BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi dan informasi yang pesat saat ini membawa dampak yang positif maupun negatif yang sangat besar dalam dunia hubungan internasional saat ini bukan hanya melanda negara-negara maju tetapi negara berkembang pun ikut mengembangkan teknologi agar dapat bertahan dalam era globalisasi saat ini.

Kebutuhan akan teknologi jaringan komputer semakin meningkat. Selain sebagai media penyedia informasi, melalui internet pula kegiatan komunikasi komersial menjadi bagian terbesar dan pesat pertumbuhannya serta menembus berbagai batas negara. Bahkan melalui internet ini kegiatan pasar dunia bisa diketahui selama 24 jam. Melalui dunia internet ataupun dapat disebut juga *cyber space*, apapun dapat dilakukan.

Saat ini hampir setiap manusia telah menggunakan berbagai macam alat elektronik dan bahkan sebagian manusia tidak lepas dari alat elektronik tersebut. Perkembangan teknologi dan komunikasi semakin memudahkan manusia dalam, berhubungan meskipun terpisah jauh, bahkan berbeda negara.

Perkembangan teknologi internet yang semakin hari semakin trend baik dari teknologi dan penggunanya, membawa banyak dampak positif maupun negetif. Tentunya yang bersifat positif kita semua harus mensyukuri karena banyak manfaat dan kemudahan yang di dapatkan dari internet dan biasanya

memasuki suatu sistem dengan memanfaatkan celah yang terdapat dalam sistem tersebut. Kejahatan dunia maya atau *cybercrime* tidak hanya menyerang individu secara pribadi. Namun serangan individu juga dapat menerang lembaga pemerintahan. Banyaknya kasus *cybercrime* mencuri data-data rahasia milik negara. Hal-hal semacam itu dapat membahayakan keamanan negara. Ancaman keamanan dunia *cybercrime* dikarenaka salah satunya terbatasnya para pakar teknologi informasi dan tenaga kerja informasi (http://www.itb.ac.id, diakses pada tanggal 20 Mei 2017).

Cyber security dapat berpengaruh terhadap kestabilan suatu negara, tindakan-tindakan yang berupa pembajakan, *espionage Industri,* sabotase, penyebaran informasi palsu dan pembobolan bank dan hal-hal lain yang merugikan negara pasti akan saja terjadi ketika keamanan *cyber* suatu negara lemah atau kurang dalam teknologi seperti zaman modern saat ini yang dimana-mana orang dapat memantau apa saja melalui teknologi. Indonesia masih rentan terhadap serangan kejahatan lewat teknologi dunia maya yang baru-baru saja terjadi di Indonesia pada tahun 2013 yaitu peretasan terhadap situs Presiden Susilo Bambang Yudhoyono (http://kompas.com. diakses pada tanggal 19 Mei 2017).

Dalam dunia hubungan internasional saat ini *cybercrime* merupakan salah satu ancaman keamanan bagi seluruh negara. Dikarenakan kejahatan yang dilakukan oleh para peretas tersebut dapat dilakukan dimana saja tidak mengenal batas-batas negara. Seperti yang terjadi pun di alami oleh DPP partai Golkar melaporkan terjadinya serangan pengrusakan terhadap situs Golkar.co.id.

Serangan terhadap situs partai berlambang pohon beringin itu terjadi 9 hingga 13 Juli 2006 hingga menyebabkan tampilan halaman berubah (*deface).* "Pada 9 Juli 2006, tersangka mengganti tokoh Partai Golkar yang termuat dalam situs gambar gorilla putih tersenyum dan di bagian bawah halaman dipasangi gambar artis Hollywood yang seronok, dengan tulisan 'bersatu untuk malu dan ini pun terjadi dalam peretasan kartu kredit (http://ilmuta.weebly.com/computer-crime/e-procurement, diakses pada tangal 20 Mei 2017).

Lemahnya penyelenggara negara atau *security* terkait dengan dunia *cyber* yang memerlukan pembatasan penggunaan layanan yang severnya berbeda di luar negeri dan diperlukan adanya *secured system,* legalitas penanganan penyerangan di dunia *cyber,* pola kejadian *cyber crime* sangat cepat sehingga sulit di tangani, tata kelola kelembagaan *cyber security* nasional, rentannya *awareness* atau kesadaran akan adanya ancaman *cyber attack* internasional yang dapat melumpuhkan infrastruktur vital suatu negara. Masih lemahnya industri kita dalam memproduksi dan mengembangkan perangkat keras atau *hardware* terkait dengan teknologi informasi yang merupakan celah yang dapat memperkuat maupun memperlemah pertahanan dalam dunia *cyber* (Ardiyanti, 2014:100).

Berdasarkan beberapa kejadian pada beberapa tahun ke belakang, Indonesia merupakan negara yang lemah *cyber securiy* nya. Hal ini dapat diketahui dari maraknya kejadian, yaitu contoh selanjutnya terjadi peretasan kartu kredit nasabah sebuah bank karena *hacker* berusaha menyusup ke sistem pengamanan kartu nasabah bank yang terjadi pada pertengahan Mei 2014 menjadi catatan buat Indonesia sendiri dan satu fakta yang mengejutkan datang dari

perusahaan *monitoring* internet Akamai mengungkap bahwa kejahatan internet di Indonesia meningkat dua kali lipat. Angka ini menempatkan Indonesia posisi pertama menjadi target *hacker* menggantikan Tiongkok. Dari 175 negara yang di inventigasi, Indonesia berkontribusi sebanyak 38 persen dari total sasaran trafik *hacking*. Angka ini seiring dengan meningkatnya kecepatan internet di Indonesia(http://m.news.viva.co.id/news/read/507480-ketika-hacker-lebih-menakutkan-ketimbang-teroris, diakses pada tanggal 12 Juni 2017).

Kerugian yang disebabkan karena tindakan kejahatan dengan memanfaatkan maupun di dunia *cyber* di Indonesia data *Central Intelligence Agency* (CIA) telah mencapai 1,20% dari tingkat kerugian akibat *cyber crime* yang terjadi di dunia sebagaimana terlihat dalam tabel berikut ini:

Tabel 1.1

Perkiraan Kerugian Akibat *Cyber Crime* di Dunia dan Indonesia

	Global	Indonesia
GDP	USD 71,630 bn	USD 895 bn
Percent of global GDP		1,20%
Cost of		
Genuine cyber crime	USD 3,457 m	USD 43 m
Transitional cyber crime	USD 46,600 m	USD 582 m
Cyber crime infrastructure	USD 24,840 m	USD 310 m
Traditional crimes becoming cyber	USD 150,200 m	USD 2,748 m

Sumber : (http://dakaadvistory.com/wp-content/uploads/DAKA-Indonesia-cyber-security-2013-web-version.pdf, diakses pada taggal 27 Juli 2017).

Dari tabel perkiraan kerugian akibat *cybercrime* yang membandingkan antara perkiraan kerugian akibat *cyber crime* di Indonesia USD 890 billion yang artinya mencapai 1,20% dari total keseluruhan perkiraan kerugian akibat *cyber crime* secara global mencapai USD 71,620 billion (Ardiyanti, 2014: 96).

Maraknya kasus *cybercrime* di Indonesia masih pula banyak kasus yang terjadi di Indonesia seperti kasus *carding*. Indonesia pun mengalami kasus *cybercrime* yang menggangu keamanan negara, ketika sistem jaringan Komisi Pemilihan Umum (KPU) diretas oleh *hacker.* Sangat mencemaskan ketika dunia semakin bergantung terhadap teknologi dan infrmasi saat ini yang sangat rentan terhadap jaringan. Maraknya kasus *cybercrime* yang terjadi di Indonesia dilatar belakangi oleh beberapa faktor yaitu pertama lemahnya penegak hukum di Indonesia kedua, keterbatasan sarana dan prasarana di bidang teknologi dan juga lembaga hukum di daerah (polda) masih terbatas dalam hal infrastruktur ketiga, kurangnya ahli *cyber security* di Indonesia.

Dengan adanya berkembangna kasus *cybercrime* saat ini mendorong setiap negara-negara untuk saling bekerjasama dalam melawan *cybercrime.* Peningkatan keamanan dalam sistem *cyber* adalah salah satu kegiatan yang telah dilakukan oleh Institut Teknologi Bandung (ITB). Kerjasama yang dilakukan *Korea International Cooperation Agency* (KOICA) dan pemerintahan Indonesia yang bertempat di Institut Teknologi Bandung (ITB) salah satu upaya untuk meningkatkan keamanan dalam sistem *cyber* ini dengan mendirikan sebuah gedung bernama KOICA-ITB R&D Center. *Cyber security* R&D *center* yaitu tempat pembelajaran mengenai *cyber security* yang berlokasi di kampus Institut

Teknologi Bandung ITB Jatinangor, Sumedang, Jawa Barat. Gedung tersebut memiliki fasilitas yang cukup lengkap.

Korea International Cooperation Agency (KOICA) yang didirikan pada tahun 1991 milik pemerintah Republik Korea Selatan, teknologi Korea Selatan dapat dikatakan sangat maju dalam bidang teknologinya dan memiliki Sumber Daya Manusia (SDM) yang cukup dalam ahli dunia *cyber security*, dalam hal ini Korea Selatan memandang bahwa *cybercrime* merupakan masalah yang besar bagi negaranya sehingga Korea Selatan memberikan pendidikan khusus tetang *cyber security* terhadap negaranya untuk mencetak para ahli-ahli yang mampu dalam dunia *cyber security* . Disinilah Korea Selatan ingin bekerjasama dengan indonesia melalui *Korea International Cooperation Agency* (KOICA) dengan Korea tujuan untuk sama-sama mencetak Sumber Daya Manusia (SDM) di Indonesia dalam bidang *cyber security* yaitu dengan bantuan hibah dan program dengan tujuan membantu negara-negara berkembang salah satunya Indonesia.

Korea International Cooperation Agency (KOICA) memiliki program-program pendidikan, kebudayaan dan infrastruktur bertujuan untuk membantu negara-negara berkembang agar dapat meningkat kualitas Sumber Daya Manusia (SDM). Salah satunya yaitu Pendidikan untuk pengembangan *cyber security* di Indonesia. Hibah yang diberikan kepada indonesia ini di karenakan Korea Selatan melihat bahwa Indonesia perlu memperkuat tentang *cyber security* nya karena indonesia merupakan negara berkembang yang memiliki jumlah penduduk yang banyak dan kekayaan alamnya yang berlimpah.

Sumber Daya Manusia (SDM) Indonesia di bidang *cyber security* cukup mampu dan diakui kualitasnya, walaupun kualitasnya yang di miliki Indonesia masih minim, karena itulah *cyber security* ini didirikan untuk menambah kuantitas ahli-ahli *cyber security* yang banyak dibutuhkan baik oleh kalangan perusahaan swasta, industri, maupun pemerintahan apabila suatu ketika kita mendapatkan serangan *cyber* dari luar. Di sini Indonesia membutuhkan ahli *cyber security* untuk menjaga semua aspek yang terpenting negara seperti PLN, BUMN dan aspek-aspek yang terpenting lainnya (http://www.itb.ac.id, diakses pada tanggal 18 Mei 2017).

Gedung KOICA-ITB R&D *Center* hibah yang di berikan Korea Selatan kepada Institut Teknologi Bandung (ITB) berupa gedung, transportasi, fasilitas proses pembelajaran, dan dimana gedung ini memiliki 3 (tiga) lantai, di mana lantai 1 (satu) untuk auditorium dan plaza pamer, lantai 2 (dua) laboratorium keamanan *cyber* dan ruang riset, dan untuk lantai 3 (tiga) untuk ruang aktifitas belajar mengajar (https://stei.itb.ac.id, diakses pada tanggal 19 Mei 2017).

Dimana *Korea International Cooperation Agency* (KOICA) memberikan hibah berupa program pembelajaran, saran dan prasarana untuk mengenalkan betapa penting *cyber* di suatu negara, dimana perang terhadap dunia maya sangat marak dibicarakan, program *wellness (kids camp)* ini di berikan kepada siswa-siswa sekolah dasar agar mereka mengetahui tentang *cyber* sejak dini dan program *E-Learning* begitupun pelatihan diberikan kepada guru-guru, dan polisi keamanan yang bertujuan untuk memberikan pengetahuan bagaimana tentang *cyber security*. Program pembelajaran tersebut tidak dikenakan biaya apapun,

program tersebut dilakukan setiap tahun berturut-turut dari pada masa berlakunya kerjasama tersebut.

Dalam kerjasama yang dijalankan antara *Korea International Cooperation Agency* (KOICA), DIKTI dan ITB sebagi tempat pelaksanaan berlangsung, yang dilator belakangi MoU antara kedua negara ini dengan tujuan menjalankan tridarma dan penggunaan hibah dalam pengembangan *cyber security* yang harus dilaksanakan dengan sebaik-baiknya.

Pada *cyber security* ini terdapat dua program yang dijalankan yaitu program pendidikan yaitu *E-learning* kepada guru SMA, polisi militer dan perbankan, we*llness (kids camp)*, dan program riset dan pembangunan. Program riset dan pengembangan berupa pendidikan Magister *cyber security* ditujukan untuk mencetak Sumber Daya Manusia (SDM) kompeten di bidang keamanan *cyber*. *Cyber security center* merupakan jurusan baru di bawah jurusan sekolah tinggi elektro dan informatika (STEI) baik berupa program S2 reguler maupun S2 eksekutif (bagi para pegawai berpengalaman) atau program training profesional dan sertifikasi. Program riset dan pengembangan sudah mulai dijalankan melalui riset mahasiswa S1, S2, S3 dan pengembangan produk.

Tujuan utama yaitu dengan keinginan untuk membantu negara Indonesia dalam menyelesaikan permasalahannya yang semakin hari semakin bergantung kepada teknologi dan bertujuan untuk menghasilkan para ahli yang berkualitas dan trampil dalam bidang keamanan teknologi informasi. Program *cyber security center* ini telah menghasilkan mahasiswa yang kreatif, inovatif, dan kemampuan di dalam *cyber security* telah menghasilkan 3 (tiga) tahap kelulusan magister

dalam jurusan *cyber security center* (www.ciso.co.id, diakses pada tanggal 20 Mei 2017).

Terpilihnya Institut Teknologi Bandung (ITB) oleh *Korea International Cooperation Agency* (KOICA), *Deputy Resident Representative* KOICA untuk Indonesia yaitu Lee Young In melihat bahwa Institut Teknologi Bandung (ITB) merupakan perguruan tinggi negeri di Indonesia terutama dari sisi teknologinya. Ini pun bisa melakukan studi banding agar bisa sama-sama kuat dalam menghadapi masalah *security* dan Institut Teknologi Bandung (ITB) merupakan universitas yang memiliki teknologi sehingga mendapatkan hibah dari Korea Selatan.

Hibah tersebut di berikan langsung dari Korea Selatan kepada pemerintahan Indonesia dan tempat dan pelaksanaannya di Institut Teknologi Bandung (ITB) kampus Jatinanggor Sumedang Jawa Barat di karenakan ada persetujuan dari rektor Institut Teknologi Bandung (ITB) untuk mengadakan pembangunan baru di kampus Institut Teknologi Bandung (ITB) yang bertempat di Jatinangor (www.bhataramedia.com, diakses pada tanggal 19 Mei 2017).

Untuk memudahkan peneliti dalam mengkaji kerjasama *Korea International Cooperation Agency* (KOICA) dan Institut Teknologi Bandung (ITB) peneliti menggunakan beberapa penelitian terdahulu yang akan digunakan yaitu pertama karya ilmiah yang berupa jurnal *Politica* yang dilakukan oleh (Handriani Ardiyanti) dengan masalah yang berjudul (dengan masalah yang berjudul (*cyber security dan tantangan pengembangannya di Indonesia*) yang diterbitkan oleh pusat pengkajian, pengelolaan, data dan informasi (P3DI) pada

tahun 2014. Kesamaan dengan peneliti Handriani Ardiyanti dalam tulisanya menuliskan ingin memperoleh gambaran tentang kebijakan *cyber security* di Indonesia saat ini dan memetakan prospek pengembangan *cyber security* di Indonesia sedangakan peneliti ingin mengetahui bagaimana *cyber security* dan tantangan di Indonesia. Sedangkan perbedaan terdapat di pengkajian masalah di mana Handriani Ardiyanti mengkaji permasalahan kebijakan cyber *security* di Indonesia sedangkan peneliti bertujuan untuk mengkaji kerjasama *Korea International Cooperation Agency* (KOICA) dan pemerintahan Indonesia dalam pengembangan *cyber security*.

Penelitian kedua, karya ilmiah yang berupa jurnal Penelitian Politik yang ditulis oleh (David Putra Setyawan dan Arwin Datumaya Wahyudi Sumari) dengan masalah yang berjudul (*diplomasi pertahanan indonesia dalam pencapaian cyber security melalui asean regional on cybersecurity intiatiaves*) yang dilakukan pada tahun 2016. Kesamaan dengan penelitian terdahulu yaitu sama-sama mengkaji mengenai *cyber security* di Indonesia dengan kerjasama yang dilakukan. Perbedaan dengan peneliti yaitu apabila peneliti kedua mengkaji mengenai diplomasi pertahanan Indonesia dalam pencapaian *cybersecurity* melalui ASEAN maka peneliti mengkaji bagaimana kerjasama *Korea International Cooperation Agency* (KOICA) dan pemerintahan Indonesia dalam pengembangan *cyber security*.

Penelitian ketiga yaitu skripsi yang ditulis oleh (Rangga Gilang Saputra Martono) dengan masalah yang berjudul (*Kerjasama Australia Melalui Cybercrime Investigation Satellite Office dalam pencegahan dan penanggulangan*

Cybercrime di Indonesia) yang di buat pada tahun 2016 Universitas Komputer Indonesia. Pada skripsi Rangga Gilang membahas mengenai kerjasama yang dilakukan oleh Indonesia dan Australia dalam menangani *cybercrime* melalui *cybercrime investigation satellite office*. Rangga ini memberikan contoh bahwa Australia dan Indonesia selalu mengalami pasang surut dan tidak jarang Australia sering ikut campur dalam urusan dalam negeri Indonesia serta mencoreng kedaulatan Republik Indonesia.

Walaupun ada beberapa perjanjian yang telah di sepakati oleh Australia dan Indonesia yang di namakan *Lombok Treaty* adalah kerjasama di bidang keamanan pada tanggal 13 November 2006, yang membawa hubungan Indonesia dan Australia dapat berhubungan baik seperi sedia kala. *Lombok Treaty* yang kemudian di ratifikasi pada tahun 2007 Tentang Pengesahan Perjanjian Antara Republik Indonesia dan Australia tentang kerangka Kerjasama Keamanan yang meliputi 21 kerjasama keamanan yang tertuang dalam 10 bidang.

Pada tahun 2010 dimana lanjutan kerjasama yang dilakukan Polri dan Australia Federal Police dalam pembangunan CCISO (*Cyber Crime Investigation Satellite office)*. Dengan adanya lanjutan kerja sama pada tahun 2010 ini makan terbentuklah sebuah kantor pencegahan dan penanggulangan *cybercrime* yang bernama CCIC atau *cyber crime Invesigation Center* di markas bersar Republik Indonesia.

Dengan adanya perjajian tersebut tetap saja masih saja terjadi tumpah tindih antara Australia dan Indonesia, tumpah tindih ini yang dikarenakan adanya

keingin tahuan tentang permasalahan atau rencana apa saja yang di alami negara tetangga demi kepentingan nasionalnya.

Kesamaan dengan peneliti sebelumnya yaitu sama-sama membahas mengenai kerjasama dalam bidang *cybercrime*. Perbedaan terdapat pada pengkajian masalah dimana peneliti sebelumnya membahas mengenai kerjasama Indonesia dan Australia melalui *Cybercrime Investigation Satellite Office* dalam pencegahan dan penanggulangan *Cybercrime* di Indonesia sedangkan peneliti membahas mengenai kerjasama *Korea International Cooperation Agency* (KOICA) dan pemerintahan Indonesia dalam pengembangan *cyber security*.

Berdasarkan uraian diatas peneliti ingin mengetahui lebih jauh mengenai kerjasama yang dilakukan oleh *Korea International Cooperation Agency* (KOICA) dan Institut Teknologi Bandung (ITB) dalam bidang *cyber security.* Dan beberapa alasan antara lain: pertama, *cyber security* Indonesia yang sangat kurang dalam teknologi sehingga rentan sekali mengalami serangan *cyber* dari negara lain. Kedua, dalam kerjasama tersebut peneliti ingin mengetahui kendala, langkah dan apa saja yang dilakukan kedua negara dalam menangani serangan *cyber.*

Dengan alasan tersebut di atas maka menjadi dasar pertimbangan peneliti untuk melakukan penelitian dengan judul:

"Kerjasama *Korea International Cooperation Agency* (KOICA) dan Pemerintahan Indonesia dalam pengembangan *Cyber Security*"

Adapun ketertarikan peneliti untuk meneliti didukung oleh beberapa mata kuliah di dalam Ilmu Hubungan Internasional yaitu :

1. Hukum Internasional, dimana *cybercrime* menjadi salah satu kajian hukum internasional, khususnya mengenai peraturan serta penanganan *cybercrime* di seluruh negara.
2. Diplomasi dan Negosiasi, mata kuliah ini yaitu mempelajari pentingnya diplomasi dan negosiasi antara negara 1 (satu) dengan negara yang lain.
3. Informasi dan komunikasi internasional, mata kulaih ini mempelajari bagaimana interaksi dan komunikasi yang baik yang melewati batas negara.
4. *ICT for International Relation* yang di dalamnya membahas tentang *cyber crime, cyber security, cyber attack* yang di bicarakan di dunia saat ini.
5. Studi Keamanan Internasional, di mana mata kuliah ini membicarakan keamanan di suatu negara, keamanan merupakan faktor paling terpenting dalam suatu negara dan dimana teknologi dan informasi berperan di dalamnya.

1.2 Rumusan Masalah

1.2.1 Rumusan Masalah Mayor

Dalam penelitian ini peneliti mengajukan rumusan masalah mayor sebagai berikut "Bagaimana kerjasama *Korea International Cooperation Agency* (KOICA) dan pemerintahan Indonesia dalam pengembangan *Cyber Security*?"

1.2.2 Rumusan Masalah Minor

Dari paparan latar belakang di atas peneliti menarik rumusan masalah minor penelitian yaitu:

1. Apa saja upaya dalam kerjasama *Korea International Cooperation Agency* (KOICA) dan pemerintahan Indonesia dalam pengembangan *cyber security*?
2. Bagaimana kendala kerjasama *Korea International Cooperation Agency* (KOICA) dan pemerintahan Indonesia dalam pengembangan *cyber security*?
3. Apa saja prospek kerjasama *Korea International Cooperation Agency* (KOICA) dan pemerintahan Indonesia dalam pengembangan *cyber security*?

1.3 Pembatasan Masalah

Pada penelitian ini, peneliti membatasan masalah penelitian dari tahun 2013-2017. Karena pada tahun 2013 dimana kerjasama *Korea International Cooperation Agency* (KOICA) dan pemerintahan Indonesia telah di bangun pada tanggal 30 Januari 2013 dan menanda tanggani MoU dan pada tahun 2017 dimana peneliti ingin melihat apa saja yang dilakukan atas tantangan dan hambatan beserta hasil dalam kerjasama *Korea International Cooperation Agency* (KOICA) dan Institut Teknologi Bandung (ITB) dalam pengembangan *cyber security* yang telah berjalan.

1.4 Maksud dan Tujuan Penelitian

1.4.1 Maksud Penelitian

Penelitian ini dimaksudkan untuk mengetahui sejauh mana kerjasama *Korea International Cooperation Agency* (KOICA) dan pemerintahan Indonesia dalam pengembangan *cyber security*.

1.4.2 Tujuan penelitian

Dari paparan latar belakang di atas peneliti menarik Tujuan penelitian yaitu:

1. Untuk mengetahui bagaimana upaya kerjasama yang disepakati *Korea International Cooperation Agency* (KOICA) dan pemerintahan Indonesia dalam pengembangan *cyber security*
2. Untuk dapat mengetahui kendala kerjasama *Korea International Cooperation Agency* (KOICA) dan pemerintahan Indonesia dalam pengembangan *cyber security*.
3. Untuk mengetahui bagaimana prospek kerjasama *Korea International Cooperation Agency* (KOICA) dan pemerintahan Indonesia dalam pengembangan *cyber security*.

1.5 Kegunaan Penelitian

Hasil Penelitian ini selain untuk kepentingan akademik, penelitian ini juga dapat di jadikan sebagai sumber informasi atau bahkan, sebagai solusi bagi para pembaca khusunya dan dapat mendorong masyarakat menjadi masyarakat yang berpendidikan dan berwawasan untuk diri sendiri dan orang lain.

Keamanan sangatlah penting untuk suatu negara negara yang baik dapat menjaga keamanan nya. Selain itu juga diharapkan memiliki kegunaan yang bersifat teoritis dan praktis yaitu sebagai berikut:

1. Aspek teoritis adalah penelitian ini diharapkan dapat menambahkan wawasan tentang Ilmu Hubungan Internasional yang berkaitan dengan penelitian ini khususnya "Bagaimaana kerjasama *Korea International Cooperation Agency* (KOICA) dan pemerintahan Indonesia dalam pengembangan *cyber security"*. Bagi ilmu pengetahuan yaitu menambahkan khazanah keilmuan tentang nilai-nilai positif dan negaif tentang dunia maya dan di harapkan dapat berguna sebagai sumbangan pemikiran bagi dunia pendidikan.
2. Aspek praktis adalah hasil penelitian ini diharapkan akan memberikan masukan sebagai berikut:
    a. Bagi peneliti yaitu dapat menambahkan wawasan yang lebih luas bagi penulis tentang dunia *cyber*
    b. Bagi para pembaca yaitu sebagai bahan referensi khususnya jurusan Ilmu Hubungan Internasional
    c. Bagi peneliti berikutnya yaitu sebagai bahan pertimbangan atau bahan yang dapat di kembangkan lebih lanjut, serta referensi terhadap penelitian yang sejenis.