BAB II

TINJAUAN PUSTAKA DAN KERANGKA PEMIKIRAN

2.1 Tinjauan Pustaka

2.1.1 Hubungan Internasional

Istilah Hubungan Internasional telah berkembang cukup pesat pada akhir abad ke-19, berbagai pakar Hubungan Internasional telah banyak memberikan definisi - definisi secara garis besar bahwa Hubungan Internasional merupakan hubungan yang terjalin antar negara - negara diseluruh belahan dunia.

Dimana di dalam Hubungan Internasional sendiri terdapat komponen - komponen yang mempengaruhi kerja dari Hubungan Internasional sendiri yakni adanya analisis mengenai perbandingan politik luar negeri suatu negara, hukum internasional, organisasi - organisasi internasional, perbandingan politik dan studi kawasan *(area studies)*, studi - studi strategis *(strategis studies)*, pembangunan internasional, komunikasi internasional, dan studi perdamaian serta upaya penyelesaian konflik **t**ermasuk yang menyangkut pengendalian dan pelucutan senjata.

Hubungan internasional dapat dilihat dari berkurangnya peran negara sebagai aktor dalam politik dunia dan ditambahkan dengan meningkatnya peranan aktor non negara. Batas-batas yang memisahkan antar negara semakin kabur dan tidak relevan. Bagi beberapa aktor non negara bahkan batas-batas wilayah secara geografis tidak dihiraukan (Perwita & Yani, 2005: 4).

Hubungan Internasional (HI) adalah ilmu yang mempelajari hubungan antar negara, termasuk peran segenap negara, organisasi antar pemerintah (IGO), organisasi non pemerintah internasional (INGO), organisasi non pemerintah (NGO), kemudian perusahaan multinasional (MNC). HI merupakan sebuah bidang akademik dan kebijakan publik yang bersifat positif/normatif, karena keduanya berupaya menganalisis dan merumuskan kebijakan luar negeri negara-negara terpilih.

Istilah hubungan internasional memiliki beberapa arti:

1. Suatu bidang spesialisasi yang meliputi aspek – aspek internasional dari beberapa cabang ilmu pengetahuan.
2. Sejarah baru dari politik internasional
3. Semua aspek internasional dari kehidupan sosial manusia, dalam arti: semua tingkah laku manusia yang terjadi atau berasal di suatu negara dan dapat mempengaruhi tingkah laku di negara lain (Darmayadi, 2015: 22).

Menurut Robert Jackson & George Sorenson dalam buku "Pengantar Studi Hubungan Internasional", mengemukakan bahwa alasan utama mengapa kita harus mempelajari hubungan internasional adalah adanya fakta bahwa seluruh penduduk dunia terbagi kedalam wilayah komunitas politik yang terpisah, atau negara-negara merdeka, yang sangat mempengaruhi cara hidup manusia. Secara bersama-sama negara-negara tersebut membentuk sistem internasional yang akhirnya menjadi sistem global (2005:3).

Hubungan Internasional adalah segala bentuk interaksi, diantara masyarakat, negara - negara, baik yang dilakukan negara maupun warga negara yang terjadi dengan melintasi batas-batas geografis negara. Terdapat lima unsur yang merupakan unsur pokok dalam pembelajaran tentang hubungan internasional, yaitu:

1. Sifat dan berlakunya atau pelaksanaan sistem kenegaraan.
2. Faktor – faktor yang mempengaruhi dan menentukan kekuatan *(power)* dari suatu negara.
3. Posisi internasional dan politik luar negeri dari negara – negara besar.
4. Sejarah hubungan internasional yang baru lampau.
5. Pembentukan suatu tertib dunia *(world order)* yang lebih stabil (Darmayadi, 2015:26).

Hubungan internasional adalah bentuk upaya yang harus dilakukan oleh semua negara di dunia, karena semakin banyaknya persoalan antar negara yang dihadapi oleh masyarakat internasional telah membuat suatu bentuk ketergantungan antar negara satu dengan lainnya. Pola interaksi hubungan internasional tidak dapat dipisahkan dengan segala bentuk interaksi dan pelakunya yang berlangsung dalam pergaulan masyarakat internasional, baik oleh pelaku negara (*state-actor)* maupun oleh pelaku bukan negara *(non-state actor)*. Pola hubungan atau interaksi ini dapat berupa kerjasama *(cooperation)*, persaingan *(competition)*, dan pertentangan *(conflict)* (Rudy, 2005:2)

2.1.2 Politik Luar Negeri

Politik luar negeri merupakan studi manajemen hubungan eksternal dengan aktivitas – aktivitas negara bangsa seperti yang berbeda dengan kebijakan dalam negeri. Politik luar negeri melibatkan cita – cita, strategi, tindakan, metode, panduan dan arahan oleh pemerintah nasional yang saling melakukan interaksi/hubungan internasional dengan aktor – aktor lain (organisasi internasional, LSM, perusahaan, dll) (Jackson dan Sorensen, 2013: 439)

Politik luar negeri mencakup segala tindakan diatas yang bersifat kooperatif maupun kompetitif yang dilakukan oleh sebuah negara dalam hubungan internasional. Semua negara di dunia diwajibkan untuk mengembangkan dan melaksanakan kebijakan luar negeri terhadap negara – negara lain dan aktor – aktor internasional. Umumnya para pembuat kebijakan luar negeri yang utama adalah pejabat pemerintah (presiden, perdana menteri, menteri luar negeri, menteri pertahanan, dsb). Para pembuat kebijakan tersebut cenderung melibatkan alat – tujuan dan biaya – analisis manfaat dengan cara – cara yang telah disusun untuk mencapai kepentingannya (Jackson dan Sorensen, 2013:536).

Keohane dan Nye menggambarkan bagaimana revolusi informasi secara dramatis merubah pola hubungan internasional, yang mereka konsepkan sebelumnya, "*complex interdependence*". Konsep ini merupakan gambaran dunia yang tidak lagi didominasi oleh hubungan keamanan dan militer. Negara terhubung satu sama lain melalui hubungan sosial dan politik. Revolusi informasi telah memperluas relasi transnasional secara cepat. Aktor non pemerintah

memiliki kesempatan yang jauh lebih besar untuk mengatur dan mempropaganda pandangan-pandangannya. Akibatnya para pemimpin politik menjadi lebih sulit untuk memelihara kohesivitas dalam isu politik luar negeri (Triwahyuni, dan Yani, 2018:6).

Kebijakan politik luar negeri dipengaruhi oleh dua faktor yaitu faktor dalam negeri (internal) dan faktor luar negeri (eksternal). Bagaimanapun, politik luar negeri merupakan gambaran dari keinginan dan aspirasi seluruh rakyat suatu negara yang harus diperjuangkan oleh pemerintahnya di dunia internasional dalam upaya menentukan keterlibatan negara di dalam kancah politik internasional.

1. Faktor Internal

Faktor dalam negeri yang mempengaruhi kebijakan politik luar negeri beberapa diantaranya yaitu sistem pemerintahan, keadaan wilayah, tujuan nasional negara, ideologi bangsa, sumber daya alam, bahkan jumlah penduduk. Di samping itu, seringnya terjadi pergantian pemimpin negara juga mempengaruhi kebijakan politik luar negeri.

2. Faktor Eksternal

Faktor luar negeri juga sangat berpengaruh kuat terhadap penyusunan kebijakan politik luar negeri suatu negara. Pergaulan dunia, bagaimana sebuah negara melihat negara lain berdasarkan pada apa yang dimiliki oleh negara tersebut (faktor *tengible* dan *integible power,* kualitas dan kemampuan diplomat negara).

Adapun keputusan-keputusan dalam politik luar negeri terdiri dari tiga kategori utama, yaitu:

1. Keputusan yang bersifat pragmatis (terencana) adalah keputusan besar yang mempunyai konsekuensi dan tujuan jangka panjang; membuat studi lanjutan, pertimbangan dan evaluasi yang mendalam mengenai seluruh opsi alternatif.
2. Keputusan yang bersifat krisis adalah keputusan yang dibuat selama masa-masa terancam berat dan darurat; waktu untuk menanggapinya terbatas, dan ada elemen mendadak yang membutuhkan respon yang telah direncanakan sebelumnya.
3. Keputusan yang bersifat taktis adalah keputusan penting biasanya bersifat pragmatis; memerlukan revaluasi, revisi dan pembalikan (Couloumbis & Wolfe, 2004:129).

2.1.3 Hubungan Bilateral

Dalam Hubungan Internasional terdapat hubungan kerjasama antar negara yang merupakan pertemuan beragam kepentingan internasional dari beberapa negara yang sifatnya tidak dapat dipenuhi oleh bangsanya sendiri.

Menurut T. May. Rudy hubungan bilateral adalah kerjasama yang terbentuk dari berbagai komitmen individu untuk mendapatkan kesejahteraan secara kolektif yang merupakan hasil dari adanya persamaan kepentingan (Rudy, 2005:5). Definisi kerjasama menurut Holsti dapat dibagi menjadi lima, yaitu:

1. Pandangan bahwa dua atau lebih kepentingan nilai atau tujuan saling bertemu dan dapat menghasilkan sesuatu, dipromosikan atau di penuhi oleh semua pihak.

2. Persetujuan atas masalah tertentu antar dua negara atau lebih dalam rangka memanfaatkan persamaan benturan kepentingan.
3. Pandangan atau harapan suatu negara bahwa kebijakan yang diputuskan oleh negara lainnya membantu negara itu untuk mencapai kepentingan dan nilai-nilainya.
4. Aturan resmi atau tidak resmi mengenai transaksi di masa depan yang dilakukan untuk melaksanakan tujuan.
5. Transaksi antara negara untuk memenuhi persetujuan mereka.

Hakikat dari pelaksanaan kerjasama yang dilaksanakan oleh setiap negara memiliki sifat universal guna membentuk suatu keadaan yang mampu menghindari berbagai permasalahan dan konflik yang bersifat internasional. Bentuk interaksi kerjasama dapat dibedakan berdasarkan pihak yang melakukan hubungan antara negara, yaitu kerjasama bilateral, trilateral, regional, dan multilateral.

Hubungan bilateral merupakan keadaan yang menggambarkan hubungan timbal balik antara kedua belah pihak yang terlibat, dan aktor utama dalam pelaksanaan hubungan bilateral itu adalah negara (Perwita dan Yani, 2005: 28)

Hubungan bilateral tercipta dari dua negara yang melakukan interaksi, hubungan bilateral dirasa lebih efektif dalam pelaksanaan untuk mencapai kepentingan nasional karena dilakukan secara intim (hanya dua negara) sehingga tidak adanya tingkatan hirarki diantara keduanya.

2.1.4 Kepentingan Nasional

Kepentingan Nasional merupakan konsep yang paling dikenal luas di kalangan penstudi hubungan internasional dan politik internasional. Hal ini terjadi selama negara bangsa masih merupkan aktor yang utama dalam hubungan internasional. Semua ahli hampir sepakat bahwa determinan utama yang menggerakkan negara-negara menjalankan hubungan internasional adalah kepentingan nasionalnya (Rudy, 2002: 60).

Konsep kepentingan nasional juga mempunyai indikasi dimana negara atau *state* berperan sebagai aktor utama di dalam formulasi politik yang merdeka berdaulat. Selanjutnya didalam mekanisme interaksinya masing-masing negara atau aktor berupaya untuk mengejar kepentingan nasionalnya. Kepentingan inilah yang akhirnya diformulasikan ke dalam konsep "*power*" kepentingan "*interest*" didefinisikan ke dalam terminologi *power* (Sitepu, 2011: 56).

Kepentingan nasional tercipta dari kebutuhan suatu negara. Kepentingan ini dapat dilihat dari kondisi internalnya, baik dari kondisi politik-ekonomi, militer, dan sosial-budaya. Kepentingan juga didasari akan suatu "*power*" yang ingin diciptakan sehingga negara dapat memberikan dampak langsung bagi pertimbangan negara agar dapat pengakuan dunia. Peran suatu negara dalam memberikan bahan sebagai dasar dari 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).

2.1.5 Kebijakan Pertahanan

Kebijakan nasional pada hakikatnya merupakan alat atau sarana unutk mengkomunikasikan kebijakan pemerintah kepada masyarakat, baik nasional maupun internasional. Untuk masyarakat, yakni memberikan pencerahan kepada masyarakat tentang penyelenggaraan pemerintahan. Sedangkan dalam kerangka hubungan internasional, kebijakan nasional, terutama kebijakan pertahanan merupakan sarana untuk membangun rasa saling percaya dengan negara – negara lain, baik dalam konteks regional maupun global. Kebijakan pertahanan diartikan oleh William Dunn sebagai berikut:

> "Kebijakan pertahanan merupakan salah satu kebijakan publik, yaitu kebijakan – kebijakan yang dibuat oleh pemerintah sebagai pembuat kebijakan untuk mencapai tujuan – tujuan tertentu di masyarakat dimana dalam penyusunannya melalui berbagai tahapan." (Dunn, 2011:24)

Kerjasama pertahanan tentunya melibatkan lembaga pertahanan setiap negara, karena lembaga pertahanan adalah sebagian dari tatanan industri nasional yang secara khusus memiliki kemampuan ataupun potensi yang dapat dikembangkan untuk menghasilkan produk berupa sistem senjata, peralatan dan perlengkapan, dukungan administrasi atau logistik ataupun jasa – jasa kepentingan penyelenggaraan pertahanan negara. Industri pertahanan menjadi sangat penting untuk berjalannya sebuah kerjasama pertahanan, kesanggupan industri pertahanan untuk mengembangkan produk persenjataan menciptakan sebuah perjanjian kerjasama di bidang pertahanan (Dunn, 2011:24)

Dalam Kamus Besar Bahasa Indonesia, kebijakan adalah rangkaian konsep dan asas yang menjadi pedoman dan dasar rencana dalam pelaksanaan suatu

pekerjaan, kepemimpinan, dan cara bertindak. Istilah kebijakan biasa diterapkan oleh pemerintahan, organisasi, kelompok sektor swasta, bahkan individu.

Kajian mengenai kebijakan tidak terlepas dari hubungannya dengan pemerintahan, baik sebagai administrator, aktor maupun pelaku kebijakan itu sendiri. Kebijakan pemerintah atau kebijakan negara sebagai terjemahan dari *public policy* yang mana cenderung menyamakan kebijakan publik dengan tindakan-tindakan yang dilakukan oleh pemerintah. Jika ditinjau dari sudut etimologis, dapat diartikan atau diterjemahkan bahwa *public policy* adalah kebijakan publik, kebijakan umum, kebijakan negara, kebijakan pemerintah, kebijakan terbuka, dan lain-lain. Akan tetapi secara terminologis kecenderungan penggunaan *public policy* dalam bahasa Indonesia diterjemahkan menjadi kebijakan pemerintah.

Berdasarkan peraturan perundang-undangan, yaitu Pasal 1, UU No. 34 Tahun 2004 tentang Tentara Nasional Indonesia, yang dimaksudkan dengan pertahanan negara adalah:

> "Pertahanan negara adalah segala usaha untuk menegakkan kedaulatan negara, mempertahankan keutuhan wilayah Negara Kesatuan Republik Indonesia, dan melindungi keselamatan segenap bangsa dari ancaman dan gangguan terhadap keutuhan bangsa dan negara, disusun dengan memperhatikan kondisi geografis Indonesia sebagai negara kepulauan."

Pada dasarnya konsep pertahanan nasional harus disertai juga dengan pembangunan sistem pertahanan negara yang disesuaikan dengan kondisi dan karakter suatu negara yang sangat berkaitan dengan sejarah nasional, kondisi geografis dan masalah kependudukan dari suatu negara. Dari hal tersebut kemudian dapat dikatakan bahwa secara umum upaya pengembangan sistem pertahanan negara di Indonesia harus memerhatikan tiga faktor utama yaitu faktor

geo strategis (baik internal maupun ekternal), faktor perubahan internasional, dan faktor gelar operasi militer guna memenangkan perang.

Dapat disimpulkan bahwa kebijakan pertahanan adalah rangkaian konsep dan asas yang menjadi pedoman dan dasar rencana dalam pelaksanaan pembangunan sistem pertahanan negara yang disesuaikan dengan kondisi dan karakter suatu negara.

2.1.6 Keamanan

Konsep keamanan menurut ilmu hubungan internasional mengenai definisi dan pengertiannya menurut Barry Buzan bahwa keamanan, dalam arti objektif apapun, mengukur tidak adanya ancaman terhadap nilai-nilai yang diperoleh, dalam arti subjektif, tidak adanya rasa takut bahwa nilai-nilai seperti itu akan diserang.

Buzan berargumen bahwa keamanan setidaknya mencakup lima aspek, yakni keamanan politik, ekonomi, sosial, lingkungan, dan militer. Perdebatan mengenai fokus utama dari keamanan diperhangat dengan munculnya gagasan mengenai keamanan yang bertitik-tolak dari semakin intensifnya proses globalisasi, yang memunculkan ancaman-ancaman baru yang bersifat global (menjangkau seluruh planet) sehingga fokus keamanan harus diletakkan pada keamanan global dengan masyarakat global yang tengah berkembang sebagai objek referensinya (Buzan, 2008:4).

2.1.6.1 *Offense – Defense Theory*

Teori ini berangkat dari konsep *security dilemma* milik Robert Jervis yang menjelaskan bahwa *security dilemma* dapat didefinisikan sebagai suatu fenomena aksi dan reaksi antara beberapa negara di mana tindakan suatu negara untuk meningkatkan keamanannya akan berakibat atau dianggap melemahkan keamanan negara lainnya. Prediksi dasar mengenai keseimbangan *offense-defense* adalah apabila *offense* mendominasi maka *security dilemma* akan meningkat, lalu diikuti oleh perlombaan senjata, dan pada akhirnya kemungkinan besar perang akan terjadi.

Oleh karena itu, perang dapat dicegah apabila *defense* dapat mengungguli dominansi *offense*. Teori *offense-defense* memiliki cakupan penjelasan yang luas, teori ini dapat menyederhanakan penyebab dan penjelasan konflik dalam sebuah garis besar. Teori *offense-defense* memiliki cakupan bidang yang luas, di antaranya juga dipengaruhi oleh kebijakan nasional, dan kebijakan luar negeri. Oleh karena itu teori teesebut juga mencakup dan menjadi subjek dari *political will* (http://global.ir.fisip.ui.ac.id/index.php/global/article/download/45/193 diakses tanggal 1 Juni 2018).

2.1.6.2 *Cyber Security*

Perkembangan teknologi informasi juga telah memberikan perubahan signifikan mengenai konsep keamanan, kini ruang interaksi tidak bisa hanya dibatasi seara fisik (*physic*) tapi juga meluas ke dunia maya (*cyber*). Konsekuensinya, negara harus beradaptasi dengan perkembangan ini konsep keamanan dunia maya *(cyber security)* sudah saatnya ditetapkan sebagai salah

satu “wilayah” negara yang jaga keamanannya sebagaimana kewajiban negara mengamankan teritorialnya. Apalagi, serangan *cyber* tidak hanya terjadi pada institusi publik saja, namun juga menyerang institusi pemerintah. Keamanan *cyber* mencakup segala sesuatu berhubungan dengan pengawasan komputer, *monitoring* sampai kontrol yang sangat ketat atau perjuangan untuk hak asasi fundamental (Triwahyuni dan Wulandari, 2016:4).

Cyber security adalah kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan *cyber* dan organisasi dan aset pengguna. Organisasi dan aset pengguna dalam *cyber security* termasuk perangkat yang terhubung komputasi, personil, infrastruktur, aplikasi, layanan, sistem telekomunikasi dan totalitas informasi yang dikirimkan dan/atau disimpan dalam lingkungan maya. *Cyber security* merupakan upaya untuk memastikan pencapaian dan pemeliharaan sifat keamanan organisasi dan aset pengguna terhadap risiko keamanan yang relevan dalam lingkungan *cyber space* (Ardianti, 2014: 98).

2.1.7 *Cyber Crime*

Kejahatan dunia maya (*cyber crime)* adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk ke dalam kejahatan dunia maya antara lain adalah penipuan lelang secara *online*, pemalsuan cek, penipuan kartu kredit/*carding*, *confidence fraud*/penipuan identitas, pornografi anak, dan lain – lain.

Bagi suatu negara, perkembangan dalam dunia maya ini selain mendatangkan keuntungan juga harus dipersiapkan akan adanya ancaman yang datang dari dunia maya. Ancaman tersebut disebut *cyber threat* (ancaman siber), bentuk dari *cyber threat* ini mempunyai bentuk yang sangat banyak mulai dari *script kiddies* yaitu orang yang bermain dalam dunia maya, *cyber criminal*, berbagai macam *malware (malicious software)*, *phising*, *spamming* sampai dengan yang lebih canggih yang dilakukan oleh aktor negara yaitu *advance persistent threat* (apt) (Wahib dan Labib, 2005:76)

Kejahatan dunia maya atau *cyber crime* umumnya mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer sebagai unsur utamanya, istilah ini juga digunakan untuk kegiatan kejahatan tradisional di mana komputer atau jaringan komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi.

Contoh kejahatan dunia maya di mana komputer sebagai alat adalah *spamming* dan kejahatan terhadap hak cipta dan kekayaan intelektual. Beberapa contohnya adalah akses ilegal (mengelabui kontrol akses), *malware* dan serangan DoS (Husein, 2011:6).

Persatuan Bangsa - Bangsa dalam Kongres X tentang *Prevention of Crime and Treatment of Offenders* di Vienna, 10-17 April 2000 memberi pengertian tentang *cyber crime* dalam dua kategori yaitu :

a) *Cyber crime* dalam pengertian sempit (kejahatan komputer) yakni apapun perilaku yang tidak sah yang diarahkan atas bantuan operasi elektronik dengan sasaran keamanan sistem komputer dan data yang diprosesnya.

b) *Cyber crime* dalam pengertian luas (kejahatan yang terkait dengan komputer) yakni apapun perilaku yang tidak sah yang dilakukan atas bantuan, atau dalam hubungan dengan suatu sistem komputer atau jaringan, mencakup kejahatan pemilikan tidak sah dan menawarkan atau membagi-bagikan informasi atas bantuan suatu sistem komputer atau jaringan (Manthovani, 2006:22-23.)

Cyber crime merupakan kejahatan yang muncul akibat adanya komunitas dalam dunia maya di internet, memiliki karakteristik tersendiri yang berbeda dari kejahatan konvensional. Karakteristik unik dari kejahatan di dunia maya, yaitu :

1. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang/wilayah siber *(cyber space),* sehingga tidak dapat dipastikan jurisdiksi negara mana yang berlaku terhadapnya,
2. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang terhubung dengan internet.
3. Perbuatan tersebut mengakibatkan kerugian material maupun immaterial (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dari kejahatan konvensional.
4. Pelakunya adalah orang yang mengetahui perkembangan internet beserta aplikasinya.
5. Perbuatan tersebut sering dilakukan secara transnasional atau melintasi batas negara (Hamzah, 2013: 30).

2.1.7.1 Sasaran Kejahatan Dalam *Cyber Crime*

Sasaran atau objek kejahatan dalam cyber crime yang dituju oleh hacker yaitu:

1. *Againts Person* (*Cyber crime* yang menyerang individu) Sasaran serangannya ditujukan kepada perseorangan / individu yang memiliki sifat / kriteria tertentu sesuai tujuan penyerangan tersebut. Contohnya pornografi dan *cyberstalking*.
2. *Againts Property* (*Cyber crime* yang menyerang hak milik) Kejahatan yang dilakukan untuk mengganggu / menyerang hak milik orang lain. Contohnya tindakan *unauthorized access, carding, cyber squatting, hijacking, data forgery,* yang bersifat merugikan orang lain.
3. *Against Government* (*Cyber crime* yang menyerang pemerintah) Sasaran / tujuan khusus yaitu penyerangan terhadap pemerintah. Contohnya *Cyber terrorism*, tindakan yang mengancam pemerintah termasuk juga *cracking* ke situs resmi pemerintah / militer (Wahib dan Labib, 2005:76).

2.1.8 *Cyber Sabotage*

Cyber Sabotage adalah gelombang baru dalam ancaman yang muncul dari ruang *cyber*. Apakah dilakukan melalui internet atau sengaja dipasang selama proses pembuatan, ranah perangkat keras atau perangkat lunak komputer sekarang menjadi perhatian. Sabotase didefinisikan sebagai tindakan yang disengaja dan berbahaya yang mengakibatkan terganggunya proses dan fungsi normal atau kerusakan atau kerusakan peralatan atau informasi. (https://www.military.com/defensetech/2008/02/06/cyber-sabotage di upload tanggal 6 Februari 2008, diakses tanggal 10 Desember 2017).

Kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer, atau sistem jaringan

komputer yang terhubung dengan internet. Kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Dalam beberapa kasus setelah hal tersebut terjadi, maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data, program komputer atau sistem jaringan komputer yang telah disabotase tersebut, tentunya dengan bayaran tertentu.

Cyber sabotage dapat menargetkan aset strategis paling penting yang dimiliki suatu negara yaitu penduduknya. Dengan cara ini, para *hacker* bisa meluncurkan serangan yang dimaksudkan untuk mengacaukan atau memecah belah persatuan penduduk itu dari sebuah negara. Tindakan tersebut dapat memukul sektor keuangan utama negara dan menyebabkan kerusakan ekonomi pada ekonomi negara dan secara tiba-tiba mengakhiri juga menutup fasilitas komunikasi publik (https://www.forbes.com/sites/quora/2013/07/18/how-does-cyber-warfare-work/#5de6ed6344ce di akses 30 Agustus 2018).

2.2 Kerangka Pemikiran

Kerangka pemikiran merupakan alur pikir peneliti yang dijadikan sebagai skema pemikiran atau dasar-dasar pemikiran untuk memperkuat indikator yang melatar belakangi penelitian ini. Dalam kerangka pemikiran ini peneliti akan mencoba menjelaskan masalah pokok penelitian. Penjelasan yang disusun akan menggabungkan antara teori dengan masalah yang diangkat dalam penelitian ini.

Rusia dan Estonia memiliki hubungan sejarah yang kurang harmonis sejak dahulu, bahkan sejak Rusia masih bernama Uni Soviet. Permasalahan etnis dan budaya yang terjadi di antara dua negara tersebut, telah berlangsung lama dan ketika tiba di masa sekarang ini dimana ranah kedaulatan sebuah negara bertambah yaitu dunia *cyber*, tak disangka telah terjadi peristiwa sabotase melalui internet di bulan April 2007.

Menurut teori hubungan bilateral bahwa hubungan bilateral merupakan keadaan yang menggambarkan hubungan timbal balik antara kedua belah pihak yang terlibat, dan aktor utama dalam pelaksanaan hubungan bilateral itu adalah negara, terpapar dalam kasus ini bahwa tindakan pemindahan patung oleh pihak Estonia telah membuat sebuah reaksi kurang baik dari pihak Rusia sehingga pihak Rusia pun melakukan tindakan protes melalui *cyber sabotage*. Serangan sabotase *cyber* yang dilancarkan tak lain adalah sebuah bentuk protes terhadap kebijakan perdana menteri Estonia Urmas Paet, karena telah memindahkan dan membongkar monumen sejarah tentara Uni Soviet dari ibukota Tallin ke daerah pedesaan. Pembongkaran monumen tersebut dianggap sebagai sebuah penghinaan bagi masyarakat Rusia karena Estonia dianggap tidak menghargai jerih payah Uni Soviet.

Serangan sabotase *cyber* itu mengakibatkan situs – situs pemerintah, media, bahkan perbankan dan seluruh nomor telepon darurat di Estonia mengalami *down* selama kurang lebih dua minggu lamanya. Aliran trafik data yang sangat banyak adalah penyebab situs – situs tersebut tidak dapat diakses dan menyebabkan kekacauan. Estonia yang dikenal sebagai negara kecil yang hampir

seluruh aktivitas warga negaranya telah terkoneksi dengan internet dan memiliki sistem pertahanan *cyber* yang baik ternyata masih menyisakan celah bagi *hacker* untuk menyusupinya. Tindakan pertahanan yang dilakukan oleh Estonia adalah memotong jaringan Estonia dari dunia luar, memblokir semua lalu lintas internet internasional.

Konstantin Goloskokov, seorang aktivis anggota kelompok pemuda pro-Kremlin, Nashi, mengatakan bahwa serangan yang ia lakukan terhadap jaringan internet Estonia adalah benar. Namun aktivis muda Nashi tersebut percaya dia melakukan sesuatu yang tidak ilegal. Menggunakan metode yang dikenal sebagai serangan *distributed denial of service* (DDoS), Goloskokov mengatakan dia dan sekelompok temannya meretas jaringan internet Estonia, secara efektif melumpuhkan berbagai bagian sistem selama tiga minggu pada bulan April dan Mei 2007. Pengakuan Goloskokov telah mendorong spekulasi bahwa aksinya telah menjadi bagian dari strategi serangan *cyber* yang lebih luas yang diperintahkan oleh otoritas Rusia.

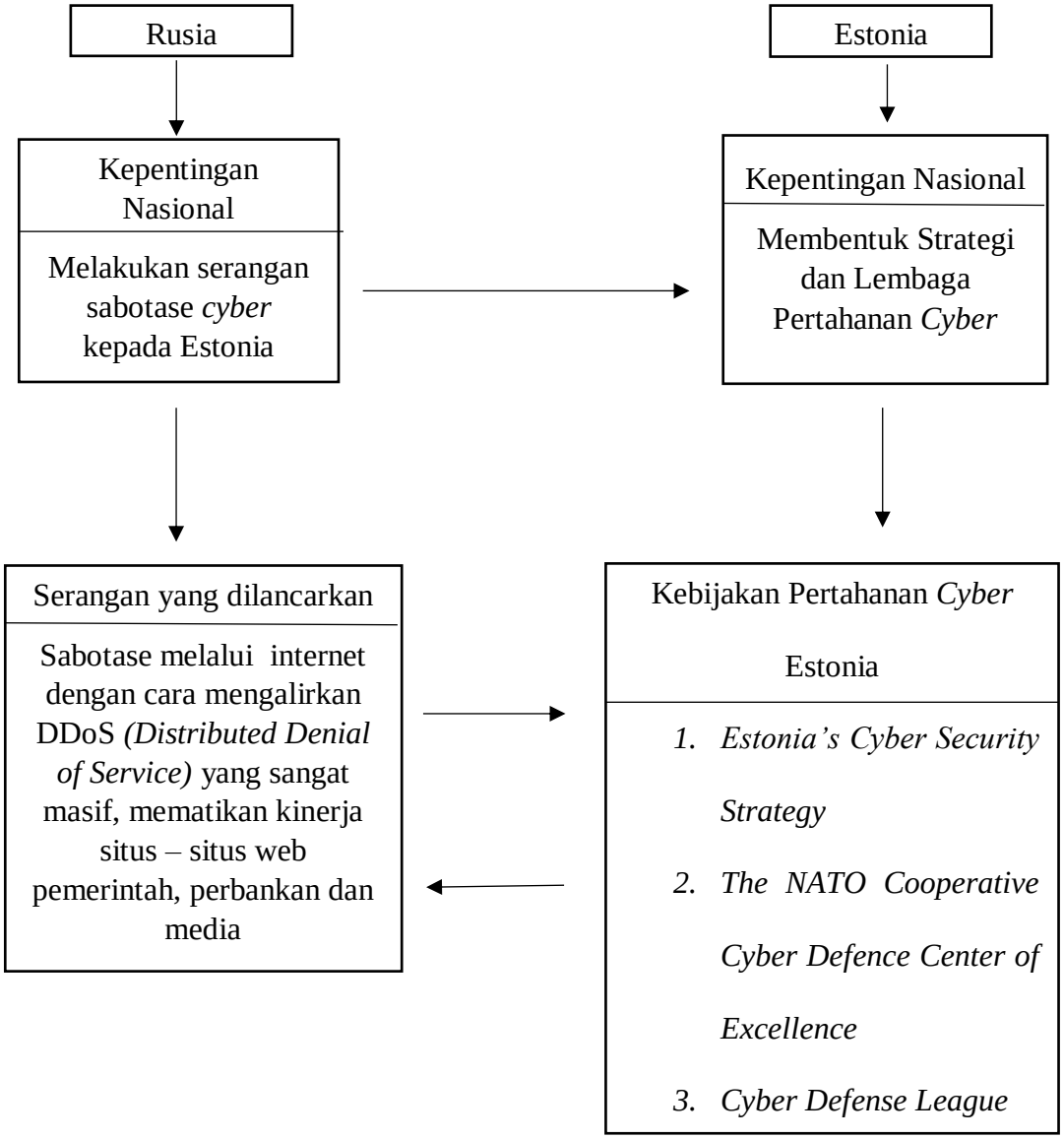
Pengakuan Goloskokov dilakukan selang 14 bulan setelah salah seorang anggota *hacker* sabotase *cyber* ke Estonia ditangkap. Tepatnya pada tanggal 24 Januari 2008, Dmitri Galushkevich, seorang *hacker* beretnis Rusia dinyatakan bersalah karena berpartisipasi dalam serangan. Dia didenda 17.500 kroons (sekitar US$ 1.640) untuk menyerang website Partai Reformasi Estonia. Dimitri bekerjasama dengan kelompok Galoskokov tetapi melalui serangan yang dilancarkan dari dalam negara Estonia, hal tersebut dilakukan guna membuat pelacakan *hacker* menjadi lebih rumit.

Menurut teori *cyber crime*, tindakan yang diambil oleh Estonia untuk memutus rantai sabotase *cyber* dengan cara menutup seluruh akses internet dari luar wilayah Estonia adalah salah satu antisipasi yang cukup efektif karena dengan matinya akses untuk masuk ke Estonia, kegiatan sabotase tersebut dapat terganggu. Dari teori *cyber security* yang didalamnya berisi pengaturan tentang perlindungan dari kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan *cyber* dan organisasi dan aset pengguna. Organisasi dan aset pengguna dalam *cyber security* termasuk perangkat yang terhubung komputasi, personil, infrastruktur, aplikasi, layanan, sistem telekomunikasi dan totalitas informasi yang dikirimkan dan/atau disimpan dalam lingkungan maya.

Cyber security merupakan upaya untuk memastikan pencapaian dan pemeliharaan sifat keamanan organisasi dan aset pengguna terhadap risiko keamanan yang relevan dalam lingkungan *cyber space* diterapkan oleh Estonia dalam rangka mengantisipasi serangan *cyber* yang memiliki banyak kemungkinan terus terjadi di kemudian hari. Dampak dari serangan sabotase *cyber* tersebut kepada negara Estonia dan sebagai bentuk implementasi dari teori *offense – defense* keamanan negara adalah Estonia semakin meningkatkan pertahanan keamanan *cyber* nya dengan membentuk lembaga pertahanan *cyber* diantaranya adalah *Estonia's Cyber Security Strategy, The NATO Cooperative Cyber Defence Center of Excellence,* dan *Cyber Defence League* dalam rangka bentuk aksi dan reaksi di antara kedua negara di mana tindakan suatu negara untuk meningkatkan

keamanannya akan berakibat atau dianggap melemahkan keamanan negara lainnya.

Gambaran kerangka pemikiran penelitian dapat dilihat dari gambar berikut:



Gambar 2.1. Bagan Kerangka Pemikiran