

BAB I

PENDAHULUAN

A. Latar Belakang

Pesatnya perkembangan dan kemajuan teknologi komputer, telekomunikasi dan informatika menjadikan internet sebagai sesuatu yang lumrah dalam kehidupan masyarakat di dunia ini. Internet telah menciptakan fenomena global yang sangat luar biasa pengaruhnya. Internet menjadikan segala bentuk informasi dengan mudah melintasi batas-batas wilayah yang tidak lagi memisahkan umat manusia. Kondisi negara-negara yang tanpa batas (*borderless*) tersebut telah membuka dan memperluas tren tejalannya komunikasi dan dialog global antar masyarakat dunia.

Internet telah menciptakan ruang bagi manusia di dunia ini yang disebut sebagai *cyberspace*. Departemen pertahanan Amerika Serikat mendefinisikan "*cyberspace*" sebagai "sebuah domain berisi informasi yang terdiri dari infrastruktur teknologi informasi yang jaringannya dapat terhubung, termasuk internet, jaringan telekomunikasi, sistem komputer, dan prosessor dan pengendali yang terintegrasi. Dengan adanya *cyberspace* setiap orang dipenjuru dunia manapun dapat merasakan berada disebuah ruang dimana mereka dapat berkomunikasi dan dialog satu sama lain".

Tidak bisa dipungkiri perkembangan internet sebagai salah satu produk kemajuan arus teknologi yang membawa dampak positif maupun juga dampak negatif. Dampak yang bersifat positif dapat disyukuri karena banyak yang bisa diperoleh dari teknologi ini. Namun, tidak dapat dipungkiri bahwa internet

sebagai produk kemajuan teknologi juga mempunyai dampak negatif yang sangat membahayakan. Bentuknya yaitu kejahatan-kejahatan seperti pengancaman, pencurian, dan penipuan di dunia maya yang disebut sebagai kejahatan dunia maya atau *cybercrime*.

Kejahatan dunia maya mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk ke dalam kejahatan dunia maya antara lain adalah penipuan lelang secara *online*, pemalsuan cek, penipuan kartu kredit, penipuan identitas dan pornografi anak.¹ Walaupun, kejahatan dunia maya atau *cybercrime* umumnya mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer sebagai unsur utamanya. Istilah ini juga digunakan untuk kegiatan kejahatan tradisional di mana komputer atau jaringan komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi. Contoh kejahatan dunia maya di mana komputer sebagai alat adalah *spamming* dan kejahatan terhadap hak cipta dan kekayaan intelektual. Contoh kejahatan dunia maya di mana komputer sebagai sasarannya adalah akses ilegal (mengelabui kontrol akses). Contoh kejahatan dunia maya di mana komputer sebagai tempatnya adalah penipuan identitas. Sedangkan contoh kejahatan tradisional dengan komputer sebagai alatnya adalah pornografi anak dan judi *online*.²

Kemajuan teknologi tersebut yang tidak hanya membantu manusia dalam memudahkan pekerjaannya, tetapi juga menjadi lahan baru bagi pelaku kriminal dunia maya untuk melakukan aksinya. Dalam dunia maya, masalah keamanan

¹ <http://wikipedia.org/cybercrime>, Diakses tanggal 16 September 2013

² H. Hussein, *Kebijakan Pemerintah Indonesia Dalam Penanganan Cyber Crime* (Studi Kasus: Cyberwar Indonesia Malaysia) 2011.

merupakan suatu hal yang sangat penting. Tingginya tingkat kriminal dalam dunia internet/cyber dan lemahnya hukum dalam hal pengamanan dan penanganan kasus *cybercrime* ini, menyebabkan semakin maraknya kejahatan-kejahatan yang terjadi dalam dunia *cyber* tersebut. Ditambah lagi kecilnya kemungkinan ditangkapnya pelaku dan kemajuan teknologi yang mempermudah aksi mereka. Seseorang yang melakukan kejahatan jenis ini, terkadang tidak memiliki motif untuk meraup keuntungan ekonomis, tetapi juga karena unsur lain seperti tantangan, hoby dan bahkan membuktikan tingkat intelijen yang dimilikinya dan kebolehan teknis yang terlibat didalamnya. Yang pada intinya, pelaku menggunakan kekreativitasnya untuk melakukan aksinya tersebut.

Aktivitas *cybercrime* dapat terjadi kapan saja dan dimana saja, tidak hanya di negara maju tetapi juga di negara berkembang. Yang patut diperhatikan dan dikhawatirkan adalah bahwa aktivitas *cybercrime* justru banyak terjadi dan berasal dari negara-negara berkembang seperti Ukraina, Pakistan dan Indonesia sendiri, yang tidak lain disebabkan karena hukum yang lemah dan kurangnya perhatian terhadap masalah ini di negara tersebut dalam mengatur penggunaan akses informasi global tersebut. Dalam hal ini *cyber law* dan *cyber policy*.³

Cybercrime tergolong tindak kejahatan internasional, sesuai dengan hukum internasional yang menjelaskan tentang defenisi tindak kejahatan internasional yaitu tindak kejahatan yang mempengaruhi legitimasi beberapa atau semua negara yang mengakibatkan ancaman bahaya terhadap hubungan masyarakat internasional

³Olan Rinto,2007, Prospek Penanganan Cyber Crime Dalam Kerangka Kerjasama Keamanan Asean, skripsi Universitas Hasanuddin, Makassar. hal 4

Sebagai contoh adalah hubungan bilateral Indonesia Malaysia yang sempat memanas. Begitu banyaknya perlakuan tidak adil masyarakat Malaysia terhadap rakyat Indonesia seperti penganiayaan para Tenaga Kerja Indonesia (TKI) di Malaysia, adanya sebutan *Indon* yang berarti pembantu untuk masyarakat Indonesia yang berada di Malaysia, hingga kasus banyaknya budaya Indonesia yang diklaim oleh Negara Malaysia sebagai budaya mereka, dan yang paling terakhir adalah kekalahan Malaysia dalam turnamen sepakbola internasional AFF. Dari kasus-kasus seperti itulah yang menimbulkan kemarahan bagi masyarakat Indonesia. Tidak hanya dalam dunia nyata tapi kini konflik kedua negara tersebut beralih ke dunia maya. Kedua negara tersebut terlibat dalam *cyberwar* atau konflik/perang di dunia maya dan tindakan seperti ini termasuk dalam kejahatan dunia maya atau *cybercrime*.

Menurut perusahaan *Security Clear Commerce* di Texas USA, saat ini Indonesia menduduki peringkat ke 2 setelah Ukraina dalam hal kejahatan *Carding* dengan memanfaatkan teknologi informasi (Internet) yaitu menggunakan nomor kartu kredit orang lain untuk melakukan pemesanan barang secara *online*. Komunikasi awalnya dibangun melalui *e-mail* untuk menanyakan kondisi barang dan melakukan transaksi. Setelah terjadi kesepakatan, pelaku memberikan nomor kartu kreditnya dan penjual mengirimkan barangnya, cara ini relatif aman bagi pelaku karena penjual biasanya membutuhkan 3 -5 hari untuk melakukan kliring atau pencairan dana sehingga pada saat penjual mengetahui bahwa nomor kartu kredit tersebut bukan milik pelaku barang sudah terlanjur terkirim.⁴

⁴Laisa Nurin, artikel dengan judul *Perkembangan Cybercrime Di Indonesia*, 2013

Indonesia menyadari bahwa *cybercrime* bukanlah kejahatan yang tidak bisa dianggap sepele. Seiring dengan perkembangan internet yang sangat pesat di dunia yang global ini semakin mudah juga para pelaku kriminal di dunia maya yang semakin leluasa untuk melakukan kejahatan. Indonesia sebagai negara dengan berada di posisi ke-2 sebagai sumber serangan siber. Setelah China, Indonesia memimpin dari 177 negara sebagai pusat pusaran arus *cyber crime*. China di urutan teratas untuk paruh awal tahun 2013. Namun prosentasenya menurun hingga di angka 34% dari tahun sebelumnya pada kuartal terakhir 2012 yang sempat di angka 41%. Indonesia sendiri angkanya melonjak jadi 21% setelah sebelumnya hanya 0,7% pada kuartal terakhir 2012. Sedangkan di posisi ke-3 ada AS yang turun jadi 8,3%. Sebelumnya AS ini miliki prosentase 10%.⁵

Ancaman *cybercrime* yang berujung pada kerugian moril dan material dan dapat menimpa siapa saja. Tidak hanya itu bahwa Kejahatan dunia maya dapat juga membahayakan dalam berbagai aspek negara seperti halnya dalam bidang ekonomi dan politik. Ancaman *cybercrime* yang sangat membahayakan perlu diwaspadai oleh Indonesia. Berbagai ancaman dapat saja membahayakan Indonesia sendiri, ancaman kejahatan dunia maya yang mungkin hanya sekedar pencemaran nama baik, pencurian data dan pembajakan data data penting negara bisa berimbas atau pemicu terjadinya putusannya hubungan dua negara yang awalnya sangat baik dan menguntungkan kedua belah pihak. Tidak hanya itu kemungkinan terburuk adalah konflik fisik yang sangat merugikan antara dua negara. Sebagai contoh adalah apa yang terjadi belum lama ini di akhir bulan

⁵<http://sidomi.com/204986/indonesia-peringkat-ke-2-di-dunia-untuk-kasus-kejahatan-cyber/> di akses pada tanggal 17 September 2013

seperti TNI dan diplomat dari Australia. Hal ini yang perlu di waspadai dan di perhatikan Indonesia lebih serius lagi.

Terkait dengan terus meningkatnya kasus *cybercrime* yang terjadi di Indonesia dan menjadikan Indonesia peringkat kedua setelah Cina, hal ini menjadi perhatian khusus pemerintah untuk menangani masalah tersebut. Pemerintah dan Kepolisian Republik Indonesia telah berupaya untuk terus mengurangi dan memerangi *cybercrime*.

B. Pokok Permasalahan

Dari pemaparan diatas dapat ditarik rumusan masalah “ Bagaimana upaya yang dilakukan Pemerintah Indonesia dalam menanggulangi masalah *cybercrime*?

C. Kerangka Dasar Pemikiran

1. Konsep Keamanan non Tradisional

Pasca Perang Dingin keamanan tidak lagi dapat diartikan sempit sebagai hubungan konflik atau kerjasama antar negara, tetapi menyangkut juga keamanan untuk masyarakat (Human Security). Hal ini didasari oleh beberapa hal. Pertama setelah berakhirnya perang tersebut penyelesaian keamanan yang lebih mengedepankan kekuatan militer dianggap hanya memberikan keamanan untuk sebagian orang, sementara di pihak lain sebagian orang merasa terancam penderitaan dan ketakutan. Kedua meningkatnya interdependensi dan semakin kompleknya jaringan hubungan antar bangsa dalam era globalisasi. Ketiga adanya berbagai konflik di berbagai belahan dunia seperti konflik etnis, konflik antara negara maju dan negara

terbelakang, pelanggaran hak asasi manusia (HAM) oleh rezim otoriter dan juga pesatnya arus globalisasi dan perkembangan teknologi informasi.

Sebagai efek dari perluasan makna dari definisi keamanan tradisional menjadi non tradisional disamping melibatkan negara sebagai aktor utama juga melibatkan aktor-aktor selain negara. Dalam keamanan juga nantinya isu-isu yang mengemuka juga menjadi beragam seperti konflik SARA, ketidakamanan ekonomi, dan degradasi lingkungan. Kemudian yang terakhir adalah adanya keinginan untuk melindungi nilai-nilai baru dalam konteks keamanan seperti penghormatan pada HAM, demokratisasi, perhatian masalah kejahatan lintas negara (transnational crime) maupun perhatian terhadap masalah lingkungan. Keamanan non tradisional sebagai bagian dari efek globalisasi kemudian menimbulkan peningkatan gerakan-gerakan mandiri yang lepas dari kerangka negara.⁶

Anthoni (2010) dalam tulisannya yang berjudul *Non-Traditional Security Challenges, Regional Governance, and the ASEAN Political Security Community (APSC)*, menyatakan bahwa keamanan non tradisional didefinisikan sebagai tantangan dan ancaman terhadap kelangsungan hidup dan kesejahteraan bangsa dan negara yang timbul terutama dari aspek aspek nontradisional. Ancaman keamanan non tradisional memiliki karakteristik umum sebagai berikut :

⁶<http://khunaipi.student.umm.ac.id/2010/04/16/konsepsi-keamanan-pasca-perang-dingin-dari-konseptradisional-menuju-non-tradisional/> diakses pada tanggal 17 September 2013

- Muncul dalam waktu yang singkat dan bertranmisi dengan cepat sebagai dampak dari globalisasi dan revolusi komunikasi
- Merupakan gejala global yang tidak dapat diselesaikan oleh satu negara saja, melainkan harus melalui kerjasama regional atau internasional.
- Sasarannya secara umum tidak lagi sebatas negara (kedaulatan negara atau integritas teritorial), tetapi juga secara khusus masyarakat suatu negara.

Pertumbuhan ancaman dalam bidang keamanan nontradisional baik nasional maupun internasional, muncul dari berbagai bidang yang berbeda, seperti gejolak keuangan, *cybercrime*, perdagangan obat-obatan terlarang, perdagangan manusia, terorisme dan lain lain. Semua bidang tersebut sebelumnya dalam sejarah manusia tidak mempunyai pengaruh yang berarti terhadap negara maupun masyarakat internasional.⁷ Namun pada saat ini ancaman yang datang dari keamanan non-tadisional semakin serius dan mengkhawatirkan seperti halnya *cybercrime* yang kasusnya semakin berkembang dan membahayakan.

Tidak bisa dipungkiri perkembangan internet sebagai salah satu produk kemajuan arus teknologi yang membawa dampak positif maupun juga dampak negatif. Dalam dunia maya, masalah keamanan merupakan suatu hal yang sangat penting. Tingginya tingkat kriminal dalam dunia intrenet/*cyber* dan lemahnya hukum dalam hal pengamanan dan penanganan kasus *cyber*

⁷<http://irchina.org/en/xueren/china/view.asp?id=709> diakses pada tanggal 17 September 2013

crime ini, menyebabkan semakin maraknya kejahatan-kejahatan yang terjadi dalam dunia *cyber* tersebut. Pada akhir akhir ini perkembangan *cybercrime* di Indonesia sangat mengkhawatirkan. Indonesia menyadari bahwa bahwa bahaya dari *cybercrime* tidak dapat dianggap sepele. Peran pemerintah dan kesadaran masyarakat sangat diperlukan dalam menangani masalah *cybercrime* tersebut.

2. Konsep Kejahatan Transnasional

Istilah kejahatan transnasional atau *transnational crime* merupakan perkembangan dari identifikasi keberadaan karakteristik baru dari bentuk kontemporer dari *organized crime* pada masa tahun 1970-an oleh sejumlah organisasi internasional. Sedangkan pengenalan istilah tersebut pertama kali dikemukakan dalam Kongres PBB mengenai Pencegahan Kejahatan dan Penanggulangan Pelaku Kejahatan (United Nations' Congress on the prevention of crime and the treatment of offenders) pada tahun 1975. Istilah *transnational crime* diperkenalkan untuk menjelaskan kaitan kompleks yang ada antara *organized crime*, *white-collar crime* dan korupsi yang merupakan masalah serius yang dimunculkan akibat "kejahatan sebagai bisnis" (*crime as business*).

Pengaturan kegiatan kejahatan melangkaui perbatasan negara dan berdampak pada pelanggaran hukum berbagai negara, telah menjadi karakteristik yang paling membahayakan dari kelompok kejahatan yang

bergiat di tingkatan internasional.⁸ Dalam perkembangannya, bentuk kejahatan yang diistilahkan tersebut, telah seringkali dikaitkan dengan konteks globalisasi (yang merupakan representasi dari kondisi sosial, ekonomi dan kultural sekarang ini).

Secara konsep, *transnational crime* merupakan tindak pidana atau kejahatan yang melintasi batas negara. Pada tahun 1995, PBB telah mengidentifikasi 18 jenis kejahatan transnasional, yaitu pencucian uang, terorisme, pencurian benda seni dan budaya, pencurian kekayaan intelektual, perdagangan senjata gelap, pembajakan pesawat, pembajakan laut, penipuan asuransi, kejahatan dunia maya, kejahatan lingkungan, perdagangan orang, perdagangan bagian tubuh manusia, perdagangan narkoba, penipuan kepaillitan, infiltrasi bisnis, korupsi, dan penyuapan pejabat publik atau pihak tertentu.⁹

Suatu kejahatan dapat dikategorikan sebagai kejahatan transnasional atau bukan dapat dilihat dari:

1. melintasi batas negara,
2. pelaku lebih dari satu, bisa nation-state actor ataupun yang lain,
3. memiliki efek terhadap negara ataupun aktor internasional (misalnya individu dalam pandangan kosmopolitan) di negara lain,
4. melanggar hukum di lebih dari satu negara.

⁸ Monica Massari, "Transnational Organized Crime between Myth and Reality: the Italian Case," 2001. diakses pada www.essex.ac.uk/ecpr/events/jointsessions/paperarchive/grenoble/ws8/massari.pdf.

⁹Garda T. Paripurna, Sekilas Tentang Kejahatan Transnasional, Riset Hukum Kejahatan Transnasional, 2008,

Dari konsep kejahatan transnasional diatas bahwa *cybercrime* termasuk salah satu dari kejahatan transasional. Hal ini dikarenakan bahwa *cybercrime* merupakan kejahatan lintas negara atau juga bisa dikatakan kejahatan internasional yang dapat mengancam negara satu dan lainnya. Para pelaku *cybercrime* juga tidak hanya aktor negara saja melainkan bisa individu dan non-state.

3. Konsep Kerjasama Internasional

Menurut *K.J Holsti* yang mendefinisikan kerjasama Internasional adalah "Sebagian besar transaksi atau interaksi negara dalam sistem Internasional sekarang ini bersifat rutin dan hampir bebas dari konflik. Berbagai jenis masalah nasional, regional dan global bermunculan dan memerlukan perhatian dari berbagai negara. Banyak kasus yang terjadi, sehingga pemerintah saling berhubungan atau melakukan pembicaraan mengenai masalah yang dihadapi dan mengemukakan berbagai bukti teknis untuk menyelesaikan permasalahan tertentu, beberapa perjanjian yang memuaskan semua pihak, ini yang disebut dengan kerjasama."¹⁰

Proses kerjasama ini tercipta dikarenakan adanya rasa saling membutuhkan satu sama lain demi kepentingan nasional kedua negara. Hal ini dikarenakan dalam hidup bermasyarakat, tidak bisa terlepas dari hubungan antara satu dengan yang lainnya, hubungan yang terjadi inilah yang bisa disebut dengan interaksi. Interaksi sendiri dapat merupakan suatu hubungan

¹⁰K.J Holsti, "Politik Internasional Studi Analisis II", Erlangga, Jakarta, 1998 hal.89

sosial yang dinamis antara orang-perorangan, antara kelompok manusia, maupun antara kelompok manusia dengan orang-perorangan.

Dalam era globalisasi frekuensi interaksi antar negara-negara menjadi bertambah tinggi yang disebabkan oleh perkembangan teknologi dan ilmu pengetahuan. Interaksi tersebut menyebabkan terbentuknya suatu kerjasama baik dalam bidang ekonomi, sosial, budaya, politik, pendidikan, kesehatan maupun dalam bidang pertahanan dan keamanan yang didasari dengan perjanjian untuk mengawasi terbentuknya kerjasama dengan negara lain. Sehingga kerjasama antar negara dapat meningkatkan hubungan negara-negara di dunia internasional menjadi semakin harmonis.

Pada akhir akhir ini perkembangan *cybercrime* di Indonesia sangat mengkhawatirkan. Indonesia menyadari bahwa bahwa bahaya dari *cybercrime* tidak dapat dianggap sepele. Peran pemerintah dan kesadaran masyarakat sangat diperlukan dalam menangani masalah *cybercrime*. Ancaman *cybercrime* yang berujung pada kerugian moral dan material dan dapat menimpa siapa saja. Tidak hanya itu bahwa kejahatan dunia maya dapat juga membahayakan dal berbagai aspek negara seperti halnya dalam bidang ekonomi dan politik.

Berdasarkan teori kerjasama internasional tersebut bahwa indonesia dalam menaggulangi masalah *cybercrime* yan terjadi didalam negri salah satu upayanya yaitu menempuh kerjasama kerjasama internasional baik dengan

negara tetangga maupun dengan organisasi organisasi keamanan internasional maupun organisasi organisasi di kawasan.

D. Hipotesa

Dari pemaparan latar belakang dan perumusan masalah diatas peneliti dapat menarik hipotesis yaitu bahwa Indonesia melakukan penanggulangan mengenai masalah *cybercrime* yang terjadi di dalam negri dengan melakukan kerjasama-kerjasama internasional baik bilateral yaitu dengan Australia maupun multilateral dalam kerangka ASEAN yaitu dengan *ASEAN Chief of Police*(ASEANAPOL).

E. Tujuan Penelitian

1. Memperluas, mengkaji, memperdalam dan mengetahui arti pentingnya pengetahuan tentang metodologi dan teori-teori Hubungan Internasional.
2. Penerapan teori-teori Hubungan Internasional pada kasus yang aktual sesuai dengan rumusan masalah.
3. Pemenuhan tugas akhir sebagai mahasiswa jurusan Ilmu Hubungan Internasional, Universitas Muhammadiyah Yogyakarta.

F. Jangkauan Penelitian

Agar pembahasan tidak meluas serta melenceng dari kajian masalah serta judul yang ada dan mudah dimengerti maka penulis membatasi penelitian hanya berfokus pada kerjasama yang dilakukan indonesia dalam kerjasamanya di lingkup Asia Pasifik baik dengan negara-negara maupun organisasi yang ada.

G. Metode Penelian

1. Jenis Penelitian

Jenis penelitian yang digunakan adalah deskriptif analitik dimana dalam penelitian ini penulis mendeskripsikan tentang upaya indonesia dalam menanggulangi masalah *cybercrime* dengan menjalin kerjasama antar negara atau dengan organisasi yang ada.

2. Jenis Data

Data dalam penelitian ini adalah data sekunder yaitu data yang diperoleh dari buku, artikel dan media elektronik.

3. Teknik Pengumpulan Data

Data dari penelitian ini adalah data sekunder yang diperoleh dari berbagai sumber, baik buku bacaan serta jurnal-jurnal ilmiah yang didapat dari berbagai media baik cetak maupun elektronik.

4. Teknik Analisis Data

Pada prosedur analisis sendiri menggunakan berbagai teori yaitu teori kepentingan nasional dan konsep kerjasama Internasional. Kemudian dikaitkan dengan fakta yang terjadi pada kasus dalam skripsi tersebut. Teknik analisis data pada penelitian ini menggunakan data kualitatif dengan metode analisis dan kajian sejarah yaitu menjelaskan dan menggambarkan data berdasarkan sumber-sumber tertulis yang ada.

H. Sistematika Penulisan

Untuk mengetahui dan memperjelas dalam mengetahui garis besar penyusunan skripsi ini, maka penulis akan menyajikan sistematika skripsi sebagai berikut :

BAB I: Pendahuluan

Dalam bab ini akan memuat ketentuan-ketentuan pokok dalam penyusunan skripsi yaitu latar belakang masalah, perumusan masalah, tujuan penelitian, manfaat penelitian, kerangka dasar penelitian, kerangka dasar pemikiran, hipotesis serta metodologi penelitian.

BAB 11: *Cybercrime* Sebagai Kejahatan Transnasional

Dalam bab ini akan dibahas secara mendalam mengenai pengertian dan mengulas lebih dalam mengenai *cybercrime* sebagai kejahatan transnasional dan bentuk bentuk *cybercrime* itu sendiri.

BAB III: *Cybercrime* di Indonesia

Dalam bab ini penulis menguraikan tentang *cybercrime* di Indonesia dan juga ancamannya sehingga perlu adanya upaya dari pemerintah untuk menaggulangnya.

BAB IV :Upaya yang dilakukan Indonesia dalam menaggulangi *Cybercrime*

Dalam bab ini akan dibahas dengan menggunakan analisis bagaimana upaya yang dilakukan Indonesia dalam menaggulangi masalah *cybercrime* itu sendiri di Indonesia.

BAB V : Kesimpulan

Pada bab Kesimpulan dan saran ini berisi mengenai kesimpulan dan dari hasil penelitian.