MANAGEMENT PENANGANAN KASUS KEJAHATAN CYBER CRIME DI INDONESIA

Seno Anggoro
Magister Hubungan Internasional
Universitas Muhammadiyah Yogyakarta
Yogyakarta Indonesia
Email: Senoanggoro90@gmail.com

Abstrak **--Pesatnya Kemajuan teknologi dan informasi pada zaman globalisasi sangatlah cepat, kemajuan teknologi juga ditandai dengan perubahan pola kehidupan manusia yang memanfaatkan teknologi untuk menunjang kehidupan sehari-hari. Seperti berkomunikasi, jual beli hingga perbankan. Tanda-tanda kemajuan era teknologi dan informasi dapat dirasakan dengan fasilitas internet, namun kemajuan teknologi informasi seperti pisau bermata dua selain dampak positif dengan kemudahnnya dalam kehidupan kita kemajuan teknologi juga memberikan kerawanan dan rasa tidak aman. Hal ini ditandai dengan maraknya kasus penipuan, pemerasan, pencemaran nama baik hingga pencurian data-data informasi dan keuangan. Indonesia yang merupakan salah satu masayarakat dunia juga mengalami perubahan yang signifikan dalam pemanfaatan teknologi informasi. Dari data survey statitstik Indonesia meruapakan salah satu pengguna internet terbesar di dunia, disamping itu Negara indonesia juga rawan akan kasus kejahatan penyalahgunaan teknologi informasi yang berupa kejahatan dunia maya (*cybercrime)* seperti pembobolan kartu kredit, pencurian identitas data nasabah, penipuan *online,* perusakan *website* milik pemerintah, pencemaran nama baik hingga terorisme *cyber terrorism* dan masih banyak jenis kejahatan lainya. Walaupun jumlah pengguna teknologi informasi dan internet tidak bisa dihubungkan dengan kejahatan mayantara *(cyber)* namun dari fakta laporan lemabaga internasional menegnai kejahatan dunia maya indonesia merupakan Negara yang rawan akan sasaran serangan dan asal serangan *cybercrime,* lebih ironisnya lagi meningkatnya kasus mayantara (*cybercrime*) di indonesia seteleh pemerintah memberlakukan Undang-Undang No 11 tentang Informasi Dan Transaksi Elektronik (UU-ITE) Tahun 2008, masih adanya celah hukum di indoensia di sinyalir menjadi penyebab meningkatnya kejahatan dunia maya (*cybercrime)* di indonesia.**

Kata kunci (keyword):cybercrime,Undang-Undang Informasi Dan Transaksi Elektronik

I. Pendahuluan

1.1 Latar Belakang Masalah

Zaman globalisasi mengalami perubahan yang sangat pesat, begitu juga dengan teknologi informasi yang mengalami banyak kemajuan dan memberikan banyak manfaat yang sangat besar terhadap aspek kehidupan manusia. Baik dari segi komunkasi dan dalam mendukung kehidupan sehari hari, manusia tidak bisa lepas dari peran teknologi informasi. Namun kemajuan teknologi dan informasi juga tidak lepas dari sisi negatif, hal ini dikarenakan penggunaan teknologi informasi dan internet semkain lama semakin meningkat dari tahun ketahun. sehingga membuat sebagian orang yang tidak bertanggung jawab ingin mengambil keuntungan. Hal ini 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 sistem keamanan 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 kekurang berhasilan pemberantasan *cyber crime* di indonesia adalah 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 crime 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 dari *cyber crime* di indoensia tidak hanya berdampak pada dalam negeri namun juga

[1] *ASPEK HUKUM PIDANA KEJAHATAN MAYANTARA* Widodo

ISBN: 978-602-19568-1-6

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 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.

Walaupaun pemerintah sudah membuat undang-undang Informasi danTransaksi Elektronik No 11 2008 tingkat kejahatan mayantara atau *cyber crime* di indonesia justru semakin meningkat . Berdsarkan data *Norton Report* tahun 2013, tingkat potensi dan resiko tindak kejahatan *cyber* di Indonesia sudah memasuki status 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, selain itu mudahnya pemasanagan jaringan internet dan kurangnya pengawasan 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 *cyber crime* 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 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.merugikan pihak lain.

1.2 Rumusan Masalah

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

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

ISBN: 978-602-19568-1-6

1.3 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 beroperasi di indonesia

1.4 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*

1.5 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 antar 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 actor-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 Indoensia 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.

1.6 Kerangka Konseptual

1.6.1 Kejahatan *Cyber Crime*

Berbicara masalah *cyber crime* tidak lepas dari permasalahan keamananjaringan computer 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 perkembvangan 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 computer untuk tujuan criminal/atau criminal berteknologi tinggi dengan mneyalah 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 rime can take the form of simple snooping into a computer system for which we have no authorization it can be the feeing of computer virus into the wild. It may be malicious vandalism by

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

ISBN: 978-602-19568-1-6

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 bekum ada kesepakatan mengenai definisi tentang *cyber crime* atau kejahatan dunia *cyber*.

II. Metode Penelitian

a. Tipe Penelitian

Metode yang digunakan dalam penelititan ini adalah penelitian kualitatif. Metode kualitatif ialah proses berpikir yang dimulai 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 factor pendukung apa saja sehingga indonesia rawan dijadikan tempat asal serangan kejahatan dunia maya *cyber crime* oleh sindikat internasional.

b. 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[7]. 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.

c. Lokasi Jangkauan Penelitian

Jangkauan penelitian dilakukan dengan menganalisis kasus *study case* mengenai kejahatan *cyber crime* yang terjadi di indonesia antara tahun 2004 hingga 2015, dengan menganalisis metode-metode yang dilakukan oleh pihak berwajib dalam mengungkap kasus kejahatan dunia maya (*cyber crime*) dan 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.

d. 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 *cybercrime* baik dari analsis kasus dan penarepan hukum *cyber* bagi pelaku kejahatan dunia maya. Adapun literatur yang digunakan dalam penelitian ini adalah kejahatan siber

[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 Kejahatan*, (Jakarta, Kencana Perdana Media Group, 2007), hal 24
[7] Sugiyono. 2011. *Metode Kuantitatif Kualitatif dan R&B*, Bandung: Alfabeta. Hal 246

ISBN: 978-602-19568-1-6

cyber crime, memerangi *cyber crime* dalam prespektif kriminologi.

aspek hukum pidana kejahatan 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 pihak kepolisian yang tergabung dalam satuan tugas penanganan kasus kejahatan dunia maya *cyber police,* pelaku *cyber crime (cracker)* dan dosen-dosen ahli dalam bidang IT seperti *cyber security* dan *network security.*

III. HASIL DAN PEMBAHASAN

Cyber crime merupakan kejahatan yang menggunakan teknologi informasi dan komunikasi dengan menggunakan computer, zaman global yang sedang berlangsung seperti saat ini mengubah kehidupan manusia baik secara komunikasi dan mnunjang pekerjaan tidak bisa lepas dari peranan teknologi informasi dan komunikasi. Dalam hal ini, sebagai contoh dengan maraknya penggunaan komputer yang menawarkan berbagai macam program aplikasi untuk menunjang efesiensi pekerjaan kita hingga merambat ke alat komunikasi yang juga menawarkan berbagai macam fasilitas dan program penunjang lainnya.Dari perkembangan itu juga memberikan kesempatan pada segelintir orang yang tidak bertanggung jawab untuk memanfaatkanya sebagai sarana aksi kejahatan yang dapat merugikan orang lain. dari fenomena tersebut maka dapat diartikan bahwa kejahatan konvensional beralih ke kejahtan virtual *(cyber*), walau dilakukan dengan cara virtual namun memiliki dampak yang nyata *(real*). Hal inilah yang menyebabkan para pengguana teknologi menjadi lebih waspada.

Kebijakan dalam perundang-undangan mutlak diperlukan oleh para penegak hukum dan pemerintah untuk menaggulangi dan menindak pelaku kejahatan, sama halnya dengan tindak kejahatan mayantara (*cyber crime),* tentunya jenis hukum perundang-undangan haruslah sesuai dengan jenis kejahatan dan cara untuk mengungkap kasus kejahtan dunia maya. Maka dari itu sejak tahun 2008 pemerintah republik Indonesia sudah berkoitmen untuk memerangi kejahatan dunia maya.Pemberlakuan dan pengesahan Undang-Undang Informasi Dan Transaksi Elektronik Tahun 2008 Atau UU ITE 2008 merupakan salah satu babak baru bagi pemerintah republik Indonesia untuk melawan kejahatan berbasis teknologi komunikasi dan informasi. Dengan aturan ini maka akan membuka jalan bagi penegak hukum untuk bertindak dan mengadili pelaku kejahatan teknologi informasi. Semakin pesatnya penggunaan teknologi maka semakin rawan untuk tingkat kejahatanya yang dilakukan oleh orang-orang yang tidak bertanggung jawab untuk melakukan aksinya baik penipuan, pencurian dan pencemaran nama baik melalui internet.

Kebijakan-kebijakan pemerintah dibuat untuk mendukung tercapainnya kepentingan nasional sesuai dengan amanah undang-undang 1945 bertujuan untuk mensejahterakan kehidupan rakyat banyak dan mencerdaskan kehidupan berbangsa. Kesejahteraan dicapai dengan memanfaatkan dan mengelola sumber daya alam baik pertambangan, kekayaan laut dan pertanian hasil bumi indonesia, sehingga kualitas sumber daya manusia indonesia bisa bersaing dalam dunia kerja dan global. Seiring dengan perkembangan zaman, pesatnya kemajuan teknologi informasi terutama internet yang sangat berperan penting untuk kehidupan manusia seperti halnya Negara indonesia yang masuk dalam salah satu masyarakat dunia tentunya tidak bisa lepas dari penggunaan fasilitas internet untuk menunjang komunikasi, perbankan dan perdagangan *online (e-commerce*), dengan fakta tersebut maka diperlukan kebijakan-kebijakan yang dapat menunjang dan melindungi penggunaan internet di indonesia, agar mendapatkan jaminan keamanaan.

Namun disamping itu semua semenak diberlakukanya undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik yang diharapkan dapat memebrikan jaminan keamanan bagi penggunaan teknologi informasi dan komunikasi tingkat kejahatan dunia maya (*cyber crime*) di Indonesia masih tinggi dan rawan akan serangan dunia maya baik dari dalam maupun luar negeri. Hal ini dibuktikan dengan adanya laporan Berdsarkan data dari *Norton Report* tahun 2013, tingkat potensi dan resiko tindak kejahatan *cyber* di Indonesia sudah memasuki status 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. Kejahatan teknologi juga bisa dirasakan dengan adanya SMS penipuan yang menawarkan berbagai macam hadiah baik berupa uang tunai dan barang. Modus yang digunakan oleh sindikat tersebut berpura-pura sebagai petugas bank yang menghubungi ke sejumlah pemilik nomor telpon tertentu untuk menawarkan hadiah undian. Berdasarkan pengungkapan kasus penipuan SMS tersebut pihak kepolisian telah menagmankan berbagai macam barang bukti seperti telpon seluler, computer/laptop, modem dan alat

ISBN: 978-602-19568-1-6

komunikasi lainnya. Pada bab ini akan menjelaskan berbagai macam kendala-kendala yang dialami oleh penegak hukum indonesia dalam mengungkap kasus kejahatan dunia maya. Pada bab ini juga akan membandingkan hokum kejahatan dunia maya antara indonesia dengan berbagai Negara didunia yang sudah lebih dulu membuat *cyber law security*.

3.1 Laporan State Of The Internet

Indonesia berada di urutan kedua dalam daftar lima besar negara asal serangan kejahatan siber atau *cyber crime*, berdasar laporan State of The Internet 2013. Wakil Direktur Tindak Pidana Ekonomi Khusus Bareskrim Polri Kombespol Agung Setya mengatakan, dalam kurun waktu tiga tahun terakhir, tercatat 36,6 juta serangan *cyber crime* terjadi di Indonesia.Hal ini sesuai dengan data Security Threat 2013 yang menyebutkan Indonesia adalah negara paling berisiko mengalami serangan *cyber crime*.Sejak 2012 sampai dengan April 2015, Subdit IT/ *Cyber Crime* telah menangkap 497 orang tersangka kasus kejahatan di dunia maya.Dari jumlah tersebut, sebanyak 389 orang di antaranya merupakan warga negara asing, dan 108 orang merupakan warga negara Indonesia.Total kerugian *cyber crime* di Indonesia mencapai Rp 33,29 miliar. "Angka ini jauh lebih besar dibandingkan perampokan nasabah bank secara konvensional," kata Agung di Jakarta, Senin (11/5/2015).Sementara itu, sepanjang 2012 sampai dengan 2014, terdapat 101 permintaan penyelidikan terhadap kasus *fraud* atau penipuan dari seluruh dunia. "Ini artinya, setiap 10 hari terdapat satu kejadian selama tiga tahun terakhir," ujar Agung.

3.2 Laporan Akamai

Serangan cyber yang berasal dari indonesia dilaporkan meningkat. Bahkan kini mengambil porsi terbesar serangan cyber dunia yang sebelumnya dikuasai china. Dibandingkan pada kuartal pertama 2013, hingga akhir kuartal kedua 2013 ini jumlah serangan yang berasal dari indonesia meningkat dua kali lipat. Berdasarkan laporan keamanan yang dirilis akamai, indonesia kini mengantongi porsi terbesar serangan dengan perolehan 38%,naik 17% dari peroide sebelumnya.Sedangkan china yang sebelumnya mendominasi kini hanya memiliki porsi 33%. Akamai menegaskan bahwa ini bukan berarti bahwa para penyerang itu memang benar dari indonesia. Karena pada dasarnya, para peretas bisa saja menggunakan alamat IP wilayah lain untuk menghilangkan jejak.[8]

	Country	Q2 '13 % Traffic	Q1 '13 %
1	Indonesia	38%	21%
2	China	33%	34%
3	United States	6.9%	8.3%
4	Taiwan	2.5%	2.5%
5	Turkey	2.4%	4.5%
6	India	2.0%	2.6%
7	Russia	1.7%	2.7%
8	Brazil	1.4%	2.2%
9	Romania	1.0%	2.0%
10	South Korea	0.9%	1.4%
–	Other	11%	18%

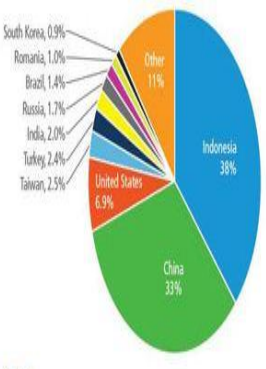

Figure 1: Attack Traffic, Top Originating Countries (by source IP address, not attribution)

Gambar 3.2.1 10 Negara dengan serangan cyber terbesar[9]

3.3 Kendala Pemerintah Dalam Menaggulangi *Cyber Crime*

Berdasarkan wawancara antara penulis dengan narasumber ketua umum ICLC (*Indonesia Cyber Law Community*) Teguh Arifiyadi yang juga salah satu staf pelayan masyarakat di Kementrian Informasi Dan Komunikasi (KOMINFO) menjelaskan bahwa tidak ada kaitannya secara langsung antara celah hukum dan *cyber attacker* (pelaku kejahatan dunia maya). Para pelaku *cyber* sebenarnya dapat melakukan serangan maya kapanpun dan dimanapun tanpa memandang hukum, namun hanya berdasarkan motif yang merupakan faktor utamanya. Seperti halnya motif dengan modus penipuan, pencurian, pembobolan kartu kredit dan motif untuk mendapatkan keuntungan pribadi lainya. Kemudian meningkatnya jumlah pengguna teknologi informasi di indonesia baik internet maupun pemakai alat komunikasi berupa *Hanpdhone* dan alat komunikasi yang lain juga tidak bisa dihubungkan dengan tingkat jumlah kejahatan *cyber* yang ada di indonesia. Kemudian yang menjadi kendala utama pemerintah dalam menangggulangi kejahatan *cyber crime* yaitu minimnya jumlah anggota personil atau tenaga ahli dalam *cyber crime* dan *cyber forensic* baik di institusi kepolisian dan Kominfo. Kemudian kendala lain yang cukup krusial adalah minimnya dukungan anggaran oleh pemerintah pusat untuk menganggulangi kejahatan dunia maya.

Besarnya kisaran anggaran yang dibutuhkan untuk kasus kejahatan dunia maya atau yang menggunakan teknologi informasi tidak bisa disebutkan secara terbuka oleh pak Teguh Arifiyadi, diakrenakan anggaran untuk manggulangi *cyber crime* merupakan kerahasian dari Departemen Komunikasi Dan Informasi (KOMINFO). Selain itu penulis juga mendapat konfirmasi dari pak Teguh bahwa ISP *(Internet Service Provider)* di indonesia hamper 95% dipegang oleh pihak swasta, dengan fakta ini bisa disimpulkan bahwa jika penyedia jasa internet dikendalikan oleh swasta maka akan terjadi minimnya pengawasan penggunaan dan peruntukan fasilitas internet oleh pengguna internet, selain itu pihak swasta juga tidak akan membatasi fasilitas jaringan internet yang mana sekarang sudah menjadi kebutuhan penting atau pokok oleh masyarakat indonesia. Sudah saatnya pemerintah ikut dan terjun langsung untuk pengawasan perizinan

[8] ww

[9] www.detiknet.com

pemasangan internet di indonesia, salh satu penyebab maraknya kejahatan dunia maya yaitu mudahnya mendapatkan pemasangan fasilitas internet, tanpa adanya campur tangan pemerintah dalam pengawasan maka keamanan internet di indonesia akan semakin rawan, jika terus dibiarkan maka akan berdampak pada alamat *IP Address* dan *Domain Name* asal indonesia akan masuk daftar yang di *balck list* oleh dunia internasional sehingga masayarakat indonesia sendiri yang akan dirugikan.

IV. KESIMPULAN

4.1 Kesimpulan

Negara kesatuan republik indonesia merupakan salah satu dari masayarakat dunia yang sedang berkembang dalam pergaulan era-globalisasi yang sedang berlangsung saat ini. Perkembangan teknologi informasi merupakan salah satu peradaban manusia di dunia termasuk indonesia sebagai salah satu bagian dari masyarakat dunia, maka dari itu keamanan jaringan internet dan teknologi informasi sudah merupakan suatu keharusan bagi pemerintah indonesia baik dari segi hukum maupun jaminan keamanan penggunaan teknologi informasi dan internet bagi seluruh rakyat indonesia.Namun walaupun pemerintah sudah mengesahkan Undang-Undang No 11 Tentang Informasi Dan Transaksi Elektronik dinilai masih memerlukan evaluasi dan kebijakan-kebijakan yang baru. Sebab tingkat kejahatan dunia maya (*cyber crime*) masih sangat tinggi dan rentan akan kemanannya, di tengarai masih barunya undang-undang ITE 2008 haruslah menyesuaikan dengan keadaan yang ada dilapangan, ditambah lagi perkembangan teknologi informasi beekembang sangat pesat dari waktu ke waktu. Mudahnya mendapatkan akses internet dan lemahnya pengawasan yang dilakukan oleh pemerintah merupakan faktor utama yang menyebabkan tingginya penyalahgunaan teknologi informasi dan internet di indonesia. Hampir 95% penyedia jasa internet atau ISP (*Internet Sevice Provider*) yang dikendalikan oleh pihak swasta sangat berdampak besar untuk penggunaan fasilitas internet sebab jika dikandalikan oleh pihak swasta seluruhnya yang mana notabenenya hanya mencari keuntungan tidak akan memperdulikan apa yang dilakukan oleh pelanggannya. Disamping itu dalam UU No 11 ITE 2008 pihak swasta sebagai penyelenggara fasilitas internet tidak terikat dalam membatasi pemberian akses pemakaian jasa layanan internet.

Jika kejahatan dunia maya semakin marak di indonesia tanpa adanya penanganan dan pengawasan yang serius dari pemerintah maka dalam waktu jangka panjang *Domain Name* dan *IP Address* yang berasal dari indonesia akan masuk dalam daftar *black list* oleh komunitas internasional, sebagai akibatnya akan menghambat pertumbuhan ekonomi dan tujuan pemabangunan nasional. Sebab seiring dengan pesatnya penggunaan teknologi informasi sebagai contoh kegiatan perbankan, jual-beli (*e-commerce*) dan kegiatan yang lainya dilakukan secara *online*. Selain membuat kebijakan tentang penyelenggaraan jasa internet ataupun teknologi informasi, pemerintah juga hendaknya meningkatkan kemampuan dan jumlah tenaga-tenaga ahli *cyber forensic* dalam hal ini yaitu para penegak hokum seperti pihak kepolisian dan kementrian komunikasi dan informasi (KOMINFO) sebagai pihak berwenang dan yang terjun langsung dalam hal kasus kejahatan dunia maya dan penyalahgunaan teknologi informasi.

Selain itu besarnya anggaran juga sangat berpengaruh dalam menciptakan keamanan, dengan anggaran yang cukup maka pemerintah akan mudah melakukan pengawasan, selain factor pengawasan dan keterbatasan tenaga ahli dalam penanggyulangan kejahatan dunia maya (*cyber crime*) factor anggaran yang minim juga ditengarai sebagai kendala pemerintah dalam kasus kejahatan dunia mayaSehingga dengan adanya aturan dan pengawasan yang ketat dalam penggunaan teknologi informasi dan internet diharapkan dimasa-masa yang akan datang akan memberikan rasa aman dan kenyamanan bagi para pengguna internet, dengan keamanan yang terjamin maka tujuan pembangunan nasional akan merata diseluruh wilayah indonesia.

4.2 Saran

Berdasarkan hasil penelitian dan kesimpulan di atas maka penulis memberikan saran sebagai berikut.

1) Pemerintah dan Pihak swasta sebagai penyelenggara jasa internet atau teknologi informasi hendaknya menerapkan aturan dan pengawasan serta pemberian izin pemasangan fasilitas internet yang cukup ketat sesuai dengan perundang-undangan yang berlaku supaya tidak terjadi penyalahgunaan teknologi informasi dan fasilitas internet
2) Pemerintah hendaknya menambah anggaran untuk menjaga keamanan fasilitas teknologi informasi dan pengawasan penggunaan internet di indonesia dalam hal ini kementrian yang terkait adalah KOMINFO sebagai salah satu kementrian yang membawahi kebijakan-kebijakan teknologi informasi.
3) Perlu adanya peningkatan kemampuan komputer forensic bagi para penegak-penegak hukum baik pihak kepolisisan maupun kementrian komunikasi dan informasi (KOMINFO) dengan merekrut mahasiswa atau orang-orang yang mampu dan mengerti akan teknologi informasi
4) Para penampu atau pembuat kebijakan sudah saatnya harus melek teknologi informasi dalam menjalankan roda pemerintahan agar birokrasi dan transparansi menjadi lebih baik sehingga akan menerapkan *e-government* dan *good governance* yang sangat bermanfaat untuk pelayanan publik

DAFTAR PUSTAKA

ISBN: 978-602-19568-1-6

[1] Akkers, Ronald L. and Christie S. Seller. 2004. *Criminological Theories: Introduction, Evolution, and Aplication, Fourth Edition, Roxbury Publishing Company. Los Angels California*
[2] Arief, Barda Nawawi. 1996. Bunga Rampai Kebijakan Hukum Pidana Bandung PT Citra Aditya Bakti
[3] Bassiouni,M.Cherif. 1978, *Substantive Criminal Law*, Charles C.Thomas *Publisher, Springfield Illinois.*
[4] Bottomoley, A.Keith, 1973. *Decixions In The Penal Process*, Law And Society Series, Martin Robertson And Company, London
[5] Casey, Eoghan. 2001. *Digital Evidence And Computer Crime,* A Harcourt Science And Technology Company, London
[6] Chambliss, William J. Chambliis. 1979. The State, *The Law And The Defenition of Behavior As Criminal Or Deliquen*, Dalam Daniel Glesse Ed, Handbook Of Criminology,Rand Mcnally And Co, Chicago.
[7] Dirjdosisworo, Soedjono. 1976 Penaggulangan Kejahatan: *Crime Prevention*, Alumni Bandung
[8] Hagan, John 1985, *Modern Criminology, Crime Criminal Behaviour and its Control. Mc Graw –Hill Inc, Singapore.*
[9] Karmasudirja, Edy Junaidi. 1993 Jurispridensi Kejahatan Komputer, Tanjung Agung, Jakarta
[10] Reid, Sue Titus, 1985 *Crime and Criminology, CBS Collage Publishing New York*
[11] Setiyono 2002. Kejahatan Korporasi: Analaisis Viktimologis dan pertanggung jawaban korporasi dalam Hukum Pidana Indonesia, Averroes Malang.
[12] Soley, Joseph F.. 1999 *Criminology Wedsworth Publishing Company, Belmont California.*
[13] Siegel, Larry J. 1989 *Criminology, Third Edition West Publshing New York*

ISBN: 978-602-19568-1-6