BAB 1

PENDAHULUAN

A. Latar Belakang Masalah

Pemerintah Indonesia pada saat ini mengalami salah satu masalah yang serius dalam kejahatan yaitu *Cybercrime*. *Cybercrime* adalah tindak Kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama, *Cybercrime* merupakan kejahatan yang memanfaatakan perkembangan teknologi komputer khususnya internet. Di Negara-negara maju kasus kejahatan seperti ini juga marak tidak hanya terjadi seperti di Amerika dan Eropa namuin juga di Negara berkembang yang ada di Asia dan Afrika.

Hal serupa juga terjadi di Indonesia. Kasus kejahatan Pencurian Transaksi elektronik dengan via *transfer* dan pencemaran nama baik melalui akun media sosial sering menjadi kasus yang terjadi hingga saat ini, Kasus kejahatan dunia maya atau yang lebih dikenal dengan *cyber crime*, untuk meminimalisir atau mengurangi kasus kejahatan tersebut maka diperlukan pengawasan yang ketat dan undang-undang untuk memberikan perlindungan serta jaminan keamanan untuk para pengguna teknologi informasi.

Kegagalan pemberantasan *cyber crime* di Indonesia berdampak buruk bagi pemerintah, masyarakat dan korban. Bagi Negara (Pemerintah) kegagalan tersebut dapat menghambat proses pencapaian tujuan Negara RI, Dan akan menurunkan kredebilitas pemerintah di mata warganya, bagi masyarakat kegagalan pemberantasan *cyber crime* akan menambah rasa kekhawatiran dan traumatik dalam pemanfaatan teknologi informasi. Bagi korban kegagalan pemberantasan *cyber crime* akan menambah penderitaannya karena kerugianya tidak akan bisa diganti (dipulihkan) Salah satu penyebab lain tentang kegagalan pemberantasan *cyber crime* di Indonesia adalah setelah pemerintah mengesahkan Undang-Undang No 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik atau yang lebih dikenal UU ITE 2008 kejahatan *cyber crime* di Indonesia justru semakin meningkat dari tahun ketahun. Selain itu belum dipahaminya secara memadai tentang apakah *cyber crime*, bagaimanakah bentuk-bentuk *cyber crime*, apakah bahaya *cyber crime*, apakah ancaman

pidana terhadap pelaku *cyber crime,* dan bagaiamankah penegakan *cyber law*. Pemahaman *cyber crime* yang memadai akan mendorong setiap orang agar tidak menjadi korban. Pemahaman *cyber law* yang sempurna bagi penegak hukum akan dapat membantu dalam menyelesaikan kasus *cyber crime* secara represif melalui penerapan hukum pidana di bidang teknologi informasi.[1]

Kejahatan *cyber crime* di Indoensia tidak hanya berdampak pada dalam negeri namun juga merambat sampai keluar negeri tanpa mengenal batas teritorial Negara lain, dan tidak terikat pada ruang dan waktu sebab kejahatan *cyber crime* bisa dilakukan dimanapun dan kapan saja. Selain rawan sebagai tempat sasaran Indoensia juga merupakan salah satu tempat beroperasinya kejahatan sindikat *cyber crime* Internasional seperti penipuan jual beli online, penipuan kartu kredit, pemerasan dan bahkan mengancam sistem pertahanan keamanan.

MABES POLRI (Markas Besar Polisi Republik Indoensia) pada tahun 2015, sudah melaksanakan operasi penggrebekan jaringan sindikat *cyber crime* Internasional dari Cina (Tiongkok) yang beroperasi di Indoensia. Sindikat tersebut melakukan motif kejahatan sebagai alat untuk menarik keuntungan berupa sejumlah uang yang di dapat dari penipuan kepada warga Cina (Tiongkok) yang tekena masalah hukum atau skandal, para sindikat tersebut berpura-pura menyamar sebagai petugas penegak hukum seperti jaksa, petugas perpajakan dan polisi, kemudian mereka mengancam dan memeras warga cina yang terkena masalah hukum tersebut untuk mengirimkan sejumlah uang ke nomer rekening yang sudah disiapkan oleh sindikat tersebut.

Selain itu pihak kepolisian juga telah mengungkap kasus pencurian uang dari perusahaan asing dan Indoensia oleh sindikat internasional dari Nigeria yang mana juga beroperasi di Indonesia, dengan membajak *e-mail* resmi dari perusahaan tersebut sindikat tersebut berpura-pura menyamar sebagai perusahaan resmi dan mengalihkan pembayaran transaksi ke nomer rekening yang telah mereka siapkan. Walaupun pemerintah sudah membuat undang-undang ITE No 11 2008 tingkat kejahatan mayantara atau *cyber crime* di Indonesia justru semakin meningkat di Indonesia. Berdsarkan data *Norton Report* tahun 2013, tingkat potensi dan resiko tindak kejahatan *cyber* di Indonesia sudah memasuki status

[1] *ASPEK HUKUM PIDANA KEJAHATAN MAYANTARA* Widodo

darurat. Diungkapkan terdapat sekitar 400 juta korban kejahatan *cyber* di Indonesia tiap tahunya dengan kerugian finanasial mencapai USD 113 Miliar, sementara menurut hasil riset yang dirilis oleh Indonesia *Security Response Team*, di tahun 2011 lalu saja tercatat kurang lebih 1 juta serangan *cyber* yang ditujukan para pengguna internet di Indonesia tiap harinya. Mayoritas serangan tersebut hadir dalam bentuk *malware* ataupun *phisisng* dan lebih menyasar pada institusi perbankan dan pemerintah.

Fakta tersebut membuktikan bahwa fasilitas internet di Indonesia masih belum aman oleh para pengguna teknologi informasi, Hal ini disebabakan fasilitas teknologi informasi di indoensia sudah memadai dan cukup lengkap namun masih lemah pada aspek pengawasan, selain itu mudahnya pemasanagan jaringan internet dan komunikasi di Indonesia dinilai merupakan faktor utama yang menyebabkan mudahnya pelaku *cyber crime* melakukan aksinya. Pelaku *cyber crime* memiliki berbagai macam motif baik secara langsung dan tidak langsung, diantaranya balas dendam, uji keahlian, ekonomi, politik dan lain sebagainya. Aksi penyalahgunaan teknologi informasi tidak bisa terlihat secara fisik namun memiliki dampak yang nyata bagi para korban.

Selain itu pelakunya juga tidak memandang usia, rata-rata diatas usia 18 tahun sampai 40 tahun dan kebanyakan dari pelaku berjenis kelamin pria. Untuk mendalami *cyber crime* maka terlebih dahulu memahami istilah *cyber space, atau* dunia maya dipandang sebagai dunia komunikasi yang berbasis komputer. Dalam hal ini, *cyber space (*dunia maya) dianggap sebagai sebuah realitas baru dalam kehidupan manusia yang dikenal dalam bahasa kehidupan sehari-hari sebagai *Internet.*

Relaitas baru ini dalam kenyataanya terbentuk melalui jaringan komputer yang menghubungkan antar Negara atau antar benua yang berbasis *protocol transmission control protocol/internet protocol*. Hal ini berarti dalam sistem kerjanya, dapatlah dikatakan *bahwa cyber space* (internet) telah mengubah jarak dan waktu menjadi tidak terbatas. Internet digambarkan sebagai kumpulan jaringan Komputer yang terdiri dari sejumlah jaringan yang lebih kecil yang mempunyai sistem jaringan yang berbeda-beda.[2] Dalam perkembangan selanjutnya perkembangan teknologi canggih Komputer dengan jaringan Internet telah

[2] Kenny Wiston, 2002*, the internet issues of jurisdiction and controversies surrounding domain names*, bandung, citra aditya hlm vii

membawa manfaat besar bagi manusia. pemanfaatanya tidak saja dalam pemerintahan, dunia swasta/perusahaan, akan tetapi sudah menjangkau pada seluruh sektor termasuk segala keperluan rumah tangga (pribadi). komputer (internet) telah membuka cakrawala baru dalam konteks kehidupan manusia baik sarana komunikasi dan informasi yang menjanjikan menembus batas-batas Negara maupun penyebaran dan petukaran ilmu pengetahuan dan gagasan kalangan ilmuan di seluruh dunia.

Akan tetapi kemajuan teknologi informasi (internet) dan segala bentuk manfaat di dalamnya membawa dampak negatif tersendiri, dimana semakin mudahnya para penjahat melakukan aksinya yang semakin merisuakan masyarakat. Penyalahgunaan yang terjadi dalam *cyber space* inilah yang dikenal sebagai *cyber crime* atau dalam literatur lain digunakan istilah *computer crime.* Dari pengertian tersebut maka dapat dirumuskan bahwa *computer crime* merupakan perbuatan yang melawan yang dilakukan dengan memakai komputer sebagai sasaran/alat atau komputer sebagai objek baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.

B. Rumusan Masalah

Dari uraian yang telah dijelaskan diatas maka rumusan masalah dalam penelitian ini adalah sebagai berikut " **Mengapa pemerintah Indonesia masih belum efektif memberantas kejahatan *cyber crime* ?**

C. Tujuan Riset

Adapun tujuan riset yang dilakukan dalam penelitian ini adalah sebagai berikut:

a) Untuk mengetahui bagaimanakah kejahatan *cyber crime* bisa terjadi di Indonesia
b) Untuk mengetahui bagimanakah upaya pemerintah dalam penanggulangan *cyber crime* yang terjadi dan beroperasi di Indonesia

D. Kontribusi Riset

Adapun kontribusi riset dari penelitian ini adalah sebagai berikut:

a) Secara akademis penelitian ini diharapkan dapat menambah wawasan kepada mahasiswa terutama mahasiswa jurusan Hubungan Internasional

mengenai *cyber crime* dikarenakan kasus kejahatan ini sudah mencakup kejahatan transnasional

b) Secara praktis penelitian ini juga dapat menambah wawasan bagi mahasiswa terhadap upaya pemerintah dalam mengungkap kasus *cyber crime*

E. Tinjauan Pustaka

Sejauh ini, sudah banyak berbagai penelitian yang membahas menegnai kejahatan dunia maya atau *cyber crime*, namun masih belum cukup untuk membahas lebih dalam dan rinci mengenai proses terjadinya *cyber crime* serta faktor-faktor apa sajakah yang membuat seseorang melakukan tindakan kejahatan *cyber crime*. Padahal dari *cyber crime* kita juga dapat menentukan langkah-langkah pencegahan tindakan kejahatan tersebut dengan memberlakukan dan mengembangkan *cyber law*, *cyber security* dan juga *cyber patrol.*

Dalam penelitian, ini penulis menggunakan beberapa penelitian yang telah dilakukan sebelumnya oleh para peneliti sebelumnya. Hal tersebut dilakukan untuk menegtahui letak perbedaan antara penelitian yang dilakukan oleh penulis dan peneliti sebelumnya. Kajian pustaka dalam penelitian ini adalah buku "kejahatan Siber *cyber crime"* suatu pengantar tentang kejahatan *cyber* yang ditulis oleh MASKUN, dalam buku tersebut menjelaskan bagaimana proses perkembangan kejahatan *cyber* dari waktu ke waktu baik dari jenis dan potensi-potensi yang memicu terjadinya kejahatan tersebut.

Buku ini juga telah melampirkan secara utuh mengenai undang-undang ITE 2008 yang telah disahkan oleh penegak hukum baik kepolisian, jaksa dan pemerintah republik Indoensia yang juga disahkan oleh presiden. Undang-undang tersebut juga menyertakan hasil konvensi atau perundang-undangan Internasional "*DRAFT INTERNATIONAL CONVENTION TO ENHANCE PROTECTION FROM CYBER CRIME AND TERRORISM*" yang disahkan oleh aktor-aktor Internasional dalam melawan kejahatan *cyber crime.*

Perlu dikethaui bahwa Undang-Undang ITE 2008 juga menjadikan konvensi ini sebagai bahan dasar acuan menerapkan *cyber law* atau undang undang kejahatan *cyber crime* oleh Indonesia dan Negara-negara lain. Dalam buku ini dijelaskan bahwa kejahatan *cyber crime* berdampak langsung pada segala aspek kehidupan masyarakat yang mana

tindak kejahatan dunia maya dilakukan secara maya atau *cyber space* namun memiliki dampak pada kehidupan nyata atau *real life*. Buku ini juga menjelaskan bahwa kerjasama Internasional dalam memerangi kejahatn *cyber crime* sangat penting untuk mempercepat pengungkapan kasus-kasus kejahatan dunia maya.

Penelitian kedua adalah tulisan Prof Dr. Widodo, SH., M.H yamg berjudul "MEMERANGI *CYBERCRIME* Karakterisitk, Motivasi dan Strategi Penagganannya dalam Prespektif Kriminologi". Penelitian pada buku ini menjelaskan tentang langkah-langkah memerangi kejahatan *cyber crime* dengan menggunakan analisis prespektif krimonologi. perlu dipahami bahwa kejahatan tindak pidana dunia maya tidak terlihat secara fisik namun memiliki dampak yang nyata. Aspek kriminologi yang digunakan untuk melacak pelaku kejahatan dunia maya/*cyber crime* berupa barang bukti dan motif pelaku.

Penanganan tindak kejahatan tentu berbeda dengan mengungkap kasus seperti pembunuhan, pencurian, perampokan dan kejahatan lain yang terjadi disekitar kita. Strategi penanganan *cyber crime* harus menggunakan teknologi informasi komputer guna melacak alamat *IP Adrress* pelaku dan merekam semua tindak kejahatan di dunia maya. Laporan dari korban juga akan sangat membantu pihak penyidik dalam mengungkap kasus tersebut.

Bukti kejahatan di dunia maya dapat dengan mudah dimusnahkan oleh pelaku, jika pelaku sudah curiga gerak geriknya sudah dilacak oleh penyidik *cyber crime*, maka akan berakibat pada proses vonis hukum di pengadilan. Untuk menangkap pelaku kejahatan *cyber* maka bukti-bukti yang disajikan oleh penyidik harus valid dan benar-benar real/nyata dengan mengamankan alat-alat yang digunakan oleh pelaku seperti komputer, telpeon/samrtphone dan peralatan elektronik lainya. Selain barang bukti yang sudah diamankan oleh pihak penyidik, motif pelaku juga akan sangat menentukan jenis kejahatan apakah motif ekonomi, politik, SARA, pencemaran nama baik, balas dendam dan lain sebagainya.

Peneleitian yang ke tiga yang digunakan sebagai acuan ialah tulisan Dr. Widodo yang berjudul "Aspek Hukum Kejahatan Mayantara" tulisan pada buku ini lebih menitikberatkan mengenai proses peradilan pelaku kejahatan mayantara atau *cyber crime* yang telah berhasil di tangkap dan diadili sesuai dengan ketentuan undang-undang ITE

2008 dan hukum pidana yang ada di Indoensia jika pelaku memang terbukti secara meyakinkan melakukan tindak kejahatan di wilayah hukum Indonesia. Adapaun Jenis jenis kejahatan mayantara yang sering marak terjadi di Indoensia diantaranya ialah sebagai berikut

a) ***Carding*** yaitu penipuan kartu kredit dengan mencuri data korban dan melakikan transaksi secara illegal atau tidak sah tanpa ijin pemilik kartu kredit.
b) ***Phishing*** yaitu penipuan yang dilakukan dengan adanya pesan e-mail penipuan dari perusahaan yang sah misalnya (universitas, penyedia layanan internet/(ISP) internet service provider, dan bank) pesan-pesan ini biasanya mengerahkan seseorang ke situs web yang palsu untuk membocorkan informasi pribadi misalnya (password, kartu kredit, atau update akun) pelaku kemudian menggunakan informasi pribadi tersebut untuk meraup keuntungan dengan transaksi secara illegal.
c) ***Typosquatting*** yaitu penjiplakkan situs yang dapat meyesatkan pengguna internet aktivitas ini pernah terjadi pada tahun 2003 dibandung terhadap situs www.Klikbca.com ke situs jebakan www.Klikbaca.com dan www.klikbca.com, keuntungan yang diperoleh pelaku adalah mengetahui nomor rekening dan PIN dari nasabah BCA yang terkecoh dengan situs jebakan tersebut.
d) ***Phreaking*** adalah menggunakan *Internet Protocol* (IP) pihak lain secara tidak sah, baik untuk aktivitas kriminal dan non kriminal. Pelaku dapat memperoleh keuntungan, karena tidak perlu membayar penggunaan jasa internet pada pengelola internet.

Selain penjelasan mengenai jenis-jenis kejahatan mayantara tulisan penelitian pada buku ini juga menjelaskan prosedur penindakan pelaku kejahatan sesuai dengan undang-undang yang berlaku seperti proses penangkapan, pengumpulan barang bukti dan saksi-saksi seperti korban dan tenaga ahli yang berkompeten dalam bidang teknologi informasi.

Penelitian ke empat yang digunakan sebagai acuan ialah tulisan tesis Try Reza Essra yang berjudul "Kerjasama ASEAN Dalam Penanggulangan *Cyber Crime* di Asia Tenggara". Peneltitian pada tesis tersebut fokus untuk membahas kerjasama dalam menghadapi kejahatan dunia maya tingkat regional ASEAN yang mana meliputi ancaman politik, ekonomi dan keamanan kawasan, pada penelitian ini juga dibahas bahwa pada

tahun 2004 kepolisian Indonesia dan Negara-negara asia tenggara telah melakukan pelatihan menghadapi *cyber crime* di Bangkok.

Kesadaran Negara-negara ASEAN akan ancaman kejahatan dunia maya tersebut sangat rentan terjadi di kawasan ini, di samping itu Negara Philipina dan Indoensia menjadi asal serangan *cyber crime* oleh sindikat internasional. Namun Berdasarkan data statistik antara kurun waktu dari tahun 2004 hingga 2011 kerjasama kepolisian ASEAN tersebut belum mampu untuk memberantas perkembangan kasus kejahatan *cyber crime* di kawasan asia tenggara.

Disamping itu faktor penghambat yang lain adalah Negara Laos dan Myanmar masih belum memiliki undang-undang keamanan *cyber crime*. Manfaat penelitian Kerjasama ASEAN Dalam Penanggulangan *Cyber Crime* di Asia Tenggara" tersebut bagi penulis ialah memberikan gambaran informasi mengenai penanggulangan kejahatan dunia maya /*cyber crime* di tingkat regional ASEAN masih belum maksimal, sehingga akan berdampak pada penindakan pelaku kejahatan *cyber* yang bersifat transnasional *crime*, padahal kerjasama internasional berperan sangat besar untuk mempercepat penyelesaian kasus cyber crime dan melacak keberadaan pelaku kejahatan dunia maya tersebut.

Penelitian ke lima yang digunakan sebagai acuan ialah tulisan tesis oleh Satriyo Wibowo yang berjudul 'Peran *IP Address* dan *Domain Name* dalam *Cyber Jurisdiction*" penelitian ini membahas peran *IP* dan *Domain Name* dalam mengungkap kasus kejahatan *cyber crime* yang bersifat lintas Negara. Sehingga akan memunculkan permasalahan hukum antar Negara, sebab pada dasarnya setiap Negara memiliki yuridis hukum tersendiri dalam menerapkan tindakan pidana dalam hal *cyber crime*. Intinya dalam menyelidiki dan menganalisis kasus *cyber* maka hal pertama yang dilakukan oleh penyidik adalah melacak alamat *IP Address* dan *Domain name*.

IP Address adalah alamat *protocol internet* nomer identifikasi yang diberikan pada sebuah perangkat yang terhubung ke jaringan internet dengan menggunakan *protocol internet, Domain Name* adalah alamat internet penyelenggara Negara, orang, badan usaha atau masyarakat yang dapat digunakan dalam berkomunikasi melalui internet yang berupa

kode atau susunan karakter yang bersifat unik untuk menunjukan lokasi tertentu dalam internet.

Manfaat peneltitian Peran *IP Address* dan *Domain Name* dalam *Cyber Jurisdiction*" bagi penulis adalah memahami proses pengungkapan kasus *cyber crime* pada tingkat internasional atau antar Negara yang mengalami kerugian akibat kejahatan dunia maya. Setiap Negara memiliki kode dan nama internet masing-masing yang menggambarkan lokasi sumber data internet. Sehingga para penegak hukum harus berkordinasi terlebih dahulu jika *IP Address* dan *Domain name* berada diluar yuridis hukum, penelitian ini juga memberikan gambaran kepada penulis bahwa penerapan *cyber border* dan *cyber territory* akan mempercepat proses menghadapi kejahatan *cyber* sindikat internasional.

F. Kerangka Konseptual

F. 1 Kejahatan *Cyber Crime*

Berbicara masalah *cyber crime* tidak lepas dari permasalahan keamanan jaringan komputer atau keamanan *internet* dalam era global ini., apalagi jika dikaitkan dengan persoalan informasi sebagai komoditi. Informasi sebagai komoditi memerlukan kehandalan pelayanan agar apa yang disajikan tidak mengecewakan pelangganya. Untuk mencapai tingkat kehandalam tentunya informasi itu sendiri harus selalu dimukhtahirkan sehingga informasi yang disajikan tidak ketinggalan zaman. Kejahatan dunia maya *(cyber crime)* ini muncul seiring dengan perkembangan teknologi informasi yang begitu cepat untuk lebih mendalam ada beberapa pendapat dibawah ini tentang apa yang dimaksud dengan *cyber crime*? Diantaranya adalah menurut kepolisisan Inggris, *cyber crime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal/atau kriminal berteknologi tinggi dengan menyalah gunakan kemudahan teknologi digital.[3] Sedangkan menurut Peter, *Cyber Crime* adalah

" The easy of cyber crime is crimes directed at computer or a computer system. The nature of cyber crime, however, is more complex. As we will see later, cyber crime can take the form of simple snooping into a computer system for which we have no authorization it

[3] Abdul Wahid dan Mohammad Labib*, Kejahatan Mayantara (Cyber Crime*), Jakarta: PT. Rafika Aditama, 2005), hal. 40

can be the feeing of computer virus into the wild. It may be malicious vandalism by a disgruntled employee. Or it may be theft of data, money, or sensitive information using a computer system. [4]

Indra Safitri mengemukakan bahwa kejahatan dunia maya jenis kejahatan yang memanfaatkan sebuah teknologi informasi tanpa batas serta memiliki karakterisktik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan pada tingkat keamanan yang tinggi dan kredibilitas sebuah informasi yang disampaikan dan diakses oleh pelanggan *internet.*[5] Dalam dua dokumen kongrtes PBB yang dikutip oleh Barda Nawawi Arief, mengenai *The Prevention Of Crime And Treatment Of Offenders* di Havana kuba pada tahun 1990 dan di Wina Austria pada tahun 2000, menjelaskan ada dua istilah yang terkait dengan *cyber crime* yaitu *cyber crime* dan *computer related crime.*[6] Dilihat dari berbagai definisi di atas, tampak bahwa belum ada kesepakatan mengenai definisi tentang *cyber crime* atau kejahatan dunia *cyber*.

F. 2 Konsep Kebijakan Publik

Kebijakan diartikan sebagai rangkaian konsep dan asas yang menjadi garis besar dan dasar rencana dalam pelaksanaan suatu pekerjaan, kepemimpinan, dan cara bertindak tentang pemerintahan , organisasi dam sebagainya. Pernyataan cita-cita, tujuan, Prinsip dan garis pedoman untuk manajemen dalam usaha mencapai sasaran. Carl J Federick sebagaimana dikutip Leo Agustino (2008:7) mendefenisiskan kebijakan sebagai tindakan dan kegiatan yang disuslkan seseorang, kelompok atau pemerintahan dalam suatu lingkungan tertentu dimana terdapat hambatan-hambatan, kesulitan dan kesmpatan-kesempatan terhadap pelaksanaan usulan kebijaksanaan tersebut dalam rengaka mencapai tujuan tertentu. Lingkup dari studi kebijakan publik sangat luas karena mencakup berbagai bidang dan sektor seperti ekonomi, politik, sosial, budaya, hukum dan sebagainya. Disamping itu dilihat dari hirarkinya kebijakan publik dapat bersifat nasional, regional maupun lokal seperti undang-undang, peraturan pemerintah, peraturan presiden, peraturan

---

[4] Peter Stephenson, *Investigating Computer Related Crime* : A Handbook for Cooperate Investigators, (London New York Washington D.C :CRS Press,2000), hal. 56

[5] Indra Safitri, *"Tindak Pidana Di Dunia Cyber "* dalam Insider, Legal Jurnal Forum Indonesia Capital & Invesment Market.

[6] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penagnggulangan Kejahata*n, (Jakarta, Kencana Perdana Media Group, 2007), hal 24

menteri, peraturan daerah/provinsi, keputusan gubernur, peraturan daerah kabupaten/kota, dan keputusan bupati/walikota.

Secara terminology kebijakan publik (*public policy*) itu ternyata banyak sekali, tergantung dari sudut mana kita mengartikanya Easton memberikan definisi kebijakan publik sebagai *the authorative allocation of values for whole society* atau sebagai pengalokasian nilai-nilai secara paksa kepada seluruh anggota masyrakat.Laswell dan Kaplan juga mengartikan kebijakan publik sebagai *a projected program of goal, value, and practice* atau sesuatu program pencapaian tujuan, nilai-nilai dalam praktek-praktek yang terarah.

F. 3 Fenomena Global *Cyber Crime* dan *Cyber Criminal*

Dalam masyarakat modern yang meng-global seperti saat ini, kejahatan dapat dilakukan dimana saja, baik dalam ruang nyata maupun ruang maya (*cyber space*). Hal ini terjadi karena globalisasi membuka peluang terjadinya kejahatan, sehingga diperlukan penanggulangan secara bersama-sama melalui kerjasama antar pihak yang berkepentingan. *Globalization opens many oppurtunities for crime, and crime rapidly becoming global, outpacing international cooperation to fight it.* [7]

Saat ini kejahatan di dunia mayantara (*cyber crime)* makin banyak jumlahnya, makin canggih modusnya, makin bervariasi karakteristik pelakunya, dan makin serius akibatnya. Secara kriminologis setiap kejahatan merupakan fenomena masyarakat (*social phenomenon*) karena eskalasi kerugian *cybercrime* bersifat global dan pelakunya lintas Negara, maka *cybercrime* dianggap sebagai fenomena global. Secara sederhana.setiap kejahatan yang dilakukan pada sistem komputer maupun menggunakan komputer sebagai sarana melakukan kejahatan disebut *cybercrime* atau *computer related crime* . kejahatan tersebut tidak menggunakan kekerasan fisik. Hal ini juga sejalan dengan pemikiran Russel G. Smith bahwa *cybercrime raise new concerns about proportionality, as the consuqences of some type of offending can be great, and yet to counduct it self involves no physical violent.* [8]

---

[7] Madison Ngafeeson*, Cybercrime Classification: A Motivational Model. Collage of Buiesness Administration, The Universities of Texas Pan American 1201 West Universities Drive*, Edinburg, Texas 78541, USA.
[8] Russel G. Smith, et all. *Cybercrime on trail*. Cambridges University Press 2004, P, 109

Kejahatan yang berkaitan dengan teknologi informasi dan komunikasi dengan menggunakan media komputer sebagaimana biasa terjadi saat ini, dapat disebut dengan berbagai istilah yaitu *computer misuse, computer abuse, computer fraude, computer-related crime, computer assisted crime*, atau *computer crime*.[9] Istilah kejahatan yang berhubungan dengan komputer (*computer related crime*) sering kali digunakan PBB (Perserikatan Bangsa- Bangsa) dalam dokumen-dokumenya. Namun demikian, konvensi internasional tahun 2001 tentang pengaturan kejahatan yang berhubungan dengan komputer dan pemberantasanya menggunakan istilah *cyber crime*.

Sehingga konvensinya berjudul *convention on cybercrime*. Barda Nawawi Arief, mengemukakan bahwa kejahatan yang berhubungan dengan komputer (*computer related crime*) sama dengan *cyber crime*.[10] Sebagai bukti tentang penggunaan istilah kejahatan yang berhubungan dengan komputer oleh PBB. Dalam laporan dokumen kongres PBB ke-10 di Wina tanggal 19 juli tahun 2000 menggunakan istilah *computer related crime* kemudian mengatur dua bentuk berikut

The term "computer related crime" had been developed encompass entairely new form of crime that were directed at computer, network and their users, and more traditional form crime that were now being commited with the use or assistance of computer equipment"

a) *Cybercrime in narrow sense (computer crime) any illegal behavior directed by means of electronic operation that target the security of computer system and the data processesd by them*
b) *Cyber crime in broader sense (computer related crime) any illegal behavior commited by means of, or in relation to, a computer system network, including such crime as illegal possession, offering or distributing information by means of computer system on network.* [11]

[9] Ibid., p.1.
[10] Barda Nawawi Arief *Perbandingan Hukum Pidana*, PT Raja Grafindo Persada, Jakarta. 2002, p, 259
[11] Agus Rahardjo, *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi* . PT Citra Aditya Bakti, Bandung 2002, p, 27

Kejahatan yang berhubungan dengan komputer merupakan keseluruhan bentuk kejahatan yang ditujukan terhadap komputer, jaringan komputer dan terhadap para penggunanya, bentuk-bentuk kejahatan konvensional yang menggunakan atau dengan bantuan peralatan komputer. Kejahatan tersebut dibedakan menjadi 2 katagori yakni, *cyber crime* dalam pengertian sempit dan dalam pengertian luas. *Cyber crime* dalam pengertian sempit adalah kejahatan terhadap sistem komputer

sedangkan *cyber crime* dalam pengertian luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan yang menggunakan sarana komputer. Hal ini selaras dengan the *Encyclopedia of Crime and Justice* yang menjelaskan bahwa ada dua ketegori *cybercrime*, yaitu.

1) *In the first computer is a tool of crime, such as fraud, embalzzment, and thieft of property, or is used to plan manage a crime.*
2) *In the second, computer is a object of crime such as sabotage theft of alteration of storage data or theft of service*

Pernyataan ini sesuai pula dengan pendapat Sue Titus Reid bahwa"*computer crime case have one commonality: the computer is ethier of the tool or the target of the felon* "[12]

Berdsarakan pernyataan di atas dapat dipahami bahwa pengertian *cyber crime* adalah aktivitas seseorang, sekelompok orang, badan hukum yang menggunakan komputer sebagai sarana kejahatan. Kejahatan tersebut adalah bentuk-bentuk kejahatan yang bertentangan dengan peraturan perundang-undangan baik melawan hukum secara materil maupun secara formal.

G. Hipotesa

Dari pendahuluan diatas, penulis mengajukan argument penelitian bahwa pemerintah Indonesia masih belum efektif memberantas kejahatan *cyber crime* (Mayantara) karena

1) Masih banyaknya celah pada perundang-undangan ITE tahun 2008

[12] Sue Titus Reid *Crime and Criminology , CBS. Collect Publishing New York* 1985 p. 316

2) Lemahnya penegakan hukum pemerintah terhadap penggunaan fasilitas akses internet, serta tidak adanya pembatasan pemakaian fasilitas internet di Indonesia di sinyalir sebagai pemicu tingginya kasus kejahatan *cyber crime* (Mayantara).

H. Metode Penelitian

H. 1 Tipe Penelitian

Metode yang digunakan dalam penelititan ini adalah penelitian kualitatif. Metode kualitatif ialah proses berpikir yang di mulai dari data yang dikumpulkan kemudian diambil kesimpulan secara umum. Metode ini berorientasi dengan logika induktif karena penelitian tidak hanya memaksakan diri untuk membatasi penelitian dalam upaya penerimaan atau penolakan dugaan-dugaanya melainkan mencoba memahami situasi sesuai dengan situasi tersebut menampakan diri.

Ciri khusus metode kualitatif adalah pengungkapan fenomena tanpa harus menyajikan penjelasan-penjelasan kuantitatif. Tujuan penelitian kualitatif adalah mengembangkan konsep-konsep yang membantu pemahaman lebih mendalam atas fenomena sosial dan perilaku dalam *setting* alamiah dalam arti peneliti tidak berusaha untuk memanipulasi setting penelitian malinkan melakukan studi terhadap suatu fenomena dimana fenomena tersebut ada. Adapun pertimbangan penggunaan metode kualitatif tersebut adalah sebagai berikut

a) Lebih mudah menyesuaikan apabila berhadapan dengan kenyataan lapangan (adaptif)
b) Metode kualitatif berhubungan secara langsung dengan khalayak sasaran sehingga diperoleh pemahaman yang lebih mendalam
c) Metode kualitatif lebih peka atau sensitif dan lebih cepat menyesuaikan diri dengan penajaman pengaruh bersama terhadap pola-pola nilai yang dihadapi.

Peneliti menggunakan penelitian yang bersifat deskriptif dengan pendekatan kulitatitf, dengan maksud tujuan untuk dapat menjawab pertanyaan peneliti (*research question*) fokus pada penelitian ini adalah untuk mengetahui faktor-faktor apa saja yang menghambat dalam mengungkap kasus kejahatan *cyber crime* di Indonesia dan faktor

pendukung apa saja sehingga Indonesia rawan dijadikan tempat asal serangan kejahatan dunia maya *cyber crime* oleh sindikat Internasional.

H. 2 Teknik Analisa Data

Menurut Miles dan Huberman, kegiatan nalisis terdiri dari tiga alur kegiatan yang terjadi bersamaan, yaitu reduksi data, penyajian data, dan penarikan kesimpulan atau verifikasi[13]. dalam menganalisa penelitian ini penulis menggunakan pola induksi dengan tiga tahapan yakni:

1. Mengumpulkan data-data tentang fenomena yang diteliti
2. Pengolahan. Pada tahapan ini penelliti mengolah data untuk di pilah-pilah mana yang cocok dan sesuai dengan kategori yang dibutuhkan oleh masing-masing sub bab penelitian.
3. Analisa. Tahapan terakhir ini menjadikan data yang mentah dan sudah diolah tadi, untuk kemudian di analisa dan di interpretasikan oleh peneliti sehingga mempengaruhi proses pembentukan hasil akhir dari riset.

H. 3 Jangkauan Penelitian

Jangkauan penelitian dilakukan dengan menganalisis kasus *study case* mengenai kejahatan *cyber crime* yang terjadi di Indonesia antara tahun 2004 hingga 2015. Adapun kaasus yang terjadi pada kurun waktu dari tahun 2004 hingga 2015 adalah sebagai berikut

1) Tahun 2004, terjadi kasus pembobolan situs KPU yang dilakukan oleh seorang hecker yang bernama Dany Firmansyah. Dia berhasil membobol dan merubah isi tampilan dari situs KPU 2004 yang menghabiskan dana Rp. 152.000.000.000 (seratus lima puluh dua miliyar rupiah)
2) Tahun 2008, pada tahun ini pemerintah indonesia baru mresmikan perundang-undangan informasi dan transaksi elektronik yang kemudian dikenal Dengan Undang-Undang ITE 2008
3) Tahun 2009, terjadi kasus pencemaran nama baik yang dilakukan oleh prita mulyasari terhadap rumah sakit omni internasional

[13] Sugiyono. 2011. *Metode Kuantitatif Kualitatif dan R&B*, Bandung: Alfabeta. Hal 246

4) Pada thun 2010, terjadi kasus video asusila yang dilakukan oleh artis dan penyanyi band Indonesia yaitu Ariel Peterpan, Cuat Tari dan Luna Maya.
5) Tahun 2014, terjadi pencemaran nama baik oleh salah satu mahasiswa S2 pergyuruan tinggi negeri di Yogyakarta yang bernama Florance Sihombing karena update status yang mendeskreditkan warga Yogyakarta melalui akun media sosial *Path*
6) Tahun 2014, terjadi pencemaran nama baik oleh warga bantul Yogyakarta yang bernama Ervani Emi Handayani kepada bos tempat suaminya bekerja melalui akunsosial *Facebook*
7) Pada tahun 2015 MABES POLRI menggerbek sindikat penipuan asal tiongkok yang beroperasi di Indonesia DAN menargetkan warga tiongkok sebagai korbanya.

dengan menganalisis metode-metode yang dilakukan oleh pihak berwajib dalam mengungkap kasus kejahatan dunia maya (*cyber crime*) dan penerapan UU ITE 2008 JUGA kebijakan pemasangan ISP (*Internet Service Provider*) di Indonesia dengan Negara lain. Penelitian ini juga akan membahas kasus *cyber crime* internasional yang terjadi di berbagai Negara di dunia untuk membandingkan dengan kasus-kasus kejahatan dunia maya yang ada di indoensia.

H. 4 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan oleh penulis dalam penelitian ini adalah telaah *(research*) yaitu dengan mengumpulkan data dari literatur yang berhubungan dengan permasalahan yang akan dibahas. literatur ini berupa buku-buku mengenai pemahaman *cyber crime* baik dari analisis kasus dan penerapan hukum *cyber* bagi pelaku kejahatan dunia maya. Adapun literatur yang digunakan dalam penelitian ini adalah kejahatan siber *cyber crime*, memerangi *cyber crime* dalam prespektif kriminologi. aspek hukum pidana keahatan mayantara, penelitian tesis kerjasama ASEAN dalam *cyber crime* dan peran *IP Adress* dan *Domain name* dalam *jurisdiction*. Dikarenakan penelitian ini bersifat deskriptif maka dalam menggambarkan permasalahan yang akan dibahas tergantung pada validitas data informan yang memberikan informasi, oleh karena itu dalam penelitian ini penulis juga melakukan wawancara dimana dalam menentukan informan dengan kriteria yang dapat memahami dunia maya dan penerapan hukum bagi kejahatan dunia maya.

Penulis melakukan wawancara dengan orang-orang yang berkompeten baik dari pihak akademisi maupun praktisi. Dalam hal ini pihak yang akan diwawancarai adalah praktisi yang merupakan salah satu staf ahli di Kementrian Komunikasi Dan Informasi (KOMINFO) yang bernama Teguh Arifiyadi. Beliau Juga Salah Satu tim ahli yang sering ambil bagian dalam mengungkap kasus *cybercrime* yang terjadi di Indonesia. Selain itu Teguh Arifiyadi juga merupakan *founder* dan ketua umum *Indonesia Cyber Law Community* (ICLC). Kemudian untuk narasumber yang ke dua ialah IR Lukito Edi Nugroho beliau adalah seorang dosen teknik informatika UGM (Universitas Gadjah Mada) selain itu beliau juga adalah pengamat *E-Government* dan sorang akademisi

I. Sistematika Penulisan

Sistematika penulisan penelitian ini akan terbagi menjadi lima bab

BAB 1 : PENDAHULUAN

Bab ini berisi tentang pendahulan yang terdiri dari latar belakang masalah yang memuat tentang seluk beluk kejahatan dunia maya yang dilakukan oleh orang-orang tertentu dengan menggunakan komputer sebagai sasaran dan sebagai alat kejahatan *cyber*. Pada bab ini juga akan membahas pengenalan lebih mendalam secara garis besar apa dan bagaimana kejahatan dunia maya. Selain itu bab pendahuluan juga membahas mengenai rumusan masalah, tujuan penelitian, manfaat penelitian, kontribusi riset.

tinjauan pustaka yeng berisis review dari beberapa penelitian dan buku yang membahas mengenai kejahatan *cyber crime*, Kerangka teori dan konsep. Bab ini juga menggambarkan mengenai metodologi penelitian, teknik pengumpulan data, jangkauan penelitian dan hipotesa atau argumen penelitian sebagai argument sementara yang akan dibuktikan keabsahanya dalam penelitian ini.

BAB II KEJAHATAN *CYBER CRIME* DI INDONESIA

Bab ini membahas tentang berbagai kejahatan yang menggunakan teknologi informasi di indonesia, Baik penipuan, pencurian data nasabah, pencemaran nama baik , perjudian *online* dan lain sebagainya. Bab ini Juga akan Membahas teori mengenai pelaku kejahatan *cyber crime.*

BAB III UPAYA DAN KEBIJAKAN CYBER CRIME DI INDONESIA

Bab ini akan membahas kebijakan pemerintah indonesia dalam menangani kejahatan *cyber crime* dalam undang-undang tindak pidana terhadap pelaku kejahatan *cyber*.

BAB IV KETIDAKEFEKTIFITASAN PEMERINTAH INDONESIA DALAM PENANGGULANGAN KEJAHATAN CYBERCRIME

Bab ini menjelaskan mengapa upaya pemerintah indoensia masih belum efektif dalam menangulangi kejahatan *cyber crime* di indonesia, walaupun undang-undang ITE Tahun 2008 ketika sudah berjalan dan di sahkan yang berlangsung hingga sekarang

BAB V PENUTUP DAN KESIMPULAN

Bab ini berisi tentang kesimpulan dari hasil-hasil penelitian yang telah dibahas pada sub bab sebelumnya dari bab satu sampai empat, sehingga akan mengetahui jawaban mengenai argumen hipotesa penulis. Pada bab ini akan ditambahkan kritik dan saran oleh penulis.