BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Arus globalisasi yang cukup cepat membuat pengaruh di berbagai bidang kehidupan. Bidang teknologi menjadi salah satu sektor yang tidak bisa menolak arus globalisasi. Globalisasi menurut Selo Soemardjan merupakan suatu proses terbentuknya sistem komunikasi dan organisasi antar masyarakat yang ada di seluruh dunia. Dengan terus berkembangnya teknologi dari masa ke masa akibat arus globalisasi menjadikan akses yang mudah serta membantu kehidupan manusia sekarang menjadi dinamis.

Perkembangan teknologi informasi dan komunikasi yang pesat membuat segala sesuatu menjadi mudah didapatkan baik itu berupa informasi maupun data dari dalam dan luar negeri. Dampak yang besar dalam pertukaran informasi dan data ini pun membuat hubungan antar negara menjadi mudah dilakukan. Negara maju terus mengembangkan teknologi agar masyarakatnya lebih mudah dan praktis dalam mengolah maupun mendapatkan informasi dan data. Begitu juga dengan negara berkembang yang juga terus mengembangkan teknologi agar tidak tertinggal dan dapat bertahan di era globalisasi.

Teknologi informasi yang menjadi penting dalam dunia kehidupan sekarang ini membuat negara dan individu terbantu dalam penyampaian dan penyebarluasan informasi melalui media komunikasi digital. Teknologi informasi ini pun tidak bisa dipungkiri memberikan kontribusi yang signifikan terhadap keberlangsungan kehidupan sosial dalam suatu negara. Melalui jaringan internet yang terus

dikembangkan juga menjadi momentum bagi negara untuk mempromosikan negaranya agar dapat menarik wisatawan mancanegara. Serta momentum bagi pelaku usaha agar produk yang di tawarkan bisa dengan mudah dan cepat menembus pasar dunia yang memberikan dampak positif bagi pelaku usaha dan menambah devisa bagi negara. Pelajar pun terbantu akan hadirnya perkembangan teknologi yang memungkinkan untuk mendapatkan wawasan yang lebih luas. Akan tetapi, adapun dampak negatif yang timbul akibat perkembangan teknologi informasi. Akses internet yang tak terbatas memungkinkan individu menyalahgunakan perkembangan ini. Dampak negatif yang ditimbulkan akibat perkambangan teknologi tidak sedikit. Pornografi, penipuan, perjudian, pencurian data, dan *hacking* yang masuk ke dalam kategori kejahatan *cyber* (*cybercrime*) menjadi suatu ancaman yang serius. *Cybercrime* adalah tindak kejahatan melalui jaringan internet yang memanfaatkan perkembangan teknologi yang dimana pelaku mencari keuntungan pribadi atau kelompoknya. Wahid dan Labib (2010:40) mendefinisikan *cybercrime* sebagai semua jenis pemakaian jaringan komputer untuk tujuan kriminal dengan penyalahgunaan kemudahan teknologi digital.

Kejahatan *cyber* dilakukan oleh peretas (*hackers*) untuk mencari keuntungan bagi individu maupun kelompoknya. Kegiatan peretasan ini juga dapat dengan mudah dilakukan dimana saja dan kapan saja. Melalui komputer internet, peretas dapat mengendalikan komputer lain melalui jaringan internet. Kehadiran peretas komputer memiliki dampak positif maupun negatif. Dampak positif yang diberikan peretas adalah membatu programmer untuk mencari atau mendapatkan celah di sistem

komputer agar perusahaan dapat terhindar dari dampak buruk kegiatan peretas. Dalam hal negatif, peretas akan mencoba mencari kekurangan atau celah agar bisa mendapatkan informasi yang terdapat pada sistem tersebut untuk kepentingan pribadi.

Salah satu kasus terbesar akibat dari perkembangan teknologi terjadi pada tahun 2000. Dalam waktu satu hari virus dapat menyebar dengan cepat ke seluruh dunia. Virus ini diciptakan oleh 2 orang programer asal Filipina dengan nama virus *Love Bug (ILOVEYOU*) menyerang sekitar 55 juta lebih komputer di seluruh dunia. *Love Bug* mengacak foto, *file* musik, dokumen dan mengunduh file yang ada di komputer korban. Kerusakan yang timbul akibat virus ini mencapai US$ 5,5 miliar dan menghabiskan dana mencapai US$ 15 Milliar untuk menghapus virus tersebut (Viva.co.id, 2017)

Seiring dengan terus bertambahnya kejahatan *cyber* transnasional, negara negara maju mulai serius menanggapi hal ini. Melalui *Budapest Convention on Cybercrime* rancangan impelentasi dibuat serta menjadi perjanjian pertama yang membahas mengenai *cybercrime* berskala internasional. Perjanjian ini dibentuk di Budapest, Hungaria pada tanggal 23 November 2001 yang digagas oleh Uni Eropa yang berjumlah 35 negara Eropa, Australia, Republik Dominician, Jepang dan Amerika Serikat. Salah satu tujuan dari perjanjian ini adalah harmonisasi unsur-unsur hukum domestik pidana substantif pelanggaran di bidang kejahatan *cyber* (*cybercrime*), yang merujuk dan sesuai dengan undang-undang yang berlaku dan mendorong kerjasama internasional. (en.wikipedia.org).

Sebagai ancaman yang serius, *cybercrime* perlu adanya penindakan sebagai upaya pencegahan aktifitas kejahatan *cyber*. Melalui *cyber security* pemerintah siap untuk menangkal dan mengamankan data serta memonitor aktifitas masyarakat di dunia maya. *Cyber Security* adalah aktifitas pencegahan dan pengamanan terhadap sumber daya telematika agar tidak terjadinya kriminalitas di dunia *Cyber (Cybercrime)* (Salahul, 2017). Pencegahan yang dilakukan untuk mengantisipasi kejahatan skala menengah-besar yaitu dengan peningkatan keamanan sistem agar meminimalisir celah sehingga perusahaan dapat terhindar dari serangan *cyber* (*cyber attack*). Melalui *penetration testing* atau lebih dikenal *pentest*, keamanan sebuah sistem di uji dan periksa apakah terdapat celah yang dapat di serang oleh *hacker*. *Penetration testing* merupakan sebuah metode untuk meng-evaluasi keamanan sistem komputer melalui simulasi penyerangan terhadap target dengan menggunakan program jahat (*malicious source*). (www.ncsc.gov.uk).

Penetration testing menjadi penting digunakan oleh perusahaan besar yang memiliki data-data penting dan sensitif seperti *bank*. Saat ini fungsi bank menjadi penting dalam kehidupan perekonomian suatu negara. Jika jaringan bank diretas maka perekonomian suatu negara dapat terganggu. Salah satu kasus dalam hal ini adalah lumpuhnya seluruh ATM di Ukraina pada 27 Juni 2017 yang menyebabkan terhambatnya siklus perekonomian bisnis. Indonesia sebagai negara yang tidak menutup arus teknologi juga sering mendapatkan ancaman serta kejahatan *cyber* secara langsung. Salah satu kasus, masyarakat kehilangan saldo di dalam rekening

BRI akibat skimming atm pada tahun 2016. Kasus ini menyebabkan kerugian hingga 2,7 miliar rupiah.

Penangkal kejahatan *cyber* tingkat menengah-kebawah (perseorangan). Anti virus masih menjadi pilihan utama sebagai penangkal serangan *cyber*. Antivirus dinilai efektif dalam menjaga komputer pribadi dari serangan *cyber* (*cyber* attack) serta penggunaan antivirus tidak membutuhkan biaya yang mahal seperti halnya *penetration testing*.

Perkembangan *cybercrime* memicu negara-negara untuk turut mengembangkan dan mengimplementasikan *cyber security* untuk menjaga data data pemerintahan dan perusahaan yang sangat sensitif. Data survey tahun 2017 yang diterbitkan oleh Asosiasi Penyelenggara Jaringan Internet Indonesia (APJII), bahwa sekitar 143,26 juta user atau sekitar 54,68 persen dari total jumlah penduduk Indonesia sebesar 262 juta jiwa, masyarakat Indonesia telah terhubung dengan internet. Indonesia sebagai negara terbesar kedua yang aktif dalam penggunaan internet serta memiliki banyak perusahaan *unicorn*, dituntut untuk bisa menanggulangi ancaman *cyber* yang mungkin terjadi. *Unicorn* sebagai perusahaan *startup* yang memiliki dampak signifikan terhadap perekonomian Indonesia karena bisnis yang dibentuk oleh putra bangsa bisa mencapai level internasional dan memiliki nilai valuasi US$ 1 miliar. Selain itu, Indonesia memiliki kurang lebih 956 unit perusahaan yang bergerak di bidang *startup*. Sebagai suatu aset negara, perusahaan unicorn maupun perusahaan yang bergerak di bidang startup harus mendapat perlindungan dari pemerintah salah

satunya melalui antisipasi serangan *cyber* dengan membentuk *cyber security* yang terjamin.

Tumbuh pesatnya pengguna internet di Indonesia, belum diimbangi dengan *cyber security* yang memadai. Pada tahun 2015 kejahatan *cyber* Indonesia meningkat 33 persen dibanding tahun 2014, Luhut Binsar Panjaitan mengatakan belum terbentuknya pertahanan yang terkoordinasi dan sistem yang memadai menjadi salah satu faktor yang membuat Indonesia masuk ke dalam negara "darurat *cyber*" (Kemenko Polhukam RI, 2016). *Cyber security* menjadi penting di era digital saat ini, karena hampir di semua sektor kehidupan dapat terhubung dengan teknologi.

Serangan *cyber* yang semakin tumbuh dan menjadi ancaman keamanan nasional, sehingga pemerintah membentuk badan untuk melindungi warganya dan menjaga kedaulatan negara khususnya di ranah *cyber*. Melalui peraturan presiden nomor 53 tahun 2017, Badan *Cyber* dan Sandi Negara (BSSN) dibentuk sebagai organisasi pemerintahan (badan) yang bertanggung jawab untuk membidangi *cyber* nasional dan berfungsi menentukan kebijakan *cyber security* nasional dengan peran dan kerjasama antara pemerintah, sektor swasta serta masyarakat. (bssn.go.id).

> BSSN bukan merupakan lembaga baru yang dibentuk, namun merupakan penguatan dari lembaga yang telah ada sebelumya, yaitu Lemsaneg dan Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika. Dengan dibentuknya BSSN, maka pelaksanaan seluruh tugas dan fungsi di bidang Persandian serta pelaksanaan seluruh tugas dan fungsi di bidang keamanan informasi, pengamanan

> pemanfaatan jaringan telekomunikasi berbasis protokol internet, dan keamanan jaringan dan infrastruktur telekomunikasi dilaksanakan oleh BSSN. (bssn.go.id).

Sebagai pengguna internet terbesar kedua di dunia, Indonesia perlu dengan aktif menekan angka kejahatan *cyber* yang terus tumbuh dan berkembang. Upaya pemerintah dalam menekan angka kejahatan khususnya di bidang *cyber* yaitu melalui perjanjian kerjasama internasional. Kerjasama merupakan serangkaian hubungan yang tidak didasari oleh kekerasan atau paksaan dan disahkan secara hukum, seperti pada organisasi internasional. Kerjasama terjadi karena adanya penyesuaian perilaku oleh para aktor sebagai respon dan antisipasi terhadap pilihan-pilihan yang diambil oleh aktor lain. Kerjasama dapat dijalankan dalam suatu proses perundingan yang secara nyata diadakan. Namun apabila masing-masing pihak telah saling mengetahui, perundingan tidak perlu lagi dilakukan. (Dougherty and Pfaltzgraff 1997 : 418). Kerjasama internasional dilakukan oleh dua negara atau lebih untuk mencapai tujuan bersama dan mendapatkan keuntungan bagi masing-masing negara. Kerjasama internasional dapat dilakukan di berbagai bidang, mulai dari bidang ekonomi, pendidikan, keamanan dan teknologi. Selain mencapai keuntungan, kerjasama internasional dianggap perlu sebagai salah satu upaya negara untuk mempererat hubungan diplomasi antar negara yang berada di lingkup kerjasama.

Kerjasama internasional menjadi hal yang sangat umum ketika suatu negara diangkap kekurangan informasi dalam bidang bidang tertentu dan dianggap perlu untuk meningkatkan atau mengambangkan bidang untuk stabilitas suatu negara.

Indonesia-Austarlia sepakat untuk melakukan kerjasama bilateral di berbagai bidang. Bidang perdaganagan, pendidikan, kesehatan, ekonomi, pariwisata, dan keamanan menjadi bagian dari kerjasama bilateral. Kondisi keamanan yang mengancam indonesia di bidang *cyber* menjadi salah satu bentuk kerjasama keamanan antara dua negara. Austalia yang memiliki *cyber security* yang cukup kuat, menjadi salah satu faktor Indonesia untuk menjalin kerjasama di bidang *cyber*. Indonesia melalui Badan *Cyber* dan Sandi Nasional serta Australia melalui *Cyber Affairs Department of Foreign Affairs and Trade* sepakat melakukan kolaborasi untuk mencapai *cyber security* dan internet yang aman bagi kedua negara. Penandatanganan nota kesepahaman dimulai pada tahun 2017 di Canberra sebagai awal mulainya kerjasama di bidang *cyber security*. Kesapakatan ini muncul atas tindak lanjut dari kerjasama sebelumnya yang dilakukan oleh Polisi Republik Indonesia dan *Australia Federal Police.* "Kerjasama yang dilakukan oleh Polri dan *Australia Federal Police* dalam pembangunan CCISO tersebut merupakan lanjutan kerjasama yang dilakukan oleh kedua kepolisian ini pada tahun 2010. Pada tahun 2010 kerjasama yang di lakukan membuahkan terbentuknya sebuah kantor pencegahan dan penanggulangan *cybercrime* yang bernama *Cybercrime Investigation Center* atau CCIC di markas besar kepolisian Republik Indonesia." (www.voa-islam.com)

Berdasarkan latar belakang penelitian yang penulis bahas diatas. Maka, penulis memilih untuk mengangkat judul **"Kerjasama Indonesia-Australia di Bidang Keamanan dalam Mengatasi *Cyber Crime* di Indonesia melalui Program *Cyber Policy Dialogue*".**

1.2 Identifikasi Masalah

Berdasarkan uraian di atas untuk memudahkan dalam menganalisa masalah, penyusun mengidentifikasi masalah sebagai berikut:

1. Bagaimana kerjasama Indonesia-Australia dalam bidang keamanan?
2. Bagaimana ancaman *cybercrime* terhadap kondisi *cyber security* di Indonesia?
3. Bagaimana implementasi *Cyber Policy Dialogue* dalam meminimalisir *cybercrime* di Indonesia?

1.3 Pembatasan Masalah

Agar penelitian ini lebih terarah, terfokus, dan tidak meluas, maka penulis membatasi masalah pada "***Implementasi* kerjasama Indonesia-Australia dalam mengatasi *Cyber Crime* di Indonesia melalui Program *Cyber Security Dialogue* pada tahun 2017-2018".**

1.4 Perumusan Masalah

Berdasarkan identifikasi masalah, untuk memudahkan penyusun dalam melakukan pembahasan, penyusun merumuskan masalah sebagai berikut:

"**Bagaimana implementasi program kerjasama *Cyber Policy Dialogue* dalam meminimalisir tingkat peretasan *cyber security* di Indonesia?"**

1.5 Tujuan dan Kegunaan Penelitian

1.5.1 Tujuan Penelitian

Sebagai upaya untuk menjelaskan arah dan tujuan umum dari pembahasan penelitian, maka penulis harus memiliki tujuan jelas dari identifikasi masalah yang sudah dipaparkan. Tujuan penelitian ini adalah:

1. Mengetahui kerjasama Indonesia-Australia di bidang *cyber security*
2. Mengatahui ancaman *cybercrime* terhadap kondisi *cyber security* di Indonesia
3. Mengetahui program kerjsama Indonesia-Australia di bidang *cyber security*

1.5.2 Kegunaan Penelitian

Adapun yang menjadi kegunaan dari penelitian ini adalah sebagai berikut:

1. Memenuhi salah satu syarat untuk menempuh Ujian Sidang Sarjana Strata Satu (S1) pada Jurusan Hubungan Internasional Fakultas Ilmu Sosial dan Ilmu Politik Universitas Pasundan.
2. Diharapkan dengan dibuatnya penelitian ini bisa menambah referensi dan informasi guna menambah pengetahuan serta memperluas wawasan bagi penulis dan pembaca terhadap *cyber* security di Indonesia.