KEBIJAKAN *CYBER SECURITY* KOREA SELATAN PASCA TERJADINYA *CYBER ATTACK* OLEH KOREA UTARA (2009-2014)

Oleh :
Ryan Fajar Prasetyo

Program Studi Ilmu Hubungan Internasional Jenjang Sarjana Strata-1
Fakultas Sosial dan Politik
Universitas Komputer Indonesia

E-mail : *Yudhistira50@gmail.com*

ABSTRAK

Penelitian ini bertujuan untuk mengetahui latar belakang Korea Utara melakukan *cyber attack* terhadap Korea Selatan, penelitian ini juga bermaksud untuk mengetahui bagaimana kerugian pasca *terjadinya cyber attack* oleh Korea Utara, serta mengetahui langkah apa saja yang dilakukan oleh Korea Selatan untuk mencegah terjadinya kembali *cyber attack* oleh Korea Utara.

Metode penelitian yang digunakan adalah kualitatif. Dalam mengumpulkan data-data, peneliti melakukan studi lapangan, studi pustaka, penelusuran online dan menggunakan teknik purposive untuk menentukan informan. Sedangkan teknik untuk menganalisis data menggunakan triangulasi data.

Peneliti menganalisa bahwa Korea Selatan sangat serius dalam menanggapi ancaman pasukan *cyber* Korea Utara yang semakin canggih. Korea Selatan membangun sekolah khusus untuk *cyber*. Para siswa diperintahkan untuk terus mengawasi Korea Utara, program *Best of The Best* di tujukan untuk melatih *hacker* dengan keterampilan *cyber elite* yang mampu dan bersedia membela Korea Selatan dari serangan peretas berbahaya, yang diyakini berasal dari Korea Utara.

Dari hasil penelitian, dapat disimpulkan bahwa latar belakang masalah Korea Utara menyerang Korea Selatan adalah karena Korea Utara ingin memperkuat militernya, sehingga membutuhkan biaya yang cukup besar. Maka dari itu, Korea Utara mencari alternatif lain agar dapat memenuhi kepentingan nasional nya tersebut dengan melakukan penyerangan *cyber*.

Terkait kerugian yang dialami Korea Selatan pasca terjadinya *cyber attack* oleh Korea Utara adalah kurangnya data tertulis yang menerangkan berapa jumlah pasti kerugian yang dialami oleh Korea Selatan, selain itu juga Korea Selatan adalah negara paling terhubung dengan internet yang menyebabkan rentan terhadap serangan *cyber*.

Kata kunci : *Cyber Security*, Korea Selatan, *Cyber Attack*, Korea Utara.

ABSTRACT

This study aims to determine the background of the North Korean problem of cyber attack agains South Korea, this research also intends to know how the loss after cyber attack by North Korea, and know what steps are done by South Korea to prevent re-occurrence of cyber attack by North Korea.

The research method used in this research is qualitative method. In collecting data, researchers conducted field studies, literature studies, online search and purposive techniques to determine sources. While the technique to analyze data using data triangulation.

Researchers analyzed that South Korea is very serious in responding to the increasingly sophisticated threat of North Korean cyber forces. South Korea is building a special cyber school, students are being instructed to continue to monitor North Korea, the Best of The Best program is to train hackers with cyber elite skills capable and willing to defend South Korea from harmful hacker attacks, believed to be from North Korea.

From the results of the research, it can be concluded that the background of North Korea's problem of attacking South Korea is because North Korea wants to strengthen its military, so it requires a considerable cost. therefore, North Korea is looking for other alternatives in order to fulfill its national interest by carrying out cyber attacks.

Related losses suffered by South Korea after the cyber attack by North Korea is the lack of written data explaining how many must be losses suffered by South Korea, additionally, South Korea is the most connected to the Internet country that causes vulnerability to cyber attacks.

Keywords : Cyber Security, South Korea, Cyber Attack, North Korea.

I. Latar Belakang Masalah

Hubungan Internasional diartikan sebagai studi yang berinteraksi antara beberapa aktor yang turut serta berpartisipasi dalam politik internasional, yang meliputi negara dengan negara, organisasi internasional, organisasi non pemerintah, kesatuan sub nasional seperti birokrasi dan pemerintah domestik serta individu dengan individu. Tujuan studi Hubungan Internasional adalah untuk mempelajari perilaku internasional, yaitu perilaku para aktor negara maupun non negara, di dalam arena transaksi Internasional. Perilaku ini meliputi kerjasama, pembentukan aliansi, perang, konflik serta

interaksi dalam organisasi internasional (Perwita & Yani, 2005: 4)

Internet sebagai "*the network of the networks*" ke seluruh belahan dunia, menjadikanya suatu ruang (*space*) atau dunia baru, yang dinamakan *Cyberspace* (Makarim, 2005:5). *Cyberspace* adalah suatu ruang komunikasi global dimana tak ada negara yang berhak mengatur informasi yang dilakukan 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 mengatas 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 ditujukan untuk melindungi informasi baik dari *physical attack* maupun *cyber attack*. *Cyber security* merupakan upaya untuk melindungi informasi dari *cyber attack*.

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 system jaringan di dunia dan membuat kerugian sekitar 10 milyar dollar US (Schmidt, 2006: 123-124).

Program *Cyber Kill Chain* ialah gagasan versi *cyber* dari sistem pertahanan misil *Kill Chain*. kebanyakan, serangan dunia maya mesti melewati beberapa tahap seperti penyediaan PC zombie, serangan target, dll. Namun, jika terlebih dahulu mendeteksi pergerakan serangan di suatu tahap, serangan tersebut bisa dicegah. Oleh karena itu, *Cyber Kill Chain* ialah gagasan untuk sistem pertahanan, mendeteksi, mencegah dan membalas. Balasan terhadap serangan *cyber* hingga saat ini dilakukan dengan hanya sekali tahap. Namun, jika *Cyber Kill Chain* diterapkan, kerugian bisa dicegah atau diminimalisir.

Menurut *Korea Information Technology Research Institute* (KITRI), gagasan *Best of the Best* dirancang untuk melatih para ahli komputer untuk melawan serangan *cyber* dari dalam maupun luar negeri. Korea Selatan adalah salah satu negara yang paling terhubung dengan internet di dunia. Artinya, Korea menjadi rentan terhadap *cyber*, terutama oleh negara tetangganya yaitu Korea Utara.

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.

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.

II. Rumusan Masalah

2.1 Rumusan Masalah Mayor

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

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 diambil Korea Selatan dalam merespon *cyber attack* yang dilakukan oleh Korea Utara ?

2.3 Pembatasan Masalah

Pembatasan masalah diajukan oleh peneliti agar mempersempit fokus terhadap masalah. Dari permasalahan yang ada, penulis membatasi masalah yang dibahas dengan berfokuskan pada kebijakan *Cyber*

Security Korea Selatan pasca terjadinya *Cyber Attack* oleh Korea Utara pada tahun 2009-2014.

III. Maksud dan Tujuan Penelitian

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).

3.2 Tujuan Penelitian

1. Untuk mengetahui apa yang melatarbelakangi terjadinya *cyber attack* yang dilakukan terhadap Korea Selatan
2. Untuk mengetahui kerugian yang dialami oleh Korea Selatan pasca *cyber attack* yang dilakukan Korea Utara.
3. Untuk mengetahui langkah-langkah apa yang dilakukan oleh Korea Selatan dalam menghadapi *cyber attack* Korea Utara.

IV. Tinjauan Pustaka

4.1 Hubungan Internasional

Hubungan internasional dapat diartikan sebagai studi tentang interaksi antar beberapa aktor yang berpartisipasi dalam politik internasional, yang meliputi negara-negara, organisasi internasional, organisasi non pemerintah, sub nasional birokrasi dengan pemerintah, serta individu dengan individu. Tujuan dari studi Hubungan Internasional ialah untuk mempelajari perilaku internasional, yaitu perilaku para aktor negara maupun non negara, di arena transaksi internasional. Perilaku ini antara lain bergerak di bidang kerjasama, pembentukan aliansi, perang, konflik serta interaksi dalam organisasi internasional (Perwita & Yani, 2005: 4).

Studi Hubungan Internasional sebenarnya merupakan sebuah kajian yang telah lama ada, bahwa perkembangan dalam sebuah bidang studi berkaitan erat dengan perkembangan dalam bidang-bidang studi lain (Sonderman Fred: 13).

Dalam perjalanannya ilmu Hubungan Internasional terus mengalami perkembangan yang pesat, Hubungan Internasional yang pada awalnya hanya mempelajari hubungan antar negar-negara yang berdaulat telah mengalami pergeseran, dimana muncul aktor-aktor lain dalam ilmu Hubungan Internasional yang juga mempunyai peranan penting seperti *nonstate actor*. Hubungan Internasional yang pada awalnya hanya mengkaji peperangan dan perdamaian kemudian memperluas bentuk kajiannya yaitu untuk mempelajari perkembangan, perubahan dan juga kesinambungan yang berlangsung dalam hubunganantar negar atau antarbangsa dalam konteks sistem global, menjadi kajian Hubungan Internasional yang tidak hanya fokus pada hubungan politik yang berlangsung antar negara, tapi juga mencakup peran dan kegiatan yang dilakukan oleh aktor-aktor bukan negara, inilah kemudian yang disebut dengan Hubungan Internasional kontemporer (Rudy, 2003 : 51).

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" (Jackson, 2005:3).

Tujuan utama dari Hubungan Internasional yaitu mempelajari perilaku internasional yaitu perilaku aktor negara maupun non-negara di dalam arena transaksi internasional, dimana perilaku tersebut bisa berupa kerjasama, aliansi, perang, dan sebagainya. Terdapat beberapa tujuan dasar dalam mempelajari ilmu Hubungan Internasional seperti dikemukakan Anak Agung Banyu Perwita dan Yanyan Mochamad Yani yaitu :

> "Tujuan dasar studi Hubungan Internasional adalah mempelajari perilaku internasional, yaitu perilaku aktor negara maupun non-negara di dalam arena transaksi internasional, dimana perilaku tersebut bisa berupa kerjasama, pembentukan, aliansi, perang, konflik serta interaksi didalam organisasi internasional" (Perwita & Yani, 2005 : 4-5).

V. Metode Penelitian

5.1 Desain Penelitian

Untuk melakukan suatu penelitian, diperlukan suatu konsep atau rancangan yang berisi rumusan perihal objek yang akan diteliti. Metode penelitian yang digunakan dalam penelitian ini adalah metode kualitatif. Penelitian dalam metode ini meneliti masalah mengenai kebijakan *cyber* yang keluarkan oleh suatu negara. Merujuk pada rumusan masalah yang diteliti berdadarkan variabel yang tersedia, maka peneliti melakukan analisa data menurut data dan informasi yang dikeluarkan oleh informan, media elektronik, publikasi, dan berita internasinal serta dipadukan dengan teori teori dalam kajian ilmu Hubungan Internasional.

5.2 Informan Penelitian

teknik pemilihan informan yang dilakukan peneliti ialah menggunakan teknik *Purposive,* yaitu peneliti menentukan pihak informan berdasarkan masalah, tujuan dan variabel penelitian. Teknik yang digunakan ialah teknik wawancara sesuai dengan masalah yang akan diteliti. Adapun pihak yang peneliti jadikan sebagai informan adalah narasumber dari Lembaga Ilmu Pengetahuan Indonesia.

5.3 Teknik Pengumpulan Data

Penelitian ini memakai teknik pengumpulan data diantaranya yaitu studi kepustakaan, penelusuran data online, dokumentasi, dan wawancara. Penelitian ini difokuskan terhadap Kebijakan *Cyber Security* Korea

Selatan Pasca Terjadinya *Cyber Attack* oleh Korea Utara, caranya yaitu mengolah data yang didapat dari informan terkait dengan rumusan masalah yang akan diteliti.

5.4 Uji Keabsahan Data

Dalam melakukan uji keabsahan data peneliti menggunakan metode triangulasi data dengan cara melakukan konfirmasi data yang diperoleh dari Lembaga Ilmu Pengetahuan Indonesia dengan melakukan studi lapangan ke lembaga tersebut. Peneliti juga akan melakukan konfirmasi data dengan menggunakan *e-mail* kepada pihak terkait.

VI. Hasil Penelitian Dan Pembahasan

6.1 Hasil Penelitian

Tinjauan Umum Korea Selatan

Semenanjung Korea berada di sebelah Timur laut Asia, semenanjung tersebut dibatasi oleh sungai Amnok yang biasa dikenal dengan sebutan sungai Yalu dan berada di sebelah barat laut yang memisahkan antara Korea dan Cina. Di sebelah timur laut terdapat sungai Duman atau sungai Tumen, sungai tersebut memisahkan Korea dari Cina dan Rusia. Semenanjung Korea terletak diantara Laut Kuning (*the Yellow Sea*) di sebelah Barat, dan laut Timur (*the East Sea*) di sebelah Timur. Di sekeliling Semenanjung Korea juga terdapat beberapa pulau yaitu pulau Jeju, pulau Ulleung, dan pulau Dokdo.

Semenanjung Korea mempiunyai diameter sepanjang 1.030 km dengan lebar 175 km. Sedangkan luas seluruhnya adalah 100.033 sq km. Korea memiliki jumlah penduduk sebanyak 49,8 juta jiwa berdasarkan sensus penduduk yang di lakukan pada tahun 2011. Letak geografis Korea termasuk wilayah yang unik, menjadikan Korea sebagai negara yang aman dan layak untuk dihuni, dan menjadikan penghubung antara Asia dengan negara luar. Sekitar 70% wilayah Korea merupakan pegunungan, sehingga Korea adalah wilayah dengan pegunungan terbanyak di dunia. Daerah perbukitan, pegunungan penghasil batu kapur menjadikan Korea memiliki pemandangan bukit dan lembah yang menarik untuk dikunjungi. Pegunungan terbentang sepanjang pantai Timur hingga Laut Timur, pantai Selatan dan Barat, hingga ke dataran pantai, semua wilayah tersebut menghasilkan pertanian terutama padi yang unggul di Korea.

6.2 Analisa Hasil Penelitian dan Pembahasan

Latar Belakang *Cyber Attack* Korea Utara terhadap Korea Selatan

Seiring perkembangan jaman dan teknologi semakin pesat. Penyebaran informasi melalui internet secara langsung mempengaruhi kebutuhan tentang informasi dalam berbagai akses dan aktifitas yang dilakukan sehari hari. Oleh karena itu informasi yang didapatkan secara cepat, tepat dan akurat memiliki pengaruh sangat besar dalam setiap aspek kehidupan bermasyarakat, diantaranya yaitu sebagai alat bantu dalam proses pengambilan suatu kebijakan, atau hanya untuk sekedar mengakses situs tertentu yang sedang hits dalam abad milenia ini. Belakangan ini banyak negara terutama kalangan pemerintah baik sipil maupun militer, bisnis, organisasi nirlaba, hingga perorangan berubah menjadi sangat bergantung pada teknologi informasi yang semakin pesat. Pada akhirnya muncul istilah yang dikenal dengan sebutan *the information age* atau jaman informasi. Tapi, kemudahan dan kecanggihan yang ditawarkan pada abad ini banyak mengundang kejadian tindakan kejahatan atau kriminalitas di dunia *cyber*, kejadian tindak kejahatan ini disebut dengan *cyber crime.*

Cyber attack adalah sebuah bentuk penyerangan terhadap jaringan komputer, Serangan *cyber* (*cyber attack*) ialah ancaman yang merugikan, kejadian ini berupa suatu kejahatan di dunia maya yang dapat menyerang siapapun, dimanapun, dan kapanpun. serangan ini sulit untuk ditebak dan diprediksi. Besar kerusakan tidak tergantung dari besarnya serangan melainkan bergantung kepada mekanisme pertahanan target dan tujuan dari pelaku penyerangan. Sudah banyak contoh kasus yang memperlihatkan bahaya dari bentuk serangan seperti ini, tapi kebanyakan masyarakat terkesan tidak peduli, hingga saat ini belum terdapat peraturan atau konvensi internasional yang secara resmi mengatur tentang kejahatan *cyber*. Bentuk kesulitan ini biasanya muncul ketika serangan *cyber* ini terjadi di ruang lingkup yang melintasi atau berbeda negara.

Kerugian Korea Selatan atas *Cyber Attack* oleh Korea Utara

Sejak tahun 2009 Korea Selatan mengalami darurat *cyber*, Korea Selatan mengalami serangkaian serangan *cyber* yang diduga serangan tersebut datangnya dari negara tetangganya sendiri Korea Utara. Korea Utara memiliki strategi serangan dunia maya untuk melumpuhkan hingga 50 persen infrastruktur teknologi informasi Korea Selatan. Sasaran Korea Utara adalah menghancurkan kepemimpinan Korea Selatan dengan serangan fisik dan psikologis yang dikaitkan dengan serangan dunia maya, kemudian menebarkan kepanikan dalam skala besar. hanya ada sedikit informasi yang tidak dirahasiakan tentang operasi dunia maya Korea Utara. Mereka juga ingin mengubah persepsi publik tentang serangan yang dihubungkan dengan Korea Utara.

Langkah yang ditempuh Korea Selatan untuk mencegah *cyber attack* Korea Utara

Jika berbicara mengenai strategi *cyber security*, secara umum seluruh negara pasti memiliki kebijakan *cyber* nya masing-masing untuk mencegah serangan *cyber* dari luar, namun setiap negara mempunyai langkah-langkah atau metode tersendiri untuk menangani masalah tersebut (Wawancara dengan Narasumber).

National Intellegency Security of Korea

Pada tahun 1994, NSP telah merevisi undang-undangnya setelah kesepakatan antara partai penguasa Korea dan partai oposisi dan membentuk "Komite Informasi" di Majelis untuk meletakkan dasar bagi netralitas politik. NSP juga meluncurkan operasi melawan kejahatan internasional dan terorisme untuk melindungi rakyat Korea dari kejahatan terorganisir internasional. Badan Intelijen Pusat Korea (KCIA) pada awalnya didirikan pada tanggal 19 Juni 1961 sebagai perwakilan langsung Dewan Tinggi Rekonstruksi Nasional segera setelah kudeta militer 16 Mei

1961. Tugasnya adalah untuk mengawasi dan mengkoordinasikan kegiatan intelijen internasional dan domestik dan investigasi kriminal oleh semua badan intelijen pemerintah, termasuk militer. Misinya mirip dengan gabungan *Central Central Intelligence Agency* dan *Federal Bureau of Investigation*.

Haura Inc

Hauri Inc. bertujuan untuk mengembangkan, memproduksi, dan mendistribusikan solusi keamanan yang melindungi pelanggan dari berbagai ancaman teknologi informasi dan memungkinkan perusahaan mengelola risiko. Perusahaan ini menawarkan *ViRobot internet Security*, solusi proteksi pribadi yang menyediakan anti-virus, anti-*spyware*, anti-*phishing*, dan *firewall*, serta mencegah PC Zombie untuk rumah.

Hauri Inc. adalah perusahaan keamanan *cyber* yang berlokasi di Seoul, dan telah menyediakan solusi untuk Angkatan Darat Korea Selatan, Departemen Pertahanan Nasional dan Pusat Keamanan *Cyber* Nasional menggunakan produk-produk seperti solusi anti-virus, solusi memblokir kerentanan OS, sistem keamanan mobile dan solusi penghapusan data," CEO *Hauri Inc* Heechum Kim menjelaskan bahwa perusahaannya menyediakan "layanan untuk perusahaan dan lembaga-lembaga publik."

Cyber Kill Chain

Cyber Kill Chain adalah gagasan militer versi *cyber* dari sistem pertahanan misil *Kill Chain*. Berbagai Alasan yang dibangun oleh militer Korea Selatan mengapa ingin membentuk *Cyber Kill Chain* yaitu seiring maraknya ancaman dunia maya yang dilakukan oleh Korea Utara. Militer Korea Selatan merancang system untuk mencegah ancaman tersebut. Kementerian Pertahanan Korea Selatan mengeluarkan *statement* bahwa pihaknya telah bekerja sama dengan pihak Institut penelitian pertahanan nasional untuk dilakukan *research* mengenai ancaman tersebut. Penelitian yang dilakukan KIDA diperkirakan akan dilakukan akhir April dan rampung hingga akhir tahun 2013. Rencana pembentukan program tersebut mengandung analisis sistem pertahanan serangan *cyber* yang dilakukan oleh Korea Utara, dan rencana pembentukan sistem balasan militer Korea Selatan terhadap ancaman *cyber* Korea Utara.

Serangan *cyber* yang dilakukan oleh Korea Utara menjadi suatu ancaman bagi Korea Selatan. Pada Januari, Korea Utara berhasil menguasai system terhadap kurang lebih 100 ribu komputer yang berada di perusahaan milik Korea Selatan. tapi, bentuk serangan tersebut telah lebih dulu tercium oleh pihak Korea Selatan, sehingga kerugian yang dialami bisa diminimalisir. Pada tahun 2013, Korea Utara telah melakukan serangan *cyber*. Pada tanggal 20 Maret, jaringan komputer milik stasiun penyiaran, lembaga keuangan milik Korea Selatan juga terkena serangan *cyber*. Akibat dari serangan tersebut, server, komputeR dan ATM terganggu dan berhenti operasi selama sepuluh hari.

Jumlah kerugian yang dialami mencapai 900 miliar won. *IP Address* yang muncul dari serangan *cyber* tersebut adalah distrik Ryugreongdong, Korea Utaran(http://world.kbs.co.kr/special/northkorea/contents/news/news_view.htm?lang=i&No=31327 diakses tanggal 11 Februari 2018).

VII. Kesimpulan

Cyber attack yang dialami oleh Korea Selatan terjadi dua kriteria. Yang pertama yaitu untuk menyerang *system* data, yang kedua yaitu untuk menyerang sistem kontrol. Bentuk yang pertama diperuntukan untuk mencuri data, merusak data, mengubah isi data, serta *denial of service*. Bentuk yang kedua yaitu bertujuan untuk menyerang *control system* agar memanipulasi atau melumpuhkan sistem infrastruktur fisik. Terdapat beberapa kemungkinan yang terjadi dalam kejahatan *cyber*, penyerangan diindikasi mengarah pada *system* jaringan komputer pemerintah, pembangkit listrik, system keuangan atau system yang menggunakan system jaringan komputer.

Cyber Attack yang dilakukan oleh Korea Utara adalah sebuah hal yang penting karena Korea Utara memiliki keterbatasan biaya, keterbatasan sumber daya manusia, dll. Dibandingkan melakukan penyerangan dengan bentuk kontak senjata (perang) atau menggunakan alat-alat militer (altileri), Korea Utara memilih menggunakan serangan melalui *cyber* dikarenakan *cyber* lebih murah, mudah dan bagaimana kemudian hal tersebut dapat dilakukan dengan nyaman dan penyerangan ditujukan terhadap suatu target untuk mencapai tujuan yang diinginkan secara tersembunyi dan tanpa diketahui oleh pihak Korea Selatan

Korea Utara berhasil melancarkan sejumlah *cyber attack* ke wilayah Korea Selatan dan berhasil mencuri data data penting dari pihak Korea Selatan. terbukti dari tahun 2009 hingga tahun 2014 Korea Selatan mengalami sejumlah serangan *cyber* yang diduga datangnya dari Korea Utara. Sehingga Korea Selatan dipaksa membentuk sebuah gagasan kebijakan *cyber security* untuk menangkal *cyber attack* korea Utara yang semakin canggih dan tak terbendung.

VIII. Saran

1. Korea Selatan seharusnya lebih meningkatkan keamanan *cyber* nya guna meminimalisir kerugian yang dialami bila sewaktu waktu mendapat serangan *cyber* dari Korea Utara, berikut adalah beberapa cara untuk memperkecil bentuk serangan *cyber* yaitu :
    a. Mempersiapkan serangkaian tanggapan langsung secara bertahap yang menarget organisasi dunia maya Korea Utara.
    b. Mengekang kebebasan operasional Korea Utara di dunia maya.
    c. Mengidentifikasi dan memanfaatkan kerentanan yang dimiliki Korea Utara untuk menjaga keseimbangan strategis.
    d. Mengadopsi langkah-langkah ketahanan dan mitigasi kerusakan dari negara maju seperti Amerika yang bekerja sama dalam penanggulangan kejahatan Internasional untuk memastikan bahwa kelangsungan operasional dari jaringan dan sistem penting tetap terjaga meskipun mengalami serangan.

2. Korea Utara seyogyanya menghentikan kebijakan membangun kekuatan militer (nuklir) sehingga dapat meminimalisir biaya yang dikeluarkan hanya demi membangun kekuatan nuklirnya tersebut, akibatnya Korea Utara harus mencari alternatif lain agar mampu menjaga kestabilan nasionalnya, salah satunya dengan melakukan *cyber attack* ke Korea Selatan dan negara negara lainya , pada akhirnya malah mengakibatkan Korea Utara sering mendapat sangsi dari PBB dan mendapat kecaman dari berbagai negara yang menilai bahwa Korea Utara dengan kebijakan nuklirnya yang setiap saat terus melakukan uji coba rudalnya sehingga malah memperkeruh suasana di Semenanjung Korea.

IX. Daftar Pustaka

A. Buku

Anak Agung Banyu Perwita dan Yanyan Mochammad Yani. 2006. *Pengantar Ilmu Hubungan Internasional*. Bandung: PT Remaja Rosdakarya.

Breuning, Marijke. 2007 . *Foreign Policy Analysis Comparative Introduction*. New York: Palgrave MacMillan.

David, Speer. 2003. Redefinig Borders*: The Challaenge of Cybercrime.* England.

Dugis, Vinsensio. 2008. *Analisis Kebijakan Luar Negeri*. Surabaya.

Eoghan, Casey 2001. *Digital Evidence and Computer Crime,* London : A Harcourt Science and Technology Company.

Howard, John D. 1995. *An Analysis of Security Insidents of the Internet*

Jackson, Robert. 2005. *Pengantar Studi Ilmu Hubungan Internasional.* Yogyakarta. Pustaka Pelajar.

Jervis, Robert. 2005. *American foreign policy in a new era*. New York : Routledge New.

Mas'oed, Mochtar. 2003. *Ilmu Hubungan Internasional: Disiplin dan Metodologi.* Jakarta: PT. Pustaka LP3S.

Muhaimin, Yahya A. 2006. *Masalah Kebijakan Pembinaan Pertahanan Indonesia*. Yogyakarta: Tiara Wacana.

Perwita, Banyu dan Mochamad Yani, 2005. *Pengantar Ilmu Hubungan Internasional*. Bandung: Rosida.

Plano, Jack C. 2000. *Kamus Hubungan Internasional*. Bandung : Abardin.

Rudy, May T. 2003. *Pengantar Ilmu Politik.* Bandung : PT Refika Aditama.

Sitepu, Anthonius. 2011. *Studi Hubungan Internasional*. Yogyakarta: Graha Ilmu

Suseno, Sigit. 2012. *Yuridiksi Tindak Pidana Cyber.* Bandung: Refika Aditama

Wuryandari, Ganewati, Alami, Athiqah Nur, Yustinigrum, Rr. Emilia, Sriyanto, Nanto. 2014. *Politik Luar Negeri Indonesia dan Terorisme Internasional.* Bandung : Graha Ilmu.

B. Jurnal

David, Arwin, *Diplomasi pertahanan Indonesia dalam pencapaian cyber security melalui Asean Regional Forum on Cyber Security Initiatives*

Fearon, James. D. 2014. *Separatist Wars, Partition, and World Order.* Departmen of Political Science. Standford University.

Handrini, Andrianty, 2014 *Cyber security dan tantangan nya di Indonesia*

Moehammad, Yuliansyah Saputera, 2015. *Pengaruh Cyber Security strategi Amerika Serikat menghadapi ancaman CyberWarfare.*

C. Rujukan Elektronik

Dimas. 2016. Microsoft bangun pusat *cyber* di Korea. Melalui https://kriptologi.com/2016/03/09/microsoft-bangun-pusat-cybersecurity-di-korea/ diakses tanggal 27 Januari 2018.

Chun Kim Hee. 2017. Sekilas tentang perusahaan Haura Inc. Melalui https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=12935767 diakses tanggal 27 Januari 2018.

Korean Tourist Organization. 2015. Geografi Korea Melalui https://www.visitkorea.or.id/bbs/page.php?hid=geografi_ko diakses tanggal 29 Januari 2018.

National Intelegence Service of Korea. 2015. National Security Melalui http://eng.nis.go.kr/EAF/1_9.do diakses tanggal 27 Januari 2018.

http://www.abadikini.com/read/02/11/2017/mengejutkan-korea-selatan-kewalahan-hadapi-cyber-attack-korea-utara/

http://www.artileri.org/2013/03/korsel-atasi-serangan-cyber-korut.html

http://www.antaranews.com/berita/400557/korut-lancarkan-ribuan-serangan-cyber-terhadap-korsel

http://apdf-magazine.com/id/keamanan-cyber-isu-prioritas-tinggi-bagi-korea-selatan/

http://www.bbc.com/indonesia/dunia-41399234

http://www.bbc.com/indonesia/majalah/2010/04/100406_nkorea_computer

http://eng.nis.go.kr/EAF/1_2.do

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

https://jurnal.dpr.go.id/index.php/politica/article/view/336/270 diakses tanggal 18 april 2017.

https://international.sindonews.com/read/1194457/40/hacker-korut-curi-rencana-perang-as-korsel-1491382277.

http://sorot.news.viva.co.id/news/read/238559-hikayat-serdadu-cyber-korea-utara

https://pinterpolitik.com/pasukan-rahasia-korut/

http://www.satucode.com/2016/06/hacker-korea-utara-mencuri-blue-print.html diakses tanggal 08 Mei 2017.

http://www.wawker.com/2014/12/pengakuan-mantan-hacker-korea-utara.html

http://*pcworld.com*

https://www.techno.id/tech-news/korea-utara-ternyata-juga-miliki-ribuan-tentara-cyber-150601o.html

http://www.nisc.go.jp/security-site/campaign/ajsympo/pdf/lecture2
http://rki.kbs.co.kr/indonesian///news/news_newsthema_detail.htm?lang=i&id=news_newsthema&No=10067101&current_page=8ndiakses tanggal 16 May 2017
http://www.radioaustralia.net.au/indonesian/2013-04-05/sejarah-di-balik-ketegangan-korea-utara-dan-korea-selatan-kilas-balik/1112046
https://www.msn.com/id-id/berita/dunia/mengintip-tempat-hacker-korea-selatan-berlatih-hadapi-korea-utara/ar-BBHv4fd
https://tirto.id/perseteruan-abadi-korea-utara--korea-selatan-clqs