mengancam nyawa
4. Kejahatan terhadap masyarakat, dapat dibuktikan seperti tindakan penipuan data, penyebaran berita bohong dan siber terorisme.

Kejahatan siber merupakan kejahatan yang berkembang saat ini. Penggunaan teknologi memberikan sisi negatif dari teknologi, hal ini menimbulkan jenis – jenis kejahatan dengan penggunaan teknologi. Berikut merupakan jenis kejahatan siber menurut *United Nations Office on Drugs and Crime* (2010, 206-207), yaitu:

1. *Phishing*

   Istilah phishing dibeberapa negara menyebutnya sebagai "*Identity Fraud"* atau penipuan identitas. Kejahatan *Phishing* merupakan sebuah trik pencurian dengan mengelabui korban menggunakan motif melalui memasukan data informasi untuk keperluan lembaga. Data informasi yang termuat yakni kata sandi dan informasi terkait korban.

2. *Malware*

   Kejahatan siber melalui *Malware* merupakan pencurian data menggunakan perangkat lunak berbahaya agar dapat memberikan informasi yang diinginkan secara langsung dari komputer korban. *Malware* dapat langsung memindai *Hard Drive* untuk mengumpulkan data yang diformat seperti kata sandi, nomor kartu kredit dan nomor sandi umum.

3. *Hacking*

   Istilah *Hacking* atau "Peretasan" ditujukan pada pelanggaran akses sistem komputer secara hukum. Peretasan merupakan kejahatan yang cukup tua dan menjadi massal di masyarakat. Target dalam peretasan diarahkan bukan hanya pada sistem keuangan melainkan data sistem komputer yang besar. Data yang diperoleh dapat digunakan untuk tindakan kejahatan lain seperti

pencucian uang dan juga identitas yang didapatkan dapat digunakan untuk tindakan terorisme dengan menggunakan identitas dari peretas.

Kejahatan siber dapat dilakukan oleh berbagai negara, salah satunya Iran. Tindak kejahatan Iran melalui siber ofensif terhadap perusahaan Saudi Aramco yang dimiliki oleh Arab Saudi merupakan bentuk kejahatan dalam pelanggaran sistem kerahasiaan data dalam sistem komputer. Pelaku dalam serangan merupakan kelompok terlatih dalam siber yakni *Cutting Sword of Justice*, secara konsep dan taktik telah menguasai dan mengorganisasikan komputer dengan baik. Operasi siber ofensif yang dilakukan menggunakan *Malware* melalui *Hard Drive*, dapat menimbulkan kerusakan atas beberapa komputer dan terganggunya sistem komputer, seperti pada serangan terhadap Saudi Aramco sebagai kejahatan siber yang dilakukan oleh Iran terhadap Arab Saudi.

2.1.6.2 Program Virus Dalam *Malware*

Malware merujuk istilah yang merujuk pada salah satu kejahatan siber. *Malware* merupakan kepanjangan dari "*Malicious Software*" yang digambarkan sebagai perangkat lunak yang mencurigakan. Meskipun penamaan *Malware* memiliki pengertian pada sebuah program, namun sebenarnya *Malware* adalah perangkat lunak berbentuk *Script / Code* (http://www.martinrecords.com/technology/mengenal-jenis-Malware-yang-berbahaya-untuk-komputer/ diakses 17/04/2020).

Menurut Aycock (2006:11), beberapa karakteristik *Malware* dapat dikategorikan ke dalam berbagai mode operasi. Berikut merupakan karakteristik *Malware* dilihat dari metode operasi:

1. Mereplika dirinya sendiri secara aktif dengan menyebar dan membuat salinan baru atau melakukan duplikasi dirinya sendiri
2. Populasi dari penyebaran *Malware* menunjukan jumlah dalam hitungan angka dalam melakukan duplikasi *Malware* tersebut.
3. *Malware parasite* dalam eksekusinya memerlukan beberapa kode yang harus dimasukan agar proses eksekusi dapat berlangsung.

Operasi dari sistem *Malware* yang digunakan berakibat pada beberapa gangguan yang ditimbulkan, berikut ini merupakan tindakan dan hasil yang diakibatkan oleh *Malware*, yaitu:

1. Pengiriman email dalam skala besar, penggunaan email dalam *Malware* digunakan untuk masuk dan terhubung ke dalam server.
2. Menghapus file penting yang merupakan kejahatan siber dalam *Malware* yang sering dilakukan yakni dengan menghapus bagian file penting dalam sistem komputer.
3. Memodifikasi file. Dalam hal ini beberapa *Malware* mencoba untuk menonaktifkan *Anti-Spyware,* Anti-Virus, dan perangkat lunak *Firewall* bahkan digunakan sebagai upaya ekploitasi dan penggunaan tidak resmi.
4. Menurunkan kinerja komputer. *Malware* yang masuk pada sistem komputer dapat menurunkan keseluruhan jaringan kinerja komputer.

5. Menyebabkan ketidakstabilan sistem komputer. Jika berlaku dalam *Malware* tersebut dapat mengganggu sistem aplikasi dan juga penundaan atau melambatnya sistem.
6. Merilis informasi rahasia, ditujukan pada kontrol izin dalam akses, hal ini memungkinkan untuk penggunaan akses tidak resmi.
7. Kompromi terhadap pengaturan keamanan. Hal ini dapat dilakukan dengan cara menemukan sistem pengaturan keamanan yang diubah atau bagian yang ditemukan saat komputer diakses oleh pengguna yang tidak sah. (Tittel, 2005: 26)

Selanjutnya, *Malware* merupakan perangkat lunak berbahaya yang memuat berbagai jenis program, salah satunya virus. Komponen atau hal yang harus termuat dalam virus adalah dapat membuat replika yang menyebar ke komputer target penyerangan. Selain itu, *Malware* memiliki ciri khusus yakni kehadirannya tidak dapat diprediksikan oleh sistem keamanan, karena virus dimasukan atas sistem yang telah di program. Dalam *Computer Viruses Demystified* (2001:8) mendefinisikan virus komputer adalah program komputer yang dapat menyebar kepada komputer dan jaringan dengan membuat replika atau salinan dengan sendirinya, tanpa sepengetahuan pengguna.

Penggunaan *Malware* virus terutama dalam kejahatan siber merupakan serangan siber menggunakan virus tertentu dan dapat digunakan untuk menyerang suatu negara. Penggunaan *Malware* jenis virus oleh Iran digunakan untuk mencapai kepentingan nasional. Karakteristik dari virus yang dapat melakukan replika secara otomatis diarahkan pada merusak sistem komputer Saudi Aramco. Virus yang

digunakan oleh Iran terhadap Arab Saudi yaitu *Shamoon* atau *W32.Disstrack*. Akibat atas serangan siber melalui virus ini, sistem komputer Saudi Aramco mengalami penurunan kinerja dan menimbulkan ketidakstabilan sistem komputer sementara. Indikasi temuan komputer Saudi Aramco terkena virus *Shamoon*, ketika pada saat perusahaan dan pegawai sedang berlibur dan virus tidak terdeteksi pada sistem keamanan perusahaan Saudi Aramco.

2.2 Kerangka Pemikiran

Hubungan Iran dan Arab Saudi merupakan sejarah panjang dalam persaingan hegemoni kawasan Timur Tengah. Konflik – konflik yang diciptakan oleh kedua negara tidak melibatkan secara langsung baik oleh Iran atau Arab Saudi, melainkan melalui pihak ketiga yang menjadi eksekutor atau penyerang terhadap Iran atau Arab Saudi. Perkembangan teknologi dan informasi menciptakan ketergantungan akan sebuah sistem yang terhubung secara daring, sehingga memberikan kerentanan atas keamanan nasional melalui serangan siber.

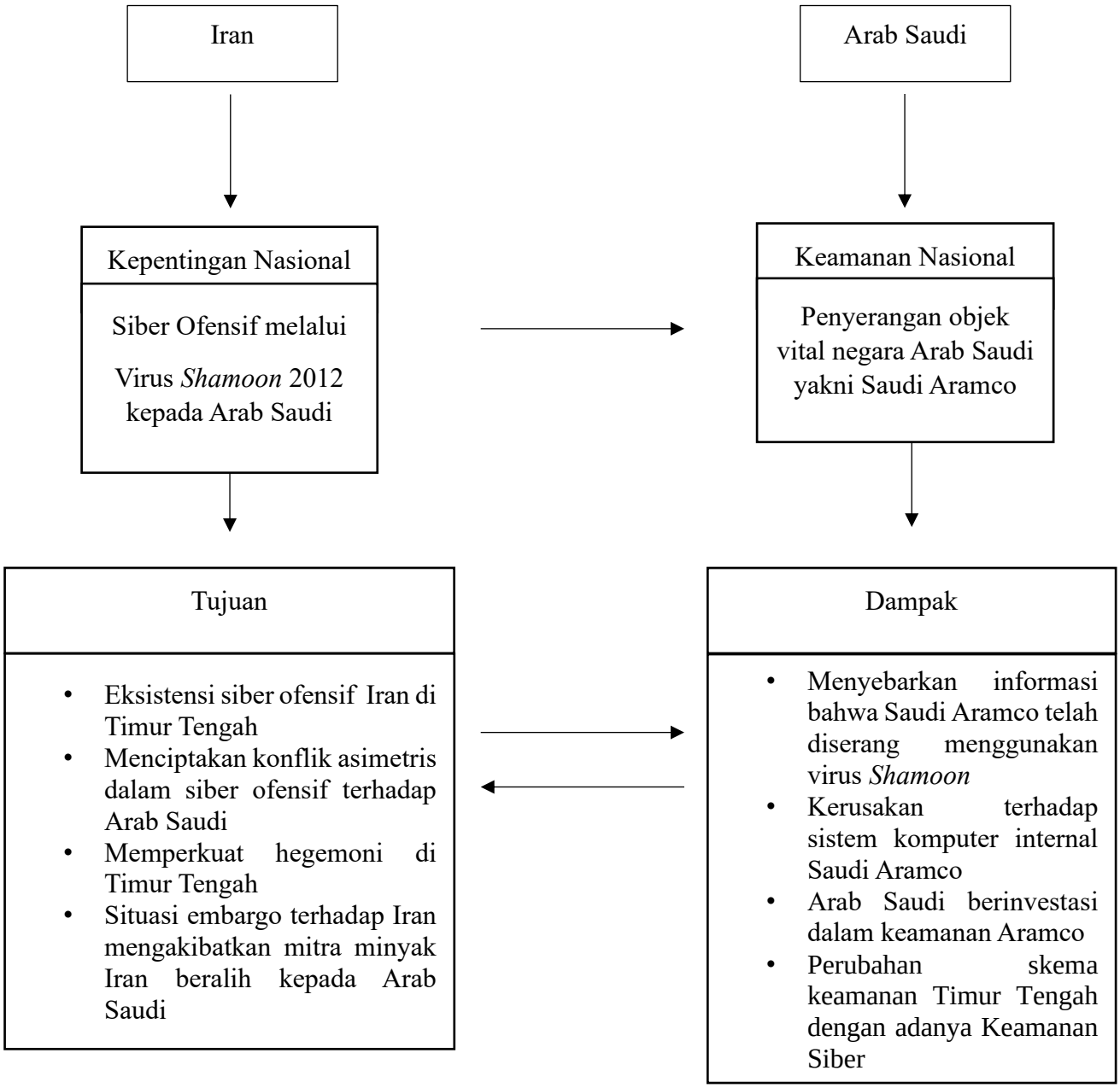
Keamanan yang menjadi dimensi penting bagi setiap negara berubah ketika setiap negara masuk dalam era globalisasi dan digitalisasi. Konsep keamanan tidak hanya melindungi kedaulatan dan garis batas negara, melainkan pada keamanan data nasional, infrastruktur kritis dan objek vital negara yang dapat berpotensi sebagai upaya tindak kejahatan di ruang maya. Eskalasi kapabilitas siber Iran mendorong Iran dalam upaya menyerang Arab Saudi melalui siber ofensif terhadap Saudi Aramco sebagai perusahaan kilang minyak Arab Saudi. Serangan siber

ofensif Iran merupakan kebangkitan Iran dalam bidang keamanan siber dan menjadi perimbangan kekuatan Arab Saudi di Timur Tengah.

Siber ofensif Iran adalah bentuk kepentingan nasional Iran salah satunya dalam respons atas kondisi internal Iran akibat tekanan internasional khususnya embargo ekonomi sehingga harus menghentikan negara – negara untuk melakukan penghentian impor minyak dari Iran dan telah mengalihkan beberapa negara pengimpor minyak Iran kepada Arab Saudi yang memiliki perusahaan minyak terbesar di dunia yaitu Saudi Aramco.

Dampak penyerangan perusahaan minyak Saudi Aramco telah melemahkan sistem komputer internal dengan menampilkan gambar bendera Amerika Serikat terbakar dan menghapus data dari perusahaan Saudi Aramco sehingga menghentikan sementara operasi di perusahaan Saudi Aramco sebagai objek vital negara. Serangan siber terhadap Saudi Aramco, dilakukan oleh salah satu kelompok peretas siber Iran yakni *Cutting Sword of Justice* dengan menggunakan *Malware* jenis virus yaitu virus *Shamoon* atau "*W32.Disstrack".*

Respons setelah terjadinya siber ofensif Iran yakni Saudi Aramco memberikan pernyataan bahwa terjadi kerusakan atas sistem komputer yang diakibatkan oleh virus. Kemudian terusiknya perusahaan Aramco sebagai keamanan siber Arab Saudi memberikan pengaruh terhadap upaya untuk membangun teknologi pertahanan serangan siber dengan melakukan investasi dalam pembangunan terhadap sistem keamanan Saudi Aramco dan membangun keamanan nasional siber Arab Saudi, berikut merupakan alur kerangka berfikir, Gambar 2.1.



Gambar 2.1 Alur Kerangka Pemikiran