

## **BAB II**

### **TINJAUAN PUSTAKA**

#### **1.1 Literatur Riview**

Dalam penelitian yang dilakukan oleh penulis mengenai *Kerjasama Indonesia-Australia dalam Meningkatkan Cyber Security di Indonesia*. Literatur mengenai kerjasama antar negara di bidang *cyber* cukup banyak karena perkembangan teknologi. Penulis memfokuskan bahasan dalam upaya meningkatkan *cyber security* di Indonesia.

Jurnal DPR RI yang ditulis oleh Handrini Ardiyanti dengan judul “**Cyber-Security dan Tantangan Pengembangannya Di Indonesia**” berpendapat bahwa Indonesia saat ini tengah dalam keadaan mendesak *cyber-security* atau keamanan dunia maya karena melihat kenyataan bahwa tingkat kejahatan di dunia maya atau *cybercrime* di Indonesia sudah mencapai tahap memprihatinkan. Data yang dihimpun oleh CIA menyebutkan bahwa kerugian yang disebabkan karena tindak kejahatan *cyber* di Indonesia telah mencapai 1,20% dari tingkat kerugian akibat *cybercrime* yang terjadi di dunia.

Kebijakan *cyber security* yang telah dijalankan di Indonesia telah diinisiasi sejak tahun 2007 dengan dibentuknya *Indonesia Security Incident Response Team on Internet Infrastructure* adalah Tim yang ditugaskan Menteri Komunikasi dan Informatika (Kominfo) untuk membantu pengawasan keamanan jaringan berbasis protokol internet. Tugas dan fungsi dari ID-SIRTII di antaranya melakukan pemantauan, pendeteksian dini, peringatan dini terhadap ancaman dan gangguan pada jaringan, berkoordinasi dengan pihak-

pihak terkait di dalam maupun luar negeri didalam menjalankan tugas pengamanan jaringan telekomunikasi berbasis protokol internet, mengoperasikan, memelihara dan mengembangkan sistem database sistem ID-SIRTII dengan upaya penyusunan katalog dan silabus yang berkaitan dengan proses pengamanan pemanfaatan jaringan, memberikan layanan informasi atas ancaman dan gangguan keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis protokol internet, menjadi *contact point* dengan lembaga terkait tentang keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis protokol internet serta menyusun program kerja dalam rangka melaksanakan pekerjaan yang berkaitan dengan keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis protokol internet.

Literatur lainnya hasil penelitian skripsi yang di tulis oleh Elin Konstantia Novel dalam judul **“Kerjasama Indonesia-Korea Selatan Dalam Mengimplementasikan *Cyber security* dengan Studi Kasus *Cyberporn*”** berpendapat bahwa *Cyberporn* sebagai salah satu bentuk *cybercrime* dalam konteks hukum era global dengan perluasan pengertian tertentu pada prinsipnya sudah dapat dikategorikan dalam jenis tindak pidana, hanya saja hukum untuk menjeratnya masih memiliki beberapa titik lemah terutama menyangkut yurisdiksi teritorial serta kelemahan ketika berhadapan dengan jenis kejahatan korporasi.

Elin Konstantia Novel menyebutkan pada abad ke-20, *cyberporn* di Korea Selatan berkembang semenjak munculnya "majalah pria" seperti *Playboy* dan *Modern Man* pada 1950-an. Sebagai salah satu negara di Asia Tenggara,

Indonesia merasakan dampak negatif dari pemanfaatan internet. Pada tahun 2011, Menteri Negara Komunikasi dan Informasi Indonesia, Tifatul Sembiring, menyatakan bahwa Indonesia merupakan pengakses internet nomor tiga terbesar setelah Tiongkok dan Korea Selatan, sekaligus pengakses situs pornografi nomor dua terbesar di dunia setelah Korea Selatan dan Inggris. Para pengakses sebagian adalah remaja yang masih di bawah umur. Internet menciptakan ruang baru yang dinamakan *cyberspace* dan dapat membawa dampak baik dan dampak buruk. *Cyberporn* merupakan salah satu sisi negatif yang ada dalam *cyberspace*. Kehadiran Internet semakin mempermudah penyebaran segala bentuk media, sehingga siapapun yang menggunakan internet dan memasuki *cyberspace* berpotensi untuk menjadi korban dalam hal ini *cyberporn*. Kejahatan *cyberporn* semakin mengerikan di jaman modern ini, bahkan situs yang disebut tahan terhadap pembajakan atau *hacking* sudah dapat ditembus oleh para pelaku kejahatan *cyber*. Itulah yang membuat pemerintah Indonesia fokus terhadap masalah ini dan melakukan pencegahan dengan melakukan kerjasama bilateral bersama Korea Selatan. Proyek KOICA-ITB ini menekankan pentingnya membangun data *center* untuk mendukung kebijakan *e-government* sehingga berbagai kebijakan dan layanan pemerintah bagi masyarakat umum dapat terintegrasi dalam sistem informasi terpusat demi menanggulangi kejahatan *cyberporn* antar kedua negara.

Literatur selanjutnya, jurnal dengan judul “**Peningkatan *cyber security* ASEAN Melalui Kerja Sama *cyber security* dengan Australia**” yang ditulis oleh Sofia Trisni, Rika Isnarti Dan Abdul Halim menuturkan bahwa keamanan non-tradisional menjadi isu penting karena dampak yang ditimbulkannya tidak

kalah dahsyat dari ancaman pada isu keamanan tradisional. Salah satu isu dalam keamanan non-tradisional adalah ancaman *cyber* yang berkaitan erat dengan teknologi komputer dan internet. Perkembangan pesat teknologi komputer dan internet telah menciptakan ketergantungan yang sangat besar terhadap keduanya. Setiap aktivitas yang biasanya diawasi dengan mengandalkan tenaga manusia perlahan dialih tugaskan kepada komputer. Tidak hanya itu, internet telah mempermudah kehidupan manusia karena segala informasi dapat diakses dengan mudah hanya dari belakang meja. Ketergantungan kepada komputer dan internet ini kemudian terganggu dengan adanya serangan *cyber*. Sekitar 2.1 miliar pengguna internet, 922 juta pengguna berasal dari kawasan ASEAN dan diperkirakan jumlah ini akan terus meningkat setiap tahunnya. Australia merupakan negara dengan kondisi *cyber security* yang sangat baik. Hal ini bisa dilihat dari strategi kewanaman *cyber* yang dimiliki oleh Australia yang dirilis pada April 2016. Strategi kewanaman *cyber* Australia dibentuk atas dasar peningkatan keterhubungan melalui dunia maya oleh warga Australia yang terkoneksi dengan semua orang dipenjuru dunia. Sebagai bukti dari peningkatan tersebut adalah 90 persen warga Australia adalah pengguna internet yang aktif, sebagian besar warga Australia menghabiskan satu hari perminggu untuk mengakses internet, serta 84% bisnis baik skala medium maupun kecil di Australia telah terkoneksi dengan internet.

Australia dengan perkembangan *cyber security* yang cukup baik tetapi, Australia bukan menjadi negara terbaik di dunia dalam bidang *cyber security*. Amerika Serikat yang menjadi posisi pertama dalam *cyber security* terbaik didunia. Namun, Australia sudah cukup atau bahkan sangat baik sebagai mitra

kerjasama potensial di kawasan sekitar ASEAN dan khususnya di Indonesia sebagai negara yang memiliki tingkat *cyber security* yang mumpuni. Australia merupakan negara yang mengembangkan *cyber*nya secara serius dan Australia juga merupakan negara tetangga terdekat ASEAN yang memprioritaskan kerjasama dengan ASEAN, sehingga kerjasama ASEAN-Australia dirasa merupakan rekomendasi yang baik bagi ASEAN. Dengan bekerjasama dengan Australia diharapkan ASEAN akan mendapatkan keuntungan yaitu peningkatan *cyber security* di kawasan.

Berbeda dengan penelitian penulis dengan judul “**Kerjasama Indonesia-Australia di Bidang Keamanan dalam Mengatasi *Cyber Crime* di Indonesia melalui Program *Cyber Policy Dialogue*.”**

Penelitian ini berfokus pada strategi pemerintah Indonesia dalam upaya peningkatan *cyber security* melalui kerjasama dengan negara lain. Melalui Badan Sandi dan Siber Indonesia, Australia dipilih menjadi salah satu negara tujuan kerjasama karena faktor kedekatan teritori dan juga Australia dinilai menjadi salah satu negara dengan sistem *cyber security* terbaik di sekitar kawasan asia tenggara. Indonesia perlu segera meningkatkan *cyber security* karena kondisi *cyber security* di Indonesia semakin mengkhawatirkan.

## **1.2 Kerangka Teori**

Untuk mempermudah proses penelitian, tentu diperlukan adanya landasan berpijak untuk memperkuat analisa. Maka dari itu, dalam melakukan pengamatan dan analisa masalah yang diangkat, diperlukan landasan teori ataupun konseptual yang relevan. Kerangka teori berfungsi sebagai dasar

argumentasi untuk menjawab pertanyaan penelitian dan merupakan sumber serta landasan untuk menganalisis masalah yang diteliti.

**Rosenau** berpendapat bahwa setidaknya ada tiga unsur mengapa suatu negara membuat suatu kebijakan luar negerinya, yaitu: (1) Kebijakan luar negeri merupakan seperangkat prinsip yang menjadi dasar pelaksanaan hubungan luar negeri suatu negara, (2) Kebijakan luar negeri sebagai komitmen dan rencana yang berguna sebagai pedoman pemerintah dalam berhubungan dengan aktor-aktor lainnya di dunia internasional, (3) Kebijakan luar negeri merupakan suatu perwujudan kepentingan nasional dengan menggunakan sumber daya dalam negerinya guna mencapai tujuan yang direncanakan (Rosenau, 1976: 16).

Konsep kepentingan nasional merupakan dasar dalam memahami perilaku internasional suatu negara. Kepentingan nasional merupakan upaya negara dalam mengejar power untuk dapat mengembangkan kekuasaan atas negara lain. Menurut Donald E. Nuechterlin terdapat empat jenis dimensi kepentingan nasional, yaitu; kepentingan pertahanan, kepentingan ekonomi, kepentingan tata internasional, dan kepentingan ideologi. Kemudian Griffiths, Terry dan Roach mengatakan bahwa kepentingan nasional merupakan tujuan dari suatu negara yang dirumuskan dalam kebijakan luar negeri "*National Interest as a guide to foreign policy*" (Griffiths Martins, 2008: 217). Selanjutnya Hans J. Morgenthau berpendapat bahwa kepentingan nasional adalah: "*Power* (pengaruh, kekuasaan, dan kekuatan) atau kemampuan minimum negara-negara untuk melindungi dan mempertahankan identitas fisik, politik, dan kultur dari gangguan negara lain."

Kepentingan nasional merupakan tolak ukur atau kriteria pokok bagi para pengambil kebijakan (*decision makers*) tiap-tiap negara sebelum merumuskan dan menetapkan sikap ataupun tindakan.

Dalam hubungan internasional, suatu negara tidak akan bisa memenuhi kebutuhan negaranya secara mandiri. Artinya setiap negara membutuhkan negara lain untuk memenuhi setiap kebutuhan suatu negara, agar kebutuhan suatu negara dapat terpenuhi maka dibutuhkan suatu kerangka kerjasama, dalam konteks ini adalah kerjasama internasional. Kerjasama internasional biasanya meliputi bidang politik, sosial, pertahanan dan keamanan, kebudayaan, dan ekonomi yang mana dalam membuat suatu kerjasama setiap negara berpedoman kepada politik luar negeri masing-masing negara.

Menurut **K. J. Holsti** konsep **kerjasama internasional** adalah:

“Kerjasama dilakukan oleh pemerintah yang saling berhubungan dengan mengajukan alternatif pemecahan, perundingan atau pembicaraan mengenai masalah yang dihadapi, mengemukakan berbagai bukti teknis untuk menopang pemecahan masalah tertentu dan mengakhiri perundingan dengan bentuk beberapa perjanjian atau saling pengertian yang memuaskan bagi semua pihak”.

Bentuk kerjasama internasional dalam konteks hubungan internasional dibagi menjadi dua bentuk kerjasama yaitu kerjasama bilateral dan kerjasama multilateral.

Kerjasama bilateral adalah suatu kerjasama yang dibentuk oleh dua negara yang mencakup bidang-bidang tertentu sesuai dengan kebutuhan negara yang akan melakukan kerjasama. Suatu kerjasama baik bilateral dan multilateral memiliki

asumsi dasar bahwa dengan adanya kerjasama antar negara akan menghasilkan suatu keuntungan bagi pihak-pihak yang melakukan kerjasama.

Didi Krisna dalam kamus politik internasional, mengatakan bahwa “Hubungan bilateral adalah keadaan yang menggambarkan adanya hubungan yang saling mempengaruhi atau terjadi hubungan timbal balik antara dua pihak atau dua negara.” (Krisna, 2003: 21).

Selanjutnya menurut Sukarwarsini Djelantik mendefinisikan hubungan bilateral yaitu, “hubungan interaksi antar dua negara yang dikembangkan dan dimajukan dengan menghormati hak-hak kedua negara untuk melakukan berbagai kerjasama pada aspek-aspek kehidupan berbangsa dan bernegara tanpa mengabaikan atau mengucilkan keberadaan negara tersebut serta menunjukkan dan memberikan nilai tambahan yang menguntungkan dari hubungan bilateral itu.”(Djelantik, 2011: 69) Dengan asumsi dasar bahwa sistem internasional bersifat anarki, semua negara tentunya akan mengutamakan keamanan negaranya dari ancaman-ancaman yang akan terjadi. Menurut Buzan, setidaknya ada lima aspek yang menyangkut kewanaman yakni keamanan politik, ekonomi, sosial, lingkungan, dan militer.

### **Teori Keamanan**

Konsep kewanaman menurut Barry Buzan adalah kemerdekaan dari suatu ancaman tertentu, sehingga negara dan masyarakat memiliki kemampuan untuk mempertahankan identitas kemerdekaan dan integritas fungsional mereka dari kekuatan luar yang dianggap sebagai musuh (Buzan, 1993: 93). Selain itu, Buzan juga mengungkapkan bahwa kewanaman tidak terbatas pada kekuasaan semata,

tetapi juga menjalin suatu pola hubungan kerjasama yang bermanfaat (Buzan, 1993: 189). Dalam konsepsi klasik, keamanan lebih diartikan sebagai usaha untuk menjaga keutuhan teritorial negara dari ancaman yang muncul dari luar. Pasca berakhirnya perang dingin, membuka era baru dalam sudut pandang masyarakat akan keamanan. Keamanan tidak lagi diartikan secara sempit sebagai hubungan konflik militer saja, tetapi keamanan pada hari ini berpusat pada keamanan masyarakat atau dikenal dengan istilah keamanan non-tradisional. Keamanan non-tradisional berfokus kepada *Human Security*. Beberapa contoh keamanan non-tradisional membahas mengenai kejahatan transnasional seperti terorisme, penyelundupan manusia, senjata, kejahatan lingkungan, kejahatan hak asasi manusia, penyelundupan manusia, teknologi dan kesehatan.

Konsep keamanan nasional menurut Berkowitz adalah kemampuan dari suatu bangsa untuk melindungi nilai-nilai internalnya dari ancaman pihak luar. Dalam penelitian ini Indonesia sebagai negara yang rentan akan serangan kejahatan *cyber* melakukan beberapa kebijakan strategis dengan mengadakan kerjasama dengan Australia dalam bidang peningkatan sistem keamanan terhadap ancaman kejahatan *cyber*.

### ***Cyber Security***

Seiring dengan arus globalisasi dan juga kemajuan dari teknologi memberikan dampak kepada konsep keamanan, pandangan tradisional menyatakan bahwa ancaman keamanan selalu berbentuk fisik namun adanya pergeseran tentang persepsi ancaman pasca perang dingin memungkinkan

ancaman kemanan dapat dilakukan secara non fisik, salah satu contohnya melalui dunia maya (*cyber*).

Adanya pergeseran tentang persepsi ancaman kearah non-tradisional melalui dunia maya harus mendapatkan perhatian yang serius, negara harus membuat *cyber security*-nya sebagai upaya dalam mengamankan kemanan nasional. Ancaman serangan *cyber* tidak saja terjadi pada institusi-institusi publik, melainkan dalam beberapa kasus menyerang institusi pemerintahan. Kemanan *cyber* mencakup segala sesuatu yang berhubungan dengan pengawasan komputer, monitoring sampai kontrol yang sangat ketat atau perjuangan untuk hak asasi fundamental (Fathika Anjani Firman, 2018: 32). *Cyber security* adalah merupakan upaya untuk memastikan pencapaian dan pemeliharaan sifat keamanan organisasi dan aset pengguna terhadap resiko keamanan yang relevan dalam lingkup *cyber space* (Fathika Anjani Firman, 2018: 33).

### **Kondisi *Cyber Security* Indonesia**

Berdasarkan data yang dikeluarkan *National Cyber Security Index*, pada data yang dikeluarkan pada tahun 2018, Indonesia menempati urutan 83 dari 100 negara yang paling rentan diretas dengan nilai *security index* 19,48 poin (Rikk, 2018: 9 ). Padahal index pengembangan digital Indonesia mencapai angka 50,22, artinya *cyber security* Indonesia belum sebanding dengan perkembangan digital. Untuk Indonesia sendiri serangan *cyber* didominasi pada sektor keuangan, sektor peretasan data, menurut data Badan *Cyber* dan Sandi Negara ada sekitar 140 juta serangan *cyber* yang menyerang Indonesia.

Tentu saja hal ini akan merugikan berbagai kalangan khususnya para pelaku ekonomi Indonesia. Salah satu contohnya adalah serangan seperti *Ransomware Wanna Cry*, yang pelaku kejahatan meminta tebusan 133 ribu USD. Bisa dibayangkan berapa banyak kerugian yang dihasilkan ketika serangan *cyber* tersebut menyerang sistem keamanan Indonesia. Dalam acara *Cyber Security Indonesia* yang digelar pada 5 – 7 Desember 2018, direktur dari *Cyber Security Indonesia* Cheah Wai Hong mengatakan “Dalam menghadapi era teknologi dan digital yang semakin berkembang pesat, ketahanan nasional akan *cyber security* sangatlah penting. Hal ini mencegah tindakan-tindakan kriminal dan menjaga keamanan industry teknologi (Hafiz, 2018).

### **Kerjasama *Cyber Security* Indonesia dan Australia**

Menteri Koordinator Bidang Politik, Hukum dan Keamanan Wiranto melaksanakan pertemuan bilateral dengan menteri Urusan *Cyber Security* Australia, Dan Tehan. Pertemuan tersebut membahas mengenai peningkatan kerjasama *Cyber* Indonesia – Australia. Wiranto mengatakan bahwa tren ancaman yang ditimbulkan dari penyalahgunaan *cyberspace* saat ini makin meningkat dan rumit karena pelakunya tidak hanya dilakukan oleh negara akan tetapi aktor non negara sudah mulai ambil bagian dalam penyalahgunaan *cyberspace* (Humas Kemenko Polhukam RI, 2017). Semua negara menyadari bahwa aspek kedaulatan dan *cyber security* adalah prioritas pengelolaan bersama secara internasional dalam upaya menjaga kepentingan dan keamanan nasionalnya masing-masing. Dunia *cyber* yang tidak memiliki batas dan melibatkan banyak aktor sehingga kompleksitas permasalahannya bersifat multi-dimensi dan membutuhkan langkah

penanganan yang komprehensif Selain itu, kerja sama bilateral dengan semua negara juga dibutuhkan. Indonesia kembali menegaskan komitmennya dengan menjalin kerja sama dengan Australia. Hal ini untuk memperkuat kerja sama *cyber security* sebagaimana disepakati dalam *2+2 Dialogue* dan pertemuan *Ministerial Council on Law and Security*, dan dalam rangka membangun sektor *e-commerce* yang kuat. “Indonesia mencatat keamanan dan ketahanan *cyber* Australia yang sudah cukup maju, sehingga berharap dapat memperoleh gambaran terkait *best practice* dan *lesson learned* Australia dalam proses pendirian Australia *Cyber Security Centre (ACSC)*, strategi ketahanan *cyber* dan contoh kasus penanganan insiden serangan *cyber* (Humas Kemenko Polhukam RI, 2017).

### 1.3 Hipotesis

**Jika kerjasama Indonesia-Australia melalui program *Cyber Policy Dialogue* dapat di implementasikan maka, kasus-kasus penyerangan sistem *cyber* Indonesia dapat diminimalisir yang ditandai dengan naiknya peringkat Indeks *cyber security* Indonesia.**

### 1.4 Verifikasi Variabel

Variable dalam Hipotesis	Indikator	Verifikasi
Variable bebas: <b>Jika kerjasama Indonesia-Australia melalui program <i>Cyber Policy Dialogue</i> dapat di</b>	1. Momorandum of Understanding, Indonesia-Australia di Bidang Siber  2. Terjalannya	1. Data (fakta) adanya ancaman <i>cyber security</i> Indonesia yang menempatkan Indonesia sebagai negara yang dalam jumlah serangan <i>cyber</i> menempati urutan ke lima dari negara-negara di kawasan Asia Pasifik.

<p><b>implementasikan</b></p>	<p>kerjasama <i>cyber</i> security dengan Australia melalui program <i>Cyber Policy Dialogue</i></p>	<p>Sumber:  <a href="https://teknologi.bisnis.com/read/20190306/84/896967/ancaman-cyber-di-indonesia-terbanyak-kelima-se-asia-pasifik">https://teknologi.bisnis.com/read/20190306/84/896967/ancaman-cyber-di-indonesia-terbanyak-kelima-se-asia-pasifik</a>.</p> <p>2. Data (fakta) Laut Indonesia melakukan kerjasama dengan Australia di bidang keamanan <i>cyber</i>          Sumber:<a href="http://treaty.kemlu.go.id/apisearch/pdf?filename=AUS-2018-0240.pdf">http://treaty.kemlu.go.id/apisearch/pdf?filename=AUS-2018-0240.pdf</a>.</p>
<p>Variable Terikat:</p> <p><b>kasus-kasus penyerangan sistem <i>cyber</i> Indonesia dapat diminimalisir yang ditandai dengan naiknya peringkat Indeks <i>cyber</i> security Indonesia</b></p>	<p>1. Adanya peningkatan indeks keamanan <i>cyber</i> Indonesia</p>	<p>1. Meningkatnya Global Security Index Indonesia naik 29 peringkat ke posisi 41 dari 175 negara Sumber:  <a href="https://inforial tempo.co/info/1001099/indeks-keamanan-cyber-indonesia-naik-29-tingkat">https://inforial tempo.co/info/1001099/indeks-keamanan-cyber-indonesia-naik-29-tingkat</a></p>

### 1.5 Alur Skema



