BAB 1V

UPAYA INDONESIA DALAM MENAGGULANGI CYBERCRIME

A. Upaya Pemerintah Indonesia

Cybercrime merupakan suatu perbuatan merugikan orang lain atau instansi yang berkaitan dan pengguna fasilitas dengan sistem Informasi dan Transaksi Elektronik yang bertujuan untuk menguntungkan diri sendiri maupun orang lain secara materi, maupun hanya untuk sekedar memuaskan jiwa pelaku atau orang tersebut. Oleh karena itu, maka tindakan atau perbuatan tersebut merupakan suatu kejahatan dan merupakan perbuatan melanggar hukum, karena adanya unsur-unsur dimana ada pihak-pihak lain yang merasa dirugikan oleh perbuatan tersebut. *Cybercrime* adalah merupakan suatu perbuatan melanggar hukum yang secara khusus di diatur dalam Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Dalam upaya-upaya yang dapat dilakukan terkait dengan masalah pembuktian oleh pengadilan dan penyidikan oleh polri dalam *cybercrime* dapat digunakan berbagai macam cara, antara lain dengan mengoptimalkan Undang- Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, mengembangkan pengetahuan dan kemampuan penyidik dalam *Dunia Cyber,* menambahkan dan meningkatkan fasilitas komputer forensik dalam POLRI.

Kejahatan internet atau yang lebih populer dengan istilah *cyber crime* ini dapat dilakukan tanpa mengenal batas teritorial dan tidak diperlukan interaksi langsung antara pelaku dan korban kejahatan. Dengan sifat seperti itu, semua negara termasuk Indonesia yang melakukan aktivitas internet akan terkena

dampak dari perkembangan kejahatan dunia maya. Para *hacker* selalu mencari celah untuk menggunakan keahliannya melakukan kejahatan. Memudarnya batas-batas geografi dalam abad 21 yang dikenal sebagai abad informasi ini telah mengubah cara pandang terhadap penyelesaian dan praktik kejahatan dari model lama (konvensional) ke model baru (elektronik). Kekuatan jaringan dan komputer pribadi berbasis pentium menjadikan setiap komputer sebagai alat yang potensial bagi para pelaku kejahatan.[43] Globalisasi aktivitas kriminal yang memungkinkan para penjahat melintas batas elektronik merupakan masalah nyata dengan potensi mempengaruhi negara, hukum, dan warga negaranya. Fakta ini tak bisa dipungkiri karena internet dapat dijadikan sarana yang efektif untuk mencapai tujuan-tujuan negatif yang diinginkan tanpa batasan geografis dan teritorial.

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik jika dilihat dalam perspektif penanggulangan penyalahgunaan internet di atas, maka semestinya tak perlu ada pro dan kontra. Ini karena pada dasarnya dibentuknya UU itu untuk melindungi masyarakat dari kerugian dan kehancuran akhlak yang akan berimplikasi pada kelangsungan hidup berbangsa dan bernegara. Walaupun demikian, kehadiran perangkat hukum itu pun tidak secara otomatis dapat menghentikan langkah para *hacker*. Bahkan, perangkat hukum pun akan memancing keberanian mereka untuk mencari titik-titik lemahnya sehingga mereka bisa terus melancarkan aksinya. Selain itu, tidak dapat selalu mengacu pada Undang-undang Informasi Transaksi elektronik

[43]http://denet.hforum.biz/t42-kejahatan-dunia-maya diakses tanggal 21 November 2013

danKitab Undang-undang Hukum Pidana lama saja, melainkan mengikuti perkembangan jaman kita membutuhkan KUHP baru.

Dalam pasal 5 ayat 1 dan 2 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik mendeskripsikan bahwa Dokumen elektronik dan Informasi Elektronik adalah merupakan alat bukti yang sah. Selain itu dalam pasal 44 Undang-undang yang sama mengatakan alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan undang-undang ini adalah sebagai berikut :

a) alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan;dan
b) alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3)

Selain deskripsi undang-undang ITE tersebut, dikenal pula alat bukti digital. Tindakan kejahatan tradisional umumnya meninggalkan bukti kejahatan berupa bukti-bukti fisikal, karena proses dan hasil kejahatan ini biasanya juga berhubungan dengan benda berwujud nyata. Dalam dunia komputer dan internet, tindakan kejahatan juga akan melalui proses yang sama. Proses kejahatan yang dilakukan tersangka terhadap korbannya juga akan mengandalkan bantuan aspek pendukung dan juga akan saling melakukan pertukaran atribut[44]. Namun dalam kasus ini aspek pendukung, media, dan atribut khas para pelakunya adalah semua yang berhubungan dengan sistem komputerisasi dan komunikasi digital. Atribut-

[44]Yuyun Yulianah, SH, MH ,*Pembuktian Tindak Pidana Cyber Crime*,Pustaka Pelajar:Yogyakarta,2005, halaman 7

atribut khas serta identitas dalam sebuah proses kejahatan dalam dunia komputer dan internet inilah yang disebut dengan bukti-bukti digital.[45]

Perangkat yang menggunakan format data digital untuk menyimpan informasi memang sangat banyak. Meskipun dalam cakupannya hanya seputar perangkat komputer dan jaringan saja, namun perangkat-perangkat lain juga memiliki potensi untuk menyimpan bukti-bukti digital. Seperti misalnya perangkat ponsel, *smart card*, bahkan *microwave* juga bisa berperan sebagai sumber buktibukti digital. Berdasarkan pertimbangan inilah maka dibuat tiga kategori besar untuk sumber bukti digital, yaitu:[46]

1) Open Computer Systems

Perangkat-perangkat yang masuk dalam kategori jenis ini adalah apa yang kebanyakan orang pikir sebagai perangkat komputer. Sistem yang memiliki media penyimpanan, *keyboard*, monitor, dan pernak-pernik yang biasanya ada di dalam komputer masuk dalam kategori ini. Seperti misalnya laptop, *desktop, server*, dan perangkat-perangkat sejenis lain. Perangkat yang memiliki sistem media penyimpanan yang kian membesar dari waktu ke waktu ini merupakan sumber yang kaya akan bukti-bukti digital. Sebuah *file* yang sederhana saja pada sistem ini dapat mengandung informasi yang cukup banyak dan berguna bagi proses investigasi. Contohnya detail seperti kapan *file* tersebut dibuat, siapa pembuatnya, seberapa sering *file* tersebut di akses, dan informasi lainnya semua merupakan informasi penting.

[45] http://yogapw.wordpress.com/2009/11/13/pengertian-bukti-digital-digital-evidence , diakses tangga 21 November 2013
[46] *ibid*

2) Communication Systems

Sistem telepon tradisional, komunikasi *wireless*, Internet, jaringan komunikasi data, merupakan salah satu sumber bukti digital yang masuk dalam kategori ini. Sebagai contoh, jaringan Internet membawa pesan-pesan dari seluruh dunia melalui e-mail. Kapan waktu pengiriman *e-mail* ini, siapa yang mengirimnya, apa isi dari *e-mail* tersebut merupakan bukti digital yang sangat penting dalam investigasi.

3) Embedded Computer Systems

Perangkat telepon bergerak (ponsel), *Personal Digital Assistant(PDA),smart card*, dan perangkat-perangkat lain yang tidak dapat disebut komputer tapi memiliki sistem komputer dalam bekerjanya dapat digolongkan dalam kategori ini. Hal ini dikarenakan bukti-bukti digital juga dapat tersimpan di sini. Sebagai contoh, sistem navigasi mobil dapat merekam ke mana saja mobil tersebut berjalan. Sensor dan modul-modul diagnosa yang dipasang dapat menyimpan informasi yang dapat digunakan untuk menyelidiki terjadinya kecelakaan, termasuk informasi kecepatan, jauhnya perjalanan, status rem, posisi *persneling* yang terjadi dalam lima menit terakhir. Semuanya merupakan sumber-sumber bukti digital yang sangat berguna.

Agar penegakan hukum *cybercrime* ini dapat dilakukan secara menyeluruh maka tidak hanya pendekatan yuridis atau penal yang dilakukan, tetapi dapat juga

dilakukan dengan pendekatan non-penal. Dalam konteks *cyber crime* ini erat hubungannya dengan teknologi, khususnya teknologi komputer dan telekomunikasi sehingga pencegahan *cyber crime* dapat digunakan melalui saluran teknologi atau disebut juga *techno-prevention.*[47] Pendekatan teknologi ini merupakan subsistem dalam sebuah sistem yang lebih besar, yaitu pendekatan budaya, karena teknologi merupakan hasil dari kebudayaan atau merupakan kebudayaan itu sendiri. Pendekatan budaya atau kultural ini perlu dilakukan untuk membangun atau membangkitkan kepekaan warga masyarakat dan aparat penegak hukum terhadap masalah *cyber crime* dan menyebarluaskan atau mengajarkan etika penggunaan komputer melalui media pendidikan. Pentingnya pendekatan budaya ini, khususnya upaya mengembangkan kode etik dan perilaku (*code of behavior and ethics).*

Ketidaksiapan hukum dan polri dalam penegakan hukum *cyber crime* ini menyebabkan pencegahan dengan menggunakan teknologi dan budaya menjadi alat yang ampuh. Hal ini terungkap dari korban *hacking* yang merasa nyaman dengan pendekatan teknologi untuk menanggulangi *cyber crime.* Ketika situs mereka dirusak, mereka menggunakan teknologi dalam memperbaikinya dan mengantisipasinya dengan menggunakan sistem pengamanan yang ketat. Dalam Resolusi Kongres PBB VIII/1990 mengenai *Computer related crimes* sebagaimana dikutip menghimbau negara-negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan komputer yang lebih efektif dengan mempertimbangkan langkah-langkah sebagai berikut:

[47] http://jurnal.pdii.lipi.go.id/admin/jurnal/1085180.pdf , diakses tanggal 27 Juni 2011

a) Melakukan Modernisasi hukum pidana material dan hukum acara pidana
b) Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer
c) Melakukan langkah-langkah untuk membuat peka warga warga masyarakat, aparat pengadilan dan penegak hukum, terhadap pentingnya pencegahan kejahatan yang berhubungan dengan komputer
d) Melakukan upaya-upaya pelatihan bagi para hakim, pejabat dan aparat penegak hukum mengenai kejahatan ekonomi dan *cyber crime.*
e) Memperluas *rule of ethics* dalam penggunaan komputer dan mengajarkannya melalui kurikulum informatika.
f) Mengadopsi kebijakan perlindungan korban *cyber crime* sesuai dengan deklarasi PBB mengenai korban dan mengambil langkah-langkah untuk mendorong korban melaporkan adanya *cyber crime.*

Tidak hanya pendekatan penal dan non-penal yang diperlukan dalam penanggulangan *cyber crime* ini, mengingat *cyber crime* yang dapat dilakukan oleh orang dengan melalui batas negara, maka perlu dilakukan kerja sama dengan negara lain. Bentuk kerja sama ini dapat berupa kerjasama ekstradisi maupun harmonisasi hukum pidana subtantif sebagaimana terungkap dari hasil Kongres Perserikatan Bangsa-Bangsa (PBB) X/2000 : *"The harmonization of substantive criminal law with regard to cyber crimes is essential if international cooperation is to be achieved between law enforcement and the judicial authorities of different*

States".[48]Menurut Agus Raharjo bahwa salah satu langkah lagi agar penanggulangan *cyber crime* ini dapat dilakukan dengan baik, maka perlu dilakukan kerja sama dengan *Internet Service Provider (ISP)* atau penyedia jasa internet. Meskipun *Internet Service Provider (ISP)* hanya berkaitan dengan layanan sambungan atau akses Internet, tetapi *Internet Service Provider (ISP)* memiliki catatan mengenai ke luar atau masuknya seorang pengakses, sehingga ia sebenarnya dapat mengidentifikasikan siapa yang melakukan kejahatan dengan melihat *log file* yang ada.[49]

Ada beberapa cara yang dapat digunakan untuk mengamankan sistem informasi berbasis internet yang telah dibangun yaitu:

a) Mengatur akses (*access control*)

Salah cara yang umum digunakan untuk mengamankan informasi adalah dengan mengatur akses ke informasi melalui mekanisme *authentication* dan *access control*. Implementasi dari mekanisme ini antara lain dengan menggunakan *password*. Di sistem UNIX dan Windows NT, untuk masuk dan menggunakan sistem komputer, pemakai harus melalui proses *authentication* dengan menuliskan *userid* (*user identification*) dan password. Apabila keduanya valid, maka pemakai diperbolehkan untuk masuk dan menggunakan sistem, tetapi apabila di antara keduanya atau salah satunya tidak valid, maka akses akan ditolak. Penolakan ini tercatat dalam berkas log berupa waktu dan tanggal akses, asal hubungan

[48]http://www.fl.unud.ac.id/blockbook/BLOCK%20BOOK%20Th.2009/BB%20Hukum%20Organisasi%20Internasional%202009.pdfdiakses tanggal 21 November 2013
[49]Agus Raharjo, *Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi,* Bandung: PT Citra Aditya Bakti, 2002., hal. 248

(*connection*) dan berapa kali koneksi yang gagal itu. Setelah proses *authentication*, pemakai diberikan akses sesuai dengan level yang dimilikinya melalui sebuah *access control*. *Access control* ini biasanya dilakukan dengan mengelompokkan pemakai dalam sebuah grup, seperti grup yang berstatus pemakai biasa, tamu dan ada pula *administrator* atau disebut juga *superuser* yang memiliki kemampuan lebih dari grup lainnya. Pengelompokan ini disesuaikan dengan kebutuhan dari penggunaan sistem yang ada.

b) Menutup *service* yang tidak digunakan

Seringkali dalam sebuah sistem (perangkat keras dan atau perangkat lunak) diberikan beberapa servis yang dijalankan sebagai *default*, seperti pada sistem UNIX yang sering dipasang dari vendor-nya adalah *finger*, *telnet, ftp, smtp, pop, echo* dan sebagainya. Sebaiknya servis-servis ini kalau tidak dipakai dimatikan saja. Karena banyak kasus terjadi yang menunjukkan *abuse* dari servis tersebut atau ada lubang keamanan dalam servis tersebut. Akan tetapi *administrator* sistem tidak menyadari bahwa servis tersebut dijalankan dikomputernya.

c) Memasang Proteksi

Proteksi ini bisa berupa filter (secara umum) dan yang lebih spesifik lagi adalah *firewall*. Filter ini dapat digunakan untuk memfilter *e-mail*, informasi, akses atau bahkan dalam *level packet*. Sebagai contoh, di sistem UNIX ada paket program *topwrapper* yang dapat digunakan untuk membatasi akses kepada servis atau aplikasi tertentu. Misalnya, servis

untuk telnet dapat dibatasi untuk sistem yang memiliki nomor IP tertentu atau memiliki domain tertentu. Sementara *firewall* digunakan untuk melakukan filter secara umum. Ada juga program filter internet yang bernama *ZeekSafe*. Program ini bisa memblokir situs-situs yang tidak diinginkan. Selain itu, ada juga program filter yang lain, yaitu *We-Blocker*, sama dengan *ZeekSafe*, program ini bisa menentukan parameter apa saja yang akan membatasi akses ke *website* yang dianggap tidak layak dilihat.

d) Firewall

Program ini merupakan perangkat yang diletakkan antara internet dengan jaringan internal. Informasi yang ke luar dan masuk harus melalui *firewall* ini.Tujuan utama dari *firewall* adalah untuk menjaga (*prevent*) agar akses (ke dalam maupun ke luar) dari orang tidak berwenang (*unauthorized access*) tidak dapat dilakukan. *Firewall* bekerja dengan mengamati paket *Internet Protocol* (IP) yang melewatinya. Berdasarkan konfigurasi dari *firewall*, maka akses dapat diatur berdasarkan *Internet Protocol* (IP) *address*, *port* dan arah informasi

e) Pemantau adanya serangan

Sistem pemantau (*monitoring system*) digunakan untuk mengetahui adanya tamu tidak diundang (*intruder*) atau adanya serangan (*attack*). Nama lain dari sistem ini adalah *Intruder Detection System* (IDS). Sistem ini dapat memberi tahu administrator melalui *e-mail* maupun melalui mekanisme lain seperti *pager*. Ada beberapa cara untuk memantau adanya *intruder*, baik yang sifatnya aktif maupun pasif. *Intruder Detection*

System(IDS) cara yang pasif misalnya dengan memonitor log file. Contoh *Intruder Detection System* (IDS) adalah, Pertama, *Autobuse*, mendeteksi *probing* dengan memonitor *log file*. Kedua, *Courtney* dan portsentry adalah mendeteksi *probing (port scanning)* dengan memonitor paket yang lalu-lalang. *Portsentry* bahkan dapat memasukkan *Internet Protocol* (IP) penyerang dalam *filter topwrapper*. Ketiga, *Shadow* dari SANS. Keempat, Snort, mendeteksi pola (*pattern*) pada paket yang lewat dan mengirimkan *alert* jika pola tersebut terdeteksi. Pola-pola atau rules disimpan dalam berkas yang disebut *library* yang dapat dikonfigurasi sesuai dengan kebutuhan.

f) Pemantau *integritas system*

Sistem ini dijalankan secara berkala untuk menguji integritas sistem. Salah satu contoh program yang umum digunakan di sistem UNIX adalah program *Tripwire*. Program ini dapat digunakan untuk memantau adanya perubahan pada berkas. Pada mulanya program ini dijalankan dan membuat data base mengenai berkas-berkas atau direktori yang ingin kita amati beserta *signature* dari berkas tersebut. *Signature* berisi informasi mengenai besarnya berkas, kapan dibuatnya, pemiliknya, hasil *checksum* atau *hash* dan sebagainya. Apabila ada perubahan pada berkas tersebut, maka keluaran dari *hash function* akan berbeda dengan yang ada di *data base* sehingga ketahuan adanya perubahan.

g) *Audit:* Mengamati berkas log

Segala kegiatan penggunaan sistem dapat dicatat dalam berkas yang biasanya disebut *log file* atau log saja. Berkas log ini sangat berguna untuk mengamati penyimpanan yang terjadi. Kegagalan untuk masuk ke sistem (*login*) misalnya tersimpan dalam berkas *log*. Untuk itu pada administrator diwajibkan untuk rajin memelihara dan menganalisis berkas *log* yang dimilikinya.

h) *Back up* secara rutin

Sering kali intruder masuk dalam sistem dan merusak sistem dengan menghapus berkas-berkas yang ditemui. Jika intruder ini berhasil menjebol sistem dan masuk sebagai superuser, maka ada kemungkinan dia dapat menghapus seluruh berkas. Untuk itu, adanya *back up* yang digunakan secara rutin merupakan hal yang esensial.

i) Penggunaan enkripsi untuk meningkatkan keamanan

Salah satu mekanisme untuk meningkatkan keamanan adalah dengan menggunakan teknologi enkripsi. Data-data yang dikirimkan diubah sedemikian rupa sehingga tidak mudah disadap. Banyak servis di internet yang masih menggunakan *plain text* untuk *authentication* seperti penggunaan pasangan *userid* dan *password*. Informasi ini dapat dilihat dengan mudah dengan program penyadap atau pengendus (*sniffer*). Untuk meningkatkan keamanan server *world wide web* dapat digunakan enkripsi pada tingkat *socket*. Dengan menggunakan enkripsi, orang tidak bisa menyadap data-data (transaksi) yang dikirimkan dari /ke server WWW.

Salah satu mekanisme yang cukup populer adalah dengan menggunakan *Secure Socket Layer* (SSL) yang mulanya dikembangkan oleh *Netscape*. Selain server WWW dari *Netscape* dapat juga dipakai server WWW dari *Apache* yang dapat dikonfigurasi agar memiliki fasilitas *Secure Socket* layer (SSL) dengan menambahkan software tambahan (*SSLeay*-implementasi *Secure Socket Layer* (SSL) dari *Eric Young* atau *OpenSecure Socket Layer* (SSL).

Penggunaan *Secure Socket Layer* (SSL) memiliki permasalahan yang bergantung kepada lokasi dan hukum yang berlaku. Hal ini disebabkan pemerintah melarang ekspor teknologi enkripsi (kriptografi) dan paten *Public Key Partners* atas *Rivest-Shamir-Adleman* (RSA) *public key cryptography* yang digunakan pada *Secure Socket Layer* (SSL). Oleh karena itu, implementasi SSLeay Eric Young tidak dapat digunakan di Amerika Utara (Amerika dan Kanada) karena melanggar paten *Rivest-Shamir-Adleman* (RSA) dan RC4 yang digunakan dalam implementasinya.

j) *Telnet* atau *shell* aman,

Telnet atau *remote login* yang digunakan untuk mengakses sebuah *remote site* atau komputer melalui sebuah jaringan komputer. Akses ini dilakukan dengan menggunakan hubungan TCP/IP dengan menggunakan *userid* dan *password.* Informasi tentang *userid* dan *password* ini dikirimkan melalui jaringan komputer secara terbuka. Akibatnya kemungkinan *password* bisa kenak sniffing. Untuk menghindari hal ini bisa memakai enkripsi yang dapat melindungi adanya *sniffing*. Selain itu

bisa juga memakai *firewall*, alat ini untuk melindungi data-data penting. Akan tetapi sistem pengamanan yang telah dipaparkan di atas tadi tidak menjamin aman 100% (seratus persen), oleh karena itu dianjurkan untuk terus memantau perkembangan sistem pengamanan internet.

k) Sertifikasi perangkat security

Perangkat yang digunakan untuk menanggulangi keamanan semestinya memiliki peringkat kualitas. Perangkat yang digunakan untuk keperluan pribadi tentunya berbeda dengan perangkat yang digunakan untuk keperluan militer. Namun sampai saat ini belum ada institusi yang menangani masalah evaluasi perangkat keamanan di Indonesia.

Dari beberapa paparan penegakan hukum dengan sarana non-penal diatas, maka yang lebih diutamakan dari pada sarana penal dengan konsekuensi segera menyiapkan penegak hukum yang menguasai teknologi informasi. Atau lebih jelasnya kita sangat membutuhkan Polisi *Cyber*, Jaksa *Cyber*, Hakim *Cyber* dalam rangka penegakan hukum *cybercrime* di Indonesia tanpa adanya penegak hukum di bidang teknologi informasi, maka akan sulit menjerat penjahat-penjahat *cyber* oleh karena kejahatan *cyber* ini *locos delicti*-nya bisa lintas negara. *Locos delicti merupakan* tempat dimana suatu tindak pidana terjadi; tempat dimana kejadian (tindak pidana) dapat menyebabkan pelaku harus bertanggung jawab. Dalam hal ini Polri sebagai aparat penegak hukum telah menyiapkan unit khusus untuk menangani kejahatan *cyber* ini yaitu Unit V IT/*Cybercrime*Direktorat II Ekonomi Khusus Bareskrim.Untuk pengawasan terhadap perilaku orang dalam pemanfaatan teknologi dan informasi diyakini hukum sangat berperan

strategis.Bagaimanapun hukum memiliki fungsi dan peranan.Fungsi hukum tersebut tentunya lebih ditik beratkan pada upaya menigkatkan kesejahteraan.

B. Kendala Indonesia dalam Menaggulangi *Cybercrime*

Penggunaan sarana jaringan melalui media internet di negara-negara dunia dewasa ini semakin berkembang pesat.Kehadiran internet tidak dapat dielakkan lagi dapat menunjang kerja dari komputer. Apabila ada seorang yang tanpa ijin masuk ke dalam jaringan komputer orang lainataupun penanggung jawab sistem jaringan komputer termasuk dalam kejahatan k omputer. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang berbunyi:

> Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

Pasal diatas merupakan landasan hukum atau perlindungan hukum bagi setiap pemilik situs internet termasuk juga dalam hal ini situs internet instansi pemerintah dari kejahatan para *hacker*. Pasal tersebut menyatakan bahwa seseorang yang dengan sengaja mengubah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dapat dipidana sebagaimana diatur dalam Pasal 48 ayat (1) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, yang berbunyi, "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/ atau denda paling banyak Rp. 2.000.000.000,00 (dua miliar rupiah). Dalam pasal tersebut menjelaskan bahwa bilamana seseorang dengan sengaja dan tanpa hak atau melawan hukum/ menambah/ merusak suatu Informasi Elektronik

dan/atau Dokumen Elektronik milik Orang lain atau milik publik, akan dikenakan sanksi pidana sebagaimana diatur dalam Pasal 48 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi. Penanggulangan terhadap *cybercrime* dalam perlu diimbangi dengan pembenahan dan pembangunan sistem hukum pidana secara menyeluruh, yakni meliputi pembangunan kultur, struktur dan subtansi hukum pidana. Dalam hal ini kebijakan hukum pidana menduduki posisi yang strategis dalam pengembangan hukum pidana modern dan Transaksi Elektronik.

Walaupun Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik telah disahkan oleh pemerintah, namun belum cukup mencakup semua aspek dari kejahatan dunia maya. Selain itu, kita tidak bisa terus mengacu pada Undang-Undang Informasi dan Transaksi Elektronik saja, mealainkan kita harus menyusun konsep Kitab Undang-undang Hukum Pidana yang baru. Karena KUHP lama sudah tidak dapat lagi menjangkau tindak-tindak pidana baru yang tercipta oleh perkembangan jaman, untuk itu dibutuhkan konsep-konsep baru tentang KUHP kita. Selain itu, menurut Madjono Reksodiputro, pakar kriminolog dari Universitas Indonesia yang menyatakan bahwa kejahatan komputer sebenarnya bukanlah kejahatan baru dan masih terjangkau oleh KUHP untuk menanganinya. Pengaturan untuk menangani kejahatan komputer sebaiknya diintegrasikan ke dalam KUHP dan bukan ke dalam undang-undang tersendiri.

Meski Indonesia menduduki peringkat pertama dalam *cyber crime* pada tahun 2004,[50] akan tetapi jumlah kasus yang diputuskan oleh pengadilan tidaklah banyak. Dalam hal ini angka *dark number* cukup besar dan data yang dihimpun oleh Polri juga bukan data yang berasal dari investigasi Polri, sebagian besar data tersebut berupa laporan dari para korban. Ada beberapa sebab mengapa penanganan kasus *cyber crime* di Indonesia tidak memuaskan:[51]

1. *Cybercrime* merupakan kejahatan dengan dimensi high-tech, dan aparat penegak hukum belum sepenuhnya memahami apa itu *cyber crime.* Dengan kata lain kondisi sumber daya manusia khususnya aparat penegak hukum masih lemah. Hal ini terkait dengan begitu banyak kejahatan *cybercrime* yang terjadi belum mendapatkan penanganan khusus. Seperti halnya kasus *cyberwar* Indonesia Malaysia yang sampai sekarang tidak ada diberitakan bahwa pelaku *cyber crime* tersebut telah ditangkap.
2. Ketersediaan dana atau anggaran untuk pelatihan SDM sangat minim sehingga institusi penegak hukum kesulitan untuk mengirimkan mereka mengikuti pelatihan baik di dalam maupun luar negeri. Hal ini disebabkan karena pemerintah masih menganggap *cybercrime* bukan ancaman besar negara.
3. Ketiadaan Laboratorium Forensik Komputer di Indonesia menyebabkan waktu dan biaya besar. Untuk membuktikan jejak-jejak para *hacker*

[50] http://nasional.kompas.com/read/2009/03/25/18505497/Cyber.Crime..Indonesia.Tertinggi.di.Dunia diakses tanggal 22 Januari 2013

[51] http://www.unsoed.ac.id/newcmsfak/UserFiles/File/HUKUM/kriminalisasi_cybercrime.htm diakses tanggal 22 November 2013

dan *cracker* dalam melakukan aksinya terutama yang berhubungan dengan program-program dan data-data komputer, sarana Polri belum memadai karena belum ada komputer forensik. Fasilitas ini diperlukan untuk mengungkap data-data digital serta merekam dan menyimpan bukti bukti berupa *softcopy* (*image*, *program*, dsb). Contohnya pada kasus Dani Firmansyah yang menghack situs KPU, Polri harus membawa harddisk ke Australia untuk meneliti jenis kerusakan yang ditimbulkan oleh *hacking* tersebut.

4. Citra lembaga peradilan yang belum membaik, meski berbagai upaya telah dilakukan. Masyarakat menilai, dari berbagai kasus yang ditangani oleh lembaga peradilan, penangannya agak lambat dan lama. Buruknya citra ini menyebabkan orang atau korban untuk menyerahkan kasusnya ke kepolisian untk ditangani.
5. Kesadaran hukum untuk melaporkan kasus ke kepolisian rendah. Hal ini dipicu oleh citra lembaga peradilan itu sendiri yang kurang baik, faktor lain adalah korban tidak ingin kelemahan dalam sistem komputernya diketahui oleh umum, yang berarti akan mempengaruhi kinerja perusahaan dan web masternya.

Meskipun hukum pidana digunakan sebagai *ultimum remidium* atau alat terakhir apabila bidang hukum yang lain tidak dapat mengatasinya, tetapi harus disadari bahwa hukum pidana memiliki keterbatasan kemampuan

dalammenanggulangi kejahatan. Keterbatasan-keterbatasan tersebut dikemukakan sebagai berikut:[52]

a. Sebab-sebab kejahatan yang demikian kompleks berada di luar jangkauan hukum pidana
b. Hukum pidana hanya merupakan bagian kecil (subsistem) dari sarana kontrol sosial yang tidak mungkin mengatasi masalah kejahatan sebagai masalah kemanusiaan dan kemayarakatan yang sangat kompleks (sebagai masalah sosio-psikologis, sosio-politik, sosioekonomi, dan sosio-kultural;
c. Penggunaan hukum pidana dalam menanggulangi kejahatan hanya merupakan *kurieren am symptom*, oleh karena itu hukum pidana hanya merupakan pengobatan simptomatik dan bukan pengobatan kausatif;
d. Sanksi hukum pidana merupakan *remedium* yang mengandung sifat kontradiktif/paradoksal dan mengandung unsur-unsur serta efek sampingan yang negatif;
e. Sistem pemidanaan bersifat *fragmentair* dan individual/personal, tidak bersifat struktural/fungsional;
f. Keterbatasan jenis sanksi pidana dan sistem perumusan sanksi pidana yang bersifat kaku dan imperatif;
g. Bekerjanya/berfungsingnya hukum pidana memerlukan sarana pendukung yang lebih bervariasi dan memerlukan biaya tinggi.

Keterbatasan-keterbatasan hukum pidana inilah yang tampaknya dialami oleh polri yang menggunakan hukum pidana sebagai landasan kerjanya. Sebab kejahatan yang kompleks ini terlambat diantisipasi oleh polri sehingga ketika terjadi kasus yang berdimensi baru mereka tidak secara tanggap menanganinya. Untuk itu, pencegahan kejahatan tidak selalu harus menggunakan hukum pidana.

---

[52]Barda Nawawi Arief,*Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana*, Bandung: PT Citra Aditya Bakti, 1998, halaman. 46-47

Agar penegakan hukum *cybercrime* ini dapat dilakukan secara menyeluruh maka tidak hanya pendekatan yuridis atau penal yang dilakukan, tetapi dapat juga dilakukan dengan pendekatan non-penal.

Upaya penanganan *cybercrime* membutuhkan keseriusan semua pihak mengingat teknologi informasi khususnya internet telah dijadikan sebagai sarana untuk membangun masyarakat yang berbudaya informasi. Keberadaan undang-undang yang mengatur *cybercrime* memang diperlukan, akan tetapi apalah arti undang-undang jika pelaksana dari undang-undang tidak memiliki kemampuan atau keahlian dalam bidang itu dan masyarakat yang menjadi sasaran dari undang-undang tersebut tidak mendukung tercapainya tujuan pembentukan hukum tersebut. Maka dari itu dari itu dibutuhkan kerjasama atau korelasi antara pemerintah dengan masyarakat, guna untuk melancarkan pelasanaan undang-undang tersebut.

C. Kerjasama Internasional Indonesia dalam menaggulangi masalah *Cybercrime*

Indonesia yang memiliki posisi geografis yang strategis bagi suburnya pertumbuhan jenis-jenis kejahatan lintas negara. Oleh karena itu, sebagai negara asal dan transit bagi operasi tindak *trans-national crime* itu, Indonesia dituntut untuk terus meningkatkan upaya dalam menekan kejahatan lintas batas tersebut melalui suatu format kerja sama dengan negara-negara tetangga secara komprehensif. Tantangan utama yang dihadapi dalam memberikan responcepat terhadap jenis kejahatan seperti ini adalah bagaimana membuat perjanjian ekstradisi dengan beberapa negara kunci, baik secara bilateral maupun multilateral

dan mengembangkan kerja sama teknis dalam pemberantasan terorisme, bajak laut, pencucian uang, penyelundupan dan perdagangan manusia dan senjata serta lalu lintas obat-obat terlarang termasuk juga *cybercrime*.

Beberapa kerjasama Internasional pun dilakukan Indonesia guna memerangi masalah cybercrime yang terus meningkat dari waktu kewaktu. Ada beberapa kerjasama internasional yang dilakukan oleh Indonesia baik dengan negara maupun organisasi dan forum forum internasional yang tentunya mengenai masalah *transnational crime* yang didalamnya memuat masalah *cybercrime* juga.

1) Kerjasama dengan negara anggota dalam bingkai kerjasama ASEAN.

Indonesia sebagai salah satu anggota dari ASEAN juga mengadakan atau melakukan kerjasama kerjasama dengan negara negara anggota dalam bingkai kerjasama ASEAN dalam rangka menaggulai masalah *cybercrime.* Hal ini dilakukan Indonesia dalam rangka memberantas *cybercrime* di Indonesia yang semakin hari semakin meningkat perkembangannnya. Alasan indonesia melakukan hubungan ini karena kerjasama antar negara dalam bingkai kerjasama internasional dalam rangka pemberantasan cybercrime di Asia Tenggara dinilai sangat rutin dilakukan dan terus mengalami kemajuan dengan cara mengadakan beberapa forum yang didalamnya dihadiri oleh negara negara anggota. Seperti halnya Indonesia, Singapura, Malaysia, Thailan dan negara anggota yang lain. Indonesia sendiri mengikuti berbagai forum yang diadakan oleh negara negara anggota ASEAN diantaranya yaitu :

a. Kerjasama Indonesia dalam kerangka *ASEAN Chief of Police* atau ASEANAPOL

ASEANAPOL adalah sebuah wadah organisasi kepolisian regional ASEAN yang berperan dan sebagai *driving force* dalam menghadapi kejahatan lintas Negara demi terwujudnya keamanan dan stabilitas kawasan ASEAN. ASEANPOL adalah sebuah forum Konferensi Kepala Polisi yang terdiri dari beberapa negara, seperti Brunei Darussalam, Indonesia, Myanmar, Filipina, Singapura, Malaysia, Kamboja, Laos, Thailand, dan Vietnam. Organisasi ASEANAPOL adalah singkatan dari *ASEAN Chief of Police* yang merupakan sebuah organisasi bersama yang didirikan bertujuan untuk merumuskan kerjasama antar negara dalam memberantas kejahatan lintas wilayah, terutama terkait terorisme, peredaran narkoba, penyelundupan senjata, perdagangan manusia, kejahatan *cyber,* kejahatan perbankan, penipuan maritim, kejahatan komersial, penipuan transnasional dan lainnnya.

Berdirnya ASEANAPOL diawali saat pertemuan resmi pertama Kepala Polisi ASEAN, yang dihadiri oleh 5 anggota negara, antara lain, Indonesia, Malaysia, Filipina, Singapura dan Thailand, pada 1981 di Manila. Pada tahun 1983, pengesahan dari model dan desain logo ASEANAPOL di Jakarta. Pada 1984, Polisi Kerajaan Brunei menjadi anggota dan bergabung dengan konferensi tahunan, di Kuala Lumpur, Malaysia. Pada 1996, Vietnam bergabung sebagai anggota baru. Pada 1998, Laos bergabung ke ASEANAPOL. Pada tahun 2000, Myanmar menjadi negara ke-10 yang bergabung sebagai

anggota baru. Pada tahun, Malaysia dipilih sebagai tuan rumah Sekretariat permanen ASEANAPOL.

Melalui organisasi atau wadah ASEANAPOL ini diharapakan peningkatan kerjasama antara kepolisian dan instansi penegak hukum lintas Negara dalam menyikapi kasus kriminal lintas batas. Pertemuan-pertemuan yang diselenggarakan ASEANAPOL membahas berbagai strategi dan peningkatan kerjasama dalam menghadapi dinamika dan tantangan global, khususnya kejahatan lintas Negara (*transnational crime*).Dalam agenda yang dilakukan oleh ASEANAPOL ini adalah pertemuan rutin setiap anggota yang membahas berbagai hal mengenai kejahatan transnasional.

- Pertemuan ke-31 Kepala Polisi Negara-negara ASEAN (ASEAN Chief of Police/ASEANAPOL) yang diselenggarakan di Vientiane, Laos, 31 Mei-2 Juni 2011

Pertemuan ke-31 Kepala Polisi Negara-negara ASEAN (ASEAN Chief of Police/ASEANAPOL) yang diselenggarakan di Vientiane, Laos, 31 Mei-2 Juni 2011, menghasilkan Komunike Bersama yang isinya merekomendasikan tindak lanjut upaya bersama dalam penanganan transnational crime, yakni peningkatan kecepatan pertukaran informasi di antara anggota, peningkatan kerjasama antara kepolisian dan instansi penegak hukum terkait, pemajuan kerjasama lintas batas, penguatan fungsi ASEANAPOL Secretariat, partisipasi aktif dalam berbagai program pelatihan dan peningkatan kapasitas anggota kepolisian serta membentuk kemitraan yang efektif antara kepolisian dan

publik. Pertemuan ke-31 ASEANAPOL dibuka oleh Menteri Public Security Laos, Thongban Seng-Aphone, dan dihadiri oleh Kepala Polisi negara-negara anggota ASEAN, mitra wicara (RRT, Jepang, Korea Selatan, Australia, dan Selandia Baru), dan peninjau dari Sekretariat ASEANAPOL.

Dalam sambutannya, Seng-Aphone menekankan peran penting ASEANAPOL untuk membahas strategi dan peningkatan kerjasama dalam menghadapi dinamika dan tantangan global, khususnya kejahatan lintas negara (transnational crime). ASEANAPOL sebagai wadah organisasi kepolisian regional terbukti mampu memainkan peran kunci dan driving force dalam menghadapi kejahatan lintas negara yang memberikan kontribusi nyata bagi terwujudnya keamanan dan stabilitas kawasan ASEAN.

Pertemuan membahas isu-isu antara lain adalah illicit drugs trafficking, terorisme, arms smuggling, human trafficking, maritime fraud, commercial crime, bank offences, credit card fraud, cybercrime, fraudulent travel documents, transnational fraud, pengembangan ASEANAPOL Database System (e-ADS), mutual assistance dan pertukaran serta pelatihan personil Kepolisian.

Delegasi RI yang dipimpin oleh Kepala Kepolisian Republik Indonesia, Jenderal (Pol) Drs. Timur Pradopo, menyampaikan country paper mengenai isu-isu yang dibahas, yang berisi antara lain latar belakang situasi dan perangkat hukum di Indonesia, implementasi terhadap Komunike Bersama Pertemuan ke-30 ASEANAPOL, berikut lesson learned dan rekomendasi yang dapat di-share

kepada negara-negara anggota ASEANAPOL dan mitra wicara. Paparan yang komprehensif dari jajaran Polri memperoleh apresiasi dan tanggapan positif dari peserta lainnya yang diharapkan dapat diimplementasikan dalam bentuk kerjasama antara kepolisian negara-negara ASEAN dan mitra wicara. Di sela-sela pertemuan, Kapolri juga berpartisipasi dalam Forum Diskusi Kepala Kepolisian negara-negara ASEAN dengan Kepala Kepolisian negara-negara mitra Wicara. Delegasi RI terdiri dari Kepala Badan Reserse Kriminal Polri, Komisaris Jenderal (Pol) Dr. Ito Sumardi dan sejumlah petinggi Polri dari unsur-unsur Bareskrim, NCB Interpol Indonesia, Polisi Perairan dan Detasemen Khusus 88/Anti Teror dan pejabat KBRI Vientiane.

Dalam konferensi ini membahasa mengenai kejahatan trasnasional yang terus berkembang yaitu teroris, perdagangan manusia dan juga cybercrime. Timur Pradopo mengajak negara anggota untuk terus giat dalam menaggulangi dan terus berkoordinasi dengan langkah nyata seperti saling bertukar informasi mengenai kasus-kasus kejahatan tersebut, mengingat kejahatan tersebut merupakan lintas negara.

- Konferensi ASEANAPOL ke-33 telah dilaksanakan pada tanggal 18 hingga 22 Februari 2013 di Hotel Dusit Thani Pattaya, Thailand.

Konferensi Tahunan Kepolisian di kawasan ASEAN atau Konferensi ASEANAPOL ke-33 telah dilaksanakan pada tanggal 18 hingga 22 Februari 2013 di Hotel Dusit Thani Pattaya, Thailand. Selaku Ketua Delegasi Polri pada konferensi dimaksud adalah Wakapolri. Selain pertemuan antar sesama Kepala

Kepolisian ASEAN, konferensi juga dihadiri oleh negara mitra dialog yaitu: China, Jepang, Korea, Australia dan New Zealand serta perwakilan dari Setjen ICPO-Interpol dan Sekretariat ASEANAPOL.

Konferensi dibuka secara resmi oleh Police Captain Dr. Chalerm Yubamrung, Deputy Prime Minister of Thailand. Dalam *opening remark* yang disampaikan oleh Police Captain Dr. Chalerm Yubamrung menggarisbawahi pentingnya memperkuat kerja sama penegak hukum di kawasan dalam upaya pemberantasan kejahatan transnasional dan Konferensi ASEANAPOL memegang peranan yang sangat signifikan dalam upaya merumuskan upaya konkrit kerja sama dimaksud.

Sebagai rangkaian dari konferensi ASEANAPOL dilakukan sejumlah agenda pokok yaitu:

- Pertemuan para Kepala Kepolisian negara anggota ASEANAPOL (Head of Delegation Dicussion Forum) yang membahas isu-isu strategis yang diusulkan oleh masing-masing kepolisian yang nantinya akan dibahas lebih konkrit pada working group.
- Pertemuan para Kepala Kepolisian negara anggota ASEANAPOL dengan Ketua Delegasi negara mitra dialog.
- Executive Committe Meeting (DHOD) yang membahas hal-hal yang berkaitan dengan operasional dari ASEANAPOL Sekretariat dan anggaran.
- Pertemuan Komisi A,B dan C yang membahas tentang tindak lanjut dari kesepakatan (joint communique) yang dihasilkan dari Konferensi ASEANAPOL ke-32 sebelumnya. Masing-masing Komisi membahas beberapa isu kejahatan transnasional dan peningkatan kapasitas.
- Working group 1 dan 2 yang membahas tentang penyusunan Plan of Action dari setiap isu yang disepakati dalam forum HOD.

Pada Konferensi ASEANAPOL ke-33 ini, Polri mengangkat beberapa topik yang dipandang cukup menjadi perhatian bersama dikawasan dan

diharapkan dapat ditindak lanjuti dalam upaya konkrit. Adapun beberapa isu tersebut adalah: Development of Intra and Inter Regional Policing Network, Promote the Existence of Integrated Electronic Library (e-Library) System, Strengthening of Cooperation amongst ASEANAPOL Member Countries on Combating Illicit Drugs Production, Combatting Cybercrime, Trafficking and Use, increased contribution of ASEANAPOL member countries and its role in Peackeeping Mission under United Nation dan Sharing Information on Response of INTERPOL Red Notice/Diffusion request. Beberapa topik lain yang dibahas adalah usulan Sekretariat ASEANAPOL terkait permintaan EUROPOL untuk berpartisipasi pada Konferensi ASEANAPOL sebagai observers, usulan Sekretariat ASEANAPOL tentang permintaan Rusia untuk berpartisipasi pada Konferensi ASEANAPOL sebagai negara mitra dialog, dan usulan Kepolisian Kerajaan Thailand tentang peningkatan kapasitas Kepolisian ASEAN pada Forensic Science.

Sebagai hasil dari rangkaian Konferensi ASEANAPOL ke-33 yang berlangsung dengan cukup produktif dan telah membahas berbagai inisiatif kerja sama, program, dan kegiatan dalam rangka penanggulangan kejahatan transnasional di kawasan, termasuk melalui kemitraan dengan negara-negara mitra dialog. Pada pelaksanaan sidang komisi A,B dan C telah berhasil memformulasikan Joint Communiqué dan telah disahkan oleh para Ketua Delegasi yang selanjutnya disampaikan kepada seluruh negara anggota ASEANAPOL untuk di follow up serta pada pelaksanaan Working Group 1 dan 2 telah berhasil melakukan pembahasan dalam rangka penyusunan Plan of

Action terhadap beberapa usulan dari negara anggota ASEANAPOL. Sedangkan beberapa topik yang menjadi usulan yang disampaikan oleh Polri mendapat apresiasi yang baik dari negara anggota ASEANAPOL maupun mitra dialog.

b. Pada tanggal 11 Oktober 2011 diadakan ASEAN Ministerial Meeting on Transnasional Crime ke 8 di Bali, Indonesia.

Dalam jangka panjang, kerja sama di antara negara ASEAN akan mengarah pada pengurangan keberagaman sistem dan standar hukum dan keamanan di kawasan ASEAN. Upaya menuju konvergensi hukum dan keamanan ini penting untuk membangun komunitas ASEAN yang direncanakan terbangun pada 2015 mendatang. Sekretaris Jenderal ASEAN Surin Pitsuwan mengatakan komitmen negara-negara ASEAN untuk memerangi kejahatan transnasional sudah tertuang dalam kesepakatan kerja sama. Tapi pelaksanaannya memerlukan komitmen dari pemimpin-pemimpin negara.

Kepala Kepolisian RI Jenderal Timur Pradopo yang menjadi ketua pelaksana acara tersebut mengatakan pertemuan ini akan difokuskan untuk menyusun langkah-langkah memerangi terorisme, perdagangan manusia, perdagangan narkotik dan obat terlarang, pencucian uang, kejahatan dunia maya, pembajakan di laut, dan kejahatan ekonomi internasional. Juga akan digelar dialog dengan negara mitra, yaitu Cina, Jepang, dan Korea Selatan," katanya. Pertemuan dengan negara mitra juga dilakukan untuk membahas perkembangan terkini kejahatan internasional dan kemungkinan memperkuat kerja sama ASEAN dengan negara mitra. ASEAN Ministerial Meeting on

Transnational Crime ke-8 digelar mulai hari ini hingga 13 Oktober mendatang. Selain dihadiri perwakilan negara-negara ASEAN, pertemuan juga diikuti oleh perwakilan dari tiga negara mitra, yakni Jepang, Cina, dan Korea Selatan.

c. Pelatihan dan peningkatan Kapasitas para ahli komputer dan penegak hukum negara negara ASEAN dalam menaggulangi *cybercrime* pada tahun 2004. Para negara anggota ASEAN mengunjungi Korea Selatan selama dua minggu dalam rangka mempelajarimetode lebih lanjut dalam menginvestigasi kasus-kasus cybercrime.[53] Korea Cyber Terror Response Center (KCTRC) selaku badan penanganan *cybercrime* bertindak sebagai trainer dalam mengidentifikasi jenis-jenis *cybrcrime,* mempelajari studi kasus, menginvestigasi tindak pidanan *cybercrime* dan lain sebagainya.
d. Mengikuti forum yang diadakan oleh ASEAN Regional Forum. Seperti Co-Chairs Summary Report ASEAN Regional Forum Conference on Terrorist Use of the Internet di Bali, Indonesia 6-8 November 2008. Pada tanggal 24 Juli 2008, negara negara yang tergabung dalam ARF yaitu negara anggota ASEAN melakukan lokakarya yang bertujuan untuk meningkatkan kapasitas penaggulangan cybercrime di Asia Tenggara, khususnya dibidang penyalahgunaan internet oleh teroris.

2) Kerjasama Indonesia dan Australia[54]

Pada bulan Oktober 2002, sebagai bagian dari program Pemerintah Australia untuk meningkatkan kapasitas terorisme di Indonesia dan dukungan

[53]http://www.crime-reseach.org/news/13.10.2004/709/ di akses tanggal 24 November 2013
[54]http://tncc.co.id/en/home/about/ diakses tanggal 22 Nobember 2013

Polri Perdana Menteri Australia mengumumkan komitmen $ 4,7 juta selama empat tahun untuk membangun Transnational Crime Centre Indonesia (TNCC) di Jakarta, Indonesia. Proyek TNCC resmi dimulai pada Juli 2003, TNCC ini terletak di Mabes Polri dan berada di bawah komando Divisi Investigasi Kriminal, Nasional Pusat Informasi Kriminal.

Adapun kasus kasus yang ditangani oleh Transnational Crime Centre Indonesia (TNCC) yaitu :

- Terorisme
- Penyelundupan manusia
- Perdagangan Manusia
- Narkoba
- Kejahatan lingkungan
- Illegal fishing , logging dan pertambangan
- pencucian uang
- Kejahatan Dunia Maya (*cybercrime*)
- Pembajakan laut
- perdagangan senjata
- kejahatan identitas

Program atau kegiatan dari Transnational Crime Centre Indonesia (TNCC) yaitu menganalisis dan berbagi informasi tentang Kejahatan Transnasional yang mempengaruhi Indonesia.TNCC mengumpulkan informasi tentang kejahatan transnasional dari berbagai sumber termasuk juga Informasi Reserse Kriminal, Mabes Polri dan Mabes Polri Propinsi, Open source pelaporan media, seperti laporan PBB, internet dan media, Lembaga penegak hukum lainnya di Indonesia, Layanan polisi lainnya di daerah Asia Pasifik.

TNCC menganalisis informasi kriminal dengan pemanfaatan dari sistem informasi manajemen elektronik yang sangat aman, yang dikenal sebagai *Case Management and Intelligence System* atau CMIS . CMIS memungkinkan personel TNCC untuk menganalisis informasi kriminal melalui mengembangkan database yang komprehensif kejahatan transnasional . Database CMIS terpusat di TNCC dan memungkinkan analis untuk mencari entitas seperti nama, alamat dan nomor telepon dan link entitas . CMIS adalah alat analisis yang kuat yang dapat menghasilkan diagram link. Melalui analisis informasi yang terkandung dalam CMIS , personil TNCC dapat menghasilkan data intelijen operasional, taktis dan strategis untuk membantu berbagai pemangku kepentingan .

Kepolisian Nasional Indonesia (Polri) Kejahatan Transnasional Koordinasi Pusat (TNCC) Proyek memiliki hasil yang sukses berikut ;

- Pengembangan kapasitas koordinasi kejahatan lintas negara dalam Polri dengan fokus utama pada peningkatan kapasitas kontra terorisme di Indonesia serta jenis kejahatan transnasional lainnya, termasuk penyelundupan manusia, narkotika dan penipuan identitas .
- Memperkuat pengetahuan dan keterampilan di bidang kontra terorisme melalui pengiriman Analisis Intelijen dan pelatihan untuk lebih dari 100 staf Polri, danTNCC telah mengembangkan hubungan dengan Polri. Sejumlah proyek intelijen gabungan telah memulai fokus pada terorisme, perdagangan narkoba dan penyelundupan manusia dan cybercrime.

- Penguatan kelembagaan TNCC dengan cara Polri telah mengkonfirmasi staf dan struktur organisasi TNCC dan berkomitmen untuk menyediakan sekitar 100 staf untuk TNCC untuk mengatasi semua jenis kejahatan transnasional.
- Kemampuan Polri Peningkatan dalam pengelolaan informasi kriminal melalui pembentukan dan pengembangan Manajemen Kasus Polri dan Sistem Intelijen (CMIS) yang telah diluncurkan di semua 31 provinsi polisi di Indonesia, memberikan Polri database nasional untuk pertama kalinya.

Ada agenda yang pernah dilakukan indonesia dan Australia yang membahas mengenai *cybercrime* yaitu dalam bentuk konferensi.

- Konferensi Gabungan Transnational Crime Assessment (TCA) 2010 pada hari Rabu, 5 Januari 2011

Konferensi Gabungan Transnational Crime Assessment (TCA) antara Australian Federal Police (AFP) dan Kepolisian Negara Republik Indonesia (POLRI) Tahun 2010 diadakan di Puncak, Indonesia pada tanggal 1 sampai 2 Desember 2010. Dihadiri oleh anggota AFP dari kantor AFP Jakarta dan Intelijen AFP and anggota POLRI dari Pusat Data & Analisa Kejahatan Transnasional TNCC, konferensi ini memberikan kesempatan bagi kedua organisasi untuk bertemu dan mendiskusikan kejahatan lintas negara yang berdampak pada Australia dan Indonesia. Informasi yang didiskusikan di rapat tersebut digunakan sebagai bahan penulisan TCA, suatu dokumen analisa

strategis atas kejahatan yang akan disajikan untuk para eksekutif AFP dan POLRI pada Senior Officers Meeting.

Konferensi TCA secara resmi dibuka secara bersama-sama oleh National Manager Intelligence AFP, Assistant Commissioner Tim Morris AM APM dan Brigjen Pol Roy Tumbelaka, Kepala Pusat Informasi Kriminal Nasional Polri. Saat membuka konferensi, National Manager Intelligence AFP, Assistant Commissioner Tim Morris AM APM mengatakan "TCA yang diadakan secara bersama oleh AFP/POLRI setiap tahun ini memberikan kesempatan ideal untuk mempromosikan kebijakan berbasis intelijen. Saya yakin TCA merupakan suatu analisa yang sangat berguna atas kejahatan lintas negara yang berdampak bagi Indonesia dan Australia.