BAB II

TINJAUAN PUSTAKA DAN KERANGKA PEMIKIRAN

2.1 Tinjauan Pustaka

2.1.1 Hubungan Internasional

Konflik dan perang adalah alasan utama terlahirnya disiplin ilmu dan menjadi fenomena bagi hubungan internasional. Hubungan internasional yang dulunya berfokus mengkaji tentang peperangan kini telah berkembang sebagai dampak globalisasi, seperti bentuk interaksi berupa konflik (*conflict*), kerjasama (*cooperation*) dan persaingan (*competition*). Hubungan internasional juga membahas bentuk hubungan antara aktor-aktor yang menjadi pemeran dalam hubungan internasional yaitu negara (*state*) maupun non-negara (*non-state*).

Setiap berkembangnya fenomena baru di tengah-tengah masyarakat internasional maka akan mempengaruhi pula pada hubungan internasional sebagai disiplin ilmu. Hal ini menjadikan hubungan internasional sebagai disiplin ilmu bersifat interdisipliner, yang membutuhkan ilmu-ilmu sosial lain yang menjadi pembentuknya (Darmayadi, 2015: 12).

Meskipun kajian hubungan internasional sebagai disiplin ilmu telah mencakup semua fenomena internasional, konflik dan perang masih menjadi fokus kajian hubungan internasional. Konflik dan perang masih mempunyai eksistensi dalam kajian hubungan internasional, sebab perang dan konflik adalah sebuah cara tradisional yang efektif untuk mencapai kepentingan nasional.

Fenomena konflik atau perang dapat dikatakan sebagai fenomena internasional dan dapat dikaji dalam hubungan internasional sebagai studi, apabila konflik atau perang tersebut melewati batas wilayah dan adanya kepentingan nasional yang ingin dicapai. Contohnya, jika dalam sebuah negara mengalami konflik akibat adanya masyarakat yang melakukan pemberontakan atas pemerintahan yang sah dalam negara tersebut, fenomena ini tidak menjadi kajian hubungan internasional. Akan tetapi, jika masyarakat yang melakukan pemberontakan tersebut mendapatkan bantuan dari negara lain untuk menggulingkan pemerintah tersebut, maka dapat dikatakan sebagai kajian hubungan internasional.

Perkembangan fenomena-fenomena dalam hubungan internasional kontemporer telah mencakup dalam bidang-bidang lain secara luas, sebagai berikut:

1. *Non-State Actors*. Aktor yang merupakan bukan sebuah negara dan memiliki pengaruh yang cukup signifikan dalam perkembangan hubungan internasional saat ini. Aktor tersebut seperti *multinational cooperation* (MNCs), organisasi internasional non-pemerintah (NGOs) dan organisasi internasional antar pemerintah (IGOs).
2. *States and Their Relationship*. Sistem negara-bangsa dan hubungan antar negara selalu berkembang dan membuat politik internasional menjadi mungkin.
3. *International Security*. Keamanan merupakan bidang yang selalu mendapatkan perhatian setiap nasional, sehingga menjadikan

keamanan sebagai hal yang perlu dijaga secara bersama-sama (internasional).

4. *The Foreign Policy of Power is Important*. Analisis kebijakan luar negeri negara-negara akan bermanfaat dalam perkembangan hubungan internasional, terutama kebijakan luar negeri negara-negara yang mempunyai pengaruh besar dalam dunia internasional.
5. *Globalization*. Dengan bangkitnya sistem ekonomi liberal pada ekonomi merkantil perdagangan sejak awal 1980, istilah globalisasi telah banyak diasumsikan dengan popularitas dan penggunaan yang meningkat dalam hubungan internasional.
6. *International Political Economy* (IPE). Dengan berkembangnya globalisasi pada tahuan 1980 mempengaruhi perkembangan minat pada IPE.
7. *International Terrorism.* Kegiatan dan paham kejahatan berskala transnasional adalah terorisme internasional. Keamanan dan perdamaian internasional terkait erat dengan masalah ini.
8. *Area Studies.* Mempelajari masalah ekonomi politik, sosial-budaya dan keamanan internasional dari perspektif secara luas lebih luas akan lebih sulit. Jadi, studi wilayah menjadi populer seiring meningkatnya proliferasi organisasi regional dan *free trade area*.
9. *International Enviroment.* Industrialisasi dan kemajuan teknologi telah meningkatkan kepedulian dunia terhadap keselamatan lingkungan hidup (Chartterjee, 2010: 5-7).

Kajian hubungan internasional sebagai ilmu akademis diharapkan mampu menganalisa, menjelaskan dan memprediksi atas fenomena-fenomena internasional yang tengah berkembang. Fenomena-fenomena internasional dapat dikatakan sebagai fenomena internasional, jika interaksi para aktor-aktor internasional tersebut melewati batas wilayah.

2.1.2 Keamanan Nasional

2.1.2.1 Tinjauan Umum Keamanan Nasional

Secara etimologis konsep keamanan (*security*) berasal dari bahasa latin "*securus*" (*se* + *cura*) yang mempunyai makna terbebas dari bahaya, terbebas dari ketakutan (*free from danger, free from fear*). Kata ini juga mempunyai makna dari gabungan kata *se* (yang berarti tanpa / *without*) dan *curus* (yang berarti '*uneasiness*). Sehingga jika digabungkan kata ini bermakana "*liberation from uneasiness, or a peaculf situation without any risks or threats*". Jika merujuk dalam berbagai literatur ilmu hubungan internasional, para sarjana hubungan internasional berargumenn bahwa konsep keamanan merupakan sebuah "*contested concept*" (Perwita, 2008: 3).

Keamanan nasional adalah kebutuhan dasar bagi suatu bangsa untuk melindungi dan menjaga kepentingan nasional. Kepentingan nasional menjadi suatu faktor utama dalam konsep keamanan nasional suatu bangsa. Selain menjaga dan melindungi, keamanan nasional juga bertujuan untuk memelihara dan mempertahankan eksistensi negara. Konsep keamanan menekankan peran

pemerintah dalam melindungi integritas teritorial negara dari ancaman yang datang dari luar maupun dari dalam negeri (Darmono, 2010: 9).

Definisi keamanan nasional pada masa Perang Dunia dan Perang Dingin adalah ketergantungan negara akan kekuatan militer. Perubahan definisi keamanan nasional sendiri berubah semenjak globalisasi telah mencakup semua lapisan masyarakat. Ancaman tidak lagi berupa ancaman militer, melainkan fenomena-fenomena kerusakan lingkungan, perkembangan teknologi informasi komunikasi dan ancaman dari aktor-aktor *non-state* (Darmono, 2010: 10).

Berbagai perkembangan seiring globalisasi kini menjadikan keamanan nasional memilik dampak yang besar dan fleksibel, hingga terciptanya keamanan dan ketidakamanan baik dalam skala lokal, regional bahkan internasional. Kaum realisme dengan pendekatan militer (*power*) menyatakan bahwa konsep keamanan merupakan sebuah kondisi yang terbebas dari ancaman militer atau kemampuan suatu negara untuk melindungi negara-bangsanya dari serangan militer yang berasal dari lingkungan eksternal (*the absence of a military threat or with the protection of the nation from external overthrow or attack*) (Perwita, 2008: 3).

Sejalan dengan perkembangan fenomena-fenomena dalam hubungan internasional begitu cepat, Barry Buzan dalam Perwita menyatakan :

> "Keamanan tidak hanya meliputi aspek militer dan aktor negara semata melainkan akan meliputi aspek-aspek non militer dan melibatkan pula aktivitas-aktivitas aktor non-negara" (2008: 4).

Buzan dalam bukunya yang bertajuk "*People, State and Fear*" membagi sektor keamanan ke dalam 5 sektor: Militer, politik, lingkungan, ekonomi, dan

societal. Berdasarkan pendekatan ini, Buzan memasukan sektor militer hanya sebagai salah satu aspek penting dari konsep keamanan. Sementara itu, keamanan lebih luas dan menyeluruh akan dipengaruhi pula pada sektor politik, ekonomi, lingkungan, dan *societal* baik dari peringkat individu, nasional, regional dan global (Perwita, 2008: 5).

Sumber ancaman tidak lagi bersifat militer, bahkan dalam banyak kasus sumber ancaman bisa bersifat militer dan non-militer. Lebih khusus, keamanan pun bukan hanya ditujukan bagi kelangsungan negara saja tetapi juga menjadi kebutuhan bagi semua aktor lainnya.

Seperti yang ditulis dalam *Report of the Secretary-General's High-Level Panel on Threat, Challenges and Changes,* "Hari ini, lebih dari sebelumnya, ancaman bagi seseorang adalah ancaman bagi semua orang. Kerentanan timbal balik yang lemah dan kuat tidak pernah jelas".

Berbagai konsepsi ancaman keamanan di atas selain menunjukan adanya perluasan makna dari persfektif tradisional menuju non tradisional, juga melibatkan aktor yang beragam (*non-state*) yang terlihat dari dinamika interaksi antara aktor dan sektor keamanan. Tingkat kerumitan dari sifat dan struktur sistem internasional yang dihasilkan oleh interaksi para aktor yang semakin tinggi, memunculkan pula beberapa alat analisa tambahan lainnya yang digunakan untuk mengkaji tipe aktor dan interaksi keamanan yang dihasilkan.

Peter Chlak dalam Perwita mengemukakan fenomena global kontemporer diwarnai oleh "fenomena abu-abu" (*Grey Area Phenomena*). Fenomena ini didefinisikan sebagai "ancaman-ancaman terhadap keamanan, stabilitas nasional

dan internasional yang diakibatkan dari proses-proses interaksi aktor negara dan non negara". Akibatnya, fenomena-fenomena global yang bermunculan semakin beragam. Fenomena-fenomena baru meliputi: ketidakamanan ekonomi, degradasi lingkungan dan penggunaan kemajuan teknologi informasi sebagai alat ancaman.

Munculnya berbagai fenomena baru seperti diatas sebagai sifat-sifat baru ancaman yang berkolerasi amat kuat dengan "*changing response*". Bila selama ini respon terhadap fenomena global adalah dengan kekuatan militer, maka kini fenomena-fenomena tersebut ditanggapi dengan berbagai pendekatan-pendekatan non-militer. Singkatnya, pendekatan menggunakan kekerasan/militer sepatutnya digeser dengan pendekatan-pendekatan yang bersifat non-militer (Perwita, 2008: 13).

Perbedaan antara pendekatan tradisional dan non tradisional dalam menyikapi konsep keamanan dapat dijelaskan dalam tabel, sebagai berikut:

Tabel 2.1

Klasifikasi Konsep Keamanan

	Tradisional	Non-Tradisional
Asal ancaman (*origin of threats*)	Negara rival	Non-negara domestik dan transional
Sifat ancaman (*nature of threats*)	Kapabilitas	Non militer: ekonomi, politik domestik, lingkungan hidup, terorisme, narkoba dan penggunaan teknologi informasi.
Pihak yang bertanggung jawab untuk menyediakan keamanan (*the responbility for providing security*)	Negara	Negara, Organisasi Internasional dan individu

Respon (*the responses*)	Militer	Non-militer: liberaliasi, ekonomi, demokratisasi, hak asasi manusia
Nilai inti (*core values*)	Kemerdekaan nasional, integritas teritorial, kedaulatan	Kesejahteraan ekonomi, hak asasi manusia, perlindungan terhadap lingkungan hidup

Sumber: Perwita. Dinamika Keamanan Dalam Hubungan Internasional dan Implikasinya Bagi Indonesia, 2008: 14

2.1.2.2 Keamanan Siber (*Cyber Security*) Sebagai Wilayah Keamanan Nasional

Fenomena globalisasi kontemporer dan agenda politik luar negeri tetap masih akan didominasi oleh persoalan tradisional yaitu batas-batas negera. Batas negara mempunyai peranan penting sebagai indikator dalam menentukan kedaulatan dan keamanan nasional suatu negara dan bahkan batas negara memiliki posisi penting dalam politik luar negeri sebuah negara sebagai upaya membentuk interaksi antar negara yang konstruktif dalam suatu cakupan wilayah.

Adapun wilayah negara yang harus dijaga kedaulatannya, yaitu: darat, laut, udara, angkasa, dan dunia maya. Dunia maya telah menjadi domain keamanan nasional yang harus dijaga, hal ini akibat adanya fenomena serangan-serangan yang ditujukan pada suatu negara melalui kerentanan dunia maya dan berimplikasi pada kerusakan pada kedaulatan sebuah negara.

Merriam-Webster mendefinisikan *cyber* sebagai: "*of, relating to, or involving computers or computer networks (as the internet)*". Dunia maya lebih dari sekedar internet, *hardware, software*, dan sistem informasi, tetapi juga orang dan interaksi sosial dalam jaringan ini. Dunia maya sekarang menjadi tempat

persaingan kepentingan antara kelompok-kelompok kepentingan, serta sebuah tempat perpanjangan tangan pemerintah dalam konflik dan perselisihan. Kita tidak bisa lagi menepis lebih jauh lagi politik tersembunyi dari dunia maya (Klimburg, 2012: 8).

Bell dan Wurman mengatakan bahwa berlimpahnya informasi dapat mengakibatkan kecemasan informasi (*information anxiety*). Hal ini merupakan implikasi dari *new online reality* (https://aptika.kominfo.go.id/index.php/artikel/138-peta-masa-depan-keamanan-siber-indonesia diakses pada tanggal 25 April 2017).

Beberapa negara maju telah menggunakan jaringan internet dalam menopang dan mengatur aktivitas-aktivitas dalam negaranya, seperti aktivitas perbankan, kontrol pada transportasi, menjalankan infrastruktur, pengendalian dan pengadaan senjata pada bidang militer, penyimpanan data dan informasi, pendidikan dll. Semua aktivitas-aktivitas interkoneksi tersebut bermuara pada dunia maya.

Dunia maya sebagai domain baru tanpa batas pada era informasi (*information age*) selain membawa beragam kemudahan bagi berbagai aspek kehidupan bernegara, dunia maya juga telah menghadirkan sebuah realitas baru yang menjadi sumber bagi kerentanan, potensi ancaman terhadap keamanan nasional dan kegaduhan terhadap tatanan internasional. Hal ini bahkan diakui oleh pemerintah Amerika Serikat melalui pernyataan presiden Obama, bahwa ancaman yang hadir dari dunia maya berpotensi melemahkan kepercayaan diri negara dalam sistem informasi yang mendasari kepentingan ekonomi dan keamanan

nasional negaranya. Kerentanan pada dunia maya sering kali menjadi celah bagi individu, kelompok bahkan negara untuk melakukan kejahatan siber.

Dalam berbagai literatur pengunaan kata yang umum untuk merujuk kejahatan siber adalah kejahatan dunia maya, kejahatan komputer, kejahatan dibidang teknologi informasi, kejahatan mayantara, dan sebagainya. Adapun beberapa pendapat mengenai definisi atau pengertian kejahatan siber diantaranya adalah :

1. *The U.S. Department of Justice* memberikan pengertian kejahatan siber sebagai: "... setiap tindakan ilegal yang memakai pengetahuan tentang teknologi komputer untuk tindakan, penyelidikan atau penuntutannya".
2. *Organization of European Community Development* (2004) mendefinisikan kejahatan siber sebagai: "perilaku ilegal, tidak pantas atau tidak sah yang berkaitan dengan pemrosesan otomatis dan/atau pengiriman data".
3. Pemerintah Rusia pada tahun 1997 menambahkan kejahatan siber, *IT crime and cyber terrorism* pada hukum pidana Rusia (Bab 28) dan mendefinisakannya sebagai: "hukum diidentifikasi karena, antara lain, akses ilegal terhadap informasi di komputer, sistem dan jaringan komputer*"*.
4. Kejahatan Siber telah ditambahkan pada hukum pidana China secara khusus dengan mendefinisikan kejahatan siber sebagai: "penyusupan ilegal ke dalam sistem informasi komputer dan yang menyebabkan kerusakan pada sistem informasi komputer" (Klimburg, 2012:13-14).

5. Konggres PBB ke 10 mengenai pencegahan kejahatan dan penanganan pelaku tindak pidana, yang membahas isu mengenai kejahatan yang berhubungan dengan jaringan komputer, membagi kejahatan siber menjadi 2 kategori :

> "Kejahatan Siber dalam arti sempit (*computer crime*): setiap perilaku ilegal yang ditujukan dengan sengaja pada operasi elektronik yang menargetkan sistem keamanan komputer dan data yang diproses oleh sistem komputer tersebut, atau singkatnya tindak pidana yang dilakukan dengan menggunakan teknologi yang canggih. Kejahatan Siber dalam arti luas (*computer related crime*): setiap perilaku illegal yang dilakukan dengan maksud atau berhubungan dengan sistem komputer atau jaringan, atau singkatnya tindak pidana apa saja yang dilakukan dengan memakai komputer (*hardware* dan *software*) sebagai sarana atau alat, komputer sebagai objek baik untuk memperoleh keuntungan atau tidak, dengan merugikan pihak lain" (http://www.un.org/press/en/2000/20000406.soccp214.doc.html diakses pada tanggal 25 April 2017).

Dari beberapa pengertian di atas, dapat disimpulkan bahwa kejahatan siber sebagai perbuatan melawan hukum dan ditujukan kepada sistem atau jaringan komputer secara illegal melalui sarana media jaringan internet.

Adapun jenis-jenis kejahatan siber dikelompokan dalam bentuk sesuai modus operasi yang dilakukan, antara lain:

1. *Unautorized Access to Computer System and Service*

   Kejahatan yang dilakukan dengan memasuki secara illegal kedalam sistem jaringan komputer. Modus operasi ini biasanya dilakukan dengan maksud untuk pencurian informasi penting dan rahasia. Namun ada juga yang melakukan kejahatan ini hanya sekedar iseng untuk mencoba keahlianya menembus suatu keamanan pada sistem jaringan komputer tersebut.

2. *Illegal Contents*

   Kejahatan dengan memasukan data atau informasi ke internet tentang suatu hal yang tidak benar dan dianggap melanggar hukum atau menggangu ketertiban publik. Contohnya, informasi palsu atau berita *hoax* yang ditujukan untuk merusak identitas seseorang, kelompok bahkan negara.

3. *Data Forgery*

   Kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan di internet. Kejahatan ini ditujukan pada dokumen-dokumen yang dimiliki lembaga yang memiliki layanan berbasis web database.

4. *Cyber Sabotage and Extortion*

   Merupakan kejahatan dengan tujuan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer hingga sistem jaringan komputer yang terhubung dengan internet. Biasanya kejahatan ini dilengkapi dengan aksi menyusupkan *malware* kedalam sistem jaringan komputer, sehingga sistem jaringan komputer tidak dapat berjalan sebagaimana mestinya atau berjalan sebagaimana yang dikehendaki oleh pelaku kejahatan tersebut.

5. *Cyber Espionage*

   Kegiatan mata-mata terhadap pihak lain melalui fasilitas jaringan internet sebagai media kejahatan. Kejahatan ini pada umumnya

dilakukan untuk melihat dokumen atau data penting pihak rival yang tersimpan dalam suatu sistem yang terkomputerisasi.

6. *Offense against Intellectual Property*

   Merupakan kejahatan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet. Contohnya, penyebaran secara ilegal terkait informasi dagang milik pihak lain di internet.

7. *Carding*

   Kejahatan dengan aksi mencuri nomor kartu kredit milik orang lain dan dipergunakan untuk transaksi perdagangan di internet.

8. *Cracking*

   Kejahatan di internet yang memiliki ruang lingkup yang luas, mulai dari aksi balas dendam terhadap instansi tertentu, membajak hak atas kekayaan intelektual dan menghapus data melalui jaringan internet (Golose, 2006: 35-37).

Semua jenis kejahatan siber di atas, dapat dilakukan oleh aktor dari negara lain yang memanfaatkan kerentanan dunia maya sebagai domain tanpa hambatan jarak dan waktu.

Semua bentuk ancaman dan kejahatan pada dunia maya diperlukan langkah untuk menjaga keamanan dalam lingkungan siber (*cybersecurity*). *Cybersecurity* adalah kumpulan alat, kebijakan, konsep keamanan, pengamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan dan organisasi lingkungan dan aset penggunaan. Aset organisasi dan penggunaan

mencakup perangkat komputasi, personalia, infrastruktur, aplikasi, layanan, sistem telekomunikasi, dan totalitas informasi yang dikirim dan/atau disimpan di lingkungan siber. *Cybersecurity* berusaha untuk memastikan pencapaian dan pemeliharaan properti keamanan organisasi dan aset pengguna terhadap risiko keamanan yang relevan di lingkungan siber.

Tujuan keamanan umum terdiri dari:

1. Ketersediaan
2. Integritas, yang mungkin termasuk keaslian dan tidak dapat ditolak
3. Kerahasiaan

(http://www.itu.int/en/ITUT/studygroups/com17/Pages/cybersecurity.aspx diakses pada tanggal 15 Juni 2017)

Kebijakan dan strategi pertahanan suatu negara harus dapat berubah secara dinamis sesuai dengan perkembangan lingkungan strategis dan sumber ancaman. Perubahan strategi keamanan tersebut terkait erat dengan kepentingan dan prioritas kemanan nasional. Untuk mengamankan kedaulatan dari kejahatan siber, beberapa negara telah menerapkan keamanan siber sebagai strategi keamanan nasionalnya. Berikut tujuan kemanan siber menurut beberapa negara, seperti: Australia pada naskah *Cyber Security Strategy* tahun 2009 mendefinisikan keamanan siber, sebagai: "tindakan yang berkaitan dengan pengamanan kerahasiaan, ketersediaan dan integritas informasi yang diproses, disimpan dan dikomunikasikan dengan cara eletronik atau sejenisnya" dan United Kingdom pada naskah *The UK Cyber Security Strategy Protecting And Promoting the UK in a Digital World* tahun 2011 mendefinisikan keamanan siber, sebagai: "tindakan

yang diambil untuk mengurangi resiko dan menjamin manfaat lingkungan digital yang terpercaya untuk bisnis dan individu" (Klimburg, 2012: 23-25).

2.1.3 Kepentingan Nasional

Kepentingan nasional (*national interest*) secara umum diartikan sebagai kepentingan vital suatu bangsa yang harus diperjuangkan demi kelangsungan hidupnya sekaligus menjaga eksistensi dalam pergaulan internasional. Kepentingan nasional tersebut termanifestasi menjadi arahan dalam pengambilan politik luar negeri. Negara memainkan peran yang penting sebagai aktor dalam mengambil keputusan dengan mempertimbangkan berbagai kebutuhan atau keinginan rakyatnya.

Kepentingan nasional dapat ditinjau dari kondisi internal dalam negeri, seperti kondisi militer, politik-ekonomi dan sosial-budaya. Menciptakan suatu *power* juga sebagai suatu dasar bagi kepentingan nasional, sehingga negara dapat pengakuan dunia. Peran negara dalam memberikan dan menjalankan kepentingan nasional tidak dapat dihindari akan menjadi kacamata masyarakat internasional sebagai negara yang menjalin hubungan yang terlampir dari kebijakan luar negerinya. Dengan demikian, kepentingan nasional secara konseptual dipergunakan untuk menjelaskan perilaku politik luar negeri dari suatu negara (Sitepu, 2011:163).

Menurut Hans J. Morgenthau dalam Sitepu, kepentingan nasional diartikan sebagai tujuan yang harus dicapai oleh setiap negara dalam melaksanakan politik luar negerinya. Kepentingan nasional merupakan hasil kompromi politik antara

berbagai pihak dalam suatu negara yang berbeda kepentingannya. Kepentingan nasional juga diartikan sebagai kemampuan minimum negara bangsa dalam melindungi identitas fisik (wilayah), identitas politik, ekonomi, identitas kulturalnya dari ancaman negara lain. Dari tinjauan itu, para pemimpin suatu negara dapat menurunkan suatu kebijakan spesifik terhadap negara lain bersifat kerjasama atau konflik (2011:52).

Kepentingan nasional pada dasarnya adalah rangkuman aspirasi suatu bangsa. Untuk mencapai tujuan-tujuan nasional tersebut, langkah awal yang perlu dilakukan adalah menetapkan rumusan prioritas kepentingan nasional. Terdapat beberapa strata yang membagi kepentingan nasional, yaitu:

1. Kepentingan Primer (*Primary Interest*), merupakan kepentingan nasional yang memberikan perlindungan pada kedaulatan dalam negara, yang termasuk di dalamnya wilayah, identitas politik, budaya dan keberlangsungan hidup dari ancaman eksternal. Kepentingan primer ini tidak dapat diganggu gugat, sehingga negara secara total mempertahankan untuk pencapaian kepentingan ini.
2. Kepentingan Sekunder (*Secondary Interest*), kepentingan yang hampir sama halnya dengan kepentingan primer, akan tetapi kepentingan sekunder diarahkan keluar negara tersebut. Contohnya, melindungi warga negara dan melindungi aset-aset yang berada di luar negeri.
3. Kepentingan Permanen (*Permanent Interest*), merupakan kepentingan yang tidak berubah dan jangka waktu yang lama.

4. Kepentingan Tidak Tetap (*Variabel Interest*), merupakan kepentingan yang dilakukan secara kondisional yang berarti dianggap penting pada waktu tertentu.
5. Kepentingan Umum (*General Interest*), merupakan kepentingan yang dilakukan dan diterapkan pada banyak negara atau untuk beberapa bidang seperti perdagangan, keamanan regional/internasional dan sebagainya.
6. Kepentingan Khusus (*Specific Interest*), merupakan kepentingan yang diterapkan pada bidang dan waktu tertentu, biasanya sebagai bentuk penekanan pada kepentingan umum (Couloumbis dan Wolfe. 2004 : 110).

Setiap langkah yang diambil para pembuat keputasan (*decision makers*) dalam merumuskan kebijakan luar negerinya (*foreign policy*) harus sesuai dengan kepentingan nasional dan di arahkan untuk mencapai serta melindungi cita-cita kepentingan nasional itu (Rudy, 2003:116).

2.1.4 *Multinational Corporations* (MNCs)

Sebagai bentuk tanda terjadinya dan peran globalisasi adalah menjamurnya keberadaan *Multinational Corporations* (MNCs) diberbagai negara, dan mempunyai peranan penting dalam hubungan internasional. Banyaknya *multinational corporations* disebabkan oleh interdepedensi yang terjadi karena suatu negara mempunyai keterbatasan *resource*. Selanjutnya, *multinational corporatioan* akan ditulis dengan MNCs. Untuk mengetahui relasi antara

pembangunan nasional dan MNCs, maka diperlukan definisi atau pengertian dan karakteristik mengenai konsep MNCs.

Sejarah perkembangan MNCs dimulai setelah Perang Dunia II, peranan MNCs dalam prosesnya tidak hanya sebagai lembaga ekonomi, bahkan menjadi lembaga politik yang dapat mempengaruhi kebijkan negara asal MNCs (*home country*) maupun di negara investasi oleh MNCs (*host country*).

Istilah MNCs pertama kali dikenalkan oleh David E. Lilienthal (1960) dalam naskahnya tentang *Management and Corporation.* Naskah Lilienthal dipublikasikan dan dikenal dengan istilah *The Multinational Corporation.* Dalam naskahnya, Lilienthal mendefinisikan pengertian MNCs sebagai perusahaan yang mempunyai kedudukan di suatu negara, tetapi dalam menjalankan dan mengoperasikan perusahaan berlandaskan dengan hukum dan aturan negera lain.

Joan Edelman Spero dalam bukunya berjudul *The Politics of International Economic Relations* mendefinisikan MNCs, sebagai:

> "Perusahaan Multinasional adalah perusahaan dengan anak perusahaan asing yang memperluas produksi dan pemasaran perusahaan di luar batas-batas negara manapun. Perusahaan multinasional bukan hanya perusahaan besar yang memasarkan produk mereka ke luar negeri, mereka adalah perusahaan yang mengirim paket modal, teknologi, bakat manajerial, dan keterampilan pemasaran ke luar negeri untuk melakukan produksi di luar negeri" (2010: 130).

Dalam pengertian di atas, Spero menjelaskan bahwa proses produksi dalam MNCs benar-benar mendunia. Langkah produksi yang berbeda dan tahap penjualan juga seringkali bertaraf internasional.

Menurut Neil H. Jacoby, MNCs yang beroperasi di seluruh dunia mempunyai karakteristik secara umum, yaitu:

1. Mempunyai dan membentuk cabang-cabang (anak perusahaan) di luar negeri
2. Visi yang ditujukan dan strategi yang digunakan untuk memproduksi suatu produk bersifat global.
3. Perolehan pendapatan yang dilakukan atas aktivitas MNCs berasal dari luar negara.
4. Menempatkan cabang pada negara-negara maju.
5. Pengembangan sistem managemen dan distribusi yang melampaui batas-batas negara.
6. Modal dan pengguasaan teknologi sangat diutamakan mengingat kedua faktor tersebut merupakan keuntungan kompetitif perusahaan internasional.
7. Kualitas produk harus diperhatikan secara khusus karena tingkat persaingan dilevel dunia.
8. Cenderung fokus pada kegiatan bisnis tertentu (http://www.yourarticlelibrary.com/india2/multinational-corporations/multinational–corporations–mncs-meaning-features-and-advantages-business/69418 diakses pada 15 Juni 2017)

2.1.5 Perang Siber (*Cyber wafare*)

2.1.5.1 Pengertian *Cyber Warfare*

Cyber warfare jika diartikan secara harfiah ke dalam bahasa Indonesia berarti Perang Sibernetika. *Cyber warfare* secara etimologi terdiri dari dua suku

kata, yaitu siber yang berarti sibernetika dan *warfare* atau perang. Dalam Kamus Besar Bahasa Indonesia, sibernetika berarti ilmu pengetahuan tentang komunikasi dan pengawasan yang khususnya berkenan dengan studi bandingan atas sistem pengawasan otomatis (sistem saraf atau otak).

Pengertian perang menurut Kamus Besar Bahasa Indonesia mempunyai banyak makna, seperti: permusuhan antar dua negara; pertempuran besar bersenjata antara dua pasukan atau lebih; perkelahian; konflik; cara mengungkapkan permusuhan.

Penjelasan secara etimologi, peneliti memahami *cyber warfare* sebagai konflik bersenjata dengan memanfaatkan teknologi siber. Inti dari terjadinya pertikaian dalam konlifk bersenjata adalah alat dan teknik yang digunakan dalam peperangan. Hal ini juga diterapkan dalam *cyber warfare* yang membutuhkan alat dan teknik dalam menjalankan peperangan (William, 2013: 387).

Dampak era informasi mengenai peperangan telah menjadi isu utama selama dua dekade terakhir karena para pembuat kebijakan, tentara, ahli strategi, dan aktor non-negara menganggap betapa terbaik untuk menggunakan dan melindungi diri dari ancaman *cyber warfare*. Tidak seperti senjata masa lalu, teknologi yang diperlukan untuk melancarkan *cyber warfare* tidak terbatas pada pelaku tertentu di dalam sistem. Setiap serangan menggambarkan potensi kerusakan *cyber warfare*. Karena *cyber warfare* adalah peperangan yang tidak konvensional dan asimetris, negara-negara yang lemah dalam kekuatan militer konvensional juga cenderung menginvestasikannya sebagai cara untuk menghilangkan kerugian konvensional.

Beberapa definisi memberi pengertian *cyber warfare* dari pendekatan dan gagasan, yaitu:

1. Organisasi Kerjasama Shanghai telah mendefinisikan *cyber warfare* sebagian sebagai "perbandingan antara dua atau lebih negara bagian di ruang informasi yang bertujuan untuk merusak sistem politik, ekonomi, dan sosial (cuci otak secara massal untuk merusuhi masyarakat dan negara)".
2. Serangan siber menurut Komando Pelatihan & Ajaran Angkatan Darat AS adalah "Penggunaan terencana dari aktivitas yang mengganggu, atau ancaman daripadanya, terhadap komputer dan / atau jaringan, dengan maksud untuk menyebabkan kerusakan atau sasaran sosial, ideologis, agama, politik atau tujuan yang lebih jauh. Atau untuk mengintimidasi siapapun yang memiliki tujuan seperti itu".
3. Schaap mendefinisikan *cyber warfare* sebagai penggunaan kemampuan berbasis jaringan dari satu negara untuk mengganggu, menolak, menurunkan, memanipulasi, atau menghancurkan informasi yang tinggal di komputer dan jaringan komputer, atau komputer dan jaringan itu sendiri, dari negara lain (Greathouse, 2014: 23).

Cyber warfare adalah penggunan *cyberpower* untuk menimbulkan ancaman atau menjatuhkan musuh untuk mencapai tujuan politik tanpa persetujuan lawan. *Cyberpower* mengandalkan *hardware* dan *software*. *Hardware* adalah perangkat mekanis, magnetik, eletronik dan listrik yang terdiri dari sistem komputer, seperti unit pemrosesan pusat, *disk drive*, papan kunci atau layar.

Kabel, satelit, *router,* chip komputer dan sejenisnya dianggap *hardware*. *Software* terdiri dari program yang digunakan untuk mengarahkan operasi dan penggunaan komputer. *Malware* adalah perangkat lunak perusak yang mengganggu fungsi aplikasi komputer dan aplikasi berbasis internet dan merupakan senjata utama dalam *cyber warfare* (Schreirer, 2015:15).

2.1.5.2 Karakteristik *Cyber Warfare*

Tujuan *cyber warfare* dalam mencapai kepentingannya tidak jauh berbeda dengan perang konvensional yang menggunakan senjata. Ada beberapa karakteristik yang menempel pada *cyber warfare* dan menjadi pembeda dengan perang konvensional (tradisional), yaitu:

1. Serangan siber (*cyber attack*) dalam *cyber warfare* dapat dilakukan oleh pihak-pihak yang tidak dikenal (*extreme anonymity*).
2. Serangan siber (*cyber attack*) dapat dilakukan oleh siapapun karena peralatan penunjangnya dapat dengan mudah didapatkan dan harganya murah (*low cost and reachable*).
3. *Cyber warfare* tidak membutuhkan tenaga fisik dalam jumlah besar.
4. *Cyber warfare* tidak terjadi pada dunia nyata tetapi terjadi di dunia yang virtual (dunia maya). Namun, implikasi dari *cyber attack* dapat dirasakan pada dunia nyata/faktual

Namun ada kemiripan *cyber warfare* dan konflik bersenjata secara konvensial yaitu sama-sama mempunyai motivasi politik (*political objective*) (Clinton, 2015:70-71).

2.2 Kerangka Pemikiran

Konflik Amerika Serikat dan Korea Utara tidak hanya terjadi dalam dunia aktual, melainkan telah terwujud dalam dunia yang baru-baru ini terbentuk, yaitu dunia maya. Dunia maya saat ini telah dipandang oleh sebagian negara merupakan domain perang masa depan. Dunia maya adalah tempat muaranya semua bentuk aktivitas-aktivitas yang dilakukan melalui jaringan komputer atau internet. Bersamaan dengan globalisasi yang terjadi, penggunaan teknologi informasi dan komunikasi telah mengantarkan pada masyarakat yang terintegrasi secara wilayah dan waktu.

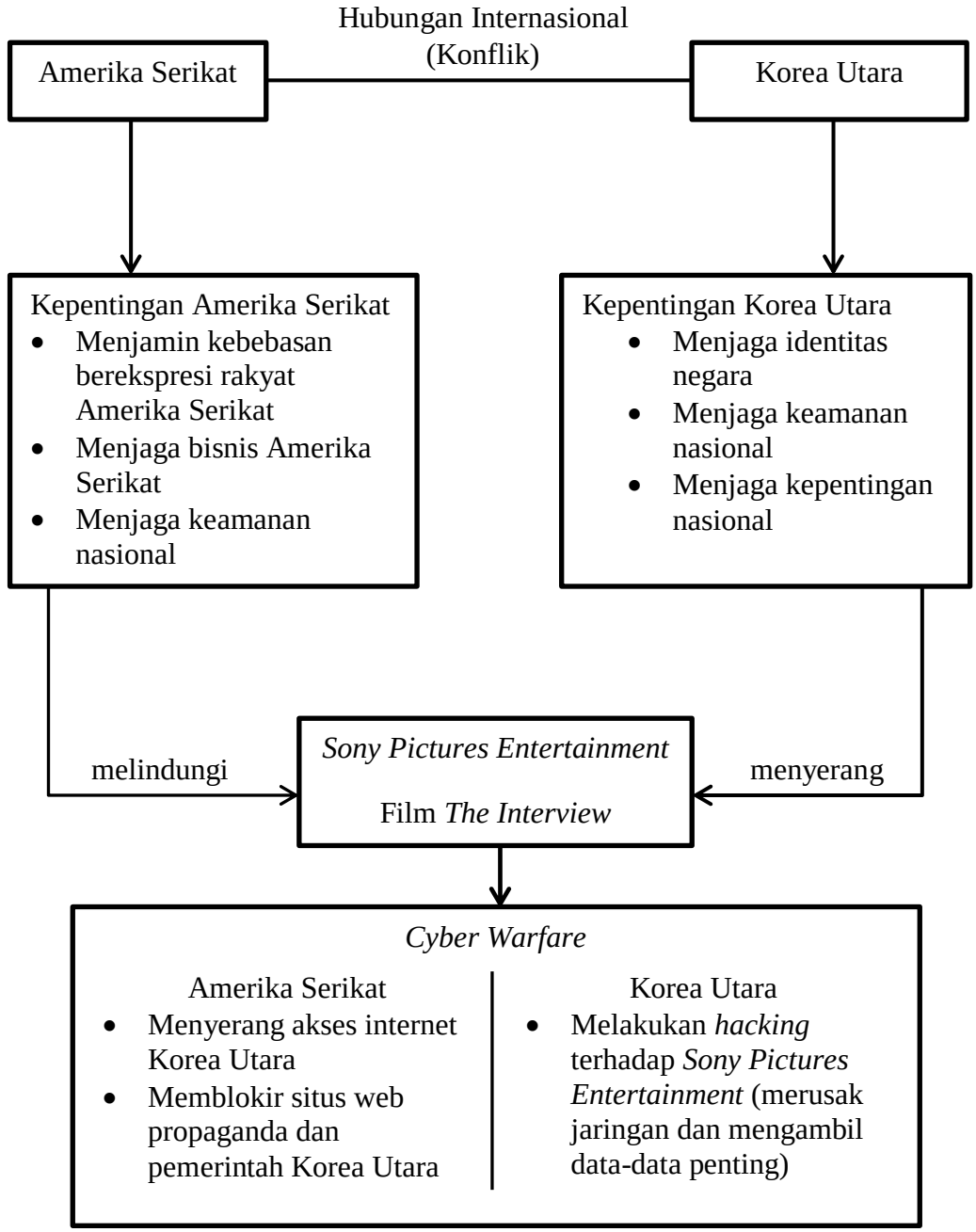
Cyber warfare antara Amerika Serikat dan Korea Utara terjadi akibat *Sony Pictures Entertainment*, salah satu industri hiburan yang berada di kedaulatan Amerika Serikat diserang oleh sekelompok *hacker*. Kelompok *hacker* yang bernamakan *The Guardians of Peace* ini, memanfaatkan dunia maya sebagai arena tempat melakukan serangan pada *Sony Pictures Entertainment.* Serangan yang ditujukan pada *Sony Pictures Entertainment* sebagai bentuk protes dan kecaman, akibat perilisan film yang dilakukan oleh *Sony Pictures Entertainment. The Interview* adalah salah satu film yang hasil produksi oleh *Sony Pictures Entertainment* yang menceritakan tentang kediktatoran Kim Jong Un selaku pemimpin Korea Utara.

Akibat film *The Interview* tersebut, *Sony Pictures Entertainment* mendapatkan serangan dan ancaman dari *The Guardians of Peace* yang diketahui merupakan kelompok *hacker* yang berasal dari Korea Utara. Serangan yang memanfaatkan jaringan komputer atau internet tersebut, membuat *Sony Picture*

Entertainment mengalami kerugian dan sempat menunda penayangan film *The Interview*.

Barack Obama sebagai presiden Amerika Serikat pada masa itu mengambil sikap atas serangan yang dialami *Sony Pictures Entertainment.* Obama menyatakan serangan yang ditujukan pada *Sony Pictures Entertainment* telah mengganggu kedaulatan Amerika Serikat. Respon yang dilakukan oleh Amerika Serikat sama dengan yang dilakukan Korea Utara, yaitu menyerang melalui jaringan komputer atau internet. Dalam serangan yang dilancarkan Amerika Serikat, Korea Utara mengalami kelumpuhan hingga mati total pada konektifitas internet di Korea Utara.

Secara lebih rinci kerangka pemikiran akan digambarkan dalam bentuk bagan sebagai berikut:



Gambar 2.1

Gambar Kerangka Pemikiran