BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

4.1 Hasil Penelitian

4.1.1 Gambaran Objek Penelitian

4.1.1.1 Hubungan Bilateral Indonesia dan Korea Selatan

Hubungan kerjasama bilateral Indonesia dan Korea Selatan yaitu telah berjalan semenjak empat dasawarsawa dimana kedua negara ini telah menanda tangani persetujuan pembukaan hubungan diplomatik pada bulan Mei tahun 1966. Dengan dibukanya kantor Konsultan Jendral Korea pada tanggal 1 Desember 1966 di Jakarta, begitupun Korea Selatan mengikuti dengan pembukaan Konsular Jendral di Indonesia pada tanggal 1 Juni 1968 di Seoul, kerjasama ini sebagai langkah pertama yang resmi di lakukan oleh kedua negara. Disinilah banyak dengan kerjasama diplomatik banyak kesempatan untuk melakukan hubungan yang lain juga di lakukan, dan pada tanggal 18 September 1973, kedua negara ini melihat bahwa hubungannya sangat baik dan dapat mengutungkan maka ditingkatkan hubungan diplomatik

(Rahmah, 2013:2).

Hubungan Indonesia dan Korea Selatan merupakan negara yang mengelami perang dingin yang memiliki ideologi yang berbeda, Korea Selatan yang digambarkan dengan warnanya masing-masing oleh idiologi yang berbeda. Sedangkan Indonesia dibawah kepemimpinan Soekarno yang tidak mau digolongkan negara Timur maupun Barat, maka Korea Selatan pro kepada

Amerika Serikat dan Indonesia dalam hubungan diplomatinya tidak berjalan dengan mulus dengan dunia barat ketika Indonesia ditanggan Bung Karno (Yoon, 2005:47).

Tahun 1966-1970, kedua negara dapat mencapai peningkatan yaitu dapat bertukar para pejabat, ketika Indonesia di tandai dengan pertemuan Ketua Dewan Perwakilan Rakyat (DPR) dan Parlemen Korea Selatan, menteri-menteri, pejabat-pejabat tinggi militer dari tiap-tiap negara. Selanjutnya pada tahun 1978-1975 Menteri Luar Negeri Indonesia, menteri perdagangan, dan menteri perindustrian saling melakukan pertemuan membahas mengenai masalah ekonomi hal ini yang mewujudnya terjadinya ketergantungan satu sama lain. Interaksi kerjasama antara pemerintah, masyarakat Indonesia dan Korea Selatan dan pada sekarang ini. Dapat dicontohkan pertukaran personal dalam wujud kunjungan kerja, pertukaran delegasi budaya, turis dan para pakar.

Pada tahun 1980 hubungan bilateral kedua negara ini mengalami pasang surut, Korea Selatan pada tahun 1980 telah menjalin kerjasama dengan negara Asia Tenggara salah satunya yaitu Indonesia walaupun ekonomi menitipberatkan pada wilayah dan merupakan blok regional yang luas Korea Selatan tetap menggunakan gaya ekonomi dan politiknya tersendiri.

Tahun 1990 hubungan kerjasama Indonesia dan Korea Selatan dalam bidang ekonomi dan politik saling menguntungkan dengan adanya pertemuan dengan pejabat tinggi pemerintah Indonesia dapat membuat hubungan kedua negara ini kearah yang lebih baik dan positif.

Tahun 2000, ketika kekuasan berada di bawah Presiden Abdurrahman Wahid ke Korea Selatan dan Presiden Kim Dae-Junh bertemu pada bulan Oktober di Seoul dengan acara penyelenggaraan KTT ASEAN ke-3 dan pada tahun yang sama kedua negara ini bertemu di Jakarta.

Tahun 2006 tanggal 4 Desember, hubungan kedua negara ini di tingkatkan ditandai dengan penandatanganan *Join Declaration Between The Republic Of Indonesia And The Republic Of Korea On Strategic Partnership To Promote Friendship And Coorporation In The 21st Century* oleh presiden Susilo Bambang Yudhoyono dan Roh Moo Hyun, dimana dalam penandatanganan tersebut dapat menyangkut 3 pilar yaitu kerjasama politik, ekonomi, perdagangan dan investasi dan kebudayaan.

Tahun 2009 kunjungan Presiden Lie Myungbak yang dapat menghasilkan kerjasama dalam bentuk *Memorandum of Understanding* (MoU), berupa dalam bidang pendidikan dan teknologi dan kehutanan dan *Letter Of Intent* (LOI) dibidang perhutanan (Rahmah, 2013:78).

4.1.1.1.1 Bidang Politik

Korea Selatan adalah mitra strategis bagi Indonesia. Hubungan dan kerjasama bilateral dalam bidang politik, kedua negara meningkatkan hubungan yang tajam dalam tahap akhir ini terutama semenjak kedua negara dimasuki kemitraan yang strategis yang ditandai dengan penandatanganan *Joint Declaration on Strategic Partnership* oleh Presiden Susilo Bambang Yudhoyono dan Preseden Korsel Roo Moo Hyun di tetapkan pada tanggal 4 Desemeber 2006 di Jakarta. *Joint Declaration on Strategic Partnership* dapat mencakup 3 (tiga)

dalam bidang kerjasama yaitu kerjasama poltik dan keamanan, kerjasama ekonomi, kerjasama sosial budaya. Hubungan dalam politik ini sangat terjaga dengan baik dan menguat dengan instansi kunjungan high dignitaries kedua negara ini, antara lain:

a. Kunjungan Presiden Republik Indonesia ke Busan dalam rangka *Commemorrative* Summit ASEAN-ROK ke-25 pada 10-20 Desember 2014.

Dalam hal ini kedua negara mencatak penegasan kembali promosi peningkatan dialog kemitraan ASEAN-ROK untuk kemitraan yang strategis yang bermakna, mengutungkan, dan bermakna, mendorong pendirian komunitas ASEAN, meningkatkan konektifitas, mengurangi pembangunan, dan memperkuat ASEAN Sekretariat dalam mewujudkan ASEAN yang didasarkan pada aturan, berpusat pada masyarakat, secara ekonomi terpadu, kondusif secara politik dan bertangung jawab pada aturan. Dalam bidang politik ini para pemimpin ASEAN dan ROK memperkuat betapa pentingnya perdamaian dan stabilitas di kawasan.

b. Pertemuan bilateral Presiden Joko Widodo dengan Presiden Park Geu-hye pada 11 Desember tahun 2014.

Dalam pertemuan ini Presiden Park Geu-hye menyampaikan bahwa Indonesia adalah mitra penting kerjasama dan mitra dagang bagi ROK. Hasil dari pertemuan kedua negara ini membicarakan mengenai sepakat untuk menghidupkan kembali *Joint Declaration on Strategic Partnership* (JCM) pada tingkat menlu kedua negara, sepakat dalam meningkatkan kerja industri pertahanan, yang diutamakan yaitu transfer pengetahuan dan teknologi terkait dengan pembangunan bersama kapal selam dan pesawat tempur yang telah berjalan saat ini, komitmen untuk

berpartisipasi dalam pembangunan kesatuan, penjaga pantai dan galangan kapal di Indonesia, penandatangan persetujuan pembentukan komite bersama di bidang *e-government* dan reformasi birokrasi, Presiden Republik Indonesia mendukung perdamaian dan stabilitas pada tingkat kawasan dan global contohnya pada semenanjung Korea.

c. pemberian penghargaan oleh Park Geun-hye kepada Presiden Joko Widodo atas partisipasi dari Presiden Susilo Bambang Yudhoyono yang telah aktif dalam memperkuat hubungan bilateral dan multilater.
d. Memberikan pengesahan kepada Dr. Susilo Bambang Yudhoyono sebagai ketua *Global Green Growth Institute* (GGGI).
e. Pada tanggal 22 Desember 2014 di Jakarta Mr. Chung Ui-hwa mengatakan kesiapan dalan meningkatkan kerjasama maritim yang khususnya kepada Republik Indonesia.
f. 19 November 2014, pertemuan tersebut membicarakan mengenai kerjasama dalam *capaciry building* dalam program-program peatihan kepada staf sekretariat jendaral maupun anggota DPD Republik Indonesia, pembangunan system IT-*based paparles governance dan e-voting.*
g. Pertemuan Bapak Wakil Ketua BPK Sapto Amal Damandari dan delegasi ke ROK dengan *Ketua Board of Audit and Inspection* ROK Hon Desember 2014, dimana pertemuan tersebut menyepakati kerjasama dalam peningkatan program auditor dan pegawai BPK untuk meningkatkan profesionalitas dan pengembangan Sumber Daya Alam (SDA).

h. Kunjungan Wakil Ketua DPD Republik Indonesia GKR Ratu Hemas dan Wakil Ketua Komisi III DPR Republik Indonesia ke Korea Selatan pada tanggal 16-17 September 2014.

4.1.1.1.2 Bidang Ekonomi

Untuk mewujudkan pilar kerjasama ekonomi, perdagangan, dan investasi, kedua negara ini menyepaki kerjasama *Joint Force on Economic Coorporation* (JTF-EC) pada tahun 2007 dan pada tahun 2011 kedua negara ini merativikasi JTF-EC menjadi *Working Level Task Force Meeting* (WLTFM) dimana pertemuan dilakukan 2 tahun sekali, pertemuan pertama dilakukan yang bertempat di Bali pada tanggal 18-18 Mei 2011. Data menunjukan bahwa nilai realisasi investasi Korea Selatan di Indonesia terus meningkat pada tahun 2013 yaitu USD 2,2 miliar. Nilai ini dimana telah melampui nilai investor Korsel pada tahu 2012 dan menempatkan Korsel sebagai investor tebesar ke-4 setelah Jepang, Singapura, dan Amerika Serikat.

Investor Korea Selatan di Indonesia terutama pada sektor industri ekonomi, telekomunikasi, konstruksi, otomotif, pertambangan, migas, air bersih, perbankkan dan perhotelan. Perusahaan besar korea seperti POSCO, *Honkook Tire, Lotte Group, dan Cheil Jendang Group* di Indonesia. Pada tahun 2011 kedua negara ini mengalami penurunan diakibatkan melemahnya perekonomia global, data tahun 2013 volume perdagangan sebesar US$ 23, miliar, turun dari tahun 2012 mencapau US$ 27,02 miliar. Kedua negara memperhatinkan terjadinya penurunan maka kedua negara melakukan upaya untuk meningkatkan volume perdagangan bilateral dan telah menargetkan pada tahun 2015 mencapai US$ 50

miliar dan pada tahun 2020 mencapai US$ 100 miliar. Pencapaian target ini didukung oleh rencana kedua negara untuk membentuk *Comprehensive Economic Partnership Agreement* (CEPA) untuk melengkapi perjanian ASEAN-ROK *Fre Trade Area* (AFTA) yang telah ada sebelumnya, pada tahun 2012 kedua negara merundingkan mengenai *Comprehensive Economic Partnership Agreement* (CEPA) yang pertama pada tang 12 Juli 2012 di Jakarta untuk membahas *Term of reference* negosiasi IK-CAPA dan cakupan IK-CAPA yaitu *Trade in Goods, Rules of Origin, Custum, Trade Facilitation, Investment, Intellectual Property Rights, Sustainable Development and Comperation.*. Pada CAPA ini Indonesia dan Korea Selatan akan menikmati keuntungan ekonomi sebesar USD 10,2 miliar dan peningkatan PDB sebesar 4,37%, dan sementara itu Korea Selatan mendapatkan keuntungan ekonomi sebesar USD 1,5 miliar dan peningkatan PDB sebesar 0,13%(http://www.kbriseoul.kr. Diakses pada tanggal 24 Juli 2017).

4.1.1.1.3 Bidang Pendidikan

Pada tahun 2009 Indonesia dan Korea Selatan penandatanganan MoU dibidang pendidikan, dalam MoU tersebut adalah proyek penelitian bersama, pertukaran pengajar, pelajar, peneliti dan ahli lainya, pertukaran informasi, pertemuan berkala, konperhensif, seminar, pameran, petukaran bahan-bahan yang diperlukan, pendirian pusat riset bersama, pendidikan, pelatihan. Jumlah mahasiswa dan pelajar Indonesia yang menuntul ilmu di Korea Selatan terus meningkat setiap tahunnya. Pada tahun 2004 jumlah mahasiswa Indonesia di Korsel hanyak sekitar 70 orang meningkat menjadi 1200 siswa sampai bulan

Januari 2015. Begitupun sebaliknya jumlah mahasiswa Korsel yang belajar di Indonesia bertambah dan tersebar di beberapa universitas di Indonesia. Mahasiswa yang belajar di Indonesia melalui program Darmasiswa yang disediakan oleh Kementrian Pendidikan dan Kebudayaan juga terus meningkat, selain dari itu ada program pendidikan singkat dari Kementerian Luar Negeri yaitu beasiswa budaya Indonesia yang memiliki tujuan mengenalkan seni budaya Indonesia kepada generasi muda Korea Selatan. Minat mahasiswa Korea Selatan untuk mempelajari bahasa Indonesia juga meningkatkan terlihat pendaftaran untuk mengikut program pendidikan bahasa Indonesia di BIPA Universitas Indonesia.

4.1.1.1.4 Bidang Teknologi dan Komunikasi

Hubungan kedua negara ini pemerintahan Republik Indonesia dan Republik Korea yang memiliki kerjasama di berbanyak bidang yang telah dijalankan, dalam bidang teknologi dan komunikasi kedua negara ini telah menandatangani *Joint Statement Between the Department of Communication of the Republic of Indonesia and the Ministry of Information and Communication of the Republic of Korea* (ROK) *on Mutual Coorporation in the Fied of Telecommunication* pada tanggal 29 Juni 2000 dan *Areegment Between the Ministry of Communnication and Information of the Republik of Indonesia and the Ministry of Information and Communication of the Republic of Korea* pada tanggal 31 Mei 2002. Dalam kerjasama ini pun di tawarkan beberapa program yang dijalankan yaitu program *capacity building* maupun partisipasi pada forum terkait sektor IT antara lain yaitu menawarkan instansi riset elektronik dan

telekomunikasi kepada pemerintahan Indonesia pada tahun 2008 dan penawaran yang diberikan kembali kepada Indonesia dalam berpartisipasi seminar *on application* dan pemegang selama tiga bulan bagi penelitian Indonesia salam bidang telekomunikasi (http://www.kemenlu.com, diakses pada tanggal 22 Juli 2017).

4.1.1.2 Gambaran Umum Mengenai *Korea International Coorporation Agency* (KOICA)

Korea International Coorporation Agency (KOICA) adalah badan pemerintahan Korea Selatan yang didirikan untuk memaksimalkan efektivitas bantuan Korea pada negara-negara berkembang. Bantuan tersebut berupa bantuan hibah maupun program kerjasama teknis, Program bantuan berupa proyek yang mendukung pembangunan sekolah, rumah sakit, balai latihan kerja yang menjadi program tekemuka KOICA. Selain itupun KOICA menawarkan pelatihan dan keahlian khusus untuk mendukung pengembangn negara-negara mitra. Korea Selatan menempatkan perhatian khusus pada daerah dimana keahlian dan pengalaman dapat memberikan kontribusi penting, termaksud pendidikan, kesehatan, dan perawantan medis, administrasi publik, pertanian, perikanan, serta teknologi informasi, untuk memperluas efektivitas program ini, KOICA berencana untuk memperkenalkan pendekatan sektor lebih luar dan memperkuat pengawasan serta evaluasi program.

1. *World Friends Korea*

   Merupakan program bagi relawan yang dikirim ke luar negeri oleh pemerintah Korea. Program ini di lakukan oleh tiga departemen yang

berbeda. Untuk meningkatkan evektifitas pada tahun 2009 pemerintah Korea menyatukan program relawan tersebut ke dalam satu nama " WFK" pada 2010 program relawan bergabung dalam WFK. Lebih Dari 20.000 WFK relawan dikirim 2009-2013 bertujuan untuk memberikan pembangunan sosial ekonomi kepada Negara-negara berkembang dan menyebarkan citra baik Korea.

2. Kerjasama Masyarakat Sipil

Kerjasama ini dapat memberikan bantuan bagi organisasi masyarakat yang melakukan kegiatan bantuan pembangunan luar negeri, dengan tujuannya yaitu mengurangi kemiskinan dan meningkatkan kesejahteraan, dimana kerjasama ini terdapat proyek-proyek yang berfokus pada masalah lokal, dengan tujuan untuk meningkatkan kondisi kehidupan (pendidikan, pelayanan medis dan pendapatan) dari penduduk lokal di negara berkembang (http://www.ranai.angklung.web.id, iakses pada tanggal 24 Juli 2017).

Cyber security merupakan aktifitas untuk melakukan keamanan terhadap sumber daya telematika demi mencegah terjadinya *cybercrime*. Sebuah proses peningkatan keamanan (*security heardeing*), dimana umumnya meliputi masalah teknis, seperti pengamanan dari sisi jaringan, sistem operasi, keamanan data, dan *source code* aplikasi. Keuangan telekomunikasi secara rutin menyewa konsultan keamanan untuk melakukan kegiatan'*penetration testing'*. Pen test ini dilakukan untuk menguji sejauh mana sistem yang mereka punya dapat bertahan dari serangan-serangan yang akan mengeksploitasi sistem tersebut. Selain dari sisi teknis, kegiatan pengutatan keamanan juga harus meliputi pengamanan terhadap

ancaman dari personil internet. Harus ada sejumlah protokol atau SOP yang harus dilakukan oleh personilnya. Bahkan biasa dibilang personil internet adalah faktor ancaman keamanan yang paling tinggi dibandingkan hal-hal teknis. Dimana apa yang telah dilakukan Edward Snowden, seorang mantan pegawai NSA yang mencuri dan membocorkan data-data kegiatan penyadapan, ini merupakan contoh sempurna, dari sisi sumber daya manusia, praktisi *cyber security* ini bisa dikelompokkan setidaknya menjadi 3 kelompok.

1. Analisis Keamanan

Bertugas untuk memetakan potensi ancaman keamanan, lalu memberikan rekomendasi untuk mitigasi terhadap potensi ancaman tersebut.

2. Apresialisasi Forensik

Bertugas untuk melakukan penyelidikan pasca insiden kebocoran keamnan. Seseorang spesialis forensik harus memiliki kemampuan teknis yang mampu untuk bisa mencari dan memetakan jejak-jejak yang ditinggalkan oleh pelaku, untuk bisa mencetak dan menemukan pelaku.

3. *Hacker*/peretas

Tindakan *hacker* merupakan tindakan kriminal padahal tidak sepenuhnya seperti yang dikatakan, dimana pengertian *hacker* secara istilah yaitu orang-orang yand memiliki kemampuan untuk mengeksploitasi terhadap sestem telematika melalui berbagai cara. *Hacker* ini memiliki kemampuan teknis, system komunikasi data, perilaku dari operating system, kemampuan membaca *source code*, dapat melakukan *reserse engineering*, memetakan mekanisme pengelolaan data memiliki *cyber security center*, yang di bangun oleh ITB dan KOICA yang

bertempat di ITB. Dimana pemerintah Korea Selatan memberikan hibah bangunan dan isinya, serta pelatihan tenaga ahli senilai 55 miliar. Kegiatan keamanan itu meliputi riset, tempat pendidikan magister keamanan informasi. Dimana tujuannya itu untuk menangkal kejahatan di dunia maya seperti pencurian data, penyebaran informasi palsu, serta pembobolan bank dan dimana Indonesia mengalami terganggunya keamanan negara Komisi Pemilihan Umum (KPU) diretas oleh para *hacker* Indonesia (http://m.detik.com, diakses pada tanggal 22 Juli 2017).

Korea Selatan merupakan target utama serangan *cyber*, karena Korea Selatan merupakan keterhubungan jaringan yang tinggi dinegara ini, penghubung jaringan yang cangih, dan kekayaan intelektual yang signifikan, Korea Selatan memiliki kecepaan internet rata-rata tecepat di dunia, yaitu 26,9 Mbps. Selain itu Korea Selatan merupakan negara yang memiliki kecepatan internet yang tertinggi rata-rata 25 Mbps, selain itu Korea Selatan memimpin prestasi *broadband* seluler dunia, dengan lebih dari 120% populasi (per kuartal 1 tahun 2017). Pemerintah memproyeksikan kecepatan internet akan 10 kali lebih cepat pada tahun 2020 nanti, yang dapat mengubah kemampuan teknologi dan kempuan Korea Selatan menjadi negara, yang sangat terhubung. *Cyber* Korea Selatan mengakui bahwa *cyber* merupakan masalah nasional, walupun Korea Selatan menawarkan infrastruktur TI tercepat dan tercepat di dunia tetapi masih saja mengalami ancaman-ancaman dari luar, disamping itu juga memiliki infrastruktur yang tidak aman yang rentan terhadap serangan *cyber*. Korea Selatan telah meningkatkan protokol keamanannya selama beberapa tahun terakhir, menyusun beberapa

kasusu peretas dengan profil tinggi, termaksud serangan *cyber* pabrik *Hydro* dan Tenaga Nuklir Korea (KHNP) pada tahun 2014. Dimana peretas tersebut telah menargetkan agen pemerintah di Korea Selatan, yang melakukan kompromi informasi sensitif dan membahayakan kesejahteraan pejabat pemerintahan dan pegawai sipil.

Frekuensi dan grativikasi ini mendorong Korea Selatan untuk menyusun kembali strategi keamanan dunia maya. Tiga tahap dalam menangani masalah keamanan dunia maya yaitu Pusat Keamanan *Cyber* Nasional, Korea internet dan Pusat Respons Teroris *Cyber Agency*, dimana badan ini dapat bertanggung jawab untuk mengidentifikasi, mencegah dan menganggapi serangan *cyber* dan ancaman keamanan dan juga sekolah yang mengkhususkan diri dengan perang *cyber* telah dewasa dengan tujuan untuk meningkatkan 400 orang ahli keamanan saat ini menjadi 5000 pada akhir 2017. Infrastruktur TIK yang maju Korea Selatan merupakan pasar yang ideal bagi perusahaan Amerika Serikat yang berusaha menguji solusi keamanan maya, sebelum melakukan penerapan dipasar lain. Untuk memasuki di pasar keamanan dunia maya, layanan komersial Amerika Serikat bermitra dengan perusahaan Korea Selatan yang berkualitivikasi dan mampu, yang mempertahankan jaringan penjualan yang ada di pasar keuangan, energy, dan pasar infrastruktur utama ainnya.

4.1.1.2.1 Visi dan Misi *Korea International Coorporation Agency* (KOICA) dan Pemerintahan Indonesia

Dalam melakukan kerjasama antara kedua negara, dapat menimbulkan visi dan misi yang ingin dicapai yaitu:

Mempromosikan hubungan dan koperatif dan saling tukar untuk pembangunan ekonomi dan sosial negara-negara berkembang dan misinya yaitu melayani baik di dalam negeri maupun di luar negeri sebagai kerjasama pembangunan yang berkontribusi untuk mencapai tujuan pembangunan yang berkelanjutan (http://wwwkbriseoul.kr, diakses pada tanggal 23).

4.1.1.2.2 Tujuan Kerjasama *Korea International Coorporation Agency* (KOICA) dan Pemerintahan Indonesia

Dalam kerjasama mempunyai tujuannya masing-masing dengan sehingga tercipta kerjasama yang jelas, berikut adalah tujuan kerjasama yaitu:

Tujuannya untuk menghasilkan Sumber Daya Manusia (SDM) yang berkualitas, trampil dalam bidang keamanan teknologi informasi untuk multi-sektor.

4.1.1.3 Pengembangan *Cyber Security* di Indonesia

Cyber security merupakan alat, kebijakan konsep keamanan, perlindungan keamanan, tidakan, pelatihan dan teknologi yang dapat untuk melindungi lingkungan *cyber* dan organisasi dan asset pengguna. Dimana dalam *cyber security* asset pengguna termaksud perangkat. *Cyber security* organisasi dan aset pengguna termasuk perangkat yang terhubung komputasi, personil, infrastruktur, layanan, aplikasi, system telekomunikasi dan totalitas informasi yang dikirimkan atau disimpan dalam lingkungan *cyber.*

Ada lima *global cyber security* dalam bidang kerja yaitu kepastian hukum (undang-undang *cybercrime*), teknis dan tindakan procedural, struktur organisasi (struktur organisasi sangat berkembang, menghindari tumpah tindih), *capacity*

building dan pendidikan pengguna (kompanye publik dan komunitas terbuka dari ancaman *cybercrime* terbuka), kerjasama internasional (termasuk didalamnya kerjasama timbal balik dalam upaya mengatasi ancaman *cyber*). *Cyber security* lebih dimaknai yaitu suatu yang melindungi kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi. Dimana tiga makna ini bisa melindungi *cyber attack*. Adapun elemen pokok mengenai *cyber security* yaitu:

1. Dokumen standar yang di jadikan acuan dalam menjalankan semua proses terkait keamanan informasi
2. Berperan atas kelangsungan operasi informasi meliputi *hardware* dan *software*
3. *Perimeter defanse* yaitu media yang berperan sebagai komponen infrastruktur informasi
4. *Netwak montoring system* merupakan media yang memiliki tujuan untuk memonitor kelayakan, ultisasi, dan *performance* infrasturktur informasi.
5. *System information and event management* yaitu bertujuan untuk memonitor berbagai kejadian di jaringan termaksud kerjadian terkait pada instansi keamanan.
6. *Network security assessment* yaitu berperan dan bertujuan kepada mekanisme kontrol dan memberikan keamanan informasi.
7. Sumber Daya Manusia (SDM) dan *awareness*nya pada keamanan informasi.

Adapun elemen pokok *cyber security* yang harus terpenuhi dalam tersedianya informasi infrastruktur merupakan media yang sangat berpengaruh dalam informasi yang meliputi *hardware* dan *software*, tersedianya *perimeter defanse* yaitu untuk media yang berperan sebagai komponen pertahanan pada infrastrukur informasi.

Pengembangan *cyber security* yang perlu diperhatikan yaitu yang pertama diperlukannya satelit khusus dalam rangka pertahanan dan keamanan dalam menyikapi secara serius *cybercrime*. Dimilikinya satelit khusus dalam rangka pertahanan dan keamanan mutlak di perlukan karena telah dimilikinya sejumlah *provider* telekomunikasi oleh pemilik modal asing. Pengembangan dan penelenggaraan telekomunikasi *cyber security* ini berkaitan dengan kebijakan *cyber security* dikhususkan di sektor pertahanan dalam penyelenggaraan telekomunikasi Dephamkam dan TNI belum mampu mendukung kegiatan penyelenggara telekomunikasi pertahanan keamanan negara. Saat ini Kemhan dan TNI menggunakan satelit untuk komunikasi *video conference*.

Pengembangan *cyber security* telah dilakukan diantara lain dengan melaksanaka serangkaian program yang suda mulai berjalan diantaranya yaitu : menginisiasi perundang-undang yang terkait dengan *cyber security* seperti undang-undang informasi dan transaksi elektronik No. 11 Tahun 2008, peraturan pemerintah No. 82 Tahun 2012, menyusun kerangka nasional *cyber security*. Pengembangan dan kebijakan *cyber security* di Indonesia hendaknya menyatu dengan strategi nasional dalam membangun ekosistem *cyber security* nasional yang telah disusun oleh pemerintah. Dimana strategi nasional dalam membangun

ekosistem *cyber security* nasional oleh pemerintah yaitu upaya hukum, upaya teknis yang meliputi standar dan operasional penataan organisasi dan kelembagaan penangganan *cyber security* dalam lingkup kepentingan nasional, *capacity building* atau peningkatan kapasitas Sumber Daya Manusia (SDM), dibidang *cyber security* dan meningkatkan kerjasama internasional.

Program pelatihan dan peningkatan keahlian *cyber security* dilakukan dalam koordinasi Tim Kerja Pusat Operasi Dunia Maya (*cyber defance operating center*). Selain itu dilakukan pembinaan SDM tentang arti pentingnya *cyber security* guna meningkatkan pemahaman langkah-langkah preventif dalam meningkat sega tindakan *cybercrime*, dalam mengembangan SDM dalam penangganan *cyber security* yang telah bekerjasama dengan *atake holder* yang memiliki kemampuan dibidang informasi teknologi. Pengembangan di Indonesia dalam membangun *cyber security* kedepannya dilakukan dengan memenuhi empat pondasi yang mendukung perkembangan teknologi perkembangan perangkat lunak (*software*) seperti system dan aplikasi dan perkembangan alat keras (*hardware*) perkembangan saran dan prasarana teknologi informasi, manajemen isi (*content management*), *telecommunication and networking*, perkembangan internet serta perdagangan *online* atau melalui internet.

Mengingat pesatnya teknologi maka pengeolaan sumber daya *cyber security* harus ditempatkan sebagai proses manajemen bisnis. Hal ini diperlukan karena penanganan *cyber security* bukanlah sesuatu yang murah dan mengalami perkembangan kapasitas infrastruktur dengan ditempatkan dengan ditempatkan sebagai proses manajemen bisnis maka potensi kerugian atau biaya yang harus

dikeluarkan karena perkembangan teknologi dapat dikurangi. Demikian dengan pengembangan Sumber Daya Manusia (SDM) yang bergerak dalam *cyber security*, dengan dikelola dengan manajemen bisnis maka diharapkan akan mampu mempecepat terpenuhinya kebutuhan Sumber Daya Manusia (SDM) yang menguasi bidang *cyber security*.

4.1.1.4 Kepentingan Nasional *Korea International Coorporation Agency* (KOICA) dan Pemerintahan Indonesia dalam Kerjasama di Bidang Pengembangan *Cyber Security*

Kepentingan nasional tercipta dari kebutuhan suatu negara, kepentingan ini dapat dilihat dari kondisi internalnya, baik dari kondisi politik, ekonomi, militer, dan sosial-budaya. Dimana kepentingan juga didasari akan suatu '*power'* yang ingin diciptakan sehinga negara dapat memberikan dampak langsung bagi pertimbangan negara agar dapat pengakuan dunia. Pada suatu negara dalam memberikan bahan sebagai dasar dari kepentingan nasional tidak dipungkiri akan menjadi penglihatan masyarakat internasional sebagai negara yang menjalin hubungan yang terlampir dari kebijakan luar negerinya.

Dalam kepentingan nasional, terdapat perbedaan yang umum atau mendasar yaitu kepentingan yang bersifat *viral* dan *non viral*. Kepentingan yang bersifat *viral* yaitu kepentingan nasional yang biasanya bersangkutan dengan kepentingan negara serta nilai-nilai yang menjadi identitas kebijakan luar negerinya. Sedangkan kepentingan yang bersifat *non viral* merupakan kepentingan yang tidak bersangkutan langsung dengan yang eksistensi negara itu namun tetap diperjuangkan melalui kebijakan luar negeri(Jamadu, 2008: 67-68).

Diatas telah menjelaskan seberapa jauh kepentingan tersebut ada dan digunakan, dimana lebih kepada keadaan darurat suatu negara sehingga harus segera diputuskan, berbedan dengan *non viral* yang digunakan sesuai dengan prosesnya yang berlangsung lama tetapi hasilnya dan fungsinya dapat dirasakan lebih baik dikemudian hari dengan jangka waktu yang lama. Demikian kepentingan merupakan strategi dalam menjalankan sebuah kerjasama demi memenuhi kepentingan-kepentingan yang ingin dicapai. Dimana strategi yang dilakukan untuk mewujudkan seberapa jauh hasil yang akan dicapai kedepannya. Dalam rena internasional, kerjasama juga merupakan tindakan yang dipandang sebagai panggung bertemunya para aktor-aktor yang mana membahas mengenai kepentingan akan aktor-aktor yang menjalin kerjasama. Sehinga dalam hal ini negara berusaha menggunakan kepentingan nasional sebagai komponen yang dibuat dan diperjuangkan dalam sebuat hubungan.

Sebagaimana dalam kerjasama *Korea International Coorporation Agency* (KOICA) dan pemerintah Indonesia dalam pengembangan *cyber security* memiliki kepentingan nasionalnya masing-masing. Kepentingan nasional dari kedua negara ini yaitu pertama Indonesia merupakan negara yang rentan terhadap serangan *cyber* dari luar, beberapa contoh kasus yang terjadi yaitu serangan terhadap partai golkar, penyadapan pun dilakukan kepada mantan presiden bapak Susilo Bambang Yudhoyono, Ani Yudhoyono dan 15 pejabat lainnya . Dengan adanya kerjasama ini Indonesia memanfaatkan dengan baik sehingga dapat menambahkan ilmu-ilmu yang diberikan dan menambahkan wawasan dan ketrampilan dalam *cyber security*. Sehingga dapat mencetak Sumber Daya

Manusia (SDM) yang ahli dalam *cyber security*. Kepentingan nasional Korea Selatan, dengan mengadakan kerjasama dalam pengembangan *cyber security* ini dengan tujuan untuk meningkatkan pengetahuan mengenai *cyber threats*, Sumber Daya Manusia (SDM) dan dapat bertukar informasi mengenai ancaman yang dialami dan dapat bersama-sama mengatasi *cyber threats.* Dilihat pada tanggal 7 tahun 2010 korea selatan mengahdapi ancaman *denal-of-service* (DDoS), pada tanggal 20 Maret 2013 tiga stasiun televisi dan sebuah bank mengalami tindakan *cyberware* yang menyebabkan sistem komputer bank dan siaran terganggu dan Korea Selatan mengalami ancaman *cyber* dari Korea Utara dimana Korea Selatan menemukan enam belas server serangan dari Korea Utara salah satunya yaitu server TV YTN, MBC menjadi down pada tahun 2013. Dilihat dari ancaman di atas maka Korea Selatan dan Indonesia membuat suatu kerjasama mengenai pengembangan *cyber security.*

4.1.1.5 Program-Program Kerjasama *Korea International Coorporation Agency* (KOICA) dan Pemerintahan Indonesia di Bidang Pengembangan *Cyber Security*

4.1.1.5.1 *E-learning*

E-Learning ini merupakan pembelajaran dan pembekalan yang diadakan untuk meningkatkan pengetahuan kepada para guru-guru tentang ancaman di dalam dunia *cyber.*

Program *e-learning* diberikan kepada guru-guru di kota Bandung yang di lakukan pada tanggal 26 Juli. Berikut adalah dokumentasi berjalannya kegiatan *e-learning.*



Gambar 4.1
Para Guru SMA kota Bandung sedang mengikuti sosialisasi *E-Learning* di Ruang *Multipurpose Hall* Gedung *Cyber Security Center*.

Sumber: (Institut Teknologi Bandung, Laporan Kegiatan ITB-KOICA *Cyber Security Research and Development Center*, 2016: 23).



Gambar 4.2
Para peserta guru SM

Sumber: (Institut Teknologi Bandung, Laporan Kegiatan ITB-KOICA *Cyber Security Research and Development Center*, 2016: 22).



Gambar 4.3
Paparan tentang *E-Learning*

Sumber: (Institut Teknologi Bandung, Laporan Kegiatan ITB-KOICA *Cyber Security Research and Development Center*, 2016: 2).

4.1.1.5.2 ASEAN *Cyber Kids*

Cyber kids ini bertujuan untuk memberikan pengetahuan sekaligus melihat kemampuan para peserta dalam menggunakan internet serta melihat *skill* apa saja yang mereka ketahui.

Camp 2016 diselenggarakan pada 29-30 Juli di Gedung *Cyber Security Center* dan 31 Juli 2016 di Aula Timur ITB. Kegiatan yang diikuti oleh 9 perwakilan negara ASEAN bertujuan untuk meningkatkan kreativitas, inovasi, critical *thinking and problems solving*, kemudian *communication and collaboration*. Indonesia (ITB –Gedung *Cyber Security Center*) sebagai tuan rumah penyelenggaraan ASEAN *Cyber Kids Camp* meraih juara pertama dengan membuat animasi game dan aplikasi komputer secara mandiri menggunakan software Scrath 1.4 *programming oftware for kids.collaboration*. Berikut adalah dokumentasi kegiatan Asean *Cyber Kids camp*.



Gambar 4.4
Foto registrasi negara Philippine

Sumber: (Institut Teknologi Bandung, Laporan Kegiatan ITB-KOICA *Cyber Security Research and Development Center*, 2016: 24).



Gambar 4.5
Perkenalan antara delegasi negara ASEAN

Sumber: (Institut Teknologi Bandung, Laporan Kegiatan ITB-KOICA *Cyber Security Research and Development Center*, 2016: 24).



Gambar 4.6
Saat kompetisi ASEAN *cyber kids camp*
Sumber: (Institut Teknologi Bandung, Laporan Kegiatan ITB-KOICA *Cyber Security Research and Development Center*, 2016: 26).

4.1.1.5.3 *Cyber Wellness*

Dalam *cyber wellness* ini merupakan salah satu tri darma perguruan tinggi, dimana kegiatan ini memiliki tujuan untuk memberikan pengetahuan sejak dini mengenai *cyber* kepada para siswa dan siswi Sekolah Dasar, agar dari kecil telah mengetahui apa saja positif dan negative *cyber*.

Kegiatan pemanfaatan fungsi sosial gedung *cyber security center* terhadap masyarakat sesuai tri dharma perguruan tinggi. Kegiatan sosialisasi *cyber wellness* dilaksanakan pada Selasa, di ruang. Terdapat 100-an siswa-siswi Sekolah internet plaza gedung *cyber security center* dasar disekitaran lingkungan ITB Jatinangor yang mengikuti acara tersebut. Berikut adalah dokumentasi kegiatan sosialisasi *cyber wellness.*



Gambar 4.7
Paparan kegiatan *cyber wellness*

Sumber: (Institut Teknologi Bandung, Laporan Kegiatan ITB-KOICA *Cyber Security Research and Development Center*, 2016: 19).



Gambar 4.8
Pratikum *cyber wellness* di ruang internet plaza

Sumber: (Institut Teknologi Bandung, Laporan Kegiatan ITB-KOICA *Cyber Security Research and Development Center*, 2016: 19).



Gambar 4.9
Foto bersama kegiatan sosialisasi *cyber wellness*

Sumber: (Institut Teknologi Bandung, Laporan Kegiatan ITB-KOICA *Cyber Security Research and Development Center*, 2016: 200).

4.1.1.5.4 *Cyber Welless Training Of Turos*

Cyber welless training of turos ini didukung oleh kementerian komunikasi dan informatika Jepang, SKACI *Fundation* bekerjasama dengan ASEAN dan Istitute Teknologi Bandung *cyber security center,* menyelenggarakan salah satu kekiatan *cyber wellness traning,* acara ini bertujuan mendukung ASEAN ICT Masterplan 2020 untuk meningktkan kesadaran "kesehatan *cyber*" dan membentuk kreatifitas *cyber* di komunitas ASEAN yang terdiri dari 5 negara tetangga yaitu Thailand, Malaysia, Lao, Camboja, dan Jepang. Berikut adalah dokumentasi semejak acara berlansung.



Gambar 4.10
Kegiatan dalam *cyber wellness of tutors*

Sumber: (Institut Teknologi Bandung, Laporan Kegiatan ITB-KOICA *Cyber Security Research and Development Center*, 2017: 14).



Gambar 4.11
Peserta 5 negara ASEAN

Sumber: (Institut Teknologi Bandung, Laporan Kegiatan ITB-KOICA *Cyber Security Research and Development Center*, 2017: 12).

4.1.1.5.5 Teknologi keamanan *cyber* terhadap militer dan keuangan

Pembangunan ekonomi nasional, Indonesia mencoba untuk mempercepat peningkatan investasi di sector TIK karena ICT telah memberikan kontribusi yang baik kepada pertubuhan ekonomi di negara. Di dalam pengembangan yang sangat

baik dan pesat di sektor TIK memberikan kemampuan keamanan, *cyber* kemampuan dan keahlian untuk mengatasi *cyber* untuk mengatasi ancaman yang datang. Program ini bertujuan untuk membuat kesadaran dan menambahkan wawasan.

4.1.1.6 Bidang Riset dan Pengembangan *Cyber Security*

4.1.1.6.1 Pendidikan

Riset dan pengembangan *cyber security* ini dilakukan S2 dan S3 bidang *cyber security*. Kegiatan perkuliahan yang berlangsung di gedung *cyber security* R&D *center* yaitu beberapa kegiatan :

a. Program magister teknik elektro jalur pilihan kepemimpinan teknologi informasi chief informasi *officer* (CIO)
b. Program magister program elektro jalur pilihan layanan teknologi informasi (LTI)
c. Program magister teknik elektro jalur pilihan rekayasa dan manajemen keamanan informasi (RMK)
d. Program magister informatika jalur pilhan Teknologi Informasi (TI).

Dalam materi pembelajaran yang berupa matematika lanjutan, Operasi keamanan dan incident response, kriptografi dan aplikasinya, keamanan perangkat lunak, manajemen resiko keamanan informasi, jaringan keamanan dan sosial, manajement pengembangan aplikasi, rekayasa layanan teknologi informasi, pembelajaran multimedia, manajemen proyek dan akuisisi system operasi, *crptography implementation*, metode penelitian, keamanan komputer dan jaringan, digital *forensic* dan komputer *crime*.



Gambar 4.12
Dokumentasi proses pembelajaran

Sumber: (Institut Teknologi Bandung, Laporan Kegiatan ITB-KOICA *Cyber Security Research and Development Center*, 2016: 6).

4.1.1.6.2 Kerjasama antara Gedung *Cyber Security Center* Institut Teknologi Bandung dan Global *Young Business Manager* (YBM) Indonesia

Kerjasama dibidang pendidikan antara institute teknologi bandung (ITB) dan Daewoo Global YBM Indonesia dilakukan dari pada tahun 2015. Program ini dibuat untuk memberikan kemampuan 40 siswa-siswa Korea dalam mengenal budaya dan mempelajari Bahasa Indonesia. Berikut adalah dokumentasi kegiatan kerjasama:



Gambar 4.13
Siswa-siswi Korea

Sumber: (Institut Teknologi Bandung, Laporan Kegiatan ITB-KOICA *Cyber Security Research and Development Center*, 2016: 10).



Gambar 4.14
Mahasiswa riset dan pengembangan

Sumber: (Institut Teknologi Bandung, Laporan Kegiatan ITB-KOICA *Cyber Security Research and Development Center*, 2016: 11)

4.1.2 Uji Validitas dan Reabilitas

Dalam sebuah penelitian, subjek penelitian atau informan sangatlah penting, bahkan hal tersebut merupakan kunci utama. Sebab subjek penelitian adalah orang yang bener-bener mengetahui dan terlibat dalam suatu penelitian, serta mendukung peneliti untuk memperoleh data atau informasi yang nantinya data tersebut akan diolah, dianalis, dan disusun secara sistematis oleh peneliti. Dalam hal ini, peneliti memastikan dan memutuskan siapa yang berhak memberkan informasi yang relavan sehingga mampu menjawab pernyataan peneliti.

Dalam hal ini peneliti telah memperoleh data dari beberapa sumber yang dilakukan yaitu melalui studi pustaka yang berupa tulisan artikel, buku, jurnal dan penulusuran data secara online yang berupa data dari situs-situs tertentu, serta metode dokumentasi berupa dokumen, buku, surat kabar, dan lain sebagainya serta dengan melakukan wawancara dengan lembaga yang dituju. Uji validitas dan reabilitas yang yang diperoleh yaitu melalui situs pemerintahan, lembaga yang terkait yaitu di gedung *cyber security* R&D *Center* Institut Teknologi Bandung

(ITB). Dalam pengujian validitas dan reabilitas mengenai data-data yang di butuhkan peneliti yang berupa kerjasama *Korea International Coorporation Agency* (KOICA) dan pemerintah Indonesia dalam pengembangan *cyber security*, peneliti melakukan situs resmi yang berupa ITB, Seoul, kominfo, *trity* kemlu dan situ lainnya. Dalam situs tersebut terdapat beberapa informasi yang dapat di uji kebenaranya serta dapat dipertanggung jawabkan kebenaranya.

4.2 Analisis Hasil Penelitian dan Pembahasan

4.2.1 Upaya-Upaya Kerjasama *Korea International Coorporation Agency* (KOICA) dan Pemerintahan Indonesia dalam Pengembangan *Cyber Security*

Kerjasama internasional merupakan bentuk hubungan yang dilakukan oleh suatu negara dengan negara lain yang bertujuan untuk memenuhi kebutuhan rakyat dan untuk kepentingan negara - negara. Adapun berbagai bentuk kerjasama internasional yang meliputi kerjasama di bidang politik, sosial, pertahanan keamanan, kebudayaan, dan ekonomi berpedoman pada politik luar negeri masing-masing negara. Dalam suatu kerjasama internasional bertemu berbagai macam kepentingan nasional dari berbagai negara dan bangsa yang tidak dapat dipenuhi di dalam negerinya sendiri (Perwita & Yani, 2005:33).

Dalam menjalin kerjasama tidak hanya melaksanakan kerjasama begitu saja tanpa ada foktor-faktor yang mempengaruhi, dimana salah satu foktor terbentuknya kerjasama ini yaitu perbedaan ilmu pengetahuan dan teknologi, dan Sumber Daya Manusia (SDM). Perbedaan ilmu pengetahuan dan teknologi yaitu

kemampuan dan penguasaan ilmu pengetahuan dan teknologi serta ketrampilan antara satu negara dengan negara yang lain tidak sama contohnya pengetahuan dan teknologi Korea Selatan lebih mendominan dibandingkan dengan Indonesia dan perbedaan Sumber Daya Manusia (SDM). Di Indonesia Sumber Daya Manusia (SDM) sangat kurang dalam konteks *cyber security*, Indonesia hanya memilik 50 ahli *cyber security* dengan jumlah penduduk yang banyak dibandingkan dengan Korea Selatan yang memiliki penduduk tidak sebanyak dengan indonesia tetapi mempunyai 200 ahli *cyber* .

Dalam menjalankan kerjasama membutuhkan upaya-upaya dalam melaksanakan kerjasama tersebut, upaya-upaya tersebut merupakan proses dari berjalannya suatu kerjasama menjadi tercapai.

Dalam hal ini upaya-upaya dalam kerjasama memiliki prinsip yaitu :

1. Memperkenalkan kebudayaan nasional, hasil-hasil pembangunan, dan daerah-daerah tujuan wisata.
2. Pertukaran pelajar, mahasiswa, pemuda, dan kegiatan olahraga dalam skala internasional
3. Berperan aktif dalam menyelesaikan permasalahan dunia yang bertentangan dengan nilai-nilai kemanusiaan dan keadilan.
4. Konstruktif dan konsisten dalam perjuangan masalah dunia yang bertantangan dengan nilai-nilai kemausiaan dan keadilan.
5. Kemampuan antisipasi dan penelesaian terhadap perkembangan, perubahan dan gejolak dunia melalui jalur diplomasi disertai dengan pendekatan yang tepat sesuai dengan kepentingan nasional. Termasuk

didalamnya aktif mengawasi jalanya kerjasama internasional, baik melalui LSM, media massa, atau lembaga lainnya.

6. Pengalaman dan pemupukan solidaritas, kesatuan, dan sikap kerjasama di antara negara-negara berkembang maupun negara maju, dilakukan untuk memanfaatkan forum organisasi internasional.
7. Tidak membuat isu negatif dari proses dan hasil kerja sama, tetapi berpartisipasi aktif dalam upaya mendukung kerjasama yang positif.
8. Jujur dan terbuka dalam menjelaskan kerjasama dan hasil-hasilnya kepada masyarakat, tidak untuk kepentingan suatu kelompok tertentu.
9. Meningkatkan kegiatan ekonomi, tukar menukar ilmu pengetahuan dan teknologi dalam rangka untuk memperkokoh persatuan dan ketahanan nasional masing-masing negara serta terwujudnya kawasan dunia yang aman, bebas, netral, sejahtera, dan bebas dari bahaya senjata nuklir (http://www.edukasippkn.com, diakses pada tanggal 24 Juli 2017).

Menurut hasil wawancara dengan Dr. Yusep Rosmansyah selaku Kepala Pusat *Cyber Security* yaitu dalam tahap yang dilakuakan pemerintahan Indonesia dan Institut Teknologi Bandung (ITB) dalam kerjasama dengan *Korea International Coorporation Agency* (KOICA) dimana upaya dalam proses kerjasama ini memiliki empat tahapan yang dilakukan dalam terciptanya kerjasama tersebut yaitu sebagai berikut:

1. Join Conference

Joint coneference yaitu pertemuan atau pertukaran untuk berunding atau bertukar pendapat tentang permasalahan yang dihadapi. Pertukaran atau bertukar

pendapat tersebut membicaran mengenai ancaman dan kasus-kasus yang terjadi oleh kedua negara. Masalah-masalah yang dibicaran yaitu kasus-kasus *cybercrime* yang terjadi antara kedua negara, yaitu di indonseia pada tahun 2003 yaitu kasus *carding, carding* merupakan kejahatan pencurian nomor kartu kredit miliki orang lain dengan menggunakan transaksi perdagangan di internet, *defacing* yang dilakukan Australia kepada pejabat pemerintah Indonesia untuk memata-matai aktifitas dan kegiatan di Indonesia, begitupun serangan *cyber* yang dihadapi Korea Selatan yang mendapatkan serangan *cyber* dari Korea Utara dan Amerika (Hasil wawancara dengan Bapak Yusep Rosmansyah).

Dimana Indonesia mendapatkan masalah mengenai *cyber security* dan Korea Selatan dimana sering mendapatkan serangan *cyber* dari Korea Utara dan Amerika. dalam menghadapi ancaman dalam menyelesaikan permasalahan tersebut maka di adakan pertemuan *Joint Conference* ini dilakukan oleh pihak *Korea International Coorporation Agency* (KOICA) dan dari indonesia Bapak kepada *cyber security* Dr. Yusep Rosmansyah, pertemuan yang bertempat di Bali membicarakan mengenai pemasalahan *cyber* yang terjadi di Indonesia yang semakin meningkat seiring dengan meningkatnya teknologi yang canggih. Dengan seiring berjalannya waktu kerjasama ini dapat dijalankan oleh kedua negara ini dalam mencetak Sumber Daya Manusia (SDM).

2. Kekeluargaan

Indonesia sangat menjunjung tinggi nilai kekeluargaan, maka dalam upaya untuk membentuk kerjasama yang baik dibentuk hubungan kekeluargaan yang erat antara Indonesia dan Korea Selatan. Hubungan kekeluargaan ini membawah

berkah untuk terbentuknya kerjasama. Kerjasama ini juga merupakan salah satu interaksi sosial antara individu dan individu lainnya untuk bersama membangun atau mewujudkan cita-cita yang berupa kerjasama ini dapat membawa koalisi yaitu dengan cara menggabungkan diri untuk mencapai tujuan yang sama (Hasil wawancara dengan Bapak Yusep Rosmansyah).

3. Mencari peluang kerjasama riset

Mencari peluang kerjasama riset ini diadakan untuk mencari tenaga-tenaga ahli dalam bidang *cyber security* untuk dapat bekerjasama. Mencari peluang riset merupaka untuk memperkuat kerjasama dalam mencapai keberhasilan bersama (Hasil wawancara dengan Bapak Yusep Rosmansyah).

4. Pendanaan

Dalam melakuakan kerjasama antaran *Korea International Coorporation Agency* (KOICA) dan pemerintahan Indonesia di mana pelaksanaannya di Institut Teknologi Bandung (ITB), dimana dalam pemprosesan kerjasama tersebut membutuhkan dana untuk berlangsungnya kegiatan yang di capai, pendanaan dalam kerjasama ini diberikan oleh Korea Selatan untuk untuk menjalankan kerjasama ini, danah yang diberikan Korea Selatan senilai 55 Milliar, dengan tujuan untuk pembangunan gedung *cyber security*, infrastuktur, saran dan prasarana. Pendanaan tersebut bermaksud untuk mencari para ahli *cyber* yang memiliki pengetahuan tentang *skill* strategi dan kemampuan dalam dunia *cyber* (Hasil wawancara dengan Bapak Yusep Rosmansyah).

Dengan adanya upaya-upaya yang dilakukan diatas dengan melihat banyaknya ancaman didunia maya yang dialami Indonesia dan Korea Selatan didorong oleh kamauan dan niat yang kuat sehingga terciptalah kerjasama antaran *Korea International Coorporation Agency* (KOICA) dan pemerintahan Indonesia dalam pengembangan *cyber security* yang telah di resmikan pada tahun 2013. Dengan adanya kerjasama telah membantu kedua negara dalam bidang keamanan *cyber*. Pembentukan berupa membuat program-program kerjasama pendidikan dan riset pengembangan.

Upaya-upaya yang dilakukan oleh Korea Selatan sendiri yaitu, pemberian hibah dan fasilitas tentang pendidikan dan riset pembangunan, dalam pendanaan Korea Selatan ikut serta dalam pendanaan dalam kerjasama tersebut, fasilitas dan infrastuktur diberikan untuk memudahkan aktifitas karyawan dan para pelajar yang berupa fasilitas pembelajaran dan trasportasi dan beberapa dosen ahli *cyber* ini bukan hanya melatih dan para programmer dan *hacker* yang ada di dalam negerinya sebagai *cyber army* tetapi para ahli *cyber* ini didatangkan untuk mengajar dan membagikan pengalaman *cyber* yang dimiliki.

Diketahui bahwa Korea selatan merupakan negara yang telah mengambil langkah yang signifikan untuk memperkuat kemampuan dunia mayanya termaksud dengan mengembangkan *firewell*, memperkerjakan spesialis *cyber*, membentuk komando perang dunia maya, memajukan organisasi dan mendorong kerangka hukum ke depan yang mendukung perlindungan *cyber* dan bekerjasama dengan negara lain contohnya Indonesia, Jepang dan Tiongkok untuk bersama-sama mengatasi kejahatan dunia maya untuk sekarang dan yang akan datang.

Upaya Korea Selatan dalam mengatasi tingginya dan banyaknya *cyber* maka Korea Selatan ini membentuk badan-badan yang bertanggung jawab yaitu Pusat Keamanan *Cyber* Nasional Badan Keamanan dan Internet dan Penanggulangan Teorisme Nasional. Badan-badan yang dibentuk dalam negara nya telah berhasil dalam mencegah terjadinya ancaman dari luar contonya yaitu serangan yang dilakukan Korea Utara dapat dicegah.

4.2.2 Kendala Kerjasama *Korea International Coorporation Agency* (KOICA) dan Pemerintahan Indonesia dalam Pengembangan *Cyber Security*

Kendala dalam kerjasama merupakan suatu hal yang sering terjadi ketika pemerintah, lembaga, atau badan maupun individu yang melakukan suatu kerjasama pasti dan ada saja kendala-kendala dalam kerjasama tersebut, di mana dalam kendala tersebut tentunya ada keinginan untuk memperbaiki kendala sehingga menjadi satu kerjasama yang berjalan dengan lancar tanpa gangguan didalamnya. Dimana dalam kendala tersebut kedua belah pihak yang terikat dalam kerjasama harus maumpu memberikan apa yang seharusnya diberikan untuk memudahkan pencapaian kerjasama tersebut contohnya yaitu dapat memberikan atau menciptakan sarana dan prasarana dengan baik apabila itu merupakan satu kendala dalam kerjasama.

Cyber security merupakan satu kendala yang dihadapi sekarang sekarang ini dimana banyak sekali *malware-malware* yang datang dan merusak komputer pengguna. Kendala merupakan halangan atau keadaan yang membatasi dalam mencapai apa yang di tuju. Maka Indonesia dan Korea Selatan membentuk kerjasama dalam pengembangan *cyber security*. Menurut hasil wawancara pada

tanggal 24 Juli 2017 dengan bapak kepala pusat *cyber security* mengatakan bahwa Kendala yang di hadapi Pihak Institut Teknologi Bandung (ITB) selaku penyelenggara atau wadah dalam aktifitas pengembangan *cyber security*.

1. Kendala kerjasama yang pertama yaitu Institut Teknologi Bandung (ITB) tidak mengetahui awalnya tentang danah hibah yang diberikan oleh Korea Selatan untuk pengembangan *cyber security* maka dari itu Institut Teknologi Bandung (ITB) mencari danah dalam pengembangan *cyber security* ini di berbagai instani dan lembaga (Hasil wawancara dengan Bapak Yusep Rosmansyah).
2. Kendala bagi kerjasama susahnya mencari kemampuan ahli penyidik dan alat bukti dimana polri masih sangat minim dalam penguasaan operasional komputer serta kemampuan dalam melakukan penyedikan terhadap kasus-kasus kejahatan dunia maya sangat rendah, dimana penulis melihat bahwa faktor-faktor yang berpengaruh dalam kendala-kendala yang dihadapi adalah, kurangnya pengetahuan mengenai pengoperasian mengenai komputer dan internet dalam *cyber*, pengetahuan teknis dan pengalaman para penyidik dalam menangani kasus-kasus *cybercrime* masih terbatas, dan yang ketiga yaitu faktor system pembuktian yang menyulitkan para penyidik. Dalam ketiga faktor tersebut untuk dapat mengatasi masalah-masalah semacam yang disebutkan diatas maka dalam pengetahuan mengenai komputer lebih ditingkatkan, karena komputer merupakan alat yang dipakai untuk mengelola data, komputer merupakan perangkat keras (*Hardware*) dan

didalam perangkat keras menggunakan perangkat lunak (*Software*) yang beroperasi (Hasil wawancara dengan Bapak Yusep Rosmansyah).

Ada pula beberapa jenis kendala yang dihadapi yaitu sebagai berikut :

1. Kendala Manajerial Kendala manajerial dibutuhkan oleh perusahaan atau organisasi dimana para pejabat yang terlibat dalam ruang lingkup penerapan dengan tujuan menerapkan keamanan informasi adalah untuk menyusun sebuah system manajemen. Komitmen dari manajemen sangat berpengaruh kepada inplementasi suatu organisasi atau perusahaan. Dengan tidak adanya komitmen yang jelas suatu system tidak akan berjalan dengan baik begitupun dengan manajemen, manajemen baik maka akan berpengaruh terhadap sistem yang baik
2. Kendala Sumber Daya Manusia (SDM)

   Kendalah satu ini yaitu kendalah yang muncul baik pada organisasi, kerjasama, dan perusahaan. Dibawah ini adalah macam-macam kendala Sumber Daya Manusia (SDM) yaitu : kurangnya pemahaman, yang dimaksud dengan kurangnya pemahaman ini yaitu kurangnya memahami mengenai dunia *cyber.*
3. Tidak adanya sosialisasi terhadap penerpan keamanan informasi.
4. Kurangnya tenaga ahli dalam keamanan informasi sehinga apa yang diterapkan atau dilakukan sulit terselesaikan.
5. Kendala teknikal, kendala yang satu ini sangat menghambat dalam kerjasama yaitu kurang teknologi informasi dan komunikasi yang mendukung dapat menjadi faktor penghambat penerapan di karenakan

kurang akruratnya estimasi sehingga dapat mengambat kerjasama yang dilakukan.

Adapun hal-hal yang membuat timbulnya kejahatan dan merupakan kendala yang harus dihadapi dalam kerjasama dalam pengembangan *cyber security* yaitu:

1. Banyaknya *software-software* untuk melakukan hal yang jahat yaitu penyusupan yang dapat di *download* secara geratis
2. Meningkatnya kemampuan pengguna internet
3. Kurangnya hukum yang mengatur
4. Disentralisasi *server* sehingga lebih banyak system yang harus ditangani, sementara Sumber Daya Manusia (SDM) terbatas
5. Meningkatnya aplikasi bisnis yang menggunakan internet
6. Banyaknya *software* yang mempunyai kelemahan
7. Banyaknya pengguna komputer dan internet
8. *Software* yang dipakai untuk audit dengan cari mencari kelemahan yang digunakan untuk melakukan *scming system* orang lain.

Adapun permasalahan terkait dengan pengembangan *cyber security* yaitu:

1. Lemahnya pemahaman penyelenggara negara atas *security* terkait dengan dunia *cyber* yang memerlukan pembatasan penggunaan layanan yang servernya berbeda diluar negeri dan diperlukan adanya penggunaan secures sistem.
2. Legalitas penanganan penyerangan di dunia *cyber*.
3. Pola kejadian *cybercrime* sangat cepat sehingga sulit ditangani.

4. Tata kelola *cyber security* nasional.
5. Rendahnya *awerness* atau kesadaran akan adanya ancaman.
6. Masih lemahnya industri nasional yang memproduksi dan mengembangkan perangkat keras terkait dengan teknologi informasi.

Cyber security di Indonesia dan Korea Selatan perlu diatur tentang berbagai elemen yang terkait dengan *cyber security* dalam berbagai kebijakan yang mengatur teknologi informasi komunikasi dan yang digunakan yang meliputi dokumen standar yang dijadikan pedoman untuk menjalankan semua proses yang menyangkut dengan keamanan informasi, standar internasional dalam menghadapi serangan *cyber* yang didalamnya terdapat *perimeter denfense* yang memadai dan adanya *network monitoring system.*

4.2.3 Prospek Kerjasama *Korea International Coorporation Agency* (KOICA) dan Pemerintahan Indonesia dalam Pengembangan *Cyber Security*

Prospek merupakan sesuatu gambaran keberlangsungan ide di masa depan yang berupa peluang yang masih harus diadaptasikan dengan berbagai keterbatasan dan kondisi yang melingkupinya, prospek kerjasama antara Korea Selatan dan pemerintahan Indonesia dalam kerjasama pengembangan *cyber security* ini tentunya mempunyai prospek untuk kedepannya yang dimana setiap kegiatan menginginkan ataupun aktifitas adanya keinginan maupun harapan untuk masa yang akan datang tentunya. Dalam kerjasama ini prospek merupakan faktor yang terpenting dalam kerjasama, dimana ada prospek disitulah ada target pencapain yang harus di tata dan harus di perbaiki sehingga apa yang diinginkan

ataupun apa yang diharapkan akan menjadi satu kemunculan prospek yang diingginkan dalam kerjasama.

Dari hasi wawancara tanggal 24 Juli 2017 dengan Bapak Kepala Pusat *cyber security* R&D *center* memberikan 4 (empat) prospek dalam kerjasama pengembangan *cyber security* yaitu:

1. Kerjasama KOICA dan pemerintahan Indonesia membentuk suatu kerjasama yang merupakan kerjasama dalam pengembangan *cyber security* dimana Indonesia merupakan negara yang banyak menghadapi *cyber threats* dari negara lain, yang bertujuan dengan kepentinganya tersendiri. Prospek kerjasama yang pertama yaitu diharapkan dalam kerjasama ini dapat menghasilkan para tenaga yang benar-benar mempunyai *skill* dalam mecegah terjadinya ancaman yang datang dari serangan dalam negeri maupun luar negeri.
2. Prospek yang kedua yaitu menciptakan kerjasama ini menjadi kerjasama yang berperan penting dalam menangani masalah-masalah dunia maya, terutama bagi Indonesia dalam mencegah dan menangani masalah-masalah *cyber threats* untuk membantu kedua negara, yang di maksud yaitu menciptakan kerjasama untuk memberikan pengetahuan dan wawasan mengenai ancaman dan dapat mengambil peran lebih besar dan perang yang penting dalam menghadapi ancaman seluruh masalah dunia maya.
3. Prospek ketiga yaitu diharapkan kerjasama ini dapat membawa dampak-dampak positif bagi Indonesia maupun Korea Selatan, serta dapat

memberikan semangat bagi para calon pelajar yang ingin mempelajari mengenai *cyber security*.

4. Prospek yang keempat yaitu di mana prospek kerjasama ini dapat membuai hasil dengan mendirikan sebuah pertahanan nasional *cyber security* sehingga dengan mudah untuk memantau, mencegah, melindungi dari ancaman *cyber* yang datang, dimana dilihat Korea Selatan yang merupakan negara yang penduduknya lebih sedikit dibandingkan Indonesia, tetapi Korea Selatan ini memiliki 3 (tiga) pertahanan nasionalnya mengenai dunia *cyber* yaitu pusat keamanan *cyber nasional* , badan keamanan dan internet, dan penanggulangan terorisme nasional. Korea Selatan dalam membentuk 3 (tiga) badan dalam penanganan *cyber threats* karena Korea Selatan memandang bahwa *cybercrime* merupakan salah satu ancaman yang dapat memberikan kerugian yang sangat besar bagi negarannya maka Korea Selatan membentuk badan-badan *cyber security* dengan tujuannya yaitu melindungi rakyatnya, menjamin keamanan nasional, melindungi jaringan *cyber* pemerintah dan institusi publik dari ancaman *cyber*. Selain itu Korea Selatan mendirikan sekolah *cyber* untuk meningkatkan para calon-calon *cyber* untuk membantu negara dalam memberantas serangan atau ancaman yang datang di kemudian hari.

Korea Selatan tidak luput dari berbagai *cyber threat* yang mengancam keamanan nasionalnya karena Korea terhubung dengan jaringan dan penggunaan perangkat mobile yang tinggi. Menurut Akamai Cloud Amerika Serikat pada kurtal pertama tahun 2017 yaitu 97%

penduduk Korea Selatan memiliki akses internet, dimana Korea Selatan memiliki kecepatan internet di dunia yaitu 26,9 Mbps. Keamanan dunia maya telah menjadi prioritas utama keamanan nasional Korea Selatan, dimana Korea Selatan menggambil langkah yang signifikan untuk memperkuat kemampuan *cyber*, termasuk pengembangan *firewall*, memperkuat spesialisasi *cyber*, mengambil komando perang *cyber*, memajukan organisasi pendidikan, dan mendorong karangka hukum ke depan yang didukung perlindungan *cyber*.

Serta dalam kerjasama tersebut dapat memberikan 4 langkah-langkah yang harus di perhatikan dan dipelajari dalam kerjasama ini yaitu:

1. *Network security*

   Dalam menjaga keamanan *cyber* maka yang dilakukan yaitu keamanan jaringan, merupakan salah satu prospek dalam kerjasama *Korea International Coorporation Agency* (KOICA) dan pemerintahan Indonesia. *Network security* ini telah dipergunakan untuk keamanan *cyber security* di Indonesia saat ini. lima ancaman terhadap sistem komputer dengan contohnya yaitu:

Tabel 4.1

Ancaman terhadap sistem komputer

Ancaman	Pengertian	Contoh
Interupsi	Sumber system computer dihancurkan atau menjadi tidak tersedia dan tidakberguna	Bagian pengrusakan terhadap perangkat keras
Intersepsi	Diartikan yaitu ancaman terhadap kerahasiaan	Penyadapan terhadap data yang bersifat rahasia
Modifikasi	Medifikasi ini berupa ancaman tidak hanya merusak data tapi merusak sumber daya	Merusak file-file data dan mengubah program sehinga berbeda
Fabrikasi	Yang dimaksud yaitu memasukan data-data palsu ke sistem komputer	Pesan-pesan palsu yang sering di temukan di jaringan/aplikaisi.

Sumber: (http://si200.ilearning.me, diakses pada tanggal 26 Juli 2017).

Dari tabel diatas dilihat bahwa 4 kejahatan yang menyakut ancaman yang sering terjadi pada komputer, yang harus diperhatikan setiap saat. Sehingga terhindar dari ancaman dari luar. Begitupun ancaman-ancaman dapat dikatagorikan menjadi 3 (tiga) yaitu kumpulan jenis serangan teknologi dan informasi menjadi alat atau senjata utama untuk melakukan kejahatan yaitu : komputer dan internet dipergunakan sebagai alat dan medium untuk menyebarkan aliran-aliran sesat, telpon dimanfaatkan untuk mengirimkan pesan-pesan atau SMS yang menipu para calon korban, elektronik mail dipakai sebagai saran untuk mengirimkan gambar-gambar atau vidio bernuansa pornografi dan sebagainya.

Kedua yaitu kumpulan peristiwa ancaman dimana komputer atau teknologi informasi menjadi sarana pusat serangan dari pelaku tindakan kejahatan, yaitu melakukan transaksi keuangan fiktif dalam sebuah system perbankan berbasis internet, menghentikan kerja sebuah jaringan internet di instansi-instansi bisnis maupun pemerintah, dan dapat menyebarkan virus untuk menggangu kinerja komputer-komputer tertentu.

Ketiga ancaman yang ditujukan untuk merusak (memodifikasi) file, data atau informasi yang tersimpan didalam media perangkat teknologi informasi, yang dimaksud yaitu merubah isi sebuah situs tanpa sepengetahuan pemiliknya, mengambil sekumpulan *password* informasi lengkap kartu kredit untuk disalahgunakan, merusak basis data utama sehingga data para pemilik sehingga data tidak dapat terbaca.

2. *Mobile*

Mobile merupakan perangkat yang mudah untuk dibawa kemana-mana. *Mobile* ini berasal dari dua kata yaitu perangkat dan *mobile*. perangakat dapat diartikan alat perlengkapan dan *mobile* yang berarti ringan tangan dan dapat dibawa kemana-mana. Contohnya handphone, smartphone yang dapat dibawa kemana-mana dengan kecanggihan nya yang di utamakan.

3. *Information manajemen*

Serangan sub sistem informasi yang menyeluruh dan terkoordinasi dan secara rasional terpadu yang mampu mentransformasi data sehingga menjadi informasi dengan serangkaian cara guna meningkatkan produktivitas yang sesuai dengan gaya dan sifat manajer atas dasar kriteria mutu yang telah diterapkan.

4. *Ditation malware development*

Kejahatan yang sering terjadi di Indonesia yaitu sebagai berikut :

1. Pencurian terhadap data merupakan tindakan kriminal di dalam dunia *cyber,* dimana akan ada penyusup ang masuk kedalam data pribadi dan mengambil tanpa izin. Pencurian data ini bersifat pribadi dan rahasi, biasanya para *hacker* ini mengambil data-data negara yang bersifat penting.disinilah dibalik lalu lintas banyak penyusupan dan mecari cela untuk mengambil data tersebut.
2. Akses terhadap jaringan internet yaitu perangkat pendukung yang dibutuhkan yaitu *software* dan *hardwa*re untuk menjalankan browser, setelah kedua perangkat telah terpenuhui maka dibutuhkanlah modem agar dapat terhubung ke internet dimana untuk menjalankan maka membutuhkan *software* yang menjalankan. *Software* merupakan perangkat lunak dari komputer untuk menjalankan perangkat keras kepada penyedia informasi seperti, interner *exploler*, sistem operasi, *microsoft outlook*.
3. Perubahan terhadap data-data penting yaitu perubahan yang dilakukan untuk menghancurkan file maupun data. Data disini yang berupa angka maupun alphabet, maupun simbol khusus seperti (#*/$) yang disusun dan diolah dalam bentuk struktur data, struktur file dan basis data.
4. Pencurian informasi dan berujung pada penjualan informasi yaitu data atau informasi yang didapatkan oleh peretas yang bersifat pentik seperti data atau file negara yang bersifat penting kemudian di jual kepada pihak yang bersangkutan dengan jumlah imbalan upah yang didapatkan.

Dengan empat kejahatan dan sembilan *malware* ini membuat kerjasama ini membuat prospek dari sekarang untuk mencegah terjadinya kejahatan yang telah disebutkan diatas. Prospek-prospek yang dilakukan untuk mengurangi ancaman yang datang dari dalam negeri mapun dari luar negeri.