BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Hubungan internasional didefinisikan sebagai studi tentang interaksi antar beberapa aktor yang berpartisipasi dalam politik internasional, yang meliputi negara-negara, organisasi internasional, organisasi non-pemerintah, kesatuan sub-nasional seperti birokrasi dan pemerintah domestik serta individu-individu. Tujuan dasar studi Hubungan Internasional adalah mempelajari perilaku internasional, yaitu perilaku para aktor negara maupun non negara, di dalam arena transaksi internasional. Perilaku ini berwujud kerjasama, pembentukan aliansi, perang, konflik serta interaksi dalam organisasi internasional (Perwita & Yani, 2005: 4)

Dengan adanya internet sebagai "*the network of the networks*" ke seluruh dunia, membuat terciptanya suatu ruang (*space*) atau dunia baru, yang dinamakan *Cyberspace* (Makarim, 2005:5). *Cyberspace* diyakini sebagai suatu ruang komunikasi global dimana tidak ada satu pun negara yang berhak mengatur apa saja isi informasi yang ingin dikomunikasikan antara dua orang atau lebih.

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*. Tujuan keamanan terdiri dari : ketersediaan; integritas termasuk didalamnya keaslian dan kemungkinan upaya mengurangi terjadinya penolakan serta terakhir kerahasiaan. *Global cyber security* dibangun diatas lima bidang kerja yaitu : kepastian hukum (undang-undang *cyber crime*); teknis dan tindakan prosedural pengguna akhir dan bisnis (pendekatan langsung dan penyedia layanan dan perusahaan perangkat lunak); struktur organisasi (struktur organisasi sangat berkembang, menghindari tumpang tindih); *capacity building* dan pendidikan pengguna (kampanye publik dan komunikasi terbuka dari ancaman *cyber crime* terbaru);

Kerjasama internasional (termasuk didalamnya kerjasama timbal balik dalam upaya mengatasi ancaman *cyber*), (undang-undang *cyber crime*); teknis dan tindakan prosedural (pengguna akhir dan bisnis (pendekatan langsung dan penyedia layanan dan perusahaan perangkat lunak); struktur organisasi (struktur organisasi sangat berkembang, menghindari tumpang tindih); *capacity building* dan pendidikan pengguna kampanye publik dan komunikasi terbuka dari ancaman *cyber crime* terbaru. Kerjasama internasional termasuk didalamnya kerjasama timbal balik dalam

upaya mengatasi ancaman *cyber* (https://jurnal.dpr.go.id/index.php/politica/article/view/336/270 diakses tanggal 18 april 2017).

Definisi *security* dalam operasi informasi adalah semua mekanisme yang dilakukan untuk melindungi dan meminimalkan gangguan kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersedian (*availability*) informasi. Mekanisme ini harus bisa melindungi informasi baik dari physical attack maupun *cyber attack. Cyber-security* lebih lanjut dimaknai sebagai semua mekanisme yang dilakukan untuk melindungi dan meminimalkan gangguan kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi. Mekanisme ini harus bisa melindungi informasi baik dari *physical attack* maupun *cyber attack. Cyber security* merupakan upaya untuk melindungi informasi dari *cyber attack*, adapun elemen pokok *cyber security* adalah:

1. Dokumen *security policy* merupakan dokumen standar yang dijadikan acuan dalam menjalankan semua proses terkait keamanan informasi.
2. *Information infrastructure* merupakan media yang berperan dalam kelangsungan operasi informasi meliputi hardware dan software. Contohnya adalah *router, switch, server,* sistem operasi, *database*, dan *website*.
3. *Perimeter Defense* merupakan media yang berperan sebagai komponen pertahanan pada infrastruktur informasi misalnya IDS, IPS, dan *firewall*.
4. *Network Monitoring System* merupakan media yang berperan untuk memonitor kelayakan, utilisasi, dan performance infrastruktur informasi.

5. *System Information and Event Management* merupakan media yang berperan dalam memonitor berbagai kejadian di jaringan termasuk kejadian terkait pada insiden keamanan.
6. *Network Security Assessment* merupakan elemen *cyber security* yang berperan sebagai mekanisme kontrol dan memberikan measurement level keamanan informasi.
7. *Human resource* dan *security awareness* berkaitan dengan sumber daya manusia dan *awareness* nya pada keamanan informasi (https://jurnal.dpr. go.id/index.php/politica/article/view/336/270 diakses tanggal 18 April 2017).

Cyber attack terjadi dalam dua bentuk, pertama untuk menyerang data dan kedua untuk menyerang sistem kontrol (*control system*). Bentuk pertama digunakan untuk mencuri, merusak atau mengubah data, dan *denial of service*. Bentuk kedua berfokus pada kontrol sistem yang digunakan untuk memanipulasi atau melumpuhkan sistem infrastruktur secara fisik. Ada beberapa yang mungkin menjadi target *cyber-terrorism*, yaitu sistem jaringan komputer pemerintah, jaringan keuangan, tenaga pembangkit listrik atau sistem-sistem yang dijalankan dengan jaringan internet (http://www.crimereseach.org/library/Robert1.html diakses tanggal 19 April 2017).

Keberadaan dunia *cyber* sekarang menjadi urusan dunia internasional dan bukan hanya menjadi urusan domestik suatu negara lagi, karena pengaruh yang ditimbulkan dapat menimpa siapa saja, kapan saja dan dimana saja. misalnya

penyebaran virus *i love you* pada tahun 2000 yang meluas ke 45 juta sistem jaringan di dunia dan membuat kerugian sekitar 10 milyar dollar US (Schmidt, 2006: 123-124).

Posisi *hacker* Korea Utara ada di seluruh dunia, mereka terbagi atas beberapa unit, unit 121 bertugas menonaktifkan kontrol komando dan komunikasi, sementara unit 110 khusus menargetkan telekomunikasi Korea Selatan, Korea Utara merekrut para *hacker* dari Universitas-Universitas dan memulai pelatihan pada usia 17 tahun, dan mereka diberikan imbalan gaji, selain itu status sosial keluarga para *hacker* juga di jamin kesejahteraanya.

Hacker Korea Utara telah mengakses *masterplan* rahasia yang disebut Oplan 5027 dalam sebuah serangan *cyber*. Oplan 5027 adalah rencana militer gabungan Amerika Serikat-Korea Selatan jika terjadi perang dengan Korea Utara. rencana itu termasuk rencana pengiriman pasukan, target kunci Korea Utara, strategi dan fasilitan kontrol militer di Korea Utara. Sumber-sumber militer Korea Selatan telah mengakui penjahat *cyber* Korea Utara telah mengakses bagian dari rencana itu yang diretas pada bulan September lalu (*Daily Star*, Diakses pada Tanggal 5 April 2017).

Korea Selatan telah mengakui "beberapa informasi militer, termasuk informasi penting" dicuri dalam serangan *cyber*. Tetapi sumber pemerintah secara pribadi telah mengakui setidaknya bagian dari Oplan 5027 berada di antara dokumen yang dicuri. penyerangan mengejutkan ini mendorong kemungkinan *masterplan* harus benar-benar direncanakan ulang. Sebuah sumber militer mengatakan bahwa para pejabat sedang mendiskusikan apakah rencana pertempuran akan segera dilaksanakan. Amerika

Serikat dan Korea Selatan melakukan latihan militer bersama dalam persiapan untuk kemungkinan invasi Korea Utara. Oplan 5027 pertama kali dibuat pada tahun 1978, ketika komando pasukan gabungan Korea Selatan-Amerika Serikat dibangun. Masterplan ini telah diperbarui setiap dua tahun sejak tahun 1994. Korea Utara kembali meluncurkan rudal balistik ke Laut Jepang. Rudal balistik KN15 jarak menengah tersebut melambung terbang sejauh 60 km menuju arah laut Jepang (https://international.sindonews.com/read/1247072/40/hacker-korut-curi-data-rencana-perang-militer-as-korsel-1507625693 Diakses Tanggal 7 April 2017).

Diluar kota Washington DC, sebuah roket meluncur dari Korea Utara. Gerak roket itu dideteksi oleh satelit Amerika Serikat. Komputer milik pemerintah AS di Colorado mengenalnya sebagai roket jarak dekat yang diluncurkan ke arah laut. Tidak lama kemudian, Korea Utara kembali meluncurkan roket lain. Lalu roket berikutnya melesat, terus hingga roket ke-7. Tentu saja Korea Utara bukan hendak ikut merayakan kemerdekaan Amerika Serikat yang berlangsung 4 Juli 2009. negara komunis itu ingin menarik perhatian Amerika, namun tak berhenti sampai disitu, aksi Korea Utara kemudian berlanjut di ranah *cyber*. Sehari sebelum kemerdekaan Amerika Serikat itu, sebuah pesan sandi diluncurkan oleh seorang agen Korea Utara kepada sekitar 40 ribu komputer yang terinfeksi oleh virus botnet, di seluruh dunia. Pesan tersandi itu mengandung set instruksi sederhana yang memerintahkan kepada komputer terinfeksi virus, untuk mulai menghujani beberapa situs penting di AS dan Korea Selatan dengan trafik data. Serangan ini lazim dalam perang *cyber*, dikenal *Distributed Denial of*

Service atau disingkat DDoS. Kendati Korea Utara dikenal negara paling primitif dalam hal infrastruktur internet, nyatanya mereka punya tim handal dalam penyerangan dan sabotase di dunia *cyber*.

Bagi Korea Utara, perang *cyber* memang memiliki keuntungan asimetrik. Di lain pihak, Korea Selatan dan musuh Korea Utara lainnya, akan mengalami kekacauan apabila sistem komputer mereka berhasil dirusak. Pada Juli 2009 sejumlah situs *website* AS sempat terkena serangan hingga kebanjiran 1 juta permintaan trafik per detik. Akibatnya, *server* web milik departeman Amerika kelebihan beban, dan situs *web* mereka tak bisa diakses. Seperti digambarkan oleh buku "*Cyber War, The Next Threat to National Security and What to Do About It*" (Klarke dan Knake : 2010), saat itu situs *web* departemen keamanan dalam negeri, departemen keuangan, *secret service*, komisi perdagangan federal, serta departemen transportasi AS sempat lumpuh antara 4 Juli sampai 9 Juli 2009.

Bahkan situs-situs *website* bursa NASDAQ, *New York Mercantile Exchange*, *New York Stock Exchange,* dan *Washington Post* juga lumpuh. Korea Utara juga menyerang situs web *White House*, walau tak berhasil melumpuhkannya. dikarenakan situs *website White House* memiliki anti teror di 20 ribu server tersebar di seluruh dunia. akibat serangan itu hanya merusak situs *website White House* di Asia.

Pada Juli 2009 serangan *cyber* itu juga mengarah kepada situs *website* di Korea Selatan. Antara 30 ribu hingga 60 ribu komputer terinfeksi virus dan menyerang situs-situs *website* perbankan Korea Selatan, juga sebuah perusahaan keamanan internet

Korea Selatan. hari berikutnya, Korea Utara malah melakukan serangan yang lebih besar. Sejak tanggal 10 Juli 2009, sekitar 166 ribu komputer bot berasal 74 negara diarahkan membombardir situs *website* pemerintah Korea Selatan, dan bank-bank mereka (https://www.viva.co.id/indepth/sorot/238559-hikayat-serdadu-cyber-korea-utara diakses tanggal 19 April 2017).

Korea Utara telah meningkatkan tentara digitalnya dalam upaya untuk menghadapi perang *cyber*. Menurut informasi bocoran terbaru dari kementerian pertahanan Korea Selatan, unit militer negara maya ini didedikasikan untuk kegiatan *cyber*, yang sekarang meningkat dua kali lipat dari Korea Selatan. Korea Utara mengerahkan 6.000 tentara untuk perang *cyber* dan melakukan serangan *cyber* untuk melumpuhkan fisik dan psikologis ke Korea Selatan sehingga menyebabkan terjadinya masalah dalam operasi militer dan infrastruktur nasional kementerian pertahanan Korea Selatan.

Pada 2013, Korea Selatan menyalahkan Pyongyang atas serangan *cyber* yang melumpuhkan bank-bank, pusat perbelanjaan dan lembaga penyiaran. Pada tahun 2013, serangan *cyber* Korea Utara diketahui telah meretas sistem komputer bank di Korea Selatan, akibatnya selama satu minggu sistem komputer sejumlah bank di Korea Selatan terpaksa dibekukan.

Alasan utama mengapa militer Korea Selatan ingin membentuk '*Cyber Kill Chain*' adalah ancaman *cyber* Korea Utara yang semakin meninggi. Pihak militer akan menyiapkan rencana terkait dalam tahun ini, dan jadwal pelaksanaan di masa yang akan

datang juga ditentukan berdasarkan rencana tersebut. Kementerian pertahanan Korea Selatan menyatakan bahwa pihaknya telah meminta kepada Institut Penelitian Pertahanan Nasional (KIDA) untuk menelitinya sebelum membuat rencana tersebut. KIDA akan melakukan penelitian sampai akhir bulan April, dan rencana pembentukan *'Cyber Kill Chain'* akan disiapkan sampai akhir tahun ini. Rencana tersebut berisi analisis sistem pertahanan serangan dunia maya yang berlaku saat ini, bentuk serangan *cyber* Korea Utara, dan rencana pembentukan system balasan militer Korea Selatan terhadap ancaman *cyber* dari Korea Utara.

Cyber Kill Chain adalah gagasan militer versi *cyber* dari sistem pertahanan misil *Kill Chain*. Biasanya, serangan dunia maya harus melewati berbagai tahap seperti penyediaan PC zombie, serangan ke target, dll. Namun, jika bisa lebih dulu mendeteksi pergerakan serangan di suatu tahap, serangan tersebut bisa dicegah. Karenanya, *Cyber Kill Chain* adalah gagasan untuk sistem pertahanan 'mendeteksi, mencegah, membalas.' Balasan terkait serangan *cyber* hingga saat ini dilaksanakan jika serangan terjadi. Namun, jika *Cyber Kill Chain* diterapkan, kerugian bisa dicegah atau diminimalkan karena ada langkah balasan terlebih dahulu.

Serangan *cyber* Korea Utara telah menjadi ancaman besar. Pada bulan Januari lalu, Korea Utara telah menguasai pengontrolan 100 ribu komputer di perusahaan besar Korea Selatan. Namun, serangan itu lebih dulu ditemukan, sehingga kerugian besar yang akan terjadi bisa dicegah. Pada tahun 2013, Korea Utara pernah melakukan serangan *cyber*. Pada tanggal 20 Maret lalu, jaringan komputer dari stasiun penyiaran

dan lembaga keuangan Korea Selatan juga mendapat serangan. Akibatnya, *server*, komputer, anjungan tunai mandiri terganggu, dan membuat operasionalnya berhenti selama 10 hari. Jumlah kerugian mencapai 900 miliar won. Alamat IP yang ditegaskan sebagai tempat asal serangan *cyber* adalah distrik Ryugreongdong, Pyongyang Korea Utara (http://rki.kbs.co.kr/indonesian///news/news_newsthema_detail.htm?lang=i&id=news_newsthema&No=10067101&current_page=8 diakses tanggal 16 Mei 2017).

Hacker atau peretas komputer meneliti komputernya masing-masing dalam sebuah ruangan. Mereka tergesa-gesa mengetik kode-kode yang sebagian besar tidak dapat dipahami oleh mata awam. Misi mereka hanya untuk menerobos *server virtual* dalam sebuah simulasi dunia. Namun, para peretas khusus ini tidak melanggar hukum. Mereka justru ada di sana untuk memperkokoh aturan-aturan yang telah dibuat oleh perusahaan. Para *hacker* dapat mengambil bagian dalam program enam bulan yang diselenggarakan oleh pemerintah Korea Selatan untuk melatih para pemecah kode cerdas menjadi garda terdepan pertahanan bangsa dalam perang melawan kejahatan *cyber*.

Menurut *Korea Information Technology Research Institute* (KITRI), program "*Best of the Best*" ini dirancang untuk melatih para ahli komputer untuk melawan serangan dari pada *cyber* dari dalam maupun luar negeri. Korea Selatan merupakan salah satu negara yang paling terhubung dengan internet di dunia. Artinya, juga menjadi subyek gempuran *cyber*, terutama dari negara tetangganya di utara, yang secara teknis masih berpotensi untuk menyerang.

Industri internet Korea Selatan berkembang sangat cepat, Sangat penting untuk melatih ahli-ahli keamanan *cyber* dalam segala bidang, termasuk mereka yang akan bekerja untuk perusahaan komersial yang sudah terkemuka dalam komunitas *hacker* Korea Selatan. Program ini diikuti oleh 60 orang ahli komputer mulai dari siswa sekolah menengah atas hingga mahasiswa. Sebagian besar peserta sudah terkenal di negeri ini dan beberapa di antaranya adalah pemenang penghargaan dari kompetisi *hacker* lokal dan asing. Kwon Hyuk, 17 tahun, adalah salah satu kandidat yang lulus dalam tahap pertama program. Dia memfokuskan karyanya pada sistem jaringan printer, yang mudah terpapar serangan *cyber*. Perusahaan dapat mencetak dokumen rahasia menggunakan jaringan printer. Jika keamanannya diterobos, informasi rahasia perusahaan bisa dicuri dengan mudahnya.

Program "*Best of the Best*" ini diikuti oleh 20 orang *hacker*, pada tahap akhir hanya menghasilkan satu pakar dari enam bidang. Yaitu para ahli komputer di bidang forensik digital, konsultan keamanan, analisis kerentanan, pengamanan telepon selular, *converged security*, dan pengamanan komputasi awam. Selain menerima hadiah senilai 20 juta won atau US$18.500, lulusan "*Best of The Best*" akan direkomendasikan ke perusahaan atau instansi pemerintah yang ingin mempekerjakan mereka di masa yang akan datang (http://kitri.kr/eng/inc_html/sub2_1.html cara korsel mengatasi kejahatan cyber.html diakses tanggal 16 Mei 2017).

Konflik antara Korea Utara dan Korea Selatan belum akan menemukan jalan damai dalam waktu dekat, situasi di kedua negara kembali tegang setelah pemerintah

Korea Selatan merilis data resmi yang mengatakan bahwa sistem komputer mereka telah diretas oleh sekelompok *hacker* yang diduga berasal dari Korea Utara, dikutip dari *Techworm.net* unit *cybercrime* kepolisian negara Korea Selatan mengatakan, Korea Utara ada dibalik serangan *cyber* ke Korea Selatan, menyusul ditemukan indikasi peretasan 140 sistem komputer dari 160 perusahaan di Korea Selatan serta dari berbagai instansi pemerintahan. Bahkan cetak biru untuk jet tempur F-15 juga berhasil diambil dari Korean Air Lines, produsen untuk kontrak militer Korea Selatan.

Ada kemungkinan besar bahwa Korea Utara bertujuan untuk menyebabkan gejolak keamanan nasional dan meluncurkan serangan simultan setelah mengamankan banyak target *cyberterror,* atau dimaksudkan untuk terus mencuri rahasia industri dan militer. Demikian pernyataan pejabat resmi pemerintah Korea Selatan, insiden ini merupakan buntut dari kejadian tahun 2014 lalu dimana dua raksasa telekomunikasi asal Korea Selatan Grup SK dan Grup Hanjin juga menjadi korban peretasan *hacker* asal Korea Utara. Sejauh ini menurut pejabat militer Korea Selatan mengatakan bahwa para peretas hanya berhasil mencuri data dari pusat data beberapa instansi pemerintah namun tidak atas kendali sistem mereka (http://www.bbc.com/indonesia/dunia-38221677 diakses tanggal 08 Mei 2017).

Pada Maret 2016 seorang agen mata-mata Korea Selatan berhasil mencegah upaya peretasan sistem jaringan komputer di Korea Selatan yang akan menyerang sistem transportasi. Sementara itu, pihak Korea Utara membantah semua tuduhan yang

ditujukan kenegaranya (https://jakartagreater.com/korut-serang-140-ribu-jaringan-komputer-korsel/ diakses tanggal 18 April 2017).

Untuk memudahkan peneliti dalam mengkaji kebijakan *cyber security* Korea Selatan pasca terjadinya insiden *cyber attack* oleh Korea Utara, peneliti menggunakan penelitian terdahulu sebagai acuan dalam pembahasan;

Salah satu penelitian terdahulu yang akan digunakan oleh penulis adalah skripsi dari Bima Yudha Wibawa Manopo dari Universitas Sebelas Maret dengan judul "Peran ASEAN Regional Forum dalam mewujudkan Regional *Cyber Security* melalui *Treaty of Amity and Coorperation* (kajian penanganan *Cyber Crime* di Asean)". Dalam skripsi Bima Yudha Wibawa Manopo membahas tentang penanganan *cyber crime* di Asean dan peran *Asean Regional Forum* dalam mewujudkan regional *cyber security* melalui *Treaty of Amity and Cooperation*. Persamaan dari penelitian ini adalah sama-sama membahas mengenai regional *cyber security* di Kawasan Asia dalam menangani segala bentuk kejahatan dunia maya dan melakukan suatu formulasi kebijakan yang mengatur dan mengikat serta menerapkan hukum terhadap para pelaku yang terbukti melakukan tindak pidana kejahatan terutama dalam kejahatan *cyber*.

Yang membedakan penelitian ini dengan penelitian sebelumya adalah peneliti akan meneliti sejauh mana kebijakan *cyber security* yang diterapkan di Korea Selatan untuk menangani segala bentuk serangan dunia maya yang dialami dalam beberapa tahun ini oleh Korea Utara.

Kedua, adalah jurnal dari Moehammad Yuliansyah Saputera dari Universitas Riau dengan judul "Pengaruh *Cyber Security* strategi Amerika Serikat menghadapi ancaman *Cyber Warfare*" penelitian ini membahas pengaruh *Cyber Security* Amerika Serikat menghadapi ancaman *Cyber Warfare* tahun 2009-2014. Persamaan dari jurnal ini adalah sama-sama membahas bagaimana solusi untuk mencegah ancaman dari negara lain, perbedaannya adalah jurnal ini berkonsentrasi di Kawasan Amerika sedangkan peneliti lebih memfokuskan penelitianya di Kawasan Asia Timur.

Ketiga, adalah jurnal dari David Putra Setyawan dan Arwin Datumaya Wahyudi Sumari, dengan judul "Diplomasi pertahanan Indonesia dalam pencapaian *Cyber Security* melalui *Asean Regional Forum on Cyber Security Initiatives"*. Persamaan dari jurnal ini adalah memahami kondisi dan bagaimana mengatasi berbagai ancaman dari penyerangan *cyber* di dunia Internasional. Perbedaanya adalah jurnal ini berkonsentrasi di Kawasan Asia Tenggara sedangkan peneliti lebih memfokuskan penelitianya di Kawasan Asia Timur.

Berdasarkan alasan tersebut yang menjadi dasar pertimbangan peneliti untuk mengadakan penelitian dengan judul: **"Kebijakan *Cyber Security* Korea Selatan Pasca Terjadinya *Cyber Attack* oleh Korea Utara (2009-2014)".**

Adapun ketertarikan peneliti untuk meneliti dan mengangkat isu tersebut didukung oleh beberapa mata kuliah disiplin Ilmu Hubungan Internasional, diantaranya adalah :

1. Studi Keamanan Internasional, dalam mata kuliah ini mempelajari mengenai masalah keamanan internasional yang membahas tentang pertahanan dan mewujudkan keamanan regional di Korea Selatan.
2. Studi Strategis, dalam mata kuliah ini mempelajari bagaimana suatu negara melakukan kerjasama dengan negara lain dengan maksud untuk mencapai kepentingan nasionalnya.
3. Hubungan Internasional di Asia Timur, dalam mata kuliah ini mempelajari bagaimana disiplin ilmu yang mempelajari Hubungan Internasional di Asia Timur tepatnya di Korea Utara dan Korea Selatan.
4. Politik Luar Negeri, dalam mata kuliah ini mempelajari bagaimana suatu negara menciptakan keamanan nasional dan memenuhi segala kepentingan nasionalnya yang bersifat kedalam dan keluar.

1.2 Rumusan Masalah

1.2.1 Rumusan Masalah Mayor

Bagaimana kebijakan *Cyber Security* Korea Selatan untuk merespon *Cyber Attack* Korea Utara ?

1.2.2 Rumusan Masalah Minor

1. Apa yang melatar-belakangi *Cyber Attack* Korea Utara terhadap Korea Selatan ?

2. Kerugian apa yang dialami oleh Korea Selatan atas *Cyber Attack* oleh Korea Utara ?
3. Kebijakan apa yang di ambil Korea Selatan dalam merespon *cyber attack* yang dilakukan oleh Korea Utara ?

1.2.3 Pembatasan Masalah

Pembatasan masalah diajukan oleh peneliti agar mempersempit fokus terhadap masalah. Dari permasalahan yang ada, penulis membatasi masalah yang dibahas dengan berfokus pada kebijakan *Cyber Security* Korea Selatan pasca terjadinya *Cyber Attack* oleh Korea Utara.

Dalam penelitian ini, peneliti melakukan pembatasan masalah dari tahun 2009 hingga tahun 2014 dikarenakan pada tahun tersebut telah terjadi serangan *cyber* (*CyberWar*) yang cukup besar oleh pasukan *hacker elite* negara Korea Utara terhadap *website* pemerintah Korea Selatan, tujuan dari serangan ini adalah untuk mengetahui dokumen-dokumen rahasia yang dimiliki pemerintah Korea Selatan, Serangan *cyber* tersebut dibalas oleh pasukan *hacker elite* Pemerintah korea Selatan yang ditujukan untuk pasukan *hacker elite* Korea Utara. *Hacker* Korea Utara bertanggung jawab atas beberapa serangan di dunia selama 10 tahun terakhir, paling banyak serangan *cyber* adalah menargetkan Korea Selatan, kejadian *cyber attack* telah banyak menutup akses situs Korea Selatan dan membanjiri banyak situs Korea Selatan dengan berbagai macam jenis serangan. Pada 9 Juli 2009 serangan *cyber* itu juga mengarah kepada situs *web* Korea Selatan. Akibatnya antara 30 sampai 60 ribu komputer terinfeksi virus dan

menyerang *website-website* perbankan dan sebuah perusahaan keamanan internet Korea Selatan. Parlemen menyebutkan bahwa militer Korea Selatan telah menjadi target dari 6.392 serangan *cyber* Korea Utara dari berbagai skala sejak tahun 2009. Serangan itu antara lain berupa intruksi laman, penyebaran virus dan penggunaan surat elektronik pembawa virus. Pada tahun 2011, *Hacker* Korea Utara bahkan berhasil menghancurkan situs rahasia Korea Selatan milik presiden yaitu *Blue House*. Pada Tahun 2013, serangan *cyber* Korea Utara diketahui telah meretas sistem komputer bank di Korea Selatan, akibatnya selama satu minggu sistem komputer sejumlah bank di Korea Selatan terpaksa dibekukan.

Pada tahun 2014, Pemerintah Korea Selatan menyatakan akan melancarkan perang untuk pertahanan *cyber*. Hal ini dilakukan untuk membentengi negara dari kejahatan *cyber*. Kantor berita Korea Selatan Yonhap mengutip seorang sumber kuat, yang mengatakan bahwa langkah tersebut diambil setelah banyak serangan *cyber* dalam beberapa bulan belakangan. bahkan, jumlah percobaan meretas sejumlah laman berkaitan dengan militer mencapai 1.202 kali dalam sembilan bulan terakhir ini. Jumlah tersebut meningkat 595 kasus dari tahun sebelumnya.

1.3 Maksud dan Tujuan Penelitian

1.3.1 Maksud penelitian

Berdasarkan pada latar belakang dan rumusan masalah yang telah diuraikan sebelumnya, maka tujuan dari penulisan karya tulis ini adalah agar

masyarakat umum mengetahui kebijakan *Cyber Security* Korea Selatan pasca terjadinya *Cyber Attack* yang dilakukan oleh Korea Utara (2009-2014).

1.3.2 Tujuan Penelitian

1. Untuk mengetahui apa yang melatar-belakangi terjadinya *cyber attack* oleh Korea Utara terhadap Korea Selatan.
2. Untuk mengetahui kerugian yang dialami oleh Korea Selatan pasca *cyber attack* yang dilakukan Korea Utara.
3. Untuk mengetahui kebijakan apa saja yang diambil oleh Korea Selatan untuk merespon *cyber attack* yang dilakukan oleh Korea Utara.

1.4 Kegunaan Penelitian

1.4.1 Kegunaan Teoritis

Diharapkan dapat menambah wawasan peneliti serta memberikan atau menambah pembendaharaan pustaka, serta dapat memberikan sedikit gambaran ilmu pengetahuan bagi pen-Studi Ilmu Hubungan Internasional mengenai kebijakan *Cyber Security* Korea Selatan pasca terjadinya *Cyber Attack* oleh Korea Utara.

1.4.2 Kegunaan Praktis

Diharapkan dapat menambah ilmu, pengalaman dan kemampuan peneliti di bidang Ilmu Hubungan Internasional, dapat dijadikan bahan tambahan informasi dan studi empiris bagi akademisi maupun masyarakat,

serta dapat dijadikan sebagai sebagai bahan referensi bagi para penstudi Ilmu Hubungan Internasional, dan umum.