BAB II

TINDAK PIDANA *CYBER CRIME*

A. *Cyber Crime*

1. Definisi *Cyber Crime*

Sistem teknologi informasi berupa internet telah dapat menggeser paradigma para ahli hukum terhadap definisi kejahatan komputer, pada awalnya para ahli hukum terfokus pada alat/perangkat keras yaitu komputer. Namun dengan adanya perkembangan teknologi informasi berupa jaringan internet, maka fokus dari identifikasi terhadap definisi *cyber crime* lebih diperluas lagi yaitu seluas aktivitas yang dapat dilakukan di dunia *cyber*/ maya melalui sistem informasi yang digunakan, jadi tidak sekedar pada komponen *hardware*-nya saja kejahatan itu dimaknai sebagai *cyber crime*, tetapi sudah dapat diperluas dalam lingkup dunia yang dijelajah oleh sistem teknologi informasi yang bersangkutan.

Pemaknaan dari *cyber crime* itu sendiri adalah kejahatan teknologi informasi, juga sebagai kejahatan mayantara yang pada dasarnya *cyber crime* meliputi semua tindak pidana yang berkenaan dengan sistem informasi itu sendiri, serta sistem informasi yang merupakan sarana untuk penyampaian/pertukaran informasi kepada pihak lainnya.[1]

[1] Sahariyanto, Budi. 2012. *Tindak Pidana Teknologi Informasi (Cyber crime) Urgensi Pengaturan dan Celah Hukumnya*. Jakarta: Rajawali Pers. Hal. 11

2. Karakteristik *Cyber Crime*

Kejahatan dibidang teknologi informasi dapat digolongkan sebagai *white colour crime* karena pelaku *cyber crime* adalah orang yang menguasai penggunaan internet beserta aplikasinya atau ahli di bidangnya. Kejahatan tersebut sering kali dilakukan secara transnasional atau melintasi batas negara sehingga dua kriteria kejahatan melekat sekaligus dalam kejahatan *cyber* ini, yaitu *white colour crime* dan *transnational crime*.

Berdasarkan beberapa pendapat para ahli hukum pidana serta prakteknya, *cyber crime* memiliki beberapa karakteristik, yaitu:[2]

a. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang/wilayah siber/*cyber space*, sehingga tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhadapnya.
b. Perbuatan tersebut dilakukan dengan menggunakan peralatan apa pun yang terhubung dengan internet.
c. Perbuatan tersebut mengakibatkan kerugian materil maupun imateril (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional.
d. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya.

[2] Ibid. Hal. 13

e. Perbuatan tersebut sering dilakukan secara transnasional/melintasi batas negara.

Karakteristik dalam tindak pidana *cyber crime* tidak dijelaskan dalam undang- undang ITE, maka jika kita membahas mengenai karakeristik pada tindak pidana *cyber crime* yaitu berdasarkan pendapat para ahli hukum atau berdasarkan hasil penelitian para ahli hukum dalam tindak pidana *cyber crime* dan juga berdasarkan yurisprudensi.

3. Bentuk-Bentuk *Cyber Crime*

Adapun pengelompokan berdasarkan bentuknya tindak pidana *cyber crime* ialah sebagai berikut:[3]

a. *Unauthorized Access to Computer System and Service;* (Akses Tidak Sah ke Sistem dan Layanan Komputer)
b. *Illegal Contents;*(Konten Ilegal)
c. *DataForgery;*(Pemalsuan Data)
d. *Cyber Espionage;*(spionase/mata-mata dunia maya)
e. *Cyber Sabotage and Extortion;*(Sabotase dan Pemerasan dunia maya)
f. *Offense against Inttectual Property:* (Pelanggaran terhadap Properti Intelektual)
g. *Infringements of Privacy;* (pelanggaran privasi)

Bentuk-bentuk pada tindak pidana *cyber crime* ini juga tidak dijelaskan dalam undang-undang ITE, namun hal ini dijelaskan para ahli hukum dan oleh para parktisi hukum dan juga penelitian para akademisi maka

[3] Ari Yuliano Gema., *Cybercrime: sebtrah Fenomena di Dunia Maya*., http/ Center For Law Information. Llhat juga dalam http://www.interpol.eo.id. Diakses tanggal 10 Juni 2019, jam 06.30 Wib.

tindak pidana *cyber crime* berdasarkan bentuk- bentuknya di bagi menjadi lima yang mana jika kita ingin mengetahui hal tersebut merupakan tindak pidana *cyber crime* atau tidak, kita dapat melihat dari hal-hal tersebut diatas.

B. Aturan Hukum *Cyber Crime*

Aturan hukum *cyber crime* merupakan suatu hal yang memiliki tantangan tersendiri. Hal ini dikarenakan peraturan perundang- undangan yang mengatur tentang kejahatan siber di Indonesia masih "sangat muda", maka dibutuhkan waktu untuk melakukan evaluasi terhadap UU. tersebut, dibutuhkan waktu untuk mempelajari dan menganalisis pasal demi pasal dalam proses penegakan hukum. Aturan perundang-undangan telah dituangkan dalam undang-undang nomor 19 tahun 2016 atas perubahan undang-undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.[4]

Adapun beberapa aturan yang dapat digunakan dalam tindak pidana *cyber crime* adalah :

1. Undang-undang nomor 19 tahun 2016 atas perubahan undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik yang diundangkan di Jakarta pada tanggal 25 November 2016 dan dicatat dalam Lembaran Negara Republik Indonesia tahun 2016 Nomor 251. Namun bukan Undang-Undang ini bukan yang pertama kali di

[4] Maskun. Op cit. hlm 58

Indonesia yang dapat menjangkau *cyber crime*, karena jauh sebelum Undang-Undang ini disahkan, penegak hukum menggunakan KUHP untuk menjerat pelaku-pelaku *cyber crime* yang tidak bertanggung jawab dan menjadi sebuah payung hukum bagi masyarakat pengguna teknologi informasi guna mencapai sebuah kepastian hukum.

Adapun pasal-pasal dalam undang-undang nomor 19 tahun 2016 tentang Informasi dan Transaksi Elektronik yaitu atas perubahan undang-undang nomor 11 tahun 2008, yang mengatur tentang sanksi pidana bagi pelaku tindak pidana *cyber crime* yaitu[5] :

1). Pasal 45

(1) Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan sebagaimana dimaksud dalam Pasal 27 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

(2) Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian sebagaimana dimaksud dalam Pasal 27 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

(3) Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik sebagaimana dimaksud dalam

Pasal 27 ayat (3) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah).

(4) Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman sebagaimana dimaksud dalam Pasal 27 ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

(5) Ketentuan sebagaimana dimaksud pada ayat (3) merupakan delik aduan.

2) Pasal 45A

(1) Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

(2) Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan

antargolongan (SARA) sebagaimana dimaksud dalam Pasal 28 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

3). Pasal 45B

Setiap Orang yang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah).

2. Aturan hukum mengenai *cyber crime* yang diatur didalam Kitab Undang-Undang Hukum Pidana, yaitu :
    1) Pasal 362 KUHP, yang dikenakan untuk kasus *carding*.
    2) Pasal 378 KUHP, dapat dikenakan untuk penipuan.
    3) Pasal 335 KUHP, dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui *e-mail* yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkannya.
    4) Pasal 311 KUHP, dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media internet) Pasal 303 KUHP, dapat dikenakan untuk menjerat permainan judi yang dilakukan secara online di internet dengan penyelenggaraan dari Indonesia.
    5) Pasal 282 KUHP, dapat dikenakan untuk penyebaran pornografi.

6) Pasal 282 dan 311 KUHP, dapat dikenakan untuk kasus penyebaran foto atau film pribadi seseorang.
7) Pasal 406 KUHP, dapat dikenakan pada kasus *deface* atau *hacking* yang membuat sistem milik orang lain.

Undang-undang nomor 19 tahun 2016 atas perubahan undang- undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik secara jelas mengatur mengenai tindak pidana *cyber crime* serta sanksi-sanksinya, undang-undang ITE ini juga pernah di amandemen atau dirubah beberapa pasal-pasalnya yang mana tujuannya adalah menyempurnakan undang- undang ITE tersebut sebagai hukum materil dalam proses penegakan hukum pidana khusus yaitu pada tindak pidana *cyber crime*.

C. Penegakan Hukum Terhadap Tindak Pidana *Cyber Crime*

1. Proses Penegakan Hukum

a. Penyelidikan

Penyelidikan merupakan tahap permulaan dalam proses penyidikan, penyelidikan merupakan bagian yang tidak terpisahkan dari fungsi penyidikan, karena untuk melakukan proses penyidikan yang menentukan tersangka dalam tindak pidana harus dilakukan penyelidikan terlebih dahulu untuk menentukan apakah perbuatan tertentu merupakan perbuatan pidana atau tidak yang dilakukan penyelidik dengan mengumpulkan bukti permulaan yang cukup. Fungsi penyelidikan antara lain sebagai perlindungan dan jaminan terhadap hak

asasi manusia, adanya persyaratan dan pembatasan yang ketat dalam penggunaan alat-alat pemaksa, ketatnya pengawasan dan adanya lembaga ganti kerugian dan rehabilitasi, dikaitkan bahwa tidak semua peristiwa yang terjadi dan diduga sebagai tindak pidana itu terlihat bentuknya secara jelas sebagai tindak pidana.[6]

Pasal 4 KUHAP menjelaskan bahwa yang dapat menjadi penyelidik adalah setiap pejabat polisi negara Republik Indonesia. Jadi yang dapat menjadi penyelidik hanya anggota kepolisian saja, berbeda halnya dengan penyidik, yang dapat menjadi penyidik bukan hanya anggota kepolisian saja tetapi pegawai negeri sipil tertentu yang diberi wewenang khusus oleh undang-undang. Dari ketentuan Pasal 1 ayat 5 tentang penyelidikan dan Pasal 5 ayat 1 huruf (a) dan (b) KUHAP tentang tugas dan wewenang penyelidik adalah:

1). Tugas penyelidik berdasarkan hukum dapat berupa:

a) Menerima laporan atau pengaduan;
b) Mencari keterangan dan alat bukti;
c) Menyuruh berhenti seseorang yang dicurigai dan menanyakan serta memeriksa tanda pengenal diri;
d) Mengadakan tindakan lain menurut hukuman yang bertanggungjawab.

2). Kewenangan penyelidik atas perintah penyidik:

[6] Lilik Mulyadi, 2007, *Hukum Acara Pidana*, Bandung: Alumni, Hal. 56.

a) Penangkapan, larangan meninggalkan tempat, penggeledahan dan penyitaan;
b) Pemeriksaan dan penyitaan surat;
c) Mengambil sidik jari dan memotret seseorang;
d) Membawa dan menghadapkan seseorang pada penyidik.

b. Penyidikan

Dalam bahasa Belanda penyidikan sama dengan *opsporing*, menyidik (*opsporing*) berarti pemeriksaan permulaan oleh pejabat-pejabat yang ditunjuk oleh undang-undang segera setelah mereka dengan jalan apapun mendengar kabar yang sekedar beralasan, bahwa ada terjadi suatu pelanggaran. Tugas penyidikan yang dilakukan oleh penyidik POLRI (Polisi Republik Indonesia) adalah merupakan penyidik tunggal bagi tindak pidana umum, tugasnya sebagai penyidik sangat sulit dan membutuhkan tanggung jawab yang sangat besar, karena penyidikan merupakan tahap awal dari rangkaian proses penyelesaian perkara pidana yang artinya akan berpengaruh bagi tahap proses pradilan selanjutnya. Tugas penyidik adalah melaksanakan penyelidikan, yaitu serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam Kitab Undang-Undang Hukum Acara Pidana untuk mencari serta mengumpulkan barang bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya.[7]

[7] Masrizal Afriald, 2016, "Pelaksanaan Penyelidikan Dan Penyidikan Perkara Pidana Oleh Kepolisian", *JOM Fakultas Hukum* , Vol. III, Nomor 2, Oktober 2016. Hal. 110-115

Penyidikan adalah tahap yang mana telah melewati tahapan penyelidikan yang berarti menuju pada proses yang lebih serius menuju prapradilan dan mencari alat-alat bukti dan saksi- saksi yang lebih jelas dan terang agar tidak salah dalam penetapan tersangka atau terdakwa dan mempermudah hakim dalam memutus perkara.

c. Prinsip Penentuan Tempat dan Waktu Kejadian (*Locus Dan Tempus Delicti*) Dalam Peradilan Pidana

Proses penyelidikan dan penyidikan oleh pihak kepolisian dan atau kejaksaan atas dugaan suatu tindak pidana yang untuk selanjutnya diperiksa dan diputus oleh pengadilan, tidak terlepas dari kewenangan dalam melaksanakan tugas dan wewenang masing-masing institusi (Kepolisian, Kejaksaan, Pengadilan).

Hukum pidana di Indonesia merupakan sistem peradilan pidana terpadu. Artinya melibatkan beberapa institusi dalam yuridiksi tertentu. Proses penyelidikan dan penyidikan oleh pihak kepolisian dan atau kejaksaan atas dugaan suatu tindak pidana yang untuk selanjutnya diperiksa dan diputus oleh pengadilan, tidak terlepas dari kewenangan dalam melaksanakan tugas dan wewenang masing-masing institusi (Kepolisian, Kejaksaan, Pengadilan), dalam menentukan kompetensi atau kewenangan suatu pengadilan dapat atau tidaknya untuk mengadili suatu perkara tindak pidana, berkaitan secara langsung dengan *locus delicti* atau tempat kejadian perkarta atas suatu tindak pidana.

Pada saat seseorang menjadi korban atas suatu tindak pidana maka dapat melaporkan suatu tindak pidana ke kantor kepolisian yang terdekat pada lokasi peristiwa pidana tersebut terjadi. Adapun daerah hukum kepolisian meliputi:[8]

1) Daerah hukum kepolisian Markas Besar (MABES) POLRI untuk wilayah Negara Kesatuan Republik Indonesia;
2) Daerah hukum kepolisian Daerah (POLDA) untuk wilayah Provinsi;
3) Daerah hukum kepolisian Resort (POLRES) untuk wilayah
4) Daerah hukum kepolisian Sektor (POLSEK) untuk wilayah kecamatan.

Pada pasal 4 ayat (1) Peraturan Pemerintah (PP) Nomor 23 Tahun 2007 tentang Daerah Hukum Kepolisian Negara Republik Indonesia. Mengenai wilayah administrasi kepolisian, daerah hukumnya dibagi berdasarkan pemerintahan daerah dan perangkat sistem peradilan pidana terpadu sebagaimana diatur Pasal 2 ayat (2) PP Nomor 23 Tahun 2007. Kepolisian yang telah melakukan penyelidikan ataupun penyidikan atas dugaan suatu tindak pidana selanjutnya melimpahkan perkara tersebut kepada pihak kejaksaan di wilayah hukum yang berwenang melakukan penuntutan atas suatu tindak pidana. Tugas dan wewenang Kejaksaan untuk melakukan penuntutan diatur dalam Pasal 14 Kitab Undang-Undang Hukum Acara Pidana (KUHAP) dan Pasal 30 Undang-Undang Nomor 16 Tahun 2006 tentang Kejaksaan Republik

[8] M. Yahya Harahap. 2010. *Pembahasan Permasalahan dan Penerapan KUHAP*. Jakarta : Sinar Grafika. Hal. 99- 100

Indonesia. Menurut aturan di atas satu satu tugas dan wewenang kejaksaan adalah melakukan penuntutan dan untuk kemudian melimpahkan perkara kepada pengadilan yang memiliki wewenang untuk mengadili suatu perkara tindak pidana, dalam hal pengadilan mana yang memiliki kewenangan untuk mengadili suatu perkara lagi-lagi tidak terlepas dari dimana tindak pidana tersebut terjadi atau dapat disebut juga sebagai kewenangan relatif pengadilan negeri.

Pengadilan Negeri yang berwenang mengadili suatu perkara diatur dalam KUHAP Bab X, Pasal 84. Bertitik tolak dari ketentuan dalam pasal tersebut, kriteria yang pertama dan utama untuk Pengadilan Negeri yaitu dapat berwenang mengadili setiap perkara pidana yang dilakukan dalam daerah hukumnya. Hal ini ditegaskan dalam Pasal 84 ayat (1) KUHAP yang berbunyi "Pengadilan negeri berwenang mengadili segala perkara mengenai tindak pidana yang dilakukan dalam daerah hukumnya."[9] Asas atau kriteria yang dipergunakan pada pasal ini adalah "tempat tindak pidana dilakukan" atau disebut locus delicti. Prinsip dimaksud didasarkan atas tempat terjadinya tindak pidana. Di tempat mana dilakukan tindak pidana atau di daerah hukum Pengadilan Negeri mana dilakukan tindak pidana, Pengadilan Negeri tersebut yang berwenang mengadili. Jika sudah nyata terjadi di lingkungan wilayah hukumnya, dia yang berwenang memeriksa dan mengadilinya. Sebaliknya, apabila dari hasil penelitian ternyata perbuatan tindak pidana

[9] Ibid, Hal. 96-97

dilakukan di luar wilayah hukumnya, tidak berwenang untuk memeriksa dan mengadilinya dan Ketua Pengadilan Negeri yang bersangkutan menyerahkan surat pelimpahan perkara tersebut kepada Pengadilan Negeri yang dianggapnya berwenang, dengan jalan mengeluarkan surat "penetapan".

D. Faktor Pendorong *Cyber Crime* di Indonesia

Kejahatan merupakan salah satu bentuk dari perilaku menyimpang yang selalu ada dan melekat pada tiap bentuk masyarakat, tidak ada masyarakat yang sepi dari kejahatan.[10] Kejahatan terjadi tidak hanya disebabkan oleh factor individu seseorang tetapi juga disebabkan oleh factor eksternal seperti yang berasal dari lingkungan seskitar dan kehidupan sosialnya. *Cyber crime* semakin marak terjadi, karena modus yang beranekaragam. Para pelaku sangat lihai dalam menjalankan aksinya, mereka adalah individu yang cerdas dan kreatif, namun menggunakan hal tersebut untuk melakukan suatu kejahatan yang dapat menimbulkan kerugian bagi orang lain baik itu kerugian materiil maupun immaterial.

Berikut ini adalah faktor-faktor yang menjadi penyebab maraknya *cyber crime*, antara lain:

1. Kurangnya Kesadaran Hukum Masyarakat

Kesadaran hukum merupakan kesadaran tentang apa yang seharusnya atau tidak seharusnya kita lakukan berkaitan dengan aturan atau

[10] Muladi dan Barda Nawawi Arief, 2010. *Teori-Teori dan Kebijakan Pidana*. Bandung: Alumni. Hal. 148

hukum yang berlaku di masyarakat. Saat ini kesadaran hukum masyarakat masih dinilai kurang terkait aktivitas *cyber crime*, hal tersebut dikarenakan kurangnya pemahaman terkait *cyber crime* baik itu tindakan maupun efek yang ditimbulkannya. Banyak masyarakat kurang atau belum sadar akan perbuatan yang dilakukan terkait aktivitas di dunia maya yang mana kita bisa melihat dimulai dari maraknya perbuatan pencemaran nama baik hingga tindakan membajak akun sosial orang lain. Perbuatan kecil tersebut dianggap biasa dan lumrah di masyarakat, bahkan cenderung sebagai candaan. Melalui pemahaman mengenai *cyber crime*, masyarakat sangat berperan penting dalam upaya penanggulangan *cyber crime*. Tanpa pemahaman pelaku *cyber crime* akan merajalela karena masyarakat tidak tahu apa yang sesungguhnya mereka lakukan hingga pada akhirnya mereka tertipu, rekening mereka dibobol dan berbagai kerugian lainnya.

2. Keamanan

Pelaku *cyber crime* tentunya akan merasa aman saat menjalankan aksinya, hal ini tidak lain karena media yang digunakan dalam menjalankan kejahatan berupa akses internet yang lazim digunakan dimana saja baik itu tempat tertutup maupun terbuka. Kurangnya sistem keamanan dari internet membuat siapapun bebas berekspresi di dunia maya tanpa memerlukan batasan sehingga mendorong pertumbuhan *cyber crime*. Hal yang senada diungkapkan oleh Ketua Pengelola Nama Domain Internet Indonesia

(Pandi) Andi Budimansyah, menurutnya[11] "Kesadaran masyarakat Indonesia soal keamanan *cyber* masih lemah. Saat ini banyak pemilik *website* di Indonesia yang tidak mengetahui bahwa *website*-nya digunakan untuk *pishing* atau tindakan memalsukan *website* orang lain. *Website* palsu itu dibuat mirip dengan yang asli untuk mengambil keuntungan dari transaksi yang dilakukan di *website* asli." Selain *pishing*, di Indonesia juga marak penanaman malware atau program jahat yang ditaruh orang lain di *server-server* Indonesia atau bahkan ditaruh di ponsel. Pada saat tertentu malware bisa meminta program untuk menyerang ke *website* tertentu. Hal tersebut menguatkan bahwa kesadaran keamanan kita masih lemah. Kita sendiri tidak bisa menjaga *website* kita, sehingga memungkinkan terjadinya perbuatan phising dan juga *malware*. Sama halnya dengan pelaku menggunakan kita untuk melakukan suatu kejahatan tanpa sepengetahuan kita.

3. Aparat Penegak Hukum

Secara umum aparat penegak hukum masih sangat minim pengetahuan dalam penguasaan operasional komputer dan pemahaman terhadap *hacking* komputer serta kemampuan melakukan penyelidikan dan penyidikan terhadap kasus-kasus kejahatan *cyber crime* (dunia maya). Hal tersebut memungkinkan pelaku *cyber crime* jauh lebih hebat dibandingkan

[11] *https://pandi.id/berita/kesadaran-keamanan-cyber-indonesia-masih-rendah-kata-pandi/* yang diakses pada tanggal 08 April 2018 Pukul 12:32 Wib.

aparat penegak hukum yang mengakibatkan semakin meningkatnya intensitas *cyber crime* di Indonesia.[12]

Pada instansi kepolisian sampai saat ini belum ada melakukan pelatihan-pelatihan khusus pada kepolisian khusunya di akademi kepolisian maka dari itu para penyidik tindak pidana *cyber crime* sendiri hingga saat ini mesih menggunakan jasa-jasa penyidik bukan berlatarbelakang dari AKPOL (akademi kepolisian) melainkan dari lulusan sarjana komputer atau teknologi informasi hal ini tentu menjadi hambatan utama kepolisian dalam menanggulangi kejahatan *cyber crime*.

E. Penanggulangan Kejahatan *Cyber Crime*

1. Lembaga yang Menanggulangi Tindak Pidana *Cyber Crime*

Lembaga yang menanggulangi tindak pidana *cyber crime* yaitu lembaga kepolisian/POLRI yang mana sebagai penyelidik dan penyidik khususnya dalam tindak pidana *cyber crime*, dalam menanggulangi tindak pidana *cyber crime* POLRI dalam hal ini memiliki perwakilan lembaga dari setiap daerah provinsi di Indonesia/POLDA, dan dari setiap POLDA memiliki satuan kerja yang menangani tindak pidana khusus yang disebut DITRESKRIMSUS yang mana dari satuan kerja tersebut memiliki beberapa SUBDIT (bagian direktorat) kemudian dalam setiap SUBDIT (bagian direktorat) memiliki Unit-unit yang menangani kasus-kasus tindak pidana khusus tertentu.

[12] Wawancara dengan AKP. Safpe Tambatua Sinaga (Penyidik) Unit *Cyber Crime* POLDA DIY, pada tanggal , 27 juni 2019 pukul 08.29 Wib

Pada perwakilan lembaga kepolisian dari daerah provinsi, dalam ini penulis akan menjelasakan di perwkilan lembaga kepolisian daerah istimewa Yogakarta/POLDA DIY karena penulis melakukan penelitian di POLDA DIY khususnya di satuan kerja DITRESKRIMSUS pada Unit *cyber crime*/ITE. POLDA DIY dalam hal ini memiliki satuan kerja yang disebut DITRESKRIMSUS yang membawahi 4 (empat) SUBDIT (bagian direktorat) yaitu: [13]

a. SUBDIT (Bagian Direktorat) I

SUBDIT I menangani tindak pidana ekonomi yang memiliki 2 (dua) unit yang mana unit 1 (satu) menangani tindak pidana perbankan dan unit 2 (dua) menangani tindak pidana fisimondev (fiskal, moneter dan devisa).

b. SUBDIT (Bagian Direktorat) II

SUBDIT II menangani tindak pidana inprogdag (industry, produksi, dan perdagangan) yang memiliki 2 (dua) Unit yang mana Unit 1 (satu) menangani tindak pidana haki dan perdagangan dan Unit 2 (dua) menangani tindak pidana informasi dan transaksi elektronik (*cyber crime*).

c. SUBDIT (Bagian Direktorat) III

SUBDIT III menangani tindak pidana pidter (pidana tertentu) yang memiliki 2 (dua) unit yang mana Unit 1 (satu) menangani tindak

[13] Wawancara dengan AKP. Safpe Tambatua Sinaga (Penyidik) Unit *cyber crime* POLDA DIY, pada tanggal , 27 juni 2019 pukul 08.29 Wib.

pidana sumdagling (sumberdaya dan lingkungan) dan Unit 2 (dua) menangani tindak pidana non sumdagling (sumberdaya dan lingkungan).

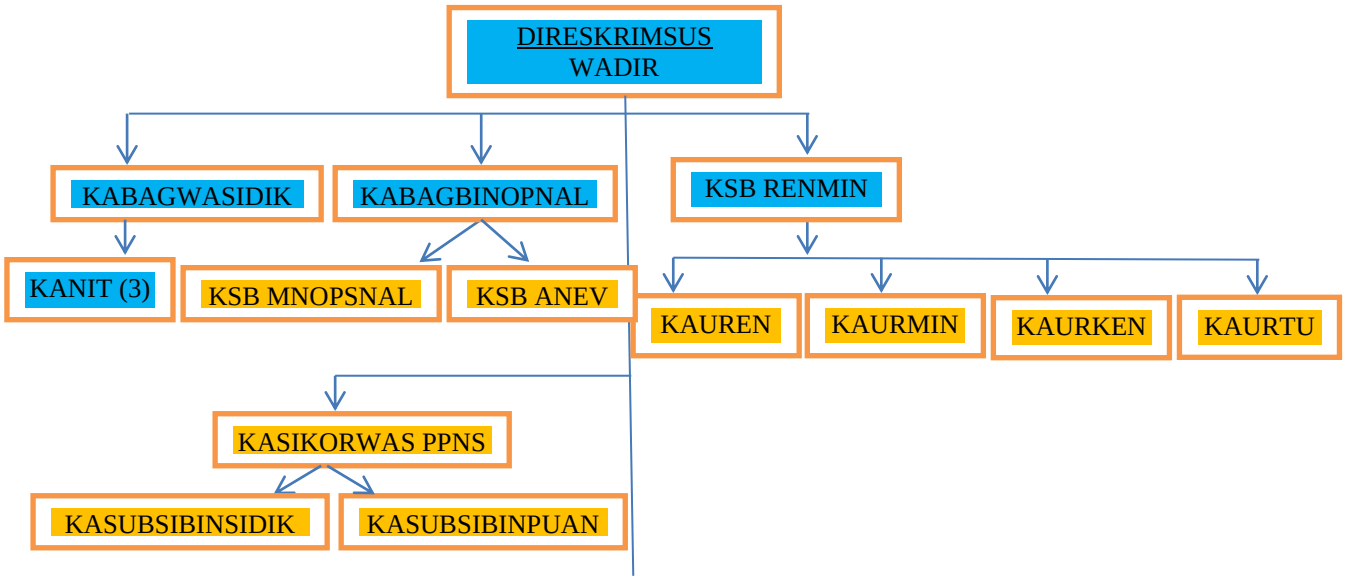
d. SUBDIT (Bagian Direktorat) IV

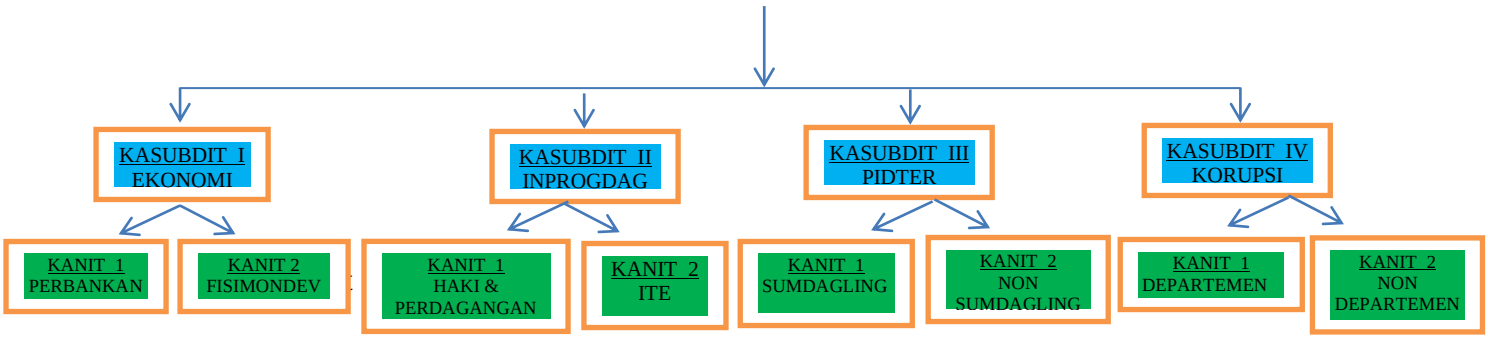
SUBDIT IV menangani tindak pidana korupsi yang memiliki 2 (dua) Unit yang mana Unit 1 (satu) menangani tindak pidana korupsi departemen dan Unit 2 (dua) menangani tindak pidana korupsi non departemen.

Pada setiap POLDA yang mewakili setiap daerah provinsi memiliki satuan kerja yang menangni tindak pidana khusus yang disebut DITRESKRIMSUS yang membawahi beberapa SUBDIT dan Unit yang memiliki tugas pokok dan fungsi. POLDA DIY memilki 4 (empat) SUBDIT yang mana tindak pidana *cyber crime* sendiri ditangani oleh SUBDIT II dan berposisi di Unit 2 (dua) yakni Unit *cyber crime*/ ITE. Beriku gambar strukur organisasi DITRESKRIMSUS POLDA DIY:

Gambar 2.1

Strukur Organisasi DITRESKRIMSUS POLDA DIY





keterangan gambar berdasarkan warna kolom:

1). Pimpinan

2). Pembantu Pimpinan/ Pelayan

3). Pelaksana Tugas Pokok

(*Sumber: Unit Cyber Crime DITRESKRIMSUS POLDA DIY*).

Berdasarkan gambar tersebut diatas kita dapat mengetahui lebih jelas bagaimana gambaran khususnya dalam hal struktur organisasi yang ada di satuan kerja pada DITRESKRIMSUS yang mana banyak bagian atau SUBDIT-SUBDIT dan Unit-unit yang dibawahi oleh DITRESKRIMSUS tersebut, yang mana hal tersebut bertujuan agar setiap SUBDIT lebih cepat dan lebih fokus dalam menangani kasus-kasus tindak pidana khusus yang dilaporkan oleh masyarakat.

Direktorat reserse kriminal khusus POLDA DIY memiliki visi dan misi yaitu :[14]

1) Visi DITRESKRIMSUS POLDA DIY

Terwujudnya DITRESKRIMSUS POLDA DIY yang professional, proporsional, akuntabel dalam penanganan tindak

[14] Wawancara dengan AKP. Safpe Tambatua Sinaga (Penyidik) Unit *Cyber Crime* POLDA DIY, pada tanggal , 27 juni 2019 pukul 08.29 Wib.

pidana khusus guna memberikan kepasian hukum dan rasa keadilan pada masyarakat di wilayah Yogyakarta.

2) Misi DITRESKRIMSUS POLDA DIY

a) Melaksanakan penegakan hukum secara professional, objektif, proporsional, transaparan, dan akuntabel guna menjamin kepastian hukum dan rasa keadilan melalui giat lidik sidik tindak pidana khusus di bidang tindak pidana ekonomi, tindak pidana inprodag, tindak pidana tertentu dan tindak pidana korupsi diwilayah hukum POLDA DIY.

b) Menyelesaikan permasalahan hukum secara professional dan akuntabel dengan menganalisa kasus besera penanganannya serta mempelajari dan mengkaji efekifitas pelaksanaan tugas di Ditreskrimsus POLDA DIY.

c) Melaksanakan pembinaan teknis, koordinasi dan pengaawasan oprasional serta adminisrasi penyidikan oleh PPNS diwilayah hukum POLDA DIY.

d) Meningkatkan kemitraan dan sinergi penegakan hukum dengan masyarakat dan instansi/lembaga terkait dengan semangat gotong royong.

e) Melaksanakan pengawasan penyidikan tindak pidana khusus secara optimal di lingkungan POLDA DIY.

f) Melakukan proses pengumpulan, pengelolaan dan menyajikan informasi data berkaitan tupoksi pada program kegiatan Ditreskrimsus secara berkelanjutan.

g) Meningkakan kualitas dan kompetensi penyidik/ penyidik pembantu/personel Ditreskrimsus POLDA DIY yang professional, kompeten, unggul, terpercaya, dan berkepribadian.

h) Meningkatkan pelayanan dibidang tindak pidana khusus dalam upaya penegakan hukum yang berkeadilan dengan menjunjung tinggi HAM diwilayah hukum POLDA DIY.

i) Meningkatkan dukungan sarana prasarana berupa peralatan yang berteknologi tinggi dan modern.

j) Mewujudkan penyempurnaan sisem dan metode yang tepat dengan berbasis pada sistem informasi dan komunikasi terkini guna menunjang pelaksanaan tugas penyidikan.

2. Upaya Penanggulangan Kejahatan

Kejahatan merupakan gejala sosial yang senantiasa dihadapi oleh setiap masyarakat di dunia ini. Kejahatan dalam kebenarannya dirasakan sangat meresahkan di samping itu juga mengganggu ketertiban dan ketentraman dalam masyarakat, oleh karena itu masyarakat berupaya semaksimal mungkin untuk menanggulangi timbulnya kejahatan. Upaya penanggulangan kejahatan telah dan terus dilakukan oleh semua pihak baik pemerintah maupun masyarakat pada umumnya, berbagai program dan

kegiatan telah dilaksanakan sambil terus mencari cara tepat dan efektif untuk mengatasi masalah tersebut.[15]

E.H. Sutherland dan Cressesy mengemukakan bahwa dalam *crime prevention* dalam pelaksanaannya ada dua buah metode yang dipakai untuk mengurangi frekuensi kejahatan yaitu:[16]

1) Metode untuk penanggulangan kejahatan, merupakan suatu cara yang ditujukan kepada pengurangan jumlah dilakukan secara konseptual.
2) Metode untuk mencegah kejahatan pertama kali, suatu cara yang ditujukan kepada upaya untuk mencegah terjadinya kejahatan yang pertama kali, yang akan dilakukan oleh seseorang dalam metode ini dikenal sebagai metode preventif. Berdasarkan uraian diatas dapat dilihat bahwa upaya penanggulangan kejahatan mencakup aktivitas preventif sekaligus berupaya memperbaiki prilaku seseorang yang dinyatakan telah bersalah (terpidana) di Lembaga Pemasyarakatan atau dengan kata lain, upaya kejahatan dapat dilakukan secara preventif dan represif. Penanggulangan kejahatan dapat berupa :[17]

a. Upaya Preventif

Upaya penanggulangan kejahatan secara preventif (pencegahan) dilakukan untuk mencegah timbulnya kejahatan pertama kali.Mencegah kejahatan lebih baik daripada mencoba mendidik penjahat menjadi lebih baik kembali, demikian semboyan dalam kriminologi, yaitu usaha-usaha

[15] Iqbal Kamalludin. 2019. "Kebijakan Formulasi Hukum Pidana Tentang Penaggulangan Tindak Pidana Penyebaran Ujaran Kebencian (*Hate Speech*) Di Dunia Maya". *Jurnal Law Reform,* Vol. 15. Nomor 1, Januari 2019. Hal. 114.
[16] E.H. Sutherland dan Cressesy dalam A.S. Alam. Op Cit. Hal. 78
[17] Ibid. Hal. 79-80

memperbaiki penjahat (narapidana) yang perlu diperhatikan dan diarahkan agar tidak terjadi lagi kejahatan ulang.

Upaya preventif diutamakan karena upaya preventif dapat dilakukan oleh siapa saja tanpa suatu keahlian yang khusus dan ekonomis, misalnya menjaga diri, jangan sampai menjadi korban kriminalitas. Dalam upaya preventif (pencegahan) itu bagaimana upaya kita melakukan suatu usaha jadi positif, bagaimana kita menciptakan suatu kondisi seperti keadaan ekonomi, lingkungan juga budaya masyarakat menjadi suatu dinamika dalam pembangunan dan bukan sebaliknya seperti menimbulkan ketegangan-ketegangan sosial atau mendorong timbulnya perbuatan atau penyimpangan. Dan disamping itu bagaimana meningkatkan kesadaran dan partisipasi masyarakat bahwa keamanan dan ketertiban adalah tanggung jawab bersama.[18]

b. Upaya Represif

Upaya represif merupakan suatu upaya penanggulangan kejahatan yang secara konsepsional ditempuh setelah terjadinya kejahatan. Penanggulangan dengan upaya represif dimaksudkan untuk menindak para pelaku kejahatan sesuai dengan perbuatannya serta memperbaiki kembali agar mereka sadar bahwa perbuatan yang dilakukannya merupakan perbuatan yang melanggar hukum dan merugikan masyarakat, sehingga tidak akan mengulanginya dan orang

[18] Hardianto Djanggih. 2013. "Kebijakan Hukum Pidana Dalam Penaggulangan Tindak Pidana *Cyber Crime"*, *Jurnal Hukum Universitas Tompotika Luwuk*, Vol. 1. Nomor 2. September 2013. Hal. 59-67.

lain juga tidak akan melakukannya mengingat sanksi yang akan ditanggungnya.[19]

Pada upaya represif ini yaitu bertujuan untuk memberi efek jera pada pelaku tindak pidana dengan sanksi atau hukuman sesuai undang-undang dan yang dilanggar oleh pelaku dengan melewati proses hukum mulai dari penyelidikan, penyidikan yang dilakukan oleh pihak penyidik/ kepolisian, jika pada tahap penyelidikan dan penyidikan alat bukti dan saksi- saksi sudah memenuhi sesuai penetapan undang-undang yang mana kitab undang-undang hukum acara pidana tepatnya pada pasal 183 bahwa sekurang-kurangnya adalah dua alat bukti yang dianggap sah untuk memperoleh keyakinan hakim bahwa tindak pidana tersebut benar-benar terjadi dan terdawkalah yang bersalah dan melakukan tindak pidana tersebut. Persidangan yang dilakukan di pengadilan dan dengan jaksa penuntut umum membuktikan bahwa tersangka atau terdakwa bersalah dengan alat-alat bukti dan keterangan saksi serta alat bukti lainnya maka berdasarkan tuntutan jaksa penuntut umum hakim menimbang dan memutus sesuai keyakinan hakim, jika hakim memutuskan bahwa terdakwa bersalah maka status terdakwa berubah menjadi terpidana dan dan mejalani hukuman sesuai dengan putusan hakim, maka hal itu disebut sebagai upaya represif dengan memberikan sanksi kepada pelaku tindak pidana.

[19] Wawancara dengan AKP. Safpe Tambatua Sinaga (Penyidik) Unit *Cyber Crime* POLDA DIY, pada tanggal , 27 juni 2019 pukul 08.29 Wib