BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

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

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

Perkembangan teknologi yang saat ini terjadi bagaikan pedang bermata dua. Jika teknologi tersebut dipergunakan dengan baik maka perkembangan teknologi tersebut akan bersifat positif bagi kehidupan manusia. Namun apabila dilakukan untuk maksud tertentu untuk hal yang merusak maka perkembangan teknologi tersebut menjadi suatu hal yang negatif. *cybercrime* merupakan salah satu penyalahgunaan kemajuan teknologi yang saat ini terjadi di dunia maya (*cyberspace*).

Masyarakat internasional saat ini sangat memperhatikan perkembangan ancaman *cybercrime.* Kekhawatiran tersebut dikarenakan *cybercrime* semakin mudah dilakukan oleh pihak-pihak tertentu. Serangan siber (*cyber attack)* merupakan salah satu bentuk *cybercrime* dapat dilakukan untuk menyerang, baik secara individu maupun digunakan untuk menyerang suatu kelompok atau organisasi bahkan negara lain.

Kemajuan teknologi komputer dan kemajuan internet yang saat ini terjadi menyebabkan semakin meningkatnya kasus yang di timbulkan oleh peretas komputer (*computer hackers*). Kegiatan para peretas komputer ini dapat dilakukan dalam hal positif maupun negatif. Dalam hal positif, para peretas komputer biasanya memasuki suatu sistem dengan memanfaatkan kekurangan atau celah yang ada pada suatu sistem tersebut. Setelah peretas memanfaatkan kekurangan yang ada pada sistem tersebut, peretas kemudian memberitahukan kepada pembuat sistem tersebut tentang kekurangan dari keamanan sistem tersebut sehingga sang pembuat dapat memperbaiki dan menyempurnakan sistemnya. Berbeda dengan dengan kegiatan negatif yang dilakukan oleh para peretas setelah mereka menemukan celah serta kekurangan pada sistem tersebut mereka mencuri dan mengambil informasi yang terdapat dalam sistem tersebut untuk kepentingan pribadi.

Kegiatan memasuki suatu sistem tanpa izin dan mengambil data atau informasi dalam sistem tersebut untuk kepentingan pribadi sudah termasuk dalam *cybercrime*. *Cybercrime* sendiri secara umum merupakan suatu kejahatan yang

menggunakan komputer internet sebagai sarananya baik untuk memperoleh keuntungan atau tidak, yang merugikan pihak lain.

Kegiatan pencurian data hasil retasan tersebut meningkat secara signifikan dari tahun-ke tahun, dengan jumlah data personal mencapai jutaan bahkan dalam beberapa kasus mencapai milyaran data yang telah dicuri oleh beberapa grup kecil para peretas. Terkadang, beberapa peretas menggunakan program jahat atau *malware* untuk memfasilitasi serangan mereka yang mana dapat menyebabkan kerugian ratusan hingga ribuan dolar akibat kerusakan di seluruh pengaturan perusahaan.

Salah satu kasus yang menarik perhatian dunia terjadi pada tanggal 5 Mei 2000 dua programmer muda asal Filipina yang bernama Reonel Ramones dan Onel de Gusman menyebarkan virus komputer yang mereka ciptakan. Virus yang mereka ciptakan bernama virus e-mail *Love Bug (ILOVEYOU).*

Virus yang mereka ciptakan telah menginfeksi dan melumpuhkan 80 juta lebih komputer pada tahun 2000 dan menyebabkan kerugian sekitar 5.5 milyar dolar – 8.75 milyar dolar AS. Virus tersebut juga menyerang komputer komputer milik Pentagon, CIA (*Central Intelligence Agency*) dan situs situs militer lainnya (http://www.cnnindonesia.com/teknologi/20150213131622-185-31891/iloveyou-kisah-virus-yang-bikin-patah-hati-pengguna-pc/ Diakses pada tanggal 18 Februari 2016).

Namun dengan lemahnya hukum pada *cybercrime* akhirnya kejahatan yang dilakukan oleh Reonel Ramones dan Onel De Gusman membuat mereka terbebas dari kejahatan yang mereka lakukan.

Dalam dunia hubungan internasional saat ini *cybercrime* merupakan salah satu ancaman keamanan bagi seluruh negara. Dikarenakan kejahatan yang dilakukan oleh para peretas tersebut dapat dilakukan dimana saja tidak mengenal batas-batas negara. Dalam kertas kerja *UNODC (United Nations Office on Drugs and Crime)* mencatat bahwa *cybercrime* adalah kejahatan transnasional tertinggi didunia. Masalah kedaulatan nasional dapat menghambat investigasi kriminal tanpa adanya kerjasama aktif antara lembaga penegak hukum dari yurisdiksi yang terlibat. Kecepatan dalam melakukan *cybercrime* dan mengindarinya menimbulkan tekanan bagi lembaga penegak hukum untuk menangkap mereka dan membuat kerjasama dalam mencegah dan menanggulangi *cybercrime* semakin penting.

Indonesia pun tidak luput dari *cybercrime*, salah satu kasus *cybercrime* yang terjadi di Indonesia adalah kasus yang terjadi pada 17 Juli 2006, DPP Partai Golkar melaporkan terjadinya serangan pengrusakan terhadap situs Golkar.or.id. Serangan terhadap situs partai berlambang pohon beringin itu terjadi pada 9 hingga 13 Juli 2006 hingga menyebabkan tampilan halaman berubah (*deface*). "Pada 9 Juli 2006, tersangka mengganti tokoh Partai Golkar yang termuat dalam situs dengan gambar gorilla putih tersenyum dan di bagian bawah halaman dipasangi gambar artis Hollywood yang seronok, dengan tulisan 'Bersatu untuk malu'.

Setelah melakukan serangan terhadap situs GOLKAR www.golkar.or.id sebanyak 1257 kali, polisi akhirnya menangkap Iqra Syafaat pada tanggal 1

Agustus 2006 (http://ilmuta.weebly.com/computer-crime/e-procurement diakses pada tanggal 18 Februari 2016).

Berkembangnya kasus *cybercrime* yang terjadi saat ini mendorong setiap negara untuk saling bekerjasama dalam melawan *cybercrime*. Dalam konvensi Perserikatan Bangsa-Bangsa yang bernama *United Nations Convention Against Transnasional Organized Crime* yang diselenggarakan di Wina bertujuan untuk memerangi dan menangulangi masalah *Transnasional Organized Crime. Cybercrime* merupakan salah satu bentuk *Transnasional Organized Crime* yang sangat meresahkan bagi suatu negara, dampak yang ditimbulkan dari *cybercrime* ini dapat mengancam keamanan suatu negara, walaupun *cybercrime* ini tidak langsung melakukan kontak fisik secara langsung namun hasil kejahatan tersebut sangat fatal dan merugikan secara materil dan non materil.

Namun bukan hanya keamanan saja yang terkena dampak dari *cybercrime* tetapi perekonomian negara juga terkena dampaknya. Kerena dengan berlakunya layanan perbankan secara elektronik seperti *E-banking, E-commerce dan Elektronik Fund transfer,* perbankan menjadi sasaran utama bagi para pelaku *cybercrime* sehingga banyak kasus yang terjadi di Indonesia melibatkan perbankan sebagai korbannya. Jika jaringan perbankan di*hack* ,ini akan berakibat pada lumpuhnya perputaran uang yang terjadi di bank. Dan jika perputaran uang di bank dilumpuhkan maka akan berakibat pada perekonomian suatu negara.

Dampak lain dari *cybercrime* dapat dirasakan pada aspek sosial dan budaya. Contohnya kasus pornografi baik video maupun gambar yang dapat

merusak nilai kesusilaan di Indonesia, dalam dunia *cybercrime* ini tergolong dalam *cyber sex*.

Perkembangan teknologi yang sangat pesat ini pun dirasakan di Indonesia, berdasarkan hasil pemantauan *Asia Pasific Network Information Center cybercrime* (APNIC) tahun 2003, Indonesia menduduki peringkat pertama negara yang paling banyak terjadi kasus *cybercrime* dalam sektor perbankan (*carding).* Hasil ini diambil dari persentasi jumlah penipuan dalam hal transaksi yang terjadi di Indonesia (http://beritasore.com/2007/05/15/polri-tangani-kejahatan-cyber-crime-capai-71-kasus/ diakses 18 Februari 2016).

Selain contoh kasus *cybercrime* yang telah di jelaskan peneliti masih banyak pula kasus *cybercrime* seperti kasus mafia *cyber* yang merebak pertengahan tahun 2004 di Amerika Serikat. Indonesia pun mengalami kasus *cybercrime* yang mengganggu keamanan negara, ketika sistem jaringan Komisi Pemilihan Umum (KPU) diretas oleh para *hacker*. Sangat mencemaskan ketika dunia semakin bergantung dengan teknologi dan informasi saat ini yang sangat rentan terhadap tindak kejahatan.

Maraknya kasus *cybercrime* yang terjadi di Indonesia dilatarbelakangi oleh beberapa faktor yaitu pertama lemahnya penegak hukum di Indonesia, terbukti dengan tidak adanya Undang-Undang khusus mengenai *cybercrime.* Kedua, keterbatasan sarana dan prasarana di bidang teknologi dan juga lembaga penegak hukum di daerah (polda) juga masih terbatas dalam hal infrastruktur, sehingga penanganan menjadi tidak maksimal.

Menanggapi hal tersebut, Pada tanggal 29 April 2013 Indonesia dan Australia meresmikan laboratorium siber yang bernama *Cyber Crime Investigation Satellite Office (CCISO)* di Polda Metro Jaya pembangunan dan peresmian *Cyber Crime Investigation Satellite Office* didanai sembilan juta dolar AS untuk infrastruktur, latihan, dan peningkatan kapasitas oleh Australia (http://metro.sindonews.com/read/743023/31/polda-metro-jaya-resmikan laboratorium-cyber-crime-1367214876 Diakses pada 16 Oktober 2015).

Pembangunan CCISO merupakan lanjutan kerjasama antara Kepolisian Republik Indonesia dan *Australia Federal Police* yang dilaksanakan sejak tahun 2010. Selain di Polda Metro Jaya, CCISO juga ada di Mabes Polri, Polda Sumatera Utara, Polda Bali, dan Polda Nusa Tenggara Barat. Di masa mendatang akan diadakan di semua Polda (http://tekno.kompas.com/read/2013/04/30/15491539/Indonesia.Bangun.Pusat.Investigasi.Kejahatan.Cyber Diakses pada 7 Mei 2016).

Jaringan CCISO di berbagai Polda juga telah tersambung dengan pusat pemantauan (*monitoring center*) atau jaringan *JCLEC (Jakarta Centre For Law Enforcement Cooperation)*, untuk menganalisa komunikasi dari jaringan kejahatan, seperti terorisme, narkotika, pencucian uang, dan korupsi (http://www.voaislam.com/read/indonesiana/2013/08/31/26579/awasccisolaboratoriumcybercanggih-polri-dibiayai-australia/#sthash.KhExH0Bc.dpuf Diakses pada 7 Mei 2016).

Menurut Wakil Direktur Kriminal Khusus Ajun Komisaris Besar Hery Santoso, Polda Metro menerima sekitar 800 kasus *cybercrime* per tahun. Sebelum

ada kerja sama dengan *Australia Federal Police*, pengungkapan kasus sangat kecil. Namun, setelah ada kerja sama dengan *Australia Federal Police*, mulai Juni 2012, penyelesaian kasus mencapai 40 persen dari total kasus yang masuk.

Dengan sudah beroperasinya CCISO yang lengkap dengan peralatannya, kami targetkan penyelesaian kasus bisa 60% pertahun (http://tekno.kompas.com/read/2013/04/30/15491539/indonesia.bangun.pusat.investigasi.kejahatan.quotcyberquot Diakses pada 7 Mei 2016).

Kepala Sub-Direktorat *Cyber Crime* Polda Metro, Ajun Komisaris Besar Audie Latuheru, mengatakan, cara kerja CCISO nantinya menyatukan sistem yang dibuat antarnegara. Ia mencontohkan pengiriman barang bukti digital dan bentuk laporan sehingga memiliki nilai secara hukum (https://m.tempo.co/read/news/2013/04/29/064476569/pusat-investigasi-cyber-crime-australia-dipolda diakses pada 10 Mei 2016).

Kerjasama yang dilakukan antara Indonesia dan Australia ini sangat menguntungkan bagi kedua belah pihak. Mengingat di Indonesia saat ini sistem *e-goverment* saat ini sudah terkoneksi satu sama lain. Jika sistem *e-goverment* ini diretas maka kegiatan pemerintahanpun akan lumpuh. Dan bagi Australia permbangunan *cybercrime investigation satelite office* ini akan sangat efektif membantu Australia dalam menumpas *cybercrime*, karena saat ini *cybercrime* dapat berhubungan dengan kejahatan lain, seperti terorisme dan kejahatan teroganisir lainnya (http://tekno.kompas.com/read/2013/04/30/15491539/indonesia.bangun.pusat.investigasi.kejahatan.quotcyberquot diakses tanggal 16 Mei 2016)

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 Kepublik Indonesia (http://www.voaislam.com/read/indonesia na/2013/08/31/26579/awasccisolaboratoriumcybercanggihpolridibiayaiaustralia/#sthash.KhExH0Bc.KwrlXIjX.dpbs diakses pada tanggal 16 Mei 2016).

Dalam kerjasama yang dilakukan antara Indonesia dan Australia dilatarbelakangi oleh perjanjian lombok atau lombok *Treaty.* Lombok *Treaty* pada awalnya merupakan kerjasama keamanan yang dilakukan oleh Australia dan Indonesia dalam memerangi kejahatan lintas negara yang terfokus pada terorisme. Namun dalam perkembangannya perjanjian ini tidak hanya terfokus dalam terorisme melainkan pada kejahatan lintas negara antara lain sepert. Penyelundupan dan perdaganngan manusia, pencucian uang, pendanaan terorisme, korupsi, penangkapan ikan ilegal, kejahatan dunia maya, perdagangan gelap narkotika dan bahan-bahan psikotropika serta prekursornya, perdagangan gelap senjata api dan jenis kejahatan lain yang di anggap perlu oleh kedua negara (http://treaty.kemlu.go.id/uploads-pub/1637_AUS-2006-0164.pdf diakses pada tanggal 15 Mei 2016).

Dalam pencegahan dan penanggulangan kejahatan lintas negara kepolisian Republik Indonesia dan *Australia Federal Police* selaku penegak hukum dikedua negara melakukan kerjasama dan menghasilkan Nota Kesepahaman Antara

Republik Indonesia dan Pemerintah Australia tentang Penanggulangan Kejahatan Lintas Negara dan Pengembangan Kepolisian serta Pengaturan Antara Kepolisian Negara Republik Indonesia dan Kepolisian Federal Austalia Tentang Kerjasama Dalam Pencegahan dan Penanggulangan Kejahatan Lintas Negara. Nota kesepahaman dan Pengaturan kerjasama ini Sesuai dengan maksud dan tujuan dari Kesepakatan antara Republik Indonesia dan Australia dalam Kerangka Kerja Sama Keamanan (Perjanjian Lombok) yang telah ditandatangani di Lombok pada tanggal 13 November 2006 (http://treaty.kemlu.go.id/uploads-pub/4236_AUS-2011-0188.pdf diakses pada tanggal 16 Mei 2016)

Pembangunan CCISO merupakan hasil dari pengaturan kepolisian antara kepolisian Republik Indonesia dan *Australian Federal Police* yang terdapat pada paragraf 3 Lingkup kerjasama 3.2 Peningkatan kapasitas untuk meningkatkan kemampuan institus melalui metode-metode; termasuk;

a) pertukaran personil;
b) program pelatihan dan pendidikan;
c) kemitraan dalam membangun fasilitas untuk pencegahan dan penanggulangan kejahatan lintas negara;
d) dukungan peralatan dan teknologi;
e) dukungan operasi (http://treaty.kemlu.go.id/uploads-pub/4236_AUS-2011-0188.pdf diakses pada tanggal 16 Mei 2016)

Untuk memudahkan peneliti dalam mengkaji kerjasama Indonesia Australia melalui *Cybercrime Investigation Satelite Office,* peneliti menggunakan beberapa penelitian terdahulu sebagai acuan dalam pembahasan. Beberapa

penelitian terdahulu yang akan digunakan peneliti adalah pertama penelitian yang dilakukan oleh Indri Novianty dari Universitas Riau pada tahun 2014 dalam jurnal yang berjudul "Kerjasama Kepolisian Negara Republik Indonesia dan Kepolisian Federal Australia dalam menanggulangi *cybercrime* di Indonesia".

Dalam penelitian ini, Indri membahas masalah kerjasama antara kepolisian Republik Indonesia dan kepolisian Federal Australia pasca penyadapan yang di lakukan oleh Australia serta penjelasan kasus *cybercrime* di Indonesia. Melalui penelitian ini, Indri memberikan contoh kasus *cybercrime* yang berdampak pada sektor keamanan, perekonomian dan sosial budaya. Indry juga menjelaskan tentang awal pelaksanaan kerjasama dalam menanggulangi *cybercrime* dan kondisi kerjasama pasca penyadapan yang di lakukan Australia.

Penelitian yang dilakukan oleh Indry ini mempunyai kesimpulan bahwa *cybercrime* membawa dampak yang besar bagi kemanan suatu negara yang berakibat pada terganggunya kemanan serta perekonomian suatu negara. Dengan melakukan kerjasama maka Indonesia dapat memerangi dan menanggulangi kasus *cybercrime* yang terjadi di Indonesia. Dan pasca penyadapan membawa hubungan Indonesia dan Australia mengalami ketegangan namun tidak berdampak pada kerjasama antara Polri dan *Australian Federal Police)* dalam menanggulangi *cybercrime* di Indonesia. Hal tersebut terbukti dengan di selenggarakannya *Senior Official Meeting* (SOM) antara Polri dan *(Australian Federal Police),* yang merupakan bagian dari program kerja tahunan dari *Transnasional Crime Centre* (TNCC) dalam mendukung diskusi antara kedua negara yang rutin dilaksanakan

setiap satu tahun sekali oleh delegasi dari Polri maupun *(Australian Federal Police).*

Persamaan peneliti dengan penelitian pertama yaitu penanganan *cybercrime* di Indonesia, Penelitian yang dilakukan peneliti berbeda dengan penelitian Pertama, dimana peneliti ingin mengetahui bagaimana kerjasama antara Indonesia dan Australia melalui *Cyber Crime Investigation Satellite Office* dalam menangani *cybercrime*. Dan perbedaan yang mendasarnya terdapat pada kerjasama yang dilakukan, jika peneliti sebelumnya membahas kerjasama antara Polri dan *Australian Federal Police* pasca penyadapan yang dilakukan oleh Australia, maka peneliti ingin membahas bagaimana kerjasama Indonesia dan Australia melalui *Cyber Crime Investigation Satellite Office* yang merupakan pelaksanaan kerjasama yang tertuang dalam *Lombok Treaty.*

Kedua adalah penelitian yang dilakukan oleh Andrew Richard Rihi Iye dari Universitas Komputer Indonesia pada tahun 2009 dengan judul "Pengaruh *United Nation Against Transnasional Organized Crime* (UNCATOC) Terhadap Kejahatan *Carding* Di Indonesia". Dalam penelitian ini Adrew Richard membahas mengenai berbahayanya *cybercrime* dalam dunia hubungan saat ini. Peneliti memberikan contoh *cybercrime* yang terjdi di Indonesia yaitu kasus *carding* dan membahas pengaruh dari *United Nation Against Transnasional Organized Crime* (UNCATOC) terdahap kasus carding di Indonesia

Pada penelitian ini Andrew berkesimpulan bahwa dengan diratifikasinya konvensi *Transnasional Organized Crime* oleh Indonesia dalam bentuk Undang-Undang nomor 15 tahun 2002 tentang Tindak Pidana Pencucian Uang

sebagaimana telah di ubah dengan Undang-Undang Nomor 25 Tahun 2003 yang berpengaruh terhadap Tindakan *cybercrime* terutama *Carding* maka penanganan tindakan kejahatan tersebut akan lebih mudah dan dapat diselesaikan secara baik dan benar. Dengan melalui aplikasi hukum internasional *Cybercrime* maka para penegak hukum dan pihak berwenang dalam memyelesaikan masalah tindak *cybercrime* ini dapat di tindak lanjuti.

Persamaan peneliti dengan penelitian kedua yaitu sama-sama meneliti tentang kejadian tindak kejahatan lintas negara yaitu *cybercrime* di Indonesia. Perbedaan yang di lakukan peneliti berbeda dengan penelitian kedua, dimana peneliti kedua hanya membahas masalah *carding* di Indonesia dan berdasarkan *United Nation Against Transnasional Organized Crime* (UNCATOC). Sedangkan peneliti membahas kerjasama Indonesia dan Australia melalui *Cyber Crime Investigation Satellite Office* yang merupakan pelaksanaan kerjasama yang tertuang dalam Perjanjian Lombok.

Ketiga adalah penelitian yang dilakukan oleh Dwi Ana Wiyatiningrum dari Universitas Negeri Yogyakarta pada tahun 2015 dengan judul "Hubungan Bilateral Indonesia-Australia Pada Masa Perdana Menteri Kevin Rudd (2007-2015)". Pada penelitian ini Dwi Ana Wiyatiningrum membahas mengenai program yang dicanangkan oleh Kevin Rudd dalam pemilu Australia dan membahas mengenai kebijakan-kebijakan Kevin Rudd dalam menjalin hubungan bilateral antara Indonesia dan Australia. Kebijakan yang dibahas dalam penelitian ini antara lain, kebijakan dalam bidang keamanan dan pertahanan, kebijakan

dalam bidang politik, kebijakan dalam bidang pendidikan dan kebijakan dalam bidang ekonomi.

Pada penelitian ini Dwi Ana Wiyatiningrum berkesimpulan bahwa terpilihnya Kevin Rudd menjadi perdana menteri Australia membawa angin segar bagi hubungan bilateral antara Indonesia dan Australia. Undangan Presiden Susilo Bambang Yudhoyono pada saat itu terkait konfrensi perubahan iklim di Bali disambut baik oleh PM Kevin Rudd. Kunjungan pertama Kevin Rudd menjadikan dasar terbukanya hubungan bilateral antara Indonesia dan Australia di masa mendatang.

Kevin Rudd membawa perubahan berarti bagi hubungan Indonesia dan Australia. Berbagai kebijakan dari bidang ekonomi, politik, pendidikan, keamanan dan pertahanan membawa hubungan Indonesia dan Australia mengalami perubahan yang signifikan dibandingkan pada masa John Howard. Kevin Rudd menjadikan Indonesia sebagai mitra penting bagi Australia dan menjadikan setiap kebijakan luar negerinya condong ke Asia terutama Indonesia.

Persamaan peneliti dengan penelitian ketiga yaitu sama-sama membahas hubungan dan kerjasama antara Indonesia dan Australia. Perbedaan yang dilakukan peneliti berbeda dengan penelitian ketiga, dimana penelitian ketiga ini hanyak membahas kebijakan-kebijakan yang dikeluarkan oleh perdana menteri Kevin Rudd mengenai hubungan bilateral antara Indonesia dan Australia. Sedangkan peneliti membahas kerjasama antara Indonesia Australia melalui *Cyber Crime Investigation Satellite Office* yang merupakan pelaksanaan kerjasama yang tertuang dalam Perjanjian Lombok.

Berdasarkan uraian diatas peneliti ingin mengetahui lebih jauh mengenai kerjasama yang dilakukan oleh Indonesia dan Australia melalui *Cyber Crime Investigation Satellite Office* dalam memerangi *cybercrime*. Dan beberapa alasan antara lain : pertama, hubungan Indonesia dan Australia selalu mengalami pasang surut, dan tidak jarang Australia sering ikut campur dalam urusan dalam negeri Indonesia serta mencoreng kedaulatan negara republik Indonesia. Kedua, dalam kerjasama tersebut peneliti ingin mengetahui kendala, langkah dan apa saja yang dilakukan kedua negara dalam menangani *cybercrime* melalui *Cyber Crime Investigation Satellite Office*.

Berdasarkan alasan-alasan tersebut yang menjadi dasar pertimbangan peneliti untuk mengadakan penelitian dengan judul :

"Kerjasama Indonesia Australia Melalui *Cybercrime Investigation Satellite Office* Dalam Pencegahan dan Penanggulangan *Cybercrime* di Indonesia".

Adapun ketertarikan peneliti untuk meneliti dan mengangkat isu tersebut didukung oleh beberapa mata kuliah disiplin Ilmu Hubungan Internasional, diantaranya adalah sebagai berikut:

1. Hukum Internasional, dimana *cybercrime* menjadi salah satu kajian hukum internasional, khususnya mengenai peraturan serta penanganan *cybercrime* di seluruh negara.
2. *Cybercrime,* merupakan mata kuliah yang menjelaskan tentang kasus kasus *cybercrime* yang ada di dunia, serta menjadi dasar kerjasama yang dilakukan oleh Indonesia dan Australia.

3. Studi Keamanan Internasional, dalam mata kuliah ini mempelajari konsep keamanan suatu negara yang menjadi faktor penting dalam kehidupan bernegara suatu bangsa. Berdasarkan mata kuliah ini peneliti menilai bahwa perkembangan teknologi dan informasi, membawa setiap negara untuk saling membantu dalam menangani *cybercrime* karena dapat mengancam setiap negara,
4. Diplomasi dan Negosiasi, dalam mata kuliah ini mempelajari mengenai strategi dalam melakukan diplomasi dan negosiasi dalam upaya Indonesia dan Australia dalam menangani *cybercrime* dikedua negara.
5. Hubungan Internasional di Australia dan Pasifik, dalam mata kuliah ini mempelajari kebijakan-kebijakan, kerjasama dan pengambilan keputusan yang dilakukan oleh setiap kepala negara pada periodenya. Dan mempelajari sejarah kerjasama Indonesia dan Australia yang pernah terjadi serta memahami karakteristik kebijakan yang diambil negara kawasan Australia dan Pasifik

1.2 Rumusan Masalah

1.2.1 Rumusan Masalah Mayor

"Bagaimana Kerjasama Indonesia Australia Melalui *Cybercrime Investigation Satelite Office* dalam Dalam Pencegahan dan Penanggulangan *Cybercrime* di Indonesia?"

1.2.2 Rumusan Masalah Minor

1. Bagaimana proses kerjasama yang disepakati Indonesia dan Australia melalui *cybercrime investigation satellite office*?
2. Bagaimana hasil kerjasama Indonesia dan Australia melalui *cybercrime investigation satellite office* dalam mencegah dan menanggulangi *cybercrime* di Indonesia ?
3. Bagaimana Prospek kerjasama Indonesia dan Australia melalui *cybercrime investigation satellite office* dalam mencegah dan menanggulangi *cybercrime* di Indonesia ?

Secara umum dalam hubungan Indonesia-Australia selalu berusaha memanfaatkan setiap peluang yang ada untuk peningkatan berbagai kerjasama bilateral. Dukungan Australia terhadap keutuhan wilayah negara kesatuan Republik Indonesia (NKRI) merupakan faktor kunci dalam upaya meningkatkan hubungan bilateral tersebut. Untuk konteks yang lebih luas, dan dalam rangka membangun hubungan yang saling menguntungkan, telah pula ada kerjasama Indonesia-Australia yang tertuang dalam "Lombok *Treaty*". Lombok Treaty adalah kerjasama di bidang keamanan yang dibuat pada 13 November 2006, yang kemudian diratifikasi pada tahun 2007. Perjanjian kerjasama ini diatur dalam Undang-Undang Republik Indonesia nomor 47 tahun 2007 Tentang Pengesahan Perjanjian Antara Republik Indonesia dan Australia tentang Kerangka Kerjasama Keamanan yang meliputi 21 kerjasama keamanan yang terangkum dalam 10 bidang. Dan dilanjutkan dengan nota kesepahaman pengembangan kepolisian dan pengaturan kepolisian Indonesia dan *Australian Federal Police* dalam mencegah dan menanggulangi kejahatan lintas negara. Dirikannya kantor *Cybercrime Investigation Satelite* yang diresmikan pada

tahun 2013 merupakan hasil dari pengaturan kepolisian Indonesia dan *Australian Federal Police* dalam mencegah dan menanggulangi kejahatan lintas negara. Penelitian ini dibatasi dari tahun 2013-2016. Karena peresmian dari kantor *Cybercrime Investigation Satelite* pada tahun 2013.

1.3 Maksud dan Tujuan Penelitian

1.3.1 Maksud Penelitian

Penelitian ini dimaksudkan untk mengetahui sejauh mana kerjasama dari Indonesia dan Australia melalui *cybercrime investigation satellite office* dalam pencegahan dan penanggulangan *cybercrime* di Indonesia

1.3.2 Tujuan Penelitian

Penelitian ini mempunyai beberapa tujuan antara lain :

1. Mengetahui proses kerjasama yang di lakukan oleh Indonesia dan Australia dalam menangani *cybercrime* melalui *cybercrime investigation satellite office*.
2. Mengetahui hasil Indonesia dan Australia melalui *cybercrime investigation satellite office* dalam mencegah dan menanggulangi *cybercrime* di Indonesia.
3. Mengetahui Prospek kerjasama Indonesia dan Australia melalui *cybercrime investigation satellite office* dalam mencegah dan menanggulangi *cybercrime* di Indonesia.

1.4 Kegunaan Penelitian

1.4.1 Kegunaan Teoritis

Secara teoritis, hasil dari penelitian ini dapat menjadi sumber atau referensi pengetahuan terkait perkembangan kerjasama Indonesia dan Australia dalam bidang keamanan untuk mengatasi masalah tindak kejahatan lintas negara yaitu *cybercrime* yang berada dikedua negara. serta dapat menambah keilmuan mengenai mengenai Keamanan Internasional tentang langkah-langkah yang dapat dilaksanakan oleh negara-negara untuk menjaga keamanan di wilayah regionalnya.

1.4.2 Kegunaan Praktis

1. Diharapkan menambah wawasan dan ilmu pengetahuan, serta dapat bermanfaat bagi para pembaca khususnya Program Studi Ilmu Hubungan Internasional mengenai *cybercrime* dan kerjasama yang di lakukan Indonesia untuk menanggulanginya.
2. Sebagai bahan referensi bagi penstudi Hubungan Internasional dan Hukum Internasional.
3. Sebagai bahan referensi bagi Pemerintah RI, Kementerian Luar Negeri dan Kepolisian Republik Indonesia