# KEBIJAKAN KRIMINAL TERHADAP TINDAK PIDANA CYBER TERRORISM

## TESIS

**Disusun Dalam Rangka Memenuhi Persyaratan**
**Program Magister Ilmu Hukum**


**Oleh :**
**NANDA IVAN NATSIR**
**NIM : B4A 008 063**


**Pembimbing :**
**PROF.DR. BARDA NAWAWI ARIEF, SH.**


**SISTEM PERADILAN PIDANA**
**PROGRAM MAGISTER ILMU HUKUM**
**UNIVERSITAS DIPONEGORO**
**SEMARANG**
**2009**

# KEBIJAKAN KRIMINAL TERHADAP TINDAK PIDANA CYBER TERRORISM

## PENULISAN TESIS

**Disusun Dalam Rangka Memenuhi Persyaratan**
**Program Magister Ilmu Hukum**

**Mengetahui**
**Pembimbing,**

**Prof. Dr. Barda Nawawi Arief, SH**
**NIP. 130350519**

**Peneliti,**

**Nanda Ivan Natsir, SH**
**NIM. B4A008063**

**Mengetahui,**
**Ketua Program Magister Ilmu Hukum**
**Universitas Diponegoro**

**Prof. Dr. Paulus Hadisuprapto, SH,MH**
**NIP. 194907211976031001KATA PENGANTAR**

## KATA PENGANTAR

*Bismillaahir Rahmaanir Rahiim,*
*Subhanaallah, Waalhaamdulillaah.*
*Laa haula wa Laa quwwata illa billaahil 'Aliyil adhiim.*

Dengan mengucapkan puji syukur kehadirat ALLAH SWT atas berkat dan rahmat-Nya sehingga penulis dapat menyelesaikan tesis ini dengan lancar dan diberi judul : **"Kebijakan Kriminal Terhadap Tindak Pidana Cyber Terrorism"** dapat diselesaikan dengan baik dan tepat pada waktunya.

Dalam penyelesaian tesis ini penulis telah mendapatkan bimbingan, arahan serta bantuan dari berbagai pihak. Untuk itu penulis mengucapkan terima kasih yang tak terhingga kepada :

1. Bapak Prof. Dr. dr. Susilo Wibowo, MS.Med.Sp.And selaku Rektor Universitas Diponegoro Semarang yang telah memberikan kesempatan yang sangat berharga kepada penulis untuk menyelesaikan studi dalam bidang Ilmu Hukum Program Magister Ilmu Hukum Universitas Diponegoro Semarang
2. Bapak Prof. Drs. Y. Warella, MPA, Ph.D selaku Direktur Program Pasca Sarjana Universitas Diponegoro Semarang yang telah memberikan kesempatan yang sangat berharga kepada penulis untuk menuntut ilmu di Program Magister Ilmu Hukum Universitas Diponegoro Semarang
3. Bapak Prof. Dr. Barda Nawawi Arief, SH dan yang amat terpelajar selaku mantan Ketua Program Magister Ilmu Hukum Universitas Diponegoro sekaligus sebagai pembimbing dan mengarahkan serta membuka cakrawala berpikir penulis terhadap kemajuan dan perkembangan ilmu hukum ke depan
4. Bapak Prof. Dr. Paulus Hadisuprapto, SH, MH sebagai Ketua Program Magister Ilmu Hukum Universitas Diponegoro saat ini sekaligus pembimbing metodologi, semua tim penguji yang penuh dengan

perhatian dan kesabaran mendampingi dan membimbing dalam penulisan skripsi ini

5. Bapak/Ibu Guru Besar dan Staf Pengajar pada Program Magister Ilmu Hukum Universitas Diponegoro yang dengan perantara penyampaiannya penulis mendapat ilmu pengetahuan yang teramat sangat penting tidak hanya untuk karier tetapi juga hidup penulis dimasa depan
6. Ibu Ani Purwanti, SH, M.Hum Sekretaris Bidang Akademik, Sekretaris Bidang Keuangan, staf dan karyawan Program Magister Ilmu Hukum Universitas Diponegoro Semarang
7. Penghargaan yang setinggi-tingginya kepada Ayahanda Mohammad Natsir dan Ibu tercinta Baiq Hasniwati beserta saudara-saudara dan seluruh keluarga dekat yang telah mendoakan penulis selama ini
8. Teman-teman PMIH terutama di SPP yang selalu memberikan semangat untuk maju bersama-sama dalam menyelesaikan study pada Program Magister Ilmu Hukum Universitas Diponegoro Semarang.

Penulis menyadari bahwa tesis ini masih jauh dari sempurna, oleh karena itu kritik dan saran yang bersifat membangun sangat penulis harapkan demi lebih sempurnanya penelitian selanjutnya.

Semoga tesis ini dapat bermanfaat bagi semua pihak, khususnya mahasiswa Program Magister Ilmu Hukum Universitas Diponegoro Semarang.

Semarang, Agustus 2009

Penulis

NANDA IVAN NATSIR, SH

## PERNYATAAN KEASLIAN KARYA ILMIAH

Dengan ini saya, Nanda Ivan Natsir, menyatakan bahwa Karya Ilmiah/Tesis ini adalah asli hasil karya saya sendiri dan Karya Ilmiah ini belum pernah diajukan sebagai pemenuhan persyaratan untuk memperoleh gelar kesarjanaan Strata Satu (S1) maupun Magister (S2) dari Universitas Diponegoro maupun Perguruan Tinggi lain.

Semua informasi yang dimuat dalam Karya Ilmiah ini yang berasal dari penulis lain baik yang dipublikasikan atau tidak, telah diberikan penghargaan dengan mengutip nama sumber penulis secara benar dan semua isi dari Karya Ilmiah/Tesis ini sepenuhnya menjadi tanggung jawab saya sebagai penulis.

Semarang,
Penulis

Nanda Ivan Natsir
NIM. B4A 008 063

## ABSTRAK

Cyber terrorism merupakan salah satu jenis *cyber crime* dari beberapa jenis- jenis *cyber crime* yang ada, yang muncul akibat dari dampak negatif perkembangan sarana teknologi informasi dan komunikasi masyarakat global, sehingga terjadi perubahan- perubahan pola perilaku masyarakat dalam bidang tersebut sebagai penyalahgunaan komputer. Motivasi dari aksi kejahatan *cyber terrorism* adalah untuk kepentingan kelompok tertentu dengan tujuan untuk menunjukkan eksistensinya dipanggung politik dunia.

Dari latar belakang tersebut di atas, maka dalam thesis ini ditetapkan dua masalah pokok, yaitu : Bagaimana kebijakan kriminal pada saat ini dalam menanggulangi tindak pidana *cyber terrorism*? dan Bagaimanakah kebijakan kriminal yang akan datang guna menanggulangi tindak pidana *cyber terrorism* di Indonesia?

Penelitian ini bersifat yuridis normatif, dilakukan dengan cara mengkaji/menganalisis data sekunder yang berupa bahan-bahan hukum terutama bahan hukum primer dan bahan hukum sekunder dengan memahami hukum sebagai seperangkat peraturan atau norma-norma positif di dalam sistem perundang-undangan yang mengatur mengenai kehidupan manusia. Selain itu digunakan kajian yuridis komparatif yaitu dengan melakukan kajian perbandingan terhadap peraturan hukum pidana diberbagai negara yang mengatur tentang *cyber terrorism.*

Hasil penelitian ini menunjukkan bahwa, dalam kebijakan kriminal yang ada saat ini, dapat digunakan dalam menanggulangi tindak pidana *cyber terrorism,* sedangkan kebijakan kriminal yang akan datang seyogyanya perlu dilakukan peningkatan dan perubahan, terlebih lagi secepat perlu disyahkan Konsep RUU KUHP agar lebih optimal dalam menanggulangi tindak pidana cyber terrorism.



**Kata Kunci : Kebijakan kriminal, Cyber terrorism, Tindak pidana.**

## ABSTRACT

Cyber terrorism is one of type of cyber crime from several types of the existing cyber crimes, it is appear resulting of the negative impact of information technology and global community communication media development, so that several changes of society's behavior patterns within the area as a computer misapplication. A motivation of cyber terrorism criminal act is for the certain importance with objective showing its existence in the political world platform.

From the background above, thus within the thesis is determined two main problems: How the criminal policy in overcoming the cyber terrorism criminal act at this time? And, how does the criminal policy in the future overcomes the cyber terrorism in Indonesia?

The thesis have the character of normative juridical, it is done by studying/analyzing the secondary data in the form of law, particularly, both primary and secondary laws by understanding those as a rule set or positive norma within legislation system regulating about mankind lives. Moreover, a comparative juridical study is by conduction a comparison study toward criminal law regulation in many countries those arranging about cyber terrorism.

The research result demonstrates that, in the existing criminal policy can be used in overcoming criminal act of cyber terrorism, while criminal policy in the future as need as properly to be performed of the increasing and modification, and Draw of Law of Concept of Criminal Code, and as soon as possible to be validated in order to be more optimum in overcoming the cyber terrorism criminal act.



**Keywords: Criminal Policy, Cyber Terrorism, Criminal Act.**

# DAFTAR ISI TESIS

# BAB I
# PENDAHULUAN

## A. Latar Belakang

Kemerdekaan bangsa Indonesia pada tanggal 17 Agustus 1945 merupakan awal dari bangsa Indonesia melaksanakan pembangunan nasional dalam rangka untuk membangun manusia Indonesia seutuhnya dan pembangunan seluruh masyarakat Indonesia berlandaskan Pancasila dan UUD 1945.

Pembangunan Nasional bertujuan untuk mewujudkan suatu masyarakat adil dan makmur yang merata materiil dan spiritual berdasarkan Pancasila didalam wadah Negara Kesatuan Republik Indonesia yang merdeka, berdaulat, bersatu dan berkedaulatan rakyat dalam suasana perikehidupan bangsa yang aman, tenteram, tertib dan dinamis serta dalam lingkungan pergaulan dunia yang merdeka, bersahabat, tertib dan damai.

Pembangunan Nasional di Indonesia telah mencapai era tinggal landas. Hal ini antara lain ditenggarai oleh semakin meningkatnya dua faktor utama yang dianggap sebagai kunci keberhasilan pembangunan dalam rangka memenuhi tuntutan era globalisasi, yaitu pertumbuhan ekonomi dan perkembangan pemamfaatan Ilmu Pengetahuan dan

Teknologi (IPTEK). Salah satu produk IPTEK yang kecanggihannya berkembang pesat dan hampir menguasai seluruh aspek kehidupan masyarakat modern adalah teknologi komputer.[1]

Teknologi informasi dan komunikasi telah mengubah perilaku masyarakat dan peradaban manusia secara global. Di samping itu, perkembangan teknologi informasi telah menyebabkan dunia menjadi tanpa batas (*borderless*) dan menyebabkan perubahan sosial yang secara signifikan berlangsung demikian cepat. Teknologi informasi saat ini menjadi pedang bermata dua, karena selain memberi kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum.[2]

Penggunaan teknologi internet banyak menyelesaikan persoalan yang rumit secara efektif dan efisien. Kecanggihan teknologi ini juga berpotensi membuat orang cenderung melakukan perbuatan yang bertentangan dengan norma-norma sosial yang berlaku. Penggunaan teknologi internet telah membentuk masyarakat dunia baru yang tidak lagi dihalangi oleh batas-batas teritorial suatu negara yang dahulu ditetapkan sangat esensial sekali yaitu dunia maya, dunia yang tanpa batas atau realitas virtual (*virtual reality*). Inilah sebenarnya yang dimaksud dengan *Borderless World*.[3]

---

[1] Kata Pengantar Prof. DR. Barda Nanawi Arief, SH., dalam *Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer* oleh Al. Wisnubroto, Universitas Atma Jaya Yogyakarta, 1999. Hal. 1

[2] Ahmad M.Ramli. *Cyber Law dan HAKI dalam Sistem Hukum di Indonesia*, 2004, hlm 1.

[3] Onno W. Purbo dalam Agus Raharjo, 2002, *Cybercrime, Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi,* (Citra Aditya Bahkti : Bandung, halaman 5)

Diantara banyaknya manfaat dari perkembangan teknologi informasi dan komunikasi, muncul sisi negatif dengan mulai berjamurannya kejahatan yang dilakukan dengan mengunakan sarana teknologi informasi dan komunikasi. Dampak negatif dari perubahan pola perilaku pada era kehidupan global tersebut nampak dari berkembangnya kriminalitas baik secara kuantitatif maupun kualitatif. Kini mulai muncul berbagai jenis kejahatan dengan dimensi baru seperti penyalahgunaan komputer, kejahatan perbankan dan lain sebagainya yang semakin sulit untuk ditanggulangi.[4]

Kejahatan yang bermunculan dengan menggunakan sarana teknologi informasi dan komunikasi hingga saat ini masih terdapat perbedaan dan belum ada kesepakatan dalam peristilahannya. Dalam menggunakan jasa pada dunia maya masyarakat cenderung bebas berinteraksi, beraktifitas dan berkreasi yang hampir sempurna pada semua bidang.

Masyarakat sedang membangun kebudayaan baru di ruang maya yang dikenal dengan istilah *Cyberspace*[5]*. Cyberspace* menawarkan

---

[4] Kata Pengantar Prof. DR. Barda Nanawi Arief, SH., dalam *Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer* oleh Al. Wisnubroto, Universitas Atma Jaya Yogyakarta

[5] Menurut Howard Rheingold bahwa Cybescpace adalah sebuah ruang imajiner atau ruang maya yang bersifat artificial, dimana setiap orang melakukan apa saja yang biasa dilakukan

manusia untuk “hidup” dalam dunia alternatif. Sebuah dunia yang dapat mengambil alih dan menggantikan realitas yang ada, yang lebih menyenangkan dari kesenangan yang ada yang lebih fantastis dari fantasi yang ada, yang lebih menggairahkan dari kegairahan yang ada. *Cyber space* menjadi sebuah simbol pelopor, yang akan mengintegrasikan seluruh sistem dunia, baik dalam aspek sosial, budaya, ekonomi dan keuangan.[6] Komputer seolah-olah benda ajaib yang menjadi rujukan apa saja, dan menjadi alat penghubung jutaan- mungkin sudah milyaran- umat manusia.[7]

Kegiatan siber meskipun bersifat virtual tetapi dikatagorikan sebagai tindakan dan perbuatan hukum yang nyata.[8] Oleh karena itu perkembangan teknologi informasi, transaksi elektronik dianggap sebagai

---

dalam kehidupan social sehari-hari dengan cara-cara yang baru, dalam Abdul Wahid, *Kejahatan Mayantara*, 2005, (Refika Aditama:Bandung, Halaman 32) istilah Cyber Space ini lahir dari William Gibson seorang penulis fiksi ilmiah (science fiction), kata cyber space di temukan dalam novelnya yang berjudul/Veiwomancerdan Virtual light.

[6] Didik J. Rachbini, *Mitos dan Implikasi globalisasi : Catatan Untuk Bidang Ekonomi dan Keuangan,* pengantar Edisi Indonesia dalam Hirst, Paul dan Grahame Thompson, *Globalisasi Adalah Mitos.* Jakarta, Yayasan Obor, 2001. hal. 1

[7] Lihat Sutanto, Hermawan Sulistyo, dan tjuk Sugiarto (Ed), *Cyber Crime Motif dan Penindakan,* Pensil 324, Jakarta, hal 1, salah satu revolusi terbesar yang mengubah nasib jutaan manusia dan kehiduopan *modern* dewasa ini adalah di temukannya komputer, yang segera disusul oleh berkembangan pesatnya tehnilogi informasi.

[8] Lihat Ahmad M.Ramli, *Pager Gunung*, Indra Apiadi, hal. 2, kegiatan siber adalah kegiatan virtual tetapi berdampak sangat nyata meskipun alat buktinya bersifat elektronik.

lokomitif dan turut mempercepat proses globalisasi di pelbagai aspek kehidupan.[9]

*Cyberspace* telah pula menciptakan bentuk kejahatan baru, sebagai bentuk kejahatan yang ditimbulkan oleh perkembangan dan kemajuan tekhnologi informasi dan telekomunikasi yaitu kejahatan yang berkaitan dengan aplikasi internet yang dalam istilah asing disebut *cyber crime.*[10] Salah satu masalah *cyber crime* yang sangat meresahkan dan mendapat perhatian baik dari kalangan nasional maupun kalangan internasional adalah masalah CT (selanjutnya disingkat CT). Jenis CT di bidang *cyber crime* ini sering diartikan sebagai suatu aksi kejahatan terrorisme yang menggunakan sarana teknologi dan informasi, elektronik[11], tujuannya melumpuhkan infrastruktur secara nasional, seperti energy, transportasi, untuk menekan/mengintimidasi kegiatan-kegiatan pemerintah atau masyarakat sipil.[12]

---

[9] Muhammad Aulia Adnan, *Tinjauan Hukum Hukum dalam E Business* Olyx76@yahoo.com.

[10] Barda Nawawi Arief menggunakan istilah Kejahatan Mayantara untuk menunjuk jenis kejahatan ini. Dalam Barda Nawawi Arief, 2003, *Kapita Selekta Hukum Pidana*, (Citra Aditya Bhakti : Bandung), halaman 255

[11] http://library.monx007.com/2009/06/9/computer/terorismaya/2

[12] James A.Lewis, Assesing the Risk Of Cyber Terrorism, *Cyber War and Other Cyber Threats, Center For Strategic and International Studies,* Washington D.C., Desember 2002, hlm 1. "Cyber Terrorism as the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government orerations) or to coerce or intimidate a government or civilian population "

Cyber terrorism kadang juga disebut dengan *cyber sabotage and exortion*. Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung ke internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu virus komputer atau program komputer tertentu sehingga data, program komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana dikehendaki oleh pelaku.[13]

Cyber terrorism telah banyak terjadi baik di negara Indonesia maupun negara- negara lainnya. Dari data yang diperoleh mengenai kejahatan CT tersebut, diantaranya pada kasus Bom Bali, yang salah satu pelakunya ialah almarhum Iman Samudra yang beberapa bulan lalu telah dipidana mati, memberikan laporan ketika masih hidup yang pada saat itu dalam proses penyelidikan, Imam jelas menyatakan bahwa internet adalah alat yang terbaik untuk mencapai misi-Nya, dan pernyataan itu diituangkan juga dalam bukunya yang berjudul Aku Melawan Teroris (I Fight terorists). Ia menyarankan kepada junior- juniornya untuk belajar internet, sehingga terampil seperti hacker. Bagi mereka, tujuan utama

---

[13] Ali Juliano Gema, sebagaimana di kutip oleh Abdul Wahid dan Mohammad Labib, dalam buku (Drs H.sutaman, M.H. Kata Pengantar dari Prof. Dr. M. Khoiden, S.H, M.H., C.N (Guru Besar universitas Jember ), *Cyber Crime, Modus Operandi dan Penangulangannya*. LeksBang komputer PRESSindo Jogjakarta. 2007. hal. 83).

untuk berbagi pengetahuan mereka mengenai hacking adalah sebagai perlawanan politik.[14]

Kasus CT ini juga diperkuat dengan pernyataan "Kepala Polisi Nasional, Komisaris Jenderal Makbul Padmanagara kepada wartawan di International Drug Enforcement Conference (IDEC dihadiri oleh beberapa participants dari 16 negara, mengatakan bahwa untuk pertama kalinya dalam sejarah, polisi Indonesia baru berhasil (menemukan/ membongkar) sebuah kasus "*cyber terorisme*" disingkat (CT) yang melibatkan Abdul Azis alias Imam Samudra, yang diancam dengan pidana mati salah satu pelaku dari Bom Bali Oktober 2002 yang lalu. Untuk pertama kalinya dalam sejarah kami, kami dapat menemukan sebuah kasus CT, suatu perbuatan pidana yang dilakukan para pelaku menggunakan dunia CT untuk menyebarkan provokasi dan propaganda. Makbul menegaskan lagi bahwa penemuan kasus CT yang melibatkan Imam Samudra dan kroni-kroninya tersebut, semua pihak harus selalu waspada terhadap bahaya nyata dari teroris.[15]

---

[14] http://www.thejakartapost.com/news/2006/09/14/cyberterrorism-creates-problems-real-world.htm...
"In his book Aku Melawan Teroris (I fight terrorists), Imam clearly stated that the Internet is the best tool to achieve his mission. He suggested that his juniors learn hacking skills. It would not be difficult for Muslim fundamentalists and the hackers to do that because both communities are anarchistic and anti-authority. To them, the primary motive of sharing their knowledge on hacking is political resistance.

[15] http://www.antara.co.id/en/arc/2006/9/13/police-uncover-their-first-cyber-terrorism-case. "For the first time in our history, we were able to uncover a CT case, a criminal act in which the perpetrators made use of the cyber-world to spread terrorist provocation and

Kasus di negara Amerika Serikat, pada bulan Februari 1998 terjadi serangan *(breaks-in or attack)* sebanyak 60 kali perminggunya melalui media *Internet* terhadap 11 jaringan komputer militer di Pentagon. Dalam *cyber attack* ini yang menjadi target utama para *cyber terrorist* adalah Departemen Pertahanan Amerika Serikat *(DoD)*.[16]

Data kasus CT lainnya lagi, ditemukan Virus "I Love You" dan "Love Bug" serta berbagai variasinya yang menyebar dengan cepat, diketahui berasal dari Filipina. Virus-virus tersebut sejauh ini menimbulkan kerusakan sangat besar dalam sejarah. Berdasarkan prakiraan, virus "I Love You" dapat merasuki 10 juta komputer dalam jaringan dunia dan menimbulkan kerugian finansial yang besar pada jaringan komputer di Malaysia, Jerman, Belgia, Perancis, Belanda, Swedia, Hongkong, Inggris Raya, dan Amerika Serikat. Virus ini menyebabkan ATM-ATM di Belgia tak berfungsi beberapa waktu, mengganggu sistem komunikasi internal Majelis Perwakilan Rendah (The House of Common) di Inggris, dan menghilangkan sistem surat elektronik (e-mail) pada Kongres Amerika Serikat.[17]

---

propaganda," the head of the National Police`s Criminal Investigation Department, Commissioner General Makbul Padmanagara, said here on Tuesday ".

[16] Mayor Sus Ir. Rudy A.G. Gultom, M.Sc. *Teknologi Militer, CYBER TERRORISM (Sudah Siapkah Kita Menghadapinya?)* http://www.tni.mil.id/2009/06/22/images/gallery/cyber_terrorism.pdf

[17] http://www.unisosdem.org/2009/06/13/kliping_detail.php?aid=2828&coid=1&caid=45

Berkaitan dengan penjelasan diatas, dapat diketahui bahwa tindak pidana CT itu merupakan kejahatan lintas negara dengan berbasis tehnologi, yang dapat meresahkan masyarakat dalam tataran yang jauh lebih luas (global). Mengingat juga bahwa Indoneisa dalam *cyber crime* diyatakan sebagai peringkat pertama dalam kejahatan dunia maya (menggunakan internet) telah menggantikan posisi Ukraina yang sebelumnya menduduki peringkat pertama.[18] Melihat fakta tersebut maka perlu dilakukan kajian serius terhadap kebijakan penanggulangan tindak pidana CT yang merupakan bagian dari jenis tindak pidana *cyber crime* itu sendiri.

Indonesia dalam menindak lanjuti hasil kongres PBB tersebut Indonesia telah meratifikasi salah satu Rancangan Undang-Undang yang berkaitan dengan kejahatan dunia maya (*cybercrime*) yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE). Undang- Undang ITE ini diharapkan dapat menganggulangi kejahatan-kajahatan yang menggunakan sarana tehnologi, informasi dan elekekrtonik *(cyber crime)*, yang juga dapat menanggulangi tindak pidana CT yang merupakan bagian dari salah satu jenis *cyber crime* tersebut.

## B. Perumusan Masalah

[18] Ade Ari Syam Indradi, Carding (Modus Operandi, Penyidikan, dan Penindakan), Pensil 234, Jakarta, 2006, hal.1 dalam buku Sutaman, *Cyber Crime (Modus Operandi dan Penanggulangannya)*, LaksBang PRESSindo, Jogjakarta, hal. 10

Berhubungan dengan latar belakang tersebut di atas, penelitian ini hanya terbatas pada ruang lingkup yang berkaitan dengan *cyber terrorism* dengan perumusan masalah sebagai berikut :

1. Bagaimana kebijakan kriminal pada saat ini dalam menanggulangi tindak pidana *cyber terrorism* ?
2. Bagaimana kebijakan kriminal yang akan datang dalam menanggulangi tindak pidana *cyber terrorism* ?

## C. Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Untuk mengetahui serta menjelaskan kebijakan kriminal hukum pidana di Indonesia yang ada saat ini dalam menanggulangi tindak pidana *cyber terrorism,*
2. Untuk mengetahui kebijakan kriminal pidana yang seyogyanya ditempuh di masa yang akan datang dalam menanggulangi tindak pidana *cyber terrorism*, dalam rangka pembaharuan hukum pidana di Indonesia.

## D. Manfaat Penelitian

Penelitian ini bermanfaat:

1. Manfaat Teoritis

Mengembangkan pemahaman teoritis tentang tindak pidana *cyber terrorism* dengan berbagai sisinya baik motif maupun cara perbuatan tersebut dilakukan, dan dalam penelitian ini diharapkan dapat diketahui peraturan perundangan di bidang hukum pidana saat ini terhadap masalah ini, sehingga dapat melengkapi khasanah kajian khususnya ilmu hukum pidana.

2. Manfaat Praktis

Hasil penelitian ini diharapkan dapat menjadi bahan pertimbangan atau masukan informasi yang lebih kongkrit bagi para legislator serta memberi solusi dalam penanggulangan tindak pidana *cyber terrorism* di Indonesia yang seyogyanya ditempuh dalam menghadapi masalah tersebut, dengan bertolak dan identifikasi pada Undang-Undang Informasi, dan Transaksi Elektronik Nomor 11 Tahun 2008, sebagai undang- undang khususyang telah diratifikasi untuk mengatur masalah tindak pidana *cyber crime,* sekiranya dapat juga digunakan dalam menanggulangi tindak pidana *cyber terrorism,* mengingat bahwa *cyber terrorism* merupakan bagian dari tindak pidana *cyber crime*, apakah dalam penerapannya sudah dapat mengakomodir dan menanggulangi tindak pidana *cyber crime* secara integral atau apakah masih terdapat keterbatasan/kelemahan dalam undang- undang tersebut, sehingga kedepannya nanti para legislator dapat membuat dan mengeluarkan

produk hukum yang menjangkau permasalahan tersebut, terutama terkait dengan upaya pembaharuan KUHP.

## E. Kerangka Teori

Cyber terrorism merupakan salah satu jenis *cyber crime* dari beberapa jenis- jenis *cyber crime* yang ada, yang muncul akibat dari dampak negatif perkembangan sarana tekhnologi informasi dan komunikasi masyarakat global, sehingga terjadi perubahan- perubahan pola perilaku masyarakat dalam bidang ini sebagai penyalahgunaan komputer. [19]

Pesatnya perkembangan teknologi informasi yang membawa dampak tumbuh suburnya *cyber crime*, kejahatan melalui Internet di jagat maya itu membuat beberapa negara-negara bersepekat melakukan usaha secara bersama- sama dalam menganggulangi tindak pidana *cyber crime* tersebut. Usaha- usaha itu terlihat dari pembahasan dalam sidang komisi di Konferensi Ke-23 Aseanapol di Manila, Filipina, September lalu, mengenai *cyber crime,* yang diyakini menjadi masalah serius yang harus segera ditangani. Kepolisian di 10 negara Asia Tenggara menyatakan

[19] Berasal dari *computer abuse* (Inggris), *computermisbruik* (Belanda). Lihat dalam Al Wisnubroto hlm 20

peduli terhadap dampak yang ditimbulkan kejahatan ini dan berupaya untuk menekannya.

Tak ada satu negara pun yang terbebaskan dari *cyber crime*. Perkembangan teknologi telah mengaburkan batas-batas fisik dan budaya sebuah negara. Mengacu pada Kongres Perserikatan Bangsa-Bangsa (PBB) untuk Pencegahan Kejahatan di Wina, Austria, April 2000, *cyber crime* meliputi melakukan akses tanpa izin, merusak data atau program komputer, melakukan sabotase untuk menghilangkan sistem atau jaringan komputer, mengambil data dari dan ke dalam jaringan komputer tanpa izin, serta mematai-matai komputer.[20]

Indonesia telah mensahkan salah satu Rancangan Undang-Undang yang berkaitan dengan kejahatan dunia maya (*cybercrime*) yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE). Undang-Undang ini bertujuan untuk mengharmonisasikan antara instrumen peraturan hukum nasional dengan instrumen-instrumen hukum internasional yang mengatur teknologi informasi diantaranya, yaitu: The United Nations Commissions on International Trade Law (UNCITRAL), World Trade Organization (WTO), Uni Eropa (EU), APEC, ASEAN, dan OECD. Masing-masing

[20] http://www.unisosdem.org/2009/06/12/kliping_detail.php?aid=2828&coid=1&caid=4,5

organisasi mengeluarkan peraturan atau model law yang mengisi satu sama lain. Dan juga instrument hukum internasional ini telah diikuti oleh beberapa negara, seperti: Australia (*The cyber crime act 2001*), Malaysia (*Computer Crime Act 1997*), Amerika Serikat (*Federal legislation: update April 2002 UNITED STATES CODE*), Kongres PBB ke 8 di Havana, Kongres ke X di Wina, kongres XI 2005 di Bangkok, berbicara tentang The Prevention of Crime and the Treatment of Offender. Dalam Kongres PBB X tersebut dinyatakan bahwa negara-negara anggota harus berusaha melakukan harmonisasi ketentuan ketentuan yang berhubungan dengan kriminalisasi, pembuktian dan prosedur (States should seek harmonization of relevan provision on criminalization, evidence, and procedure)[21] dan negara-negara Uni Eropa yang telah secara serius mengintegrasikan regulasi yang terkait dengan pemanfaatan teknologi informasi ke dalam instrumen hukum positif (*existing law*) nasionalnya.[22]

Penulis ingin memberikan rincian sekilas mengenai pengertian dan ruang lingkup dari tindak pidana CT. Pengertian tindak pidana CT menurut penulis pada prinsipnya berdimensi luas dan belum memiliki keseragaman

---

21 Barda Nawawi Arife. *Tindak Pidana Mayantara*, *Perkembangan Kajian CyberCrime di Indonesia*. PT. Raja grafindo Persada : Jakarta, hal. v

22 http://google.co.id/ *Naskah Akademik Rancangan Undang-Undang tentang informasi dan transaksi elektronik*

mengenai peristilahannya, tetapi dari beberapa para ahli hukum memberikan definisi mengenai tindak pidana CT.

Dorothy E. Denning,[23] memberikan definisi bahwa CT secara umum dipahami sebagai:

> ”penyerangan dengan menggunakan komputer atau mengancam, mengintimidasi atau memaksa pemerintahan atau masyarakat, dengan tujuan untuk mencapai target politik, agama atau ideology. Sarana itu cukup untuk menimbulkan rasa takut yang berasal dari tindakan psikis teroris. Serangan itu secara tidak langsung dapat menimbulkan kematian atau cacat badan, kecelakaan pesawat, pencemaran air, dan kelumpuhan ekonomi secara makro. Kerusakan infrastruktur seperti tenaga listrik atau pelayanan keadaan darurat yang dapat disebabkan oleh tindakan terorisme mayantara”.

Definisi CT lainnya dapat dilihat dari definisi yang diberikan oleh The National Conference of State Legislatures (NCSL) sebuah organisasi gabungan 2 partai, para kader dan anggota- anggota legislatif, membantu

---

[23] Dorothy E. Denning, cyber terrorism, *“ …is generally understood to mean a computer-based attack or threat of attack intended to intimidate or coerce governments or societies in pursuit of goals that are political, religious, or ideological. The attack should be sufficiently destructive or disruptive to generate fear comparable to that from physical acts of terrorism. Attacks that lead to death or bodily injury, extended power outages, plane crashes, water contamination, or major economic losses would be examples. Depending on their impact, attacks against critical infrastructures such as electric power or emergency services could be acts of cyber terrorism. Attack that disrupt non essential services or that are mainly a costly nuisance would not.* Dalam buku Dikdik M. Arief Mansur, & Eli Satris Gultom, *Cyber Law, aspek Hukum Teknologi Informasi*., hal. 65

pemerintah 50 bagian menyampaikan isu penting yang mempengaruhi perekenomian atau keamanan dalam negeri dengan memfasilitasi mereka dengan sebuah forum tukar ide, riset (studi kasus), dan bantuan tehnis. bahwa CT *:* [24]

> adalah penggunaan teknologi informasi oleh individu dan kelompok teroris untuk agenda mereka". Hal ini termasuk penggunaan teknologi informasi untuk mengatur dan melakukan serangan terhadap jaringan komputer dan infrastruktur telekomunikasi, atau untuk bertukar informasi atau membuat ancaman elektronik. Contohnya adalah hacking."

Hacking yaitu memasukkan ke dalam sistem komputer dengan mengenalkan virus agar mudah kena serangan ke jaringan situs internet atau ancaman terroristik yang dilakukan melalui komunikasi elektronik.[25], hacking dengan kata lain diartikan sebagai perusakan komputer jaringan pihak lain.[26]

---

[24] http://en.wikipedia.org/wiki/Cyber-terrorism bna, 30-4-2009. The National Conference of State Legislatures (NCSL), a bipartisan organization of legislators and their staff created to help policymakers of all 50 states address vital issues such as those affecting the economy or homeland security by providing them with a forum for exchanging ideas, sharing research and obtaining technical assistance. "defines cyberterrorism as follows: *the use of information technology by terrorist groups and individuals to further their agenda. This can include use of information technology to organize and execute attacks against networks, computer systems and telecommunications infrastructures, or for exchanging information or making threats electronically. Examples are hacking into computer systems, introducing viruses to vulnerable networks, web site defacing,*

[25] *Ibid*. http://en.wikipedia.org/wiki/Cyber-terrorism

[26] Abdul Wahib dan Mohammad Labib, *Kejahatan Mayantara (Caber Crime),* Refika Aditama, Bandung, 2005, hal. 130

Aksi kejahatan CT sering diistilahkan sebagai *cyber criminal,* sehingga sukar untuk memisahkan antara istilah CT dengan *cyber criminal*. Mungkin yang bisa dibedakan adalah motifnya. Seorang CT mempunyai tujuan lebih dari sekedar ketenaran dan uang. Mereka juga biasanya lebih terorganisir dan mempunyai sumber dana untuk melakukan aksi-aksi teror. Target dari aksi CT biasanya adalah sarana-sarana umum di dunia maya (online facility). Sedangkan, *cyber criminal* biasanya bertujuan lebih 'singkat' dan bersifat 'komersil'. Sebagaimana layaknya seorang penjahat (criminal), sebagian besar tujuan utamanya adalah uang dan ketenaran, walaupun dalam melakukan aksinya, banyak dari mereka lebih mengutamakan kepuasan pribadi dengan menaklukkan targetnya.[27]

Akan tetapi aksi keduanya tidak jauh berbeda. Keduanya sering melakukan aksi pembobolan sistem dan meninggalkan identitas pada mangsa agar orang lain mengetahui siapa pelakunya. Dalam hal ini biasanya seorang CT akan menyertakan pesan sebagai alasan baginya untuk beraksi, sedangkan *cyber criminal* biasanya hanya meninggalkan identitas dan berharap hal tersebut membuatnya terkenal dan ditakuti.

Aksi CT biasanya menyerang jaringan komputer yang digunakan sebagai fasilitas umum. Mereka bisa membobol bank dengan menyusup ke dalam sistem jaringan informasi, lalu mengambil atau mengubah

[27] http://library.monx007.com/2009/06/9computer/terorismaya/2

informasi yang ada di dalam pusat data. Dengan demikian, mereka dapat merampok bank tersebut tanpa harus datang ke penyimpanan uang dan memperlihatkan keberadaan dirinya.

Dari pejelasan di atas mengenai pengertian tindak pidana CT, maka dapat diketahui batasan ruang lingkup tindak pidana CT ini sangat tergantung pada penggunaan unsur media telekomunikasi, dimana komputer digunakan sebagai sarana dan objek sasaran aksi terrorisme.

Sarana itu cukup untuk menimbulkan rasa takut yang berasal dari tindakan psikis teroris. Serangan itu secara tidak langsung dapat menimbulkan kematian atau cacat badan, kecelakaan pesawat, pencemaran air, dan kelumpuhan ekonomi secara makro, kerusakan Dalam rangka menanggulangi kejahatan terdapat berbagai sarana sebagai reaksi yang dapat diberikan kepada pelaku kejahatan, baik berupa sarana pidana maupun non hukum pidana, yang dapat diintegrasikan satu dengan yang lainnya. Apabila sarana pidana dipanggil untuk menanggulangi kejahatan, berarti akan dilaksanakan politik hukum pidana, yakni mengadakan pemilihan untuk mencapai hasil perundang-undangan pidana yang sesuai dengan keadaan dan situasi pada suatu waktu dan untuk masa-masa yang akan datang. [28]

---

[28] Sudarto, 1983, *Hukum dan Hukum Pidana*, Sinar Baru : Bandung, halaman. 109

Usaha dan kebijakan untuk membuat peraturan hukum pidana yang baik pada hakekatnya tidak dapat dilepaskan dari tujuan penanggulangan kejahatan. Jadi, kebijakan atau politik hukum pidana juga merupakan bagian dari politik kriminal. Dengan kata lain, dilihat dari sudut politik kriminal, maka politik hukum pidana identik dengan pengertian "kebijakan penanggulangan kejahatan dengan hukum pidana."[29] Politik kriminal ini merupakan bagian dari politik penegakan hukum dalam arti luas (*law enforcement policy*), semua merupakan bagian dari politik sosial (*sosial policy*), yakni usaha dari masyarakat atau negara untuk meningkatkan kesejahteraan warganya.[30]

Sudarto, pernah mengemukakan bahwa apabila hukum pidana hendak digunakan hendaknya dilihat dalam hubungan keseluruhan politik kriminal atau "social defence planning" yang inipun harus merupakan bagian integral dari rencana pembangunan nasional.[31]

---

[29] Barda Nawawi Arief, 2008, *Bunga Rampai Kebijakan Hukum Pidana (Perkembangan Penyusunan Konsep KUHP Baru)*, Kencana, Jakarta, halaman 24

[30] Muladi, disampaikan pada Penataran Hukum Pidana Nasional Angkatan IV; Kerjasama Hukum Indonesia-Belanda di Purwokerto tanggal, 18 dan 19 Agustus 1990, dalam buku Muladi dan Barda Nawawi Arief, *Bunga Rampai Hukum Pidana,* Penerbit Alumni, Bandung, 2002. hal. 1

[31] Sudarto, *Hukum dan Hukum Pidana, 1983, h.104.lihat pula W. Clifford, Reform in criminal Justice in Asia and the Far East,* Resource Material Serie No.6, UNAFEL, 1973,p.7 : …. There is the need for a wider view of criminal policy as an integral part of general political and social policy of a given country". Demikian pula G>P Hoefnagels, "The other side of criminology", 1973, h. 57 : " Criminal policy as as science of policy is part of a larger policy; the law enforcement policy…The legislative and enforcement policy is in turn part of social policy". dalam buku Muladi dan Barda nawawi Arief, *Teori-Teori dan Kebijakan Pidana.* P.T. Alumni, Bandung, 2005, hal. 157

Politik kriminal adalah pengaturan atau penyusunan secara rasional usaha-usaha pengendalian kejahatan oleh masyarakat.[32] Politik kriminil ini dapat diberi arti sempit, lebih luas dan paling luas. Dalam arti sempit politik kriminil itu digambarkan sebagai keseluruhan asas dan metode, yang menjadi dasar dari reaksi terhadap pelanggaran hukum yang berupa pidana.

Dalam arti yang lebih luas ia merupakan keseluruhan fungsi dan aparatur penegak hukum, termasuk di dalamnya cara kerja pengadilan dan polisi, sedang dalam arti yang paling luas ia merupakan keseluruhan kebijakan, yang dilakukan melalui perundang- undangan dan badan-badan resmi, yang bertujuan untuk menegakkan norma- norma sentral dari masyarakat.[33]

Kebijakan kriminal atau kebijakan penanggulangan kejahatan bila dilihat lingkupnya, sangat luas dan kompleks. Hal ini wajar karena pada hakikatnya, kejahatan sebagai masalah kemanusiaan sekaligus masalah sosial yang memerlukan pemahaman tersendiri. Kejahatan sebagai

---

[32] Marc Ancel, *Social defence.* 1965, h. 209, merumuskan sebagai "the rational organization of the control of crime by society"; dalam buku G.P. Hoefnagels, The other side of criminolgy, h. 57, pendapat M. Ancel itu dirumuskan sebagai "the rational organization of the social reaction to crime"; Hoefnagels sendiri mengumakakan berbagai rumusan yaitu "the science of responses", "the science of crime prevention", "a policy of designating human behavior as crime" dan "a rational toral of the rensponses to crime"The other side of criminolgy h. 57, 99, 100);

[33] Politik kriminal dalam arti sempit, luas dan paling luas dekemukakan oleh Sudarto, *Kapita Selekta Hukum Pidana,* 1981, h. 113-114.

masalah sosial merupakan gejala yang dinamis, selalu tumbuh dan terkait dengan gejala dan struktur kemasyarakatan lain yang sangat kompleks. Hal itu merupakan *socio-polical problems.*[34]

Upaya atau kebijakan untuk melakukan pencegahan dan penanggulangan kejahatatan yang merupakan bagian kebijakan kriminal *("criminal policy")* ini, tidak terlepas dari kebijakan yang lebih luas, yaitu "kebijakan sosial *("sosial policy")* yang terdiri dari " kebijakan/ upaya-upaya untuk kesejahteraan sosial". *("social-welfare polcy")* dan 'kebijakan upaya-upaya untuk perlindungan masyarakat" *("social-defence policy).* Dengan demikian, sekiranya kebijakan penanggulangan kejahatan (politik kriminal) dilakukan dengan menggunakan sarana "penal" (hukum pidana), maka "kebijakan hukum pidana" *(penal policy)*, khususnya pada tahap kebijakan yudikatif/aplikatif (penegakan hukum pidana in concreto) harus memperhatikan dan mengarah pada tercapainya tujuan dari kebijakan sosial itu, berupa "social-welfare" dan "social-defence" [35]

Ada dua masalah sentral dalam kebijakan/ politik kriminal dengan menggunakan sarana penal (hukum) ialah masalah penentuan :

1. perbuatan apa yang seharusnya dijadikan tindak pidana, dan

---

[34] Muladi, 1995, *Kapita Selekta Sistem Peradila Pidana,* hal. 7, dalam Buku Paulus hadisuprapto, *Delikuensi Anak, Pemahaman dan Penaggulangannya.* Bayumaedia,Madang, 2008, hal. 82

[35] Barda Nawawi Arief, *Masalah Penegakan hukum dan Kebijakan Penanggulangan Kejahatan.* PT. Citra Aditya Bakti : Bandung. 2001, hal. 73

2. sanksi apa yang sebaiknya digunakan atau dikenakan kepada si pelanggar.[36]

Pembaharuan hukum pidana *(penal reform)* pada hakekatnya juga merupakan bagian dari kebijakan/politik hukum pidana (*penal policy*). Pembaharuan hukum pidana pada hakikatnya mengandung makna, suatu upaya untuk melakukan reoreintasi dan reformasi hukum pidana yang sesuai dengan nilai- nilai sentral sosiopolitik, sosiofilosofis, dan sosiokultural masyarakat Indonesia yang melandasi kebijakan kriminal dan kebijakan penegakan hukum di Indonesia.

Secara singkat dapatlah dikatakan bahwa pembaharuan hukum pidana pada hakekatnya harus ditempuh dengan pendekatan yang berorientasi pada kebijakan (*policy-oriented approach*) dan pendekatan yang berorientasi pada nilai *(value-oriented approach)*[37] atau dengan kata lain upaya penanggulangan kejahatan perlu ditempuh dengan pendekatan kebijakan dalam arti ada keterpaduan antara politik kriminal dan politik sosial serta ada keterpaduan antara upaya penanggulangan kejahatan dengan penal dan non penal dan di dalam setiap kebijakan *(policy*) terkandung pula pertimbangan nilai.

---

[36] Barda Nawawi Arief, *Kebijakan Legislatif, dalam Penanggulangan Kejahatan dengan Pidana Penjara,* Badan Penerbit UNDIP Semarang. 1996, hal. 35

[37] Barda Nawawi Arief, 2008. *Opcit*, halaman 25

Pembaharuan hukum pidana, disamping itu juga mengandung arti suatu upaya yang terus-menerus dilaksanakan melalui perundang-undangan guna menyerasikan peraturan perundang- undangan pidana degan asas-asas hukum serta nilai-nilai yang berkembang dengan masyarakat, baik ditingkat nasional maupun internasional.[38]

Bertolak dari pendekatan kebijakan, Sudarto berpendapat bahwa dalam menghadapi masalah sentral dalam kebijakan kriminal terutama masalah pertama yang disebut juga masalah kriminalisasi, harus diperhatikan hal-hal yang pada intinya sebagai berikut :[39]

1. Penggunaan hukum pidana harus memperhatikan tujuan pembangaunan nasional yang mewujudkan masyarakat adil dan makmur yang merata, materiil, spirituil berdasarkan Pancasila; sehubungan dengan hal ini maka (penggunaan) hukum pidana bertujuan untuk mengangulangi kejahatan dan mengadakan pengugeran terhadap tindakan penanggulangan itu sendiri, demi kesejahteraan dan pengayoman masyarakat;
2. Perbuatan yang diusahakan untuk dicegah atau ditanggulangi dengan hukum pidana harus merupakan “perbuatan yang tidak dikehendaki, yaitu perbuatan yang mendatangkan kerugian (materiil dan atau spirituil) atas warga masyarakat;
3. Penggunaan hukum pidana harus pula memperhitungkan prinsip-prinsip biaya dan hasil *(cost and benefit principle*);
4. Penggunaan hukum pidana harus pula memperhatikan kapasitas atau kemampuan daya kerja dari bagian-bagian penegak hukum, yaitu jangan sampai ada kelampauan beban tugas *(overbelasting)* .

Sejalan dengan yang dikemukakan Sudarto diatas, Barda Nawawi Arief mengatakan bahwa menurut Bassiouni keputusan untuk melakukan

---

[38] Nyoman Serikat Putra Jaya, *Makalah Pembaharuan Hukum pidana.* Magister Ilmu Hukum UNDIP, UNSOED, dan UNTAG. 2007. hal 20

[39] Barda Nawawi Arief, 2008. *Opcit*, halaman 27-28

kriminalisasi dan dekriminalisasi harus didasarkan pada faktor-faktor kebijakan tertentu yang mempertimbangkan bermacam-macam faktor, termasuk :

1. Keseimbangan sarana-sarana yang digunakan dalam hubungannya dengan hasil-hasil yang ingin dicapai;
2. Analisis biaya terhadap hasil-hasil yang diperoleh dalam hubungannya dengan tujuan-tujuan yang dicari;
3. Penilaian atau penafsiran tujuan-tujuan yang dicari itu dalam kaitannya dengan prioritas-prioritas lainnya dalam pengalokasian sumber-sumber tenaga manusia;
4. Pengaruh sosial dari kriminalisasi dan dekriminalisasi yang berkenaan dengan atau dipandang dari pengaruh-pengaruh yang sekunder. [40]

Kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana menjadi suatu tindak pidana. Pada hakikatnya, kebijakan kriminalisasi merupakan bagian dari kebijakan kriminal *(criminal policy)* dengan menggunakan sarana hukum pidana *(penal)*, dan oleh karena itu termasuk bagian dari kebijakan hukum pidana *(penal policy)*.[41]

---

[40] Barda Nawawi Arif, 2008, *Bunga Rampai Kebijakan Hukum Pidana (Perkembangan Penyusunan Konsep KUHP Baru)*, Kencana, Jakarta, halaman. 29-30. Mengenai pendapat M. Cherif Bassiuoni dalam bukunya Substantive Criminal Law, yang menyebutkan bahwa : The decision to sriminalize or decriminalize should be based on certain policy factor which take into account a variety of factor, including :
1. the proportionality of the means used in relationship to the outcome obtained;
2. the cost analysis of the outcome obtained in relationship to the objectives sought;
3. an appraisal of the objectives sought in relationship to other priorities in the allocation of human- power ; and
4. the social impact of criminalization and decriminalization in terms of its secondary effects.

[41] Barda Nawawi Arief, 2002, *Bunga Rampai Kebijakan Hukum Pidana*, Citra Aditya Bakti, Bandung, hlm.2-3

Di Indonesia saat ini tengah berlangsung usaha untuk memperbaiki Kitab Undang-Undang Hukum Pidana (KUHP) sebagai bagian dari usaha pembaharuan hukum nasional yang menyeluruh. Usaha pembaharuan itu tidak hanya karena alasan bahwa KUHP yang sekarang diberlakukan dianggap tidak sesuai lagi dengan tuntutan perkembangan masyarakat, tetapi juga karena KUHP tersebut tidak lebih dari produk warisan penjajah Belanda, dan karenannya tidak sesuai dengan pandangan hidup bangsa Indonesia yang merdeka dan berdaulat.

Usaha pembaharuan hukum pidana di Indonesia tentunya tidak terlepas dari politik hukum yang bertugas untuk meneliti perubahan-perubahan yang perlu diadakan terhadap hukum yang ada agar supaya memenuhi kebutuhan baru didalam masyarakat. Politik hukum tersebut meneruskan arah perkembangan tertib hukum, dari "*ius contitutum*' yang bertumpu pada kerangka landasan hukum yang terdahulu menuju pada penyusunan "*ius constituendum*" atau hukum pada masa yang akan datang.

Hal tersebut diatas sejalan dengan yang dikemukakan oleh Barda Nawawi Arief, yaitu :[42]

> Pembaharuan hukum pidana pada hakekatnya mengandung makna, suatu upaya untuk melakukan reorientasi dan reformasi hukum pidana yang sesuai dengan nilai-nilai sentral sosio-politik,

[42] Barda Nawawi Arief, 2002, *Ibid.* hlm 30-31

sosio-filosofik, sosio-kultural masyarakat Indonesia yang melandasi kebijakan sosial, kebijakan kriminal dan kebijakan penegakan hukum di Indonesia.

Dari pendapat Barda Nawawi Arief tersebut dapat dilihat bahwa beliau merumuskan tiga latar belakang dan urgensi pembaharuan hukum pidana dengan meninjaunya dari aspek sosio-politik, sosio-filosofik, dan sosio-kultural. Sedangkan Sudarto menyebut ada tiga alasan mengapa KUHP perlu diperbaharui yakni alasan politik, sosiologis dan praktis.[43]

Upaya pembaharuan hukum di Indonesia yang sudah dimulai sejak lahirnya UUD 1945, tidak dapat dilepaskan pula dari landasan sekaligus tujuan yang ingin dicapai oleh bangsa Indonesia seperti telah dirumuskan dalam pembukaan UUD 1945 yaitu, "melindungi segenap bangsa Indonesia dan untuk mewujudkan kesejahteraan umum berdasarkan Pancasila".[44]

Dilihat dari sudut "*criminal policy*", upaya penanggulangan kejahatan CT yang merupakan jenis dari *Cyber Crime* tentunya tidak dapat dilakukan secara parsial dengan hukum pidana (sarana *"penal")*, tetapi harus ditempuh pula dengan pendekatan integral/ sistemik. Sebagai

---

[43] Sudarto, 1983, *Hukum Pidana Dan Perkembangan Masyarakat*, (Sinar Baru : Bandung), halaman 66-68

[44] Barda Nawawi Arief, 1994, *Beberapa Aspek Pengembangan Ilmu Hukum Pidana (Menyongsong Generasi Baru Hukum Pidana Indonesia)*, Kumpulan Pidato Pengukuhan Guru Besar FH UNDIP, Semarang, halaman 1.

salah satu bentuk dari "*hitech crime*", adalah wajar upaya penanggulangan CT juga harus ditempuh dengan pendekatan teknologi (*techno prevention*)[45]. Di samping itu diperlukan pula pendekatan budaya/kultural, pendekatan edukatif dan bahkan pendekatan global (kerja sama internasional) karena kejahatan ini melampaui batas-batas negara (bersifat "*transnational/ transborder*")[46].

## F. Metode Penelitian

1. Metode Pendekatan

Penelitian ini menggunakan pendekatan yuridis normatif, yaitu dengan mengkaji/menganalisis data sekunder yang berupa bahan-bahan hukum terutama bahan hukum primer dan bahan hukum sekunder dengan memahami hukum sebagai seperangkat peraturan atau norma-norma positif di dalam sistem perundang-undangan yang mengatur mengenai kehidupan manusia. Selain itu digunakan kajian yuridis komparatif yaitu dengan melakukan kajian perbandingan

---

[45] Barda Nawawi Arief, *Pembaharuan Hukum Pidana, Dalam Persepektif Kajian Perbandingan.* PT.Citra Aditya Bakti, Bandung. hal. 126

[46] Lihat antara lain *Eighth UN Congress on the Prevention of Crime and the Treatment of Offenders*, Report, 1991, hal. 141 dst. dan ITAC, *"IIIC Common Views Paper On: Cyber Crime"*, IIIC 2000 Millenium Congress, September 19th, 2000, p. 5, dalam Barda Nawawi Arief, *Sari Kuliah Perbandingan Hukum Pidana*, PT RajaGrafindo, Jakarta, 2002, hal. 253 – 256.

terhadap peraturan hukum pidana diberbagai negara yang mengatur tentang *cyber terrorism*.

2. Spesifikasi Penelitian

Spesifikasi dalam penelitian ini adalah penelitian deskriptif analitis yang merupakan penelitian untuk menggambarkan dan menganalisa masalah yang ada dan termasuk dalam jenis penelitian kepustakaan *(library research)* yang akan disajikan secara deskriptif.

3. Sumber Data

Penelitian ini termasuk penelitian hukum normatif maka jenis data yang akan digunakan adalah data sukunder karena menitikberatkan pada studi kepustakaan, sehingga data sekunder atau data pustaka lebih diutamakan dari pada data primer.

Data Sekunder dapat dibedakan menjadi bahan hukum primer bahan hukum sekunder dan bahan hukum tersier.[47]

Dalam metode riset data sekunder yang berupa bahan pustaka memiliki ciri – ciri umum sebagai berikut :

a. Data sekunder pada umumnya ada dalam keadaan siap ( ready made ).
b. Bentuk maupun data sekunder dapat diperoleh tanpa terikat atau dibatasi oleh waktu dan tempat.[48]

[47] Sorjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, Rajawali, Jakarta, 1985, Hal 39.

Dalam penelitian ini yang dimaksud data sekunder meliputi :

a. Bahan hukum primer yaitu bahan hukum yang mengikat yang terdiri dari peraturan perundangan hukum pidana positif di Indonesia yaitu KUHP, Undang- Undang Informasi, Transaksi dan Elektronik, KUHAP, data dari internet, dan data- data lainnya yang terkait dengan permasalahan penelitian ini.

b. Bahan hukum sekunder yaitu bahan hukum yang erat hubungannya dengan bahan hukum primer dan dapat membantu menganalisis serta memahami bahan hukum primer, misalnya Konsep KUHP Nasional, hasil – hasil penelitian para ahli terkait, karya para pakar hukum (berbagai peraturan perundangan yang diperoleh dari berbagai negara sebagai pembandingan yang erat kaitannya dengan penelitian ini, buku – buku yang relevan ), hasil pertemuan ilmiah ( seminar, simposium, diskusi ).

c. Bahan hukum tersier yang akan memberikan petunjuk informasi / penjelasan terhadap bahan hukum primer dan sekunder, seperti kamus hukum, indeks dan lain – lain.

4. Metode Pengumpulan Data

---

[48] Op.Cit Hal 24

Berdasarkan pendekatan yang dipergunakan dalam penelitian ini, maka tekhnik pengumpulan data yang digunakan adalah studi kepustakaan dan dokumen. Data yang dikumpulkan adalah data sekunder yang diperoleh dari bahan-bahan tertulis yang terdiri dari bahan-bahan hukum primer dan sekunder serta digunakan juga dokumen-dokumen pendukung yang dikelompokkan sesuai dengan kepentingannya

5. Metode Analisa Data

Data dianalisis secara normatif-kualitatif dengan jalan menafsirkan dan mengkonstruksikan pernyataan yang terdapat dalam dokumen dan perundang-undangan. Normatif karena penelitian ini bertitik tolak dari peraturan-peraturan yang ada sebagai norma hukum positif, sedangkan kualitatif berarti analisis data yang bertitik tolak pada usaha-usaha penemuan asas-asas dan informasi-informasi.

## G. Sistematika Penulisan

Penulisan hasil penelitian ini secara garis besar disusun secara sistematis yang terbagi dalam 4 (empat) bab. Bab I Menguraikan Pendahuluan, permasalahan yang diangkat, kerangka teori yang secara singkat memberikan penjabaran mengenai pengertian dan tujuan *cyber terrorism,* menjabarkan mengenai pengertian dan ruang lingkup kebijakan kriminalisasi serta kerangka konseptual yang digunakan dalam

membahas permasalahan-permasalahan seperti yang telah diuraikan sebelumnya.

Bab II menjabarkan tentang Tinjauan Pustaka yang ada kaitannya dengan judul penelitian ini yaitu pengertian/ruang lingkup *cyber crime* dan juridiksinya, pengertian terrorisme, pengertian/ruang lingkup *cyber terrorism*, dan pengertian kebijakan kriminal.

Bab III dikemukakan hasil penelitian yang akan menjabarkan permasalahan- permasalahan yang diangkat, diantaranya : 1. kebijakan kriminal pada saat ini dalam menanggulangi tindak pidana *cyber terrorism*, 2. kebijakan kriminal yang akan datang dalam menanggulangi tindak pidana *cyber terrorism*.

Bab IV Penutup yang berisi simpulan yang di dapat dari hasil penelitian ini yang telah dianalisa untuk menjawab permasalahan-permasalahan yang diajukan beserta beberapa saran atas hasil penelitian ini.

# BAB II

# TINJAUAN PUSTAKA

## A. Tinjauan Umum Mengenai Cyber Crime

### A.1. Pengertian c*yber crime* dan *jurisdiksinya*

Teknologi merupakan hasil dari perkembangan budaya, ia dapat menjadi alat perubahan di tengah masyarakat. Kemajuan teknologi merupakan hasil budaya manusia di samping membawa dampak positif, dalam arti dapat didayagunakan untuk kepentingan

manusia juga membawa dampak negatif terhadap perkembangan dan peradaban manusia sendiri. Dampak negatif yang dimaksud adalah yang berkaitan dengan dunia kejahatan.

Pada perkembangannya, dengan ditemukannya komputer sebagai produk ilmu pengetahuan dan teknologi, terjadilah konvergensi antara teknologi komunikasi, media dan komputer menghasilkan sarana dan sistim informasi terbaru yang disebut dengan *internet* atau jaringan internasional (*International Networking),* sebagai sebuah penemuan terbesar abad 20. Internet basisnya adalah komputer, dimana *Personal Computer (PC)* yang dihubungkan dengan menggunakan sebuah sistem jaringan terbaru yang berhubungan langsung dengan satelit komunikasi sehingga terbentuklah jaringan antar *personal computer.*

Berawal dari rangkaian beberapa komputer dari suatu tempat atau ruangan atau gedung yang disebut dengan LAN (*Local Area Network),* sementara di gedung lain ada lagi LAN. Jika beberapa LAN ini digabung atau dirangkai menjadi satu akhirnya menjadi kelompok LAN yang disebut WAN *(Wide Area Network)*. Beberapa WAN ini dapat dirangkai menjadi WAN lagi yang lebih besar dan banyak serta bukan saja berhubungan antar gedung tetapi juga menjadi antar kota, antar propinsi bahkan antar negara yang terangkai menjadi satu, maka disebutlah internet.[49] Internet disebut juga dengan istilah *Net, Online* dan *Web* atau *World Wide Web (WWW)*[50] sebagai ruang yang bebas dan menyediakan akses untuk

---

[49] Al Wisnubroto, 1999, *Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan Komputer*, (Penerbit Universitas Atmajaya: Yogyakarta).

[50] *WWW (World Wide Web)* merupakan sarana internet yang berfungsi sebagai sarana untuk *transfer file, data* dan *software* di internet. WWW ini didesain untuk memudahkan

layanan telekomunikasi dan sumber daya informasi untuk jutaan pemakainya yang tersebar diseluruh dunia.[51]

*The US Supreme Court*[52] mendefinisikan internet sebagai *international network of interconnected computers* yaitu jaringan internasional dari komputer yang saling berhubungan. Dari definisi ini terlihat dimensi internasionalnya yaitu bahwa jaringan antar komputer tersebut melewati batas-batas teritorial suatu negara.

Sementara itu **Agus Raharjo** mendefinisikan internet sebagai jaringan komputer antar negara atau antar benua yang berbasis P*rotocol Transmission Control Protocol/Internet Protoco\l* (TCP/IP).[53] *The Federal Networking Council (FCN)* memberikan definisinya mengenai internet dalam Resolusinya tanggal 24 Oktober 1995. Definisi yang diberikan adalah berikut :

*Internet Refers to the global information system that :*
*(i) is logically linked together by a globally unique address space based in the Internet Protocol (IP) or its bubsequent exstensions/follow-ons:*
*(ii) is able to support communications using the Transmission Control Protocol (TCP/IP) suite or its subsequent extentions/follow-ons, and/or other internet Proocol (IP)-comptible protocols, and*
*(iii) providers, uses or makes accessesible, either publicly or*

---

pengguna dalam melakukan transfer file dan juga ia memperkaya tampilan isi (*content*) internet. Dengan WWW seseorang dapat secara mudah masuk dan terhubung ke internet. Sebagaimana ditulis oleh Asril Sitompul dalam *Hukum Internet, Pengenalan Mengenai Masalah Hukum di Cyberspce*, 2004, (Citra Aditya Bhakti:Bandung), kata pengantar halaman viii.

[51] *My Pesonal Library Online, Cyber Crime*. Dapat dijumpai pada situs internet :http://dhani.singcat.com/internet/modul/php.

[52] Dalam Abdul Wahid dan Moh. Labib, 2005, *Kejahatan Mayantara (Cyber Crime)*, (Refika Aditama:Bandung), halaman 31

[53] Agus Raharjo, 2002, *Cyber Crime-Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, (Citra Aditya Bhakti:Bandung), halaman 59

*privately, high level services layered on the communications and related inftastructure described herein*.[54]

Dengan adanya teknologi informasi dan komunikasi yang modern, manusia mendapatkan kenyamanan dan kemudahan-kemudahan untuk menyebarkan informasi dan menjalin komunikasi dengan orang lain di belahan dunia manapun. Pengaruh internet telah mengubah jarak dan waktu menjadi tidak terbatas. Media internet orang bisa melakukan berbagai aktivitas yang sulit dilakukan dalam dunia nyata (*real*) karena kendala jarak dan waktu. Internet mengubah paradigma komunikasi manusia dalam bergaul, berbisnis, berasmara bahkan dalam menikmati hubungan seks sekalipun.

Penggunaan teknologi internet tidak hanya menyelesaikan persoalan yang rumit secara efektif dan efisien serta membawa dampak positif di berbagai kehidupan, seperti adanya *e-mail, e-commerce, e-learning, "EFTS"* (*Electronic Funds Transfer System* atau "sistem transfer dana elek-tronik"), *"Internet Banking", "Cyber Bank", "On-line Business"* dan sebagainya. Tetapi di sisi lain, juga membawa dampak negatif, yaitu dengan munculnya berbagai jenis *"hitech crime*" dan "*cyber crime*", sehingga dinyatakan bahwa *"cyber crime is the most recent type of crime"* [55] dan juga oleh Panitia Kerja Perlindungan Data *(Data Protection Working Party)* Dewan Eropa dinyatakan bahwa *"cybercrime is part of the seamy side of the Information Society"* (*Cybercrime* merupakan bagian sisi paling buruk

[54] Dalam Agus Raharjo, 2002, *Cyber Crime-Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, (Citra Aditya Bhakti:Bandung), halaman 60

[55] Seperti dikemukakan oleh Barda Nawawi Arief yang mengutip pendapat V.D. Dudeja dalam *Cyber Crimes and Law*, Volume 2, 2002, p. v., dalam *Antisipasi Hukum Pidana dan Perlindungan Korban Cyber Crime di Bidang Kesusilaan*", makalah pada Seminar "Kejahatan Seks melalui Cyber Crime dalam Perspektif Agama, Hukum, dan Perlindungan Korban", FH UNSWAGATI, di Hotel Zamrud Cirebon, 20 Agustus 2005.

dari masyarakat informasi*")*[56]. Kecanggihan teknologi ini juga berpotensi membuat orang cenderung melakukan perbuatan yang bertentangan dengan norma-norma sosial yang berlaku, kemajuan teknologi informasi dan komunikasi telah membawa perubahan yang mendasar terhadap sensitifitas moral masyarakat kita ketika teknologi itu disalahgunakan.

Penggunaan teknologi internet telah membentuk masyarakat dunia baru yang tidak lagi dihalangi oleh batas-batas teritorial suatu negara yang dahulu ditetapkan sangat esensial sekali yaitu dunia maya, dunia yang tanpa batas atau realitas virtual (*virtual reality*). Inilah sebenarnya yang dimaksud dengan *Borderless World*.[57]

Dalam menggunakan jasa pada dunia maya tersebut masyarakat cenderung bebas berinteraksi, beraktifitas dan berkreasi yang hampir sempurna pada semua bidang. Masyarakat sedang membangun kebudayaan baru di ruang maya yang dikenal dengan istilah *Cyberspace.* Menurut ***Howard Rheingold*** bahwa *Cybescpace* adalah sebuah ruang imajiner atau ruang maya yang bersifat artificial, dimana setiap orang melakukan apa saja yang biasa dilakukan dalam kehidupan sosial sehari-hari dengan cara-cara yang baru.[58] *Cyber space* merupakan tempat kita berada ketika kita mengarungi dunia informasi global interaktif yang bernama internet.

Istilah ini pertamakali digunakan oleh **William Gibson** dalam

---

[56] *Data Protection Working Party, Council of Europe*, *"Opinion 4/2001 On the Council of Europe's Draft Convention on Cyber-crime",* adopted on 22 March 2001, 5001/01/EN/Final WP 41, page. 2

[57] Onno W. Purbo dalam Agus Raharjo, 2002, *Cybercrime, Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi,* (Citra Aditya Bahkti : Bandung, halaman 5)

[58] Dalam Yasraf Amir Pialang sebagaimana dikutip oleh Abdul Wahid, *Kejahatan Mayantara*, 2005, (Refika Aditama:Bandung, Halaman 32)

novel fiksi ilmiahnya (*science fiction*), kata *cyber space* ini ditemukan dalam novelnya yang berjudul *Neuromancer* dan *Virtual Light*.[59] Istilah ini memang pertamakali dipakai oleh **William Gibson**, tetapi dalam konteks internet, **John Perry Barlow** mengklaim sebagai pengguna pertama. Pada waktu itu istilah *cyber space* oleh **William Gibson** belum ditunjukan pada interaksi yang terjadi melalui jaringan komputer. Istilah *cyberspace* yang benar-benar ditujukan pada interaksi yang terjadi di internet adalah pada tahun 1990 ketika **John Perry Barlow**[60] untuk pertama kalinya mengaplikasikan istilah *cyberspace* untuk dunia yang terhubung atau *online* ke internet.[61]

Menurut **John Suler** dalam artikelnya yang berjudul *The Psykology of Cyberspace, Overview And Guided Tour* menganggap bahwa *cyberspace* adalah ruang psikologis, dan sebagai ruang psikologis, keberadaannya tidaklah tergantung pada batas-batas konvensional mengenai keberadaan benda-benda berwujud. Bedanya dengan benda yang wujudnya berada dalam dunia nyata, *cyberspace* sebagai hasil teknologi tidak berada dalam dunia nyata tapi ia betul-betul ada.[62]

---

[59] Dalam Agus Raharjo, 2002, *Cyber crime, Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi,* (Citra Aditya Bhakti : Bandung, halaman 4-5

[60] *Cyber space* menurut *John Perry Barlow* adalah ruang yang muncul ketika anda sedang menelpon, yaitu setiap ruang informasi tetapi ia adalah ruang interaksi interaktif yang diciptakan oleh media yang begitu padat sehingga disana ada kesadaran tentang kahadiran orang lain, seperti dikutip oleh Agus Raharjo, 2002, *Cybercrime, Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi,* (Citra Aditya Bahkti : Bandung), halaman 92

[61] *The Growth And Development of Cyberspace Law in the United States : Highlights of the past decade, The UCLA Online institute for Cyberspace Law and Policy*, seperti ditulis oleh Agus Raharjo, 2002, *Cybercrime, Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi,* (Citra Aditya Bhakti : Bandung), halaman 93.

[62] Dalam Agus Raharjo, 2002, *Cybercrime, Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi,* (Citra Aditya Bhakti : Bandung), halaman 93

Internet merupakan ruang yang bebas karena tidak ada kontrol dari manapun dan tidak ada pusatnya, sehingga ketika pemerintah suatu negara hendak membatasi dengan cara melakukan sensor, mendapat tanggapan yang cukup serius dari para cyberis diantaranya **John Perry Barlow** dengan mengeluarkan *Declaration Of Independent of Cyberspace* sebagai bentuk protesnya. Isi deklarasi tersebut lebih ditekankan pada kebebasan ruang saja yaitu kebebasan di *cyberspace*, sedangkan kebebasan para penghuninya tidak menjadi perhatian pokok.

Realitas atau alam baru yang terbentuk oleh medium internet ini pada perkembangannya menciptakan masyarakat baru sebagai warganya yang dalam istilah pengguna dan pemerhati internet lazim disebut *Netizen*. *Cyberspace* menawarkan manusia untuk "hidup" dalam dunia alternatif. Sebuah dunia yang dapat mengambil alih dan menggantikan realitas yang ada, yang lebih menyenangkan dari kesenangan yang ada, yang lebih fantastis dari fantasi yang ada, yang lebih menggairahkan dari kegairahan yang ada, sehingga kehidupan manusia tidak lagi hanya merupakan aktifitas yang bersifat fisik dalam dunia nyata (*real*) belaka akan tetapi menjangkau juga aktifitas non fisik yang dilakukan secara virtual.

*Cyberspace* telah pula menciptakan bentuk kejahatan baru, sebagai dampak negatif yang ditimbulkan oleh perkembangan dan kemajuan teknologi informasi dan telekomunikasi yaitu kejahatan yang berkaitan dengan aplikasi internet yang dalam istilah asing disebut *cyber crime* yaitu segala kejahatan yang dalam modus operandinya menggunakan fasilitas internet. Kejahatan ini sering dipersepsikan sebagai kejahatan yang dilakukan dalam ruang atau wilayah siber. *Cyber crime* merupakan kejahatan bentuk baru yang sama sekali berbeda dengan bentuk-bentuk kejahatan konvensional

yang selama ini dikenal. Dengan menggunakan internet, jenis kejahatan *cyber crime* tidak dapat sepenuhnya terjangkau oleh hukum yang berlaku saat ini bahkan tidak dapat sepenuhnya diatur dan dikontrol oleh hukum.

Dalam beberapa literatur, *cyber crime* sering diidentikan dengan *computer crime*. Menurut Kepolisian Inggris, *cyber crime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital. [63]

Selain itu di dalam beberapa literatur, *cyber crime* juga disebut sebagai dimensi baru dari *hi-tech crime, transnational crime* atau dimensi baru dari *white collar crime*. **Volodymyr Golubev** menyebutnya sebagai "*the new form of anti-social behaviour*"[64], sedangkan **Barda Nawawi Arief** menggunakan istilah "*kejahatan mayantara*" atau "*tindak pidana mayantara*" untuk menunjuk jenis kejahatan ini. Menurut beliau, dengan istilah "*tindak pidana mayantara*" dimaksudkan identik dengan tindak pidana di ruang siber (c*yber space*).[65]

Tentang kejahatan ini **Muladi** mengatakan bahwa, "sampai saat ini belum ada definisi yang seragam tentang *cyber crime* baik secara nasional maupun global. Sekalipun demikian kita bisa mendefinisikan beberapa karakteristik tertentu dan merumuskan

---

[63] Ade Maman Suherman sebagaimana dikutip oleh Abdul Wahid, *Kejahatan Mayantara*, 2005, (Refika Aditama:Bandung, Halaman 32)

[64] Volodymyr Golubev, *Cyber-crime and legal problems of internet usage*, p.1 sebagaimana dikutip oleh Barda Nawawi Arief dalam Sari kuliah Perbandingan Hukum Pidana, 2002, (Raja Grafindo Persada:Jakarta), halaman 252

[65] Dalam Barda Nawai Arief, 2003, *Kapita Selekta Hukum Pidana*, (Citra Aditya Bhakti : Bandung), halaman 239.

suatu definisi. Kebanyakan masih menggunakan *soft law* berbentuk *code of conduct* seperti di Jepang dan Singapura.[66]

Dikemukakan oleh **Muladi** bahwa *cyber crime* merupakan suatu istilah umum yang pengertiannya mencakup berbagai tindak pidana yang dapat diketemukan dalam KUHP atau Perundang-undangan pidana lain yang menggunakan teknologi komputer sebagai suatu komponen sentral. Dengan demikian *cyber crime* bisa berupa : tindakan sengaja merusak *property*, masuk tanpa ijin, pencurian hak milik intelektual, perbuatan cabul, pemalsuan, pornografi anak, pencurian dan beberapa tindak pidana lainnya.

Hal yang sama juga diungkapkan oleh **Agus Raharjo** bahwa istilah *cyber crime* sampai saat ini belum ada kesatuan pendapat bahkan tidak ada pengakuan internasional mengenai istilah baku, tetapi ada yang menyamakan istilah *cyber crime* dengan *computer crime*.[67] Demikian juga sampai saat ini sepengetahuan penulis belum ada istilah baku atau definisi secara juridis untuk menunjuk jenis kejahatan ini, dan lebih dikenal sebagai *cyber crime*.

Berdasarkan modus operandinya, *cyber crime* terdiri dari dua jenis kejahatan, yaitu :

a. Kejahatan yang sasaran/targetnya adalah fasilitas serta sistem teknologi komunikasi informasi. Para pelaku menggunakan sarana ini untuk menyerang atau merusak sarana teknologi informasi lainnya yang menjadi target. Pada posisi ini

---

[66] Dapat dijumpai dalam harian Suara Merdeka edisi 24 juli 2002.

[67] Dalam Agus Raharjo, 2002, *Cybercrime, Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi,* (Citra Aditya Bhakti : Bandung), halaman 227

komputer/internet adalah alat sekaligus korban kejahatan. Kejahatan ini lebih dikenal *Hacking/cracking* yang menyerang program-program operasi jaringan komputer. Ini mempunyai sifat sebagai kejahatan baru (*new category of crime*)

b. Kejahatan umum/biasa yang difasilitasi oleh tekhnologi komunikasi informasi. Jenis kejahatan ini telah ada sebelum teknologi informasi bergerak menuju kearah penyalahgunaannya, contohnya penipuan kartu kredit, pengancaman, pencemaran nama baik, terorisme, pornografi dan sebagainya. Ini merupakan kejahatan yang bersifat biasa *(Ordinary crime)* yang pengaturannya telah terdapat dalam KUHP.[68]

Dalam perspektif hukum pidana, kejahatan ini ada yang merupakan kejahatan konvensional tetapi dengan modus baru seperti pornografi, penipuan, pencemaran nama baik, *cyber sex,* CT dan sebagainya. Disamping itu juga ada kejahatan baru yang tidak dikenal sebelumnya seperti *hacking.*

Kemajuan teknologi ternyata tidak digunakan sebagai sarana positif untuk meningkatkan kualitas kehidupan, tetapi justru digunakan sebagai sarana negatif yang dapat membawa dampak negatif.

Masalah kejahatan di internet *(cyber crime)* ternyata telah

---

[68] Dikutip oleh Tim Peneliti, *Tindak Pidana Teknologi Komunikasi Informasi/cyber crime dan Upaya Penaggulangannya* (Laporan hasil Penelitian), Penelitian Dan Pengembangan Ilmu Pengetahuan Dan Tehnologi Kepolisian Perguruan Tinggi Ilmu Kepolisian (PPITK-PTIK), Jakarta, Desember, 2003, halaman 41, Dalam Did Dik M. Arief Mansyur dan Elisatris Gultom, *Cyber Law aspek hukum Teknologi Informasi,* 2005, (Refika Aditama;Bandung), halaman 87

menimbulkan keprihatinan dan mengundang perhatian dari berbagai pihak baik secara nasional maupun internasional. Kejahatan siber sudah menjadi issue internasional, hal ini pula yang mendorong *Council of Europe* memprakarsai pembentukan Konvensi tentang Kejahatan *Cyber*.

Tindakan Internasional selanjutnya guna lebih merinci segala hal yang berkaitan dengan kejahatan *cyber* adalah dengan disusunnya Draft *Convention on Cyber Crime of Council of Europe* yang dimulai pada bulan April 2000. Draft konvensi ini dipublikasikan lewat internet untuk mendapat tanggapan dari berbagai pihak secara Internasional. Setelah melalui berbagai debat publik di internet, draft mengalami berbagai perubahan dan penyesuaian sesuai dengan usul dan tanggapan, maka akhirnya draft terakhir disetujui dan menjadi *Convention Cybercrime* atau *Council of Europe Cybercrime Convention* yang ditandatangani di Budapest tanggal 23 November 2001.

Dalam konvensi tentang kejahatan siber, disebutkan jenis-jenis kejahatan tersebut, yaitu :

1. *Illegal access (Art.2);*
2. *Illegal interception (Art.3);*
3. *Data interference (Art.4);*
4. *System interference (Art.5);*
5. *Misuse of devices (Art.6);*
6. *Computer-related forgery (Art.7);*
7. *Computer related fraud (Art.8);*
8. *Offences related to child pornography (Art.9);*
9. *Offences related to infringements of copyrights and related rights (Art.10);*
10. *Attempt and aiding or abetting (Art.11)*.

Namun demikian karena modus operandi dari kejahatan semakin berkembang seiring dengan perkembangan ilmu

pengetahuan dan teknologi sehingga beberapa jenis kejahatan yang terdapat dalam konvensi tersebut belum dapat mengcover berbagai perkembangan jenis kejahatan yang ada dan mungkin akan ada.

Kecemasan dan kekhawatiran akan *cyber crime* juga terungkap dalam sebuah makalah yang disampaikan oleh *Information Technology Association of Canada (ITAC)* dalam "*International Informaion Industry Congress (IIIC) 2000 Milenium Congress di Quebec 19* September 2000 dalam sebuah makalahnya yang berjudul *"IIIC Common Views Paper on Cyber Crime*" yang menyatakan bahwa "*Cyber crime is real and growing threat to economic and social development around the world, information technology touches every aspect of human life and so can electronically enabled crime"*

Kongres PBB mengenai "*The Prevention of Crime and the Treatment of Offenders*"[69] (yang diselenggarakan tiap 5 tahun) telah pula membahas masalah *cyber crime* ini sebanyak tiga kali, yaitu pada Kongres VIII/1990 di Havana-Kuba, Kongres X/2000 di Wina, dan terakhir pada Kongres XI/2005 di Bangkok (tanggal 18-25 April 2005).

Pada Konggres VIII PBB, terhadap kejahatan yang berkaitan dengan komputer *(computer related crimes)* perlu dilakukan upaya penanggulangannya dengan mengajukan beberapa kebijakan, yaitu :

1. Menghimbau negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan komputer yang lebih efektif dengan mempertimbangkan beberapa langkah yaitu :
   a. Melakukan modernisasi hukum pidana materiil dan hukum acara pidana.
   b. Mengembangkan tindakan-tindakan pencegahan dan

[69] Dalam Kongres XI, judul kongres berubah menjadi *Congress on Crime Prevention and Criminal Justice*

pengamanan komputer.

c. Melakukan langkah-langkah untuk membuat peka (sensitif) warga masyarakat, aparat pengadilan dan penegak hukum, terhadap pentingnya pencegahan kejahatan yang berhubungan dengan komputer. (untuk selanjutnya dalam kutipan ini disingkat dengan inisial "*Cyber Crime* (CC)".
d. Melakukan upaya-upaya pelatihan (training) bagi para hakim, pejabat dan aparat penegak hukum mengenai kejahatan ekonomi dan "*Cyber Crime* (CC)".
e. Memperluas "*rules of ethics"* dalam penggunaan komputer dan mengajarkannya melalui kurikulum informasi.
f. Mengadopsi kebijakan perlindungan korban "*Cyber Crime* (CC)" sesuai dengan deklarasi PBB mengenai korban dan mengambil langkah-langkah untuk mendorong melaporkan adanya "*Cyber Crime* (CC)"

2. Menghimbau negara anggota meningkatkan kegiatan nasional dalam upaya penanggulangan "*Cyber Crime* (CC)".
3. Merekomendasikan kepada Komite Pengendalian Dan Pencegahan Kejahatan (*Commitee of Crime Prevention And Control* ) PBB untuk :
   a. Menyebarluaskan pedoman dan standar untuk membantu negara anggota menghadapi "*Cyber Crime (CC)*" ditingkat nasional, regional dan internasional;
   b. Mengembangkan penelitian dan analisis lebih lanjut guna menemukan cara-cara baru menghadapi problem " *Cyber Crime (CC)"* dimasa yang akan datang;
   c. Mempertimbangkan "*Cyber crime (CC)*' sewaktu meninjau pengimplementasian perjanjian ekstradisi dan bantuan kerjasama dibidang penanggulangan kejahatan[70].

Pada Konggres PBB ke –10 (*Tenth United Nations Conggress on The Prevention of Crime and the Treatment of Offender)* di Wina (Vienna) pada tanggal 10-17 April 2000, c*yber crime* dijadikan topik bahasan tersendiri dengan judul C*rimes Related to Computer Network*, menyebutkan hal-hal sebagai berikut :

[70] Dalam Barda Nawawi Arief, 2003, *Kapita Selekta Hukum Pidana*, (Citra Aditya Bhakti : Bandung), halaman 244.

** Cyber crime refers to any crime that can be commited by means of a computer system or network, in a computer system or network or against a computer system or network. In principles, it encompasses any crime acpable of being commited in en elecronic environment. In this paper, "rime" refers to form of behavior generally defined as illegal, or likely to be criminalized within a shord period of time. Certain conduct may be criminalized in one state where it is not in others but, as explained in paragraph 13, a common understanding has developed on certain internatonal forums about which behaviour I relation to computer system and networks should be criminalized.*[71]

** Two sub categories of cyber crimes exist*[72] *:*

*1) Cyber crime in a narrow sense "Computer crime") : any illegal behaviour directed by means of elecronic operations that targets the security of computer systems and the data processed by them;*

*2) Cyber crime in broader sense ("computer-related-crime"): any illegal behaviour commited by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network.*

Dalam "*background paper*" lokakarya "*Measures to Combat Computer-Related Crime*" Kongres XI PBB di Bangkok (tanggal 18-25 April 2005) menyatakan bahwa "teknologi baru yang mendunia di bidang komunikasi dan informasi memberikan "bayangan gelap" (*a dark shadow*) karena memungkinkan terjadinya bentuk-bentuk eksploitasi baru, kesempatan baru untuk aktivitas kejahatan, dan bahkan bentuk-bentuk baru dari kejahatan".[73]

---

[71] Dokumen United Nations A/CONF.187/10, (*Tenth United Nations Conggress on The Prevebtion of Crime and the Treatment of Offender)* di Wina (Vienna) pada tanggal 10-17 April 2000, halaman 4

[72] Dokumen United Nations A/CONF.187/10, (*Tenth United Nations Conggress on The Prevebtion of Crime and the Treatment of Offender)* di Wina (Vienna) pada tanggal 10-17 April 2000, halaman 5

[73] Dokumen United Nations A/CONF.203/14, (*Eleventh United Nations Congress on Crime Prevention and Criminal Justice)*, Bangkok, 18-25 April 2005, Background paper, Workshop

Semakin berkembangnya *cyber crime* terlihat pula dari munculnya berbagai istilah seperti ***Cyber Terrorism****, Cyber Stalking, Cyber Sex, Cyber Harrasment, Hacking, Cracking, Carding, Cyber Pornography, Cyber Defamation, Cyber-Criminals, Economic Cyber Crime*, *EFT (Electronic Funds Transfer) Crime, Cybank Crime, Internet Banking Crime, On-Line Business Crime, Cyber/Electronic Money Laundering, Hitech WWC (white collar crime), Internet fraud* (antara lain *Bank fraud, Credit card fraud, On-line fraud)* dan sebagainya.

Salah satu masalah *cyber crime* yang juga sangat meresahkan dan mendapat perhatian berbagai kalangan adalah masalah CT.

Dengan memperhatikan jenis-jenis kejahatan sebagaimana dikemukakan di atas, dapat digambarkan bahwa *cyber crime* memiliki ciri-ciri khusus yaitu :[74]

1. *Non-violence* (tanpa kekerasan);
2. Sedikit melibatkan kontak fisik;
3. Menggunakan peralatan (*equipment*) dan teknologi;
4. Memanfatkan jaringan telematika (telekomunikasi, media dan informatika) global.

Kejahatan-kejahatan sebagaimana disebutkan di atas tidak saja bersifat “baru dan modern” tetapi sekaligus menimbulkan

---

6: *Measures to Combat Computer-related Crime : “The worldwide multiplication of new information and communication technologies also casts a dark shadow: it has made possible new forms of exploitation, new opportunities for criminal activity and indeed new forms of crime*”. dalam Barda Nawawi Aief, *Antisipasi Hukum Pidana Dan Perlindungan Korban Cyber Crime Di Bidang Kesusilaan,* makalah pada Seminar “Kejahatan Seks melalui Cyber Crime dalam Perspktif Agama, Hukum, dan Perlindungan Korban”*,* F.H UNSWAGATI, di Hotel Zamrud Cirebon, tanggal 20 Agustus 2005

[74] Dalam Tb. Ronny Rahman Nitibaskara, 2001, *Ketika Kejahatan Berdaulat*, (Peradaban : Jakarta), halaman 45

dampak yang sangat luas karena tidak saja dirasakan secara nasional tetapi juga internasional. Sehingga sangat wajar jika *cyber crime* dimasukan kedalam jenis kejahatan yang sifatnya internasional berdasarkan *United Nation Convention, Against Transnational Organized Crime (Palermo Convention*) Nopember 2000 dan berdasarkan Deklarasi ASEAN tanggal 20 Desember 1997 di Manila.

Dalam *Palermo Convention* ditetapkan bahwa kejahatan-kejahatan yang termasuk *transnasional crime* adalah :

1. Kejahatan Narkotika;
2. Kejahatan *Genocide*;
3. Kejahatan uang Palsu;
4. Kejahatan dilaut bebas;
5. *Cyber Crime*.

Sedangkan dalam Deklarasi ASEAN di Manila, yang termasuk *transnational crime* adalah :

1. *Illicit Drug Trafficking;*
2. *Money Laundering;*
3. *Terrorism;*
4. *Arm Smuggling;*
5. *Trafficking in Person;*
6. *Sea Piracy;*
7. *Currency Counterfeiting;*
8. *Cyber Crime*

Sehubungan dengan adanya unsur internasional dari kejahatan di dunia maya *(cyber crime*) tentunya akan menimbulkan masalah tersendiri, khususnya berkenaan dengan masalah yurisdiksi. Yurisdiksi merupakan hal yang sangat *crucial* sekaligus kompleks khususnya berkenaan dengan pengungkapan kejahatan-kejahatan di dunia maya yang bersifat internasional *(international cyber crime)*. Dengan adanya kepastian yurisdiksi maka suatu negara memperoleh pengakuan dan kedaulatan penuh untuk

berbagai aturan dan kebijakannya secara penuh.

Dalam *Black Laws Dictionary,* disebutkan *jurisdiction is* :[75]

a. *The word is a term of large and comprehensive import, and embraces every kind of judicial action;*
b. *It is the uthority by which couerts and judicial officers take cognizance of end decide cases;*
c. *The legal right by which judges exercise their autority;*
d. *Its exists when courts has cognizance of class o cases involved, proper parties are presents, and point to be decide is within powers of courts;*
e. *Power and authority of courts to har and determine a juicial procceding;*
f. *The right of power of a courts to adjudicate concerning the subject matter in a given case.*

Dalam *Encyclopedia of International Law* definisi jurisdiksi adalah :

*"juisdiction is the authority of the state to affect legal interests. International Law defines the jurisdiction a state may exercise over persons or property with connection that a beyond that state's own territory."*

**Cheriff Bassiouni** mendefinisikan yurisdiksi sebagai "*the authority of states to prescribe their law, to subjects persons and things to adjudication in their courts and other tribunals, and to enforce their law, both judicial and non judicially*"

Yurisdiksi menurut Kamus Bahasa Indonesia[76], didefinisikan sebagai :

1. kekuasaan mengadili lingkup kuasa kehakiman; peradilan

2. Lingkungan hak dan kewajiban serta tanggungjawab disuatu

[75] Henry Campbell Black, M.A. Fifth Edition, St. Paul Minn, West Publishing Co, 1979 page 766

[76] Kamus Besar Bahasa Indonesia, 1997, edisi kedua, Departemen Pendidikan Nasional, (Balai Pustaka: Jakarta), halaman 1134

wilayah atau lingkungan tertentu; kekuasaan hukum.

Yurisdiksi ini merupakan refleksi dari prinsip dasar kedaulatan negara, kesamaan derajat negara, dan prinsip tidak campur tangan, sebagai suatu bentuk kedaulatan yang vital dan sentral yang dapat mengubah, menciptakan atau mengakhiri suatu hubungan atau kewajiban hukum.[77]. Yurisdiksi adalah kekuasaan atau kompetensi hukum negara terhadap orang, benda atau peristiwa (hukum) atau berkaitan dengan masalah berlakunya hukum disuatu wilayah/kedaulatan negara yang merdeka yang terdiri atas wilayah darat, laut, dan wilayah udara yang ada di atas wilayah suatu negara.

Dalam hukum pidana terdapat asas-asas yang membatasi berlakunya hukum pidana itu sendiri yang dibedakan berdasarkan waktu (*tempus delicti*) untuk menentukan apakah suatu undang-undang dapat diterapkan terhadap suatu tindak pidana, dan berdasarkan lokasi/tempat *(locus delicti*) untuk menentukan apakah undang-undang pidana Indonesia dapat diperlakukan serta pengadilan mana yang berkompeten untuk mengadili orang yang melakukan suatu tindak pidana (kompetensi relatif).

Dalam pembatasan terhadap berlakunya hukum pidana berdasarkan lokasi atau tempat, terdapat beberapa asas yang dapat digunakan yaitu :

1. Asas teritorial.

Asas ini berkaitan dengan tempat terjadinya delik, yang

[77] Shaw, Interational Law, London : Butterworths, 1986, halaman 342 sebagaimana dikutip oleh Huala Adolf, *Aspek-Aspek Negara dalam Hukum Internasional*, (Rajawali Pers :Jakarta), 1996, halaman 143.

diatur dalam Pasal 2 KUHP yang berbunyi sebagai berikut :[78]

> "Aturan pidana dalam undang-undang Indonesia berlaku bagi setiap orang yang melakukan sesuatu tindak pidana di wilayah Indonesia"

Berdasarkan prinsip ini negara dapat menerapkan yurisdiksi nasionalnya terhadap semua orang (baik warga negara Indonesia maupun warga negara asing), badan hukum atau semua benda yang ada didalamnya. Asas ini diperluas oleh pasal 3 KUHP yang menyebutkan bahwa :

> " Peraturan Pidana Indonesia dapat diterapkan kepada setiap orang yang berada diluar Indonesia, melakukan suatu tindak pidana di dalam perahu Indonesia".

2. Asas Personal atau asas Nasional Aktif

Ketentuannya terdapat dalam Pasal 5 KUHP, yaitu hukum pidana Indonesia berlaku bagi setiap warga negara Indonesia yang melakukan tindak pidana baik di dalam maupun di luar negeri.

Prinsip ini menyatakan bahwa negara dapat memberlakukan yurisdiksi nasionalnya terhadap warga negaranya yang melakukan tindak pidana sekalipun tindak pidana itu dilakukan dalam yurisdiksi negara lain.

3. Asas Perlindungan (Nasional Pasif)

Ketentuannya terdapat dalam pasal 4 KUHP, yaitu hukum pidana Indonesia berlaku bagi setiap orang yang diluar Indonesia menyerang/merugikan kepentingan nasional tertentu yang ditetapkan dalam KUHP atau undang-undang di luar KUHP (asas nasinal pasif), yaitu :

---

[78] Lihat Moeljatno, KUHP : *Kitab Undang-Undang Hukum Pidana*, 2001, Cet.21, (PT. Bumi Aksara:Jakarta), Halaman 3

a. Yang berkaitan dengan kepentingan nasional tertentu,

berupa :[79]

1) Kejahatan mengenai mata uang, uang kertas, materai, dan merek (pasal 4 ke-2 KUHP) dan
2) Pemalsuan surat/sertifikat hutang atas tanggungan Indonesia atau tanggungan daerah/ bagian daerah Indonesia (Pasal 4 ke-3 KUHP).

b. Yang berkaitan dengan kepentingan internasional tertentu,

disebutkan dalam pasal 4 k3-4 KUHP, berupa :

3) Kejahatan yang berkaitan dengan pembajakan laut dalam (Pasal 438, Pasal 444- Pasal 446);
4) Penyerahan perahu dalam kekuasaan bajak laut (Pasal 447);
5) Pembajakan pesawat udara (Pasal 479 j);
6) Kejahatan yang mengancam penerbangan sipil (Pasal 479 I sampai dengan 0).

Dari uraian di atas ketentuan tersebut Memuat prinsip bahwa peraturan hukum Pidana Indonesia berlaku terhadap tindak pidana yang menyerang kepentingan hukum negara Indonesia, baik dilakukan oleh warga negara Indonesia atau bukan yang dilakukan di luar Indonesia. Prinsip ini menyatakan bahwa suatu negara mempunyai hak untuk menerapkan hukum (pidana) nasionalnya pada pelaku tindak pidana sekalipun dilakukan di luar wilayah negara tersebut jika tindak pidana tersebut mengancam keamanan dan keutuhan negara yang bersangkutan.

4. Asas Universal

[79] Barda Nawawi Arief, 2005, *Pembaharuan Hukum Pidana, Persepektif Kajian Perbandingan.* PT. Citra Adyta Bakti :Bandung. Hal 43-44

Asas ini menyatakan peraturan-perturan hukum Pidana Indonesia berlaku terhadap tindak pidana baik dilakukan di dalam negeri maupun di luar negeri, baik dilakukan oleh warga negara Indonesia maupun warga negara asing, yaitu tindak pidana yang dimaksud adalah tindak pidana sebagaimana tersebut dalam Pasal 4 sub 2 dan sub 4 KUHP. Kepentingan yang dilindungi adalah kepentingan Internasional dari tindak pidana yang membahayakan nilai-nilai yang universal dan kepentingan umat manusia.

Sedangkan untuk menetapkan *locus delicti* (lokasi/tempat), dikenal ada tiga (3) teori, yaitu :

1. Teori Perbuatan Materil

   Bahwa tempat terjadinya tindak pidana ditentukan oleh perbuatan jasmaniah yang dilakukan oleh sipembuat dalam melakukan tindakannya tersebut.

2. Teori Instrumen (alat)

   Bahwa tempat terjadinya tindak pidana adalah tempat bekerjanya alat yang digunakan oleh sipembuat yang dapat berupa benda atau orang yang dapat dipertanggungjawabkan

3. Teori Akibat

   Bahwa tempat terjadinya suatu tindak pidana adalah didasarkan pada tempat terjadinya akibat dari perbuatannya, sehingga besar kemungkinan terjadi pelaku berada diwilayah yang berbeda dengan akibat yang timbul dari perbuatannya.

Dalam perkembangannya seiring dengan terjadinya kemajuan di berbagai bidang, masalah jurisdiksi dan teori-teori tentang jurisdiksi tersebut banyak mengalami perubahan di dalam penerapannya, apalagi dengan keberadaan internet sebagai suatu

lingkungan yang tanpa batas. Harus diakui bahwa untuk menerapkan jurisdiksi yang tepat dalam kejahatan-kejahatan di dunia maya (*cybercrime*) bukanlah merupakan pekerjaan yang mudah, karena jenis kejahatannya bersifat transnasional yang melewati batas-batas negara, sehingga banyak bersinggungan dengan kedaulatan banyak negara khususnya sistim hukum negara lain.

Yurisdiksi suatu negara dalam pengertian konvensional, yang prinsip-prinsipnya telah diakui oleh hukum Internasional didasarkan pada batas-batas geografis, sementara komunitas multimedia bersifat internasional, multi yurisdiksi dan tanpa batas, sehingga sampai saat ini belum dapat ditentukan secara pasti bagaimana yurisdiksi suatu negara atau suatu forum yang berlaku terhadap komunikasi multimedia sebagai salah satu pemanfaatan teknologi informasi.[80]

Membicarakan masalah jurisdiksi-cyber pada hakekatnya berkaitan dengan masalah kekuasaan atau kewenangan, yaitu siapa yang berkuasa/berwenang mengatur dunia internet. Mengenai masalah jurisdiksi di dunia internet, ada beberapa pendapat sarjana yang antara lain didasarkan pada prinsip-prinsip jurisdiksi konvensional, namun ada pula yang mengemukakan teori-teori jurisdiksi modern.

**Masaki Hamano** dalam tulisannya yang berjudul "*Comparative Study in the Approach to Jurisdiction in Cyberspace*"[81]

---

[80] Tien S. Saefullah, *Yurisdiksi Sebagai Upaya Penegakan Hukum Dalam Kegiatan Cyberspace*, artikel dalam *Cyber Law :Suatu Pengantar*, (ELIPS: Jakarta), 2002, halaman 96.

[81] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, 2003, (Citra Aditya Bhakti: Bandung ), halaman 246.

mengemukakan terlebih dahulu adanya jurisdiksi yang didasarkan pada prinsip-prinsip tradisional atau jurisdiksi tradisional yang berkaitan dengan batas-batas kewenangan negara dalam tiga bidang penegakan hukum, yaitu :

1. Jurisdiksi legislatif (*Legislative Jurisdiction* atau *Jurisdiction to Prescribe*) yaitu yurisdiksi untuk menetapkan ketentuan pidana atau kewenangan pembuat hukum substantive.
2. Jurisdiksi Judisial (*Judicial Jurisdiction atau Jurisdiction to Adjudicate*) yaitu jurisdiksi untuk memaksakan ketentuan hukum oleh badan peradilan atau disebut juga kewenangan untuk mengadili atau menerapkan hukum.
3. Jurisdiksi eksekutif (*Executive Jurisdiction* atau *Jurisdiction to enforce*) yaitu yurisdiksi untuk melaksanakan ketentuan yang telah ditetapkan oleh badan legislatif atau berkaitan dengan kewenangan untuk melaksanakan/memaksakan kepatuhan hukum yang dibuatnya.

**Barda Nawawi Arief** dalam tulisannya mengatakan, bahwa **Masaki Hamano** membedakan pengertian "*Cyberjurisdiction*" dari sudut pandang dunia *cyber*/virtual dan dari sudut hukum. Dari sudut dunia virtual, *"cyberjurisdiction"* sering diartikan sebagai kekuasaan sistem operator dan para pengguna (*users*) untuk menetapkan aturan dan melaksanakannya pada masyarakat di ruang siber atau virtual, dari sudut hukum "*cyberjurisdiction"* atau "*jurisdiction in cyberspace"* adalah kekuasaan fisik pemerintah dan kewenangan mengadili terhadap pengguna internet atau terhadap aktifitas mereka

di ruang siber (*Phisical government's power and court's authority over netusers or their activity in cyberspace)*.[82]

Seperti halnya yang disebutkan **Masaki Hamano** di atas, **Darrel Menthe** juga membedakan tiga jenis jurisdiksi yang diakui secara internasional yaitu Jurisdiksi Legislatif (*Legislative Jurisdiction* atau *Jurisdiction to Prescribe,* Jurisdiksi Judisial (*Judicial Jurisdiction atau Jurisdiction to Adjudicate*), dan Jurisdiksi Eksekutif (*Executive Jurisdiction* atau *Jurisdiction to enforcer*).[83]

Dalam kegiatan di *cyberspace*, **Darrel Menthe** menyatakan bahwa yurisdiksi di *cyberspace* membutuhkan prinsip-prinsip yang jelas yang berakar dari hukum Internasonal, dan hanya melalui prinsip-prinsip yurisdiksi dalam hukum Internasioanl ini negara-negara dapat dihimbau untuk mengadopsi pemecahan yang sama terhadap pertanyaan mengenai yurisdiksi di internet.[84]

Untuk kasus-kasus di *cyberspace*, **Menthe** menunjuk pada beberapa teori yang berlaku di Amerika Serikat, yaitu [85]:

1. *The Theory of The Uploader and the Downloader*.

   Berdasarkan teori ini, bahwa selama berinteraksi di dunia *cyber* ada dua hal utama yaitu *uploader* adalah pihak

---

[82] Barda Nawawi Arief, *Sari Kuliah Perbandingan Hukum Pidana*, 2002, (Raja Grafindo Persada:Jakarta), halaman 276

[83] Darrel Menthe, *Jurisdiction in Cyberspace : A Theory of International Space*, available at http:/www.mttlr.org/vlogfour/menthe.html, halaman 1

[84] Darrel Menthe, *Jurisdiction in Cyberspace : A Theory of International Space*, available at http:/www.mttlr.org/vlogfour/menthe.html, halaman 2

[85] Tien S. Saefullah, *Yurisdiksi Sebagai Upaya Penegakan Hukum Dalam Kegiatan Cyberspace*, artikel dalam *Cyber Law :Suatu Pengantar*, (ELIPS: Jakarta), 2002, halaman 102-103.

yang memberikan informasi kedalam *cyberspace* sedangkan *downloader* adalah pihak yang mengakses informasi. Suatu negara dapat melarang dalam wilayahnya kegiatan *uploading* dan *downloading* yang diperkirakan dapat bertentangan dengan kepentingan negara.

2. *The Theory of the Law of The Server*

Pendekatan lain yang dilakukan adalah dengan memperlakukan server dimana *webpages* secara fisik berlokasi, yaitu dimana mereka dicatat sebagai data elektronik. Menurut teori ini sebuah *web pages* yang berlokasi di *server* pada Stanford University tunduk pada hukum California. Namun teori ini akan sulit digunakan jika *uploader* berada di dalam yurisdiksi asing.

3. *The Theory of International Space*

Menurut teori ini, *cyberspace* adalah suatu lingkungan hukum yang terpisah dengan hukum konvensional dimana setiap negara memilki kedaulatan yang sama. Dalam kaitan dengan teori ini **Menthe** mengusulkan agar *cyberspace* menjadi *fourth space*. Dalam Hukum internasional dikenal ruang dimensi keempat yaitu ruang angkasa,[86] bahwa kegiatan di *cyberspace* dianalogikan sebagai kegiatan ruang angkasa, semua kegiatan disana diatur secara bersama oleh negara-negara.

Sementara itu, **David R. Johnson** dan **David G. Post** dalam artikelnya yang berjudul "*And How Should The Internet Be*

[86] Ruang angkasa merupakan ruang bebas yang tidak tunduk pada kedaulatan negara manapun. Hukum yang mengatur kegiatan di ruang angkasa adalah hukum internasional yaitu berupa perjanjian antar negara-negara, sebagaimana dikemukakan oleh Tien S. Saefullah, *Yurisdiksi Sebagai Upaya Penegakan Hukum Dalam Kegiatan Cyberspace*, artikel dalam *Cyber Law :Suatu Pengantar*, (ELIPS: Jakarta), 2002, halaman 103.

*Governed?*" mengemukakan 4 (empat) model yang bersaing, yaitu : [87]

1. Pelaksanaan kontrol dilakukan oleh badan-badan pengadilan yang saat ini ada ("*the existing judicial forums"*);
2. Penguasa nasional melakukan kesepakatan Internasional mengenai *"the governance of cyberspace";*
3. Pembentukan suatu organisasi internasional baru ("*A New International Organization*") yang secara khusus menangani masalah-masalah di dunia internet; dan
4. Pemerintahan/pengaturan sendiri *("Self Governance")* oleh para pengguna internet.

Menurut **Johnson** dan **Post** yang mendukung model ke-4 (*self governnce*) berpendapat bahwa penerapan prinsip-prinsip tradisional dari "*Due Process and Personal Jurisdiction*" tidak sesuai dan mengacaukan apabila diterapkan pada *cyberspace*. Menurut mereka, *cyberspace* harus diperlakukan sebagai suatu ruang yang terpisah dari dunia nyata dengan menerapkan hukum yang berbeda untuk *cyberspace*.[88]

Menurut **Christopher Doran**, pandangan **Johnson** dan **Post** mengenai tidak dapat diterapkannya jurisdiksi personal terhadap para terdakwa internet, bukanlah pandangan yang menonjol/berpengaruh. **Masaki Hamano** juga menyatakan bahwa ide **Johnson** dan **Post** tidak terwujud dalam kenyataan. Menurut **Masaki Hamano**, sekalipun banyak kasus-kasus hukum yang berhubungan dengan dunia cyber, namun Pengadilan-pengadilan di Amerika Serikat telah menerima pendekatan tradisional terhadap sengketa jurisdiksi *cyberspace* dari pada

---

[87] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, 2003, (Citra Aditya Bhakti: Bandung ), halaman 248

[88] *Cyberspace should be treted as a separate "space" from the "real world" by applying distinct to cyberspace*, sebagaimana ditulis oleh Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, 2003, (Citra Aditya Bhakti: Bandung ), halaman 248-249

membuat seperangkat peraturan baru yang lengkap mengenai *cyberlaw*[89].

Hal senada juga dikemukakan oleh **Barda Nawawi Arief**, bahwa sistim hukum dan jurisdiksi nasional/teritorial memang mempunyai keterbatasan karena tidaklah mudah menjangkau pelaku tindak pidana di ruang *cyber* yang tidak terbatas. Namun tidak berarti ruang *cyber* dibiarkan bebas tanpa hukum. Ruang *cyber* merupakan bagian atau perluasan dari "lingkungan" *("environment")* dan "lingkungan hidup" (*"life environment*") yang perlu dipelihara dan dijaga kualitasnya; jadi merupakan suatu "kepentingan hukum" yang harus dilindungi. Oleh karena itu jurisdiksi legislatif atau "*jurisdiction to prescribe*", tetap dapat dan harus difungsikan untuk menanggulangi *"cyber crime*" yang merupakan dimensi baru dari "*environmental crime"*[90].

Menghadapi masalah jurisdiksi di *cyberspace* ini, **Barda Nawawi Arief** mengemukakan bahwa dalam menanggulangi masalah kejahatan *cyber* mengapa tidak digunakan asas universal atau prinsip ubikuitas *(the principle of ubiquity)*. Prinsip ubikuitas adalah prinsip yang menyatakan bahwa delik-delik yang dilakukan/terjadi sebagian di wilayah teritorial negara dan sebagian di luar teritorial suatu negara, harus dapat dibawa ke

---

[89] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, 2003, (Citra Aditya Bhakti: Bandung ), halaman 249

*Cyber law* adalah hukum yang mengatur aktifitas di *cyberspace* yang juga sering disebut sebagai "*the law of the internet", "the law of information and technology" ," telecommunication law"* dan "*lex informatica"*

[90] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, 2003, (Citra Aditya Bhakti: Bandung ), halaman 250

jurisdiksi setiap negara yang terkait. Prinsip ini pernah direkomendasikan dalam "*International Meeting of Experts on The use of Criminal Sanction in the Protection of Environment, Internationally, Domestically an Regionally"* di Portland, Oregon, Amerika Serikat 19-23 Maret 1994.[91]

## B. Pemahaman Mengenai Terorisme

Terorisme dewasa ini telah menjadi kejahatan yang meresahkan bukan hanya pada masyarakat suatu negara, namun juga menjadi keresahan masyarakat internasional. Sifat kejahatan terorisme yang memiliki jaringan internasional dan tingkat mobilitas sangat tinggi serta mengancam keamanan domestik, regional dan internasional menuntut perhatian masyarakat internasional[92].

Berbagai konvensi-konvensi yang berhubungan dengan terorisme telah beberapa kali diadakan dalam rangka menanggulangi terorisme[93],

---

[91] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, 2003, (Citra Aditya Bhakti: Bandung ), halaman 253

[92] Dikdik M. Arief Mansur & Eli Satris Gultom, Cyber Law, aspek Hukum Teknologi Informasi, hal. 51.

[93] Dimulai dengan The League of Nation Convention for the Prevention and Punishment of Terrorism di Jenewa Tahun 1937. Pada 2001 PBB dalam *International Instrumen Related to the Prevention Crime and Suppression Crime of international Terrorism* menyebutkan beberapa konvensi PBB seperti antara lain: The Convention on Offence and Certain other Act Commited On Board Aircraft (Tokyo Convention, 1963), Convention for the Suppression on Unlawful Seizure of Aircraft (Hague Convention, 1970), Convention for the Suppression on Unlawful Acts Againts the Safety of Civil Aviation (Montreal Convention, 1971), Convention on the Prevention and Punishment of Crime Againts Internationaly Protected Persons (New York Convention, 1973), International Convention Againts the Taking of Hostage (Hostages Convention, 1979); Convention on the Pysical Protection of Nuclear Material (Nuclear Material Convention, 1980), Protocol for the Suppression of Unlawful Acts

resolusi berbagai organisasi-organisasi internasional[94], dan beberapa perjanjian internasional yang dibentuk oleh negara-negara di tingkat regional[95].

Sebenarnya, terorisme telah berlangsung lama dalam perkembangan sejarah manusia. Kekerasan berbau teror dapat ditemukan dalam bukunya xenophone (431-350 s.M) mengenai perang psikologis, kekerasan bangsa Roma yang terjadi di Spartacus pada tahun 73 S.M serta sejarah bagaimana Kaisar Tiberius (41-37s.M) dan Caligula yang berupaya menyingkirkan, membuang, merampas harta benda dan hukum lawan-lawan politiknya[96].

Hingga saat ini definisi mengenai terorisme masih beragam, belum ada kesepahaman diantara definisi-definisi yang ada.

---

of Violence at Airport Servings International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts The Safety of Civil Aviation (1988), Convention for the Suppression of Unlawful Acts Againt the Safety Maritim Navigation (Maritim Convention 1988), Protokol for the Suppression of Unlawful Acts Againts the Safety of Fixed Platforms Located on the continental shelf (1988), Convention on the Marking of Plastic Explosives for the purposes of Detection (1991), International Convention for the Suppression of Terroris Bombings (1997) dan International Convention for the Suppression of Financing of Terroris (1999).

[94] General Assembly Resolution GA-Res. 34/145; Security Council Resolution 635 (1989) Declaration on Measure to Eliminate International Terrorisme.

[95] Organization of American States (OAS) dengan Convention to Prevent and Punish the Acts of Terrorism Taking the Forms of Crimes Againts Persons and Related Extrortion That are of International Significance 1971

[96] Dikdik M. Arief Mansur, & Eli Satris Gultom, Cyber Law, Aspek Hukum Teknologi Informasi, hal. 48.

1. Ayatullah Sheikh Muhammad Al Taskhiri menyatakan bahwa Terrorism is an act carried out to achieve on in “Human and Corrupt objektive and involving threat to security of man kind, and violation of rights acknowledge by religion and mankind”

2. FBI menyatakan bahwa “terorrism is unlawful use of violence “against persons or property to intimidate or coerce a governed, civilian populations, or any segment threat, in furtherance or political or social objektive”

3. Sebuah forum bersama dalam forum brainstorming, akademisi, profesional, pakar, pengamat politik dan diplomat, terkemuka pada pertemuan bersama di kantor MenkoPolkam tanggal 15 September 2001 berpendapat bahwa, terorisme dapat diartikan sebagai tindakan kekerasan yang dilakukan sekelompok orang (ekstrimis, separatis, suku bangsa) sebagai jalan terakhir untuk memperoleh keadilan yang tidak dapat dicapai mereka melalui saluran resmi atau jalur hukum.

4. T.P. Thornton dalam bukunya Terror as a Weapon of Political Agitation yang ditulis pada tahun 1964, menyatakan bahwa terorisme merupakan :

> “penggunaan teror sebagai tindakan simbolis untuk mempengaruhi kebijakan dan tingkah laku politik dengan cara-cara ekstra normal, khususnya penggunaan kekerasan dan ancaman kekerasan. Menurut Thornton, terorisme dapat dibagi menjadi dua macam yaitu, enforcement terror dan agitational terror. Bentuk pertama adalah teror oleh penguasa untuk menindas yang melawan kekuasaannya, sedangkan bentuk kedua yaitu, teror yang

dilakukan untuk mengganggu tatanan politik yang mapan untuk kemudian dikuasai".

5. Igor Primoratz menyatakan bahwa "terrorism is based defined as the deliberate use of violence or threat of its use, againts innocent people, with the aim of intimidating some other people into a coerce of action they otherwise would not take".

6. F.Budi Hardiman menyatakan bahwa dalam mendefinisikan secara objektif mengenai terorisme, harus dilihat unsur kualitas aksinya. Kualitas aksi tersebut adalah adanya penggunaan kekerasan secara sistematik untuk menimbulkan ketakutan yang meluas. Menurut Hardiman, pendefinisian, dengan melihat kualitas aksi atau peristiwa lebih menguntungkan karena dapat mengidentifikasi, pola-pola yang luas dari aksi, dapat mengenali kecenderungan di masa depan dan dapat mengetahui pertumbuhan terorisme serta menumbuhkan penyebarannya di dunia[97].

Menurut konvensi PBB tahun 1939, terorisme adalah segala bentuk tindak kejahatan yang ditujukan langsung kepada negara dengan maksud menciptakan bentuk teror terhadap orang-orang tertentu atau kelompok orang atau masyarakat luas. Menurut kamus Webster's New School and Office Dictionary, terrorism is the use of violence, intimidation,

[97] Dikdik M. Arief Mansur, & Eli Satris Gultom, Cyber Law, Aspek Hukum Teknologi Informasi, hlm. 63.

etc to gain to end; especially a system of government ruling by teror, pelakunya disebut terrorist. Selanjutnya sebagai kata kerja terrorize is to fill with dread or terror'; terrify; ti intimidate or coerce by terror or by threats of terror.

Menurut ensiklopedia Indonesia tahun 2000, terorisme adalah kekerasan atau ancaman kekerasan yang diperhitungkan sedemikian rupa untuk menciptakan suasana ketakutan dan bahaya dengan maksud menarik perhatian nasional atau internasional terhadap suatu aksi maupun tuntutan. RAND Corporation, sebuah lembaga penelitian dan pengembangan swasta terkemuka di AS, melalui sejumlah penelitian dan pengkajian menyimpulkan bahwa setiap tindakan kaum terorris adala tindakan kriminal. definisi konsepsi pemahaman lainnya menyatakah bahwa : (1) terorisme bukan bagian dari tindakan perang, sehingga seyogyanya tetap dianggap sebagai tindakan kriminal, juga situasi diberlakukannya hukum perang; (2) sasaran sipil merupakan sasaran utama terorisme, dan dengan demikian penyerangan terhadap sasaran militer tidak dapat dikategorikan sebagai tindakan terorisme; (3) meskipun dimensi politik aksi teroris tidak boleh dinilai, aksi terorisme itu dapat saja mengklaim tuntutanan bersifat politis[98].

[98] www.wikipedia.orgrism

## C. Pemahaman Terhadap Cyber Terrorism

### Definisi umum *Cyber Terrorism*

Umumnya tindak pidana CT belum memiliki keseragaman mengenai peristilahannya. CT digambarkan sebagai suatu tindakan terrorisme yang dilakukan dengan menggunakan komputer.

Bentuk terrorisme tersebut beralih dari terrorisme yang di lakukan di dunia nyata (fisik) ke dalam bentuk terrorisme melalui dunia maya (cyber)[99], atau dengan kata lain CT itu merupakan kejahatan terrorisme dengan menggunakan ruang maya (cyber space) dalam melakukan kejahatannya.

*Cyber Terorism* dapat didefinisikan sebagai berikut :

- James A. Lewis mendefinisikan Cyber Terorism sebagai Penggunaan jaringan computer sebagai sarana untuk melumpuhkan insfrastruktur secara nasional, seperti energy, transportasi, untuk menekan/mengintimidasi kegiatan-kegiatan pemerintah atau masyarakat sipil "[100]

  (The use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government

[99] Dikdik M. Arief Mansur & Eli Satris Gultom, *Cyber Law, aspek Hukum Teknologi Informasi*, hal 65

[100] *Ibid,* hal. 65

orerations) or to coerce or intimidate a government or civilian population).

- Menurut Dorothy E. Denning, *cyber terrorism*[101], sebagai

  "Penyerangan dengan menggunakan komputer atau mengancam, mengintimidasi atau memaksa pemerintahan atau masyarakat, dengan tujuan untuk mencapai target politik, agama atau ideology. Sarana itu cukup untuk menimbulkan rasa takut yang berasal dari tindakan psikis teroris. Serangan itu secara tidak langsung dapat menimbulkan kematian atau cacat badan, kecelakaan pesawat, pencemaran air, dan kelumpuhan ekonomi secara makro. Kerusakan infrastruktur seperti tenaga listrik atau pelayanan keadaan darurat yang dapat disebabkan oleh tindakan terorisme mayantara".

  *(" …is generally understood to mean a computer-based attack or threat of attack intended to intimidate or coerce governments or societies in pursuit of goals that are political, religious, or ideological. The attack should be sufficiently destructive or disruptive to generate fear comparable to that from physical acts of terrorism. Attacks that lead to death or bodily injury, extended power outages, plane crashes, water contamination, or major economic losses would be examples. Depending on their impact, attacks against critical infrastructures such as electric power or emergency services could be acts of cyber terrorism. Attack that disrupt non essential services or that are mainly a costly nuisance would not)*".

- Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) mendefinisikan terorisme mayantara sebagai suatu tindakan yang dapat meresahkan dan menggangu stabilitas masyarakat secara umum. Termasuk dalam definisi ini adalah *spamming* dan *abusing*. ***Spamming*** adalah pengiriman surat elektronik yang berbau iklan

[101] *Ibid*. hal, 65

kepada seorang pemilik surat elektronik tanpa sepengetahuan si empunya. Selain itu *spamming* juga menunjuk pada penggunaan server orang lain untuk menyerang server target. Sedangkan ***abusing*** adalah tindakan penyalahgunaan internet seperti distributed denial on service, hacking, penghinaan, menyebarkan SARA, dan juga pornografi[102]

- The Indian National Cyber Security Forum (INCSF) in its first formal meeting on 6th December 2008 at Bangalore, mendefinisikan

  "cyber terrorism sebagai Using or Causing a Computer, Mobile or any or any associated device or an Electronic Document to intimidate or coerce the Government, its civilian population, or any segment thereof, of India or its friendly countries to create disharmony in the Indian society or the society of any of the friendly countriesto create destabilization of the economy or any segment there of either on the physical space or cyber space in India or in any of the friendly countries in furtherance of political, religious or social objectives or to harm the community injuriously by any means. or any attempt thereof, or providing any assistance thereof".[103]

---

[102] Tempo Interaktif, diakses pada 13/04/2009

[103] http://www.bloggernews.net/118946 bna 30-4-2009, *How Do We Define "Cyber Terrorism",* Posted on December 10th, 2008 by naavi in All News, Country News, India News Read 1,092 times.

(Menggunakan atau menyebabkan komputer, mobile atau atau apapun yang terkait atau perangkat dokumen elektronik untuk mengancam atau memaksa pemerintah, para penduduk sipil, atau segmen itu, di India atau negara sahabat untuk membuat perselisihan di masyarakat India atau masyarakat dari salah satu negara sahabat untuk membuat stabilitas kembali dari ekonomi atau segmen yang ada di salah satu ruang fisik atau ruang cyber di India atau di salah satu negara sahabat pemajuan dalam politik, agama atau sosial atau untuk tujuan yang merugikan kesehatan masyarakat dengan cara apapun atau coba itu, atau memberikan bantuan itu).

Dalam pertemuan itu juga FBI in USA memberikan definisi mengenai cyber terroris sebagai setiap pertimbangan sebelumnya, bermotivasi politik terhadap serangan informasi lainnya, sistem komputer, program komputer dan data yang dihasilkan dalam kekerasan terhadap non-pejuang sasaran oleh kelompok-kelompok sub-nasional atau agen rahasia.

(Cyber terrorism as any premeditated, politically motivated attack against information, computer systems, computer programs and data which results in violence against non-combatant targets by sub-national groups or clandestine agents).

Masih dalam pertemuan tersebut US National Infrastructure Protection Center mendefinisikan *“Cyber Terrorism”* sebagai

"Sebuah tindakan kriminal melakukan dengan menggunakan komputer dan kemampuan telekomunikasi, menghasilkan kekerasan, perusakan dan/atau gangguan layanan, untuk menciptakan rasa takut dengan menyebabkan kebingungan dan ketidakpastian dalam suatu penduduk dengan tujuan mempengaruhi pemerintah atau populasi tertentu untuk mengikuti tujuan politik, sosial atau agenda ideologisnya”.

(Cyber terrorism as A criminal act perpetrated by the use of computers and telecommunication capabilities, resulting in violence, destruction and/or disruption of services, to create fear by causing confusion and uncertainty within a given population with the goal of influencing a government or population to conform to particular political, social or ideological agenda).[104]

- ARTIKEL CYBER TERRORISM, memberikan definisi *cyber terorisme* yaitu :

  "Direncanakan terlebih dahulu penggunaan mengganggu aktivitas, atau ancaman itu, terhadap komputer dan/atau jaringan, dengan maksud untuk lebih lanjut atau menyebabkan kerugian sosial, ideologis, agama, politik atau tujuan yang hampir sama, atau untuk mengancam orang yang menjadi objek tujuannya".

  (Cyber terrorism is the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives).[105]

- South Asian Free Media Association (SAFMA) memberikan pernyataan mengenai *cyber terrorism*. *Cyber terorism* (terorisme via internet) didefinisikan sebagai :

  "Setiap orang, kelompok, atau organisasi, dengan tujuan melakukan teror, mengakses atau menyediakan akses komputer atau jaringan komputer atau sistem elektronik atau dengan peralatan apapun yang

---

[104] Ibid

[105] http://www.directionsmag.com/article.php?article_id=432

tersedia, dan diketahui terlibat atau berusaha terlibat dalam aksi terorisme, termasuk pelanggaran *cyber terrorism*.[106]

- Definisi dari Wikipedia

Data dari wikipedia ini memberikan beberapa definisi dan penjelasan mengenai tindak pidana *cyber teterrorism,* diantaranya :

Wikipedia memberikan definisi cyberterrorism as "… subsumed over time to encompass such things as simply defacing a website or server, or attacking non-critical systems, resulting in the term becoming less useful …." [107]

(cyber terrorism sebagai suatu yang digolongkan dari waktu ke waktu untuk meliputi hal-hal seperti hanya menodai suatu website atau server, atau menyerang sistem tidak kritis, menghasilkan istilah menjadi lebih sedikit bermanfaat).

Beberapa hal yang perlu diperhatikan dalam tindak pidana CT tersebut, yaitu :[108]

- CT dalam menjalankan aksinya memerlukan suatu alasan politis dan tidak terutama semata memusatkan pada keuntungan moneter;

---

[106] Rian Ahmed, *Aturan Dunia Maya Langgar HAM,* Media 28 Januari 2008 | 1058 kata*, Journal*, Daniel Pearl, pada Februari 2002, di kota pelabuhan Pakistan, Karachi, berkomunikasi melalui email

[107] Cyberterrorism From Wikipedia, the free encyclopedia http://en.wikipedia.org/wiki/Cyber-terrorism.

[108] Ibid.

- Berdasarkan pada pengamatan di atas, definisi sederhana CT adalah penggunaan teknologi informasi dan alat/makna nya oleh kelompok teroris dan agen.
- Pelaku harus menggunakan sistem informasi atau alat elektronik lainnya untuk meluncurkan serangan melalui dunia cyber.
- Satu pendekatan pemahaman bahwa CT adalah melakukan perusakan dibagian- bagian yang terpenting dalam suatu infranstruktur.

Dari definisi- definisi dan penjelasan di atas penulis memberikan batasan/ruang lingkup mengenai tindak pidana CT. Kesimpulan penulis mengenai batasan/ruang lingkup CT dari di atas yaitu bahwa *cyber terroris* adalah segala tindakan melawan hukum yang bermotivasi politik untuk mencapai ideologinya, yang secara langsung ataupun tidak langsung yang dapat menyebabkan kematian terhadap orang, hilangnya harta benda, menimbulkan ancaman, keresahan atau rasa takut masyarakat atau menimbulkan kelumpuhan ekonomi makro, kelumpuhan infrastuktur negara dengan menggunakan sarana teknologi informasi.

Penulis juga memberikan batasan bahwa ada sedikitnya lima unsur-unsur yang harus terpenuhi sehingga dapat dikatakan telah terjadinya tindak pidana *cyber terrorism* antara lain :[109]

---

[109] The above definitions suggest that there are at least five elements which must be satisfied to construe cyberterrorism:
1. Politically motivated cyberattacks that lead to death or bodily injury;
2. Cause fear and/or physical harm through cyberattack techniques
3. Serious attacks against critical information infrastructure such as financial, energy, transportation and government operations;
4. Attacks that disrupt non-essential services are not considered as cyberterrorism;
5. Attacks that are not primarily focused on monetary gain.

*Ibid.* Cyberterrorism From Wikipedia, the free encyclopedia http://en.wikipedia.org/wiki/Cyber-terrorism

1. serangannya melalui dunia maya bermotivasi politik yang dapat mengarah pada kematian luka-luka.
2. menyebabkan ketakutan atau merugikan secara fisik atas tekhnik serangan dari dunia maya tersebut.
3. serangannya serius untuk melawan atau ditujukan ke infrastruktur informasi kritis seperti keuangan, energi, transportasi dan operasi pemerintah.
4. serangan yang mengganggu sarana yang tidak penting, bukan dikategorikan sebagai aksi cyber terrorism.
5. serangan itu tidaklah semata-mata dipusatkan pada keuntungan moneter.

Tindak pidana CT sering juga diistilahkan sebagai tindak pidana internasional. Ini dikarenakan tindak pidana CT merupakan tindak pidana lintas Negara yang dapat mengancam perdamain dan stabilitas keamanan suatu Negara. Jika ditinjau dari unsur-unsur tindak pidana internasional yang dikemukakan oleh Cherif Bassiouni Ciri pokok suatu tindak pidana internasional adalah adanya unsur internasional, transnasional, *necessity element* (unsur kebutuhan).

Cherif Bassiouni juga mengungkapkan bahwa unsur-unsur tindak pidana internasional a.l :

1. Unsur Internasional
   - Ancaman secara langsung atas perdamaian dan keamanan dunia.
   - Ancaman secara tidak langsung atas perdamaian dan keamanan dunia.

- Menggoyahkan perasaan kemanusiaan (*shocking to the conscience of humanity*)

2. Unsur transnasional
   - Tindakan yang memiliki dampak terhadap lebih dari satu negara.
   - Tindakan yang melibatkan atau memberikan dampak terhadap warga negara lebih dari satu negara.
   - Sarana dan prasarana serta metoda-metoda yang digunakan melampaui batas-batas territorial suatu negara.
3. Unsur *necessity*

   Kebutuhan akan kerjasama antar negara-negara untuk melakukan penanggulangan.

Berdasarkan dari data- data yang penulis peroleh baik dari berberapa literatur dan media internet ditemukan bahwa dalam Tindak pidana CT memiliki berbagai ragam bentuk- bentuk atau modus operandi dalam menjalankan aksinya.

Macam aksi kejahatan CT antara lain : ***unauthorized access to computer system dan service*** merupakan kejahatan yang dilakukan dengan memasuki atau menyusup kedalam suatu sistem jaringan computer secara tidak sah atau tanpa seijin dari pemilik jaringan. ***Denial of service attack*** penyerangan terhadap salah satu servis yang dijalankan oleh jaringan dengan cara membanjiri server dengan jutaan permintaan layanan data dalam hitungan detik yang menyebabkan server

bekerja terlalu keras dan berakibatkan dari matinya jaringan atau lambatnya kinerja server. ***Cyber sabotage and extortion*** kejahatan ini dilakukan dengan membuat gangguan atau pengerusakan atau penghancuran terhadap suatu data program komputer atau sistem jaringan computer yang terhubung dengan internet. ***Viruses*** adalah perangkat lunak yang telah berupa program script atau macro yang telah didesain untuk menginfeksi menghancurkan memodifikasi dan menimbulkan masalah pada computer atau program computer lainnya sebagai contoh worm yang dulu telah ada sejak perang dunia II. ***Physical attacks*** penyerangan secara fisik terhadap sistem komputer atau jaringan .cara ini dilakukan dengan merusak fisik seperti pembakaran pencabutan salah satu devices computer atau jaringan menyebabkan lumpuhnya sistem komputer. ***Phreaker,*** *merupakan Phone Freaker* yaitu kelompok yang berusaha mempelajari dan menjelajah seluruh aspek sistem telepon misalnya melalui nada-nada frekwensi tinggi (system multy frequency). Pada perkembangannya setelah perusahaan-perusahaan telekomunikasi di Amerika Serikat menggunakan computer untuk mengendalikan jaringan telepon, para pheaker beralih ke komputer dan mempelajarinya seperti hacker. Sebaliknya para hacker mempelajari teknik pheaking untuk memanipulasi sistem komputer guna menekan biaya sambungan telepon dan untuk menghindari pelacakan. ***Carding*** atau yang disebut *Credit Card Fraud* merupakan tindakan memanfaatkan

kartu credit orang lain untuk berbelanja di toko-toko online guna membeli peralatan terorisme dan pembiayaan operasional. Teroris mencari nomor-nomor credit card orang lain melalui chanel di IRC, melalui CC Generator, meng-hack toko online dan masuk data basenya. Membuat website palsu mengenai validitas kartu kredit seperti pada umumnya di situs-situs porno. ***E-mail***, Teroris dapat menggunakan email untuk menteror, mengancam dan menipu, spamming dan menyebar virus ganas yang fatal, menyampaikan pesan di antara sesama anggota kelompok dan antara kelompok. ***Cyber Espionage*** merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-ata terhadap pihak lain, dengan memasuki sistem jaringan komputer (computer network system) pihak sasaran. Membajak media dengan menungganggi satelit dan siaran-siaran TV Kabel untuk menyampaikan pesan-pesannya. Selain itu, teroris dapat mencari metode-metode untuk menyingkap “penyandian” signal-signal TV Kabel yang ada dan menyadap siarannya. Contoh kasus demikian “Captain Midnight” memanipulasi siaran HBO yang berjudul “The Falcon and the Snowman”. ***Hacking*** untuk merusak sistem dilakukan tahap mencari sistem komputer (foot printing) dan mengumpulkan informasi untuk menyusup seperti mencari pintu masuk (scanning). Setelah menyusup, penjelajahan sistem dan mencari akses ke seluruh bagian (enumeration) pun dilakukan.

Kemudian, para hacker membuat backdoor (creating backdoor) dan menghilangkan jejak.[110]

*Cyber terrorism* sebenarnya terdiri dari dua aspek yaitu *cyber space* dan *terrorism,* sementara para pelakunya disebut dengan CT. Para *hackers* dan *crackers* juga dapat disebut dengan CT, karena seringkali kegiatan yang mereka lakukan di dunia maya (Internet) dapat menteror serta menimbulkan kerugian yang besar terhadap korban yang menjadi targetnya, mirip seperti layaknya aksi terorisme. Keduanya mengeksploitasi dunia maya (internet) untuk kepentingannya masing-masing. Mungkin perbedaan tipis antara CT dan *hackers* hanyalah pada motivasi dan tujuannya saja, dimana motivasi dari para CT adalah untuk kepentingan politik kelompok tertentu dengan tujuan memperlihatkan eksistensinya di panggung politik dunia. Sementara motivasi para *hackers* atau *crackers* adalah untuk memperlihatkan eksistensinya atau adu kepintaran untuk menunjukan superiotasnya di dunia maya dengan tujuan kepuasan tersendiri atau demi uang.

Secara umum kegiatan *hacking* adalah setiap usaha atau kegiatan diluar ijin atau sepengetahuan pemilik jaringan untuk memasuki sebuah jaringan serta mencoba mencuri *files* seperti *file password* dan sebagainya. Atau usaha untuk memanipulasi data, mencuri file-file

---

[110] Andreasbuvois, *August 13, 2008*. cyber Terrorism. http://andreasbuvois.blog.friendster.com/27/06/2009

penting atau mempermalukan orang lain dengan memalsukan *user identity* nya. Pelakunya disebut *hacker* yang terdiri dari seorang atau sekumpulan orang yang secara berkelanjutan berusaha untuk menembus sistim pengaman kerja dari *operating sistem* di suatu jaringan komputer. Para *hacker* yang sudah berpengalaman dapat dengan segera mengetahui kelemahan sistim pengamanan *(security holes)* dalam sebuah sistim jaringan komputer. Selain itu kebiasaan *hacker* adalah terus mencari pengetahuan baru atau target baru dan mereka akan saling menginformasikan satu sama lainnya. Namun pada dasarnya para *hacker* sejati tidak pernah bermaksud untuk merusak data didalam jaringan tersebut, mereka hanya mencoba kemampuan untuk menaklukan suatu sistim keamanan komputer demi kepuasan tersendiri. Sedangkan seorang atau sekumpulan orang yang memang secara sengaja berniat untuk merusak dan menghancurkan integritas di seluruh jaringan sistim komputer disebut *cracker*, dan tindakannya dinamakan *cracking*. Pada umumnya para *cracker* setelah berhasil masuk kedalam jaringan komputer akan langsung melakukan kegiatan pengrusakan dan penghancuran data-data penting *(destroying data)* hingga menyebabkan kekacauan bagi para *user* dalam menggunakan komputernya. Kegiatan para *cracker* atau CT ini mudah dikenali dan dapat segera diketahui dari

dampak hasil kegiatan yang mereka lakukan. Beberapa metode atau cara kerja yang sering digunakan para **CT** dan ***hackers*** antara lain :[111]

- ***Spoofing***, yaitu sebuah bentuk kegiatan pemalsuan dimana seorang *hacker* atau *cyber terrorist* memalsukan *(to masquerade)* identitas seorang *user* hingga dia berhasil secara legal *logon* atau *login* kedalam satu jaringan komputer seolah-olah seperti user yang asli.
- ***Scanner*****,** merupakan sebuah program yang secara otomatis akan mendeteksi kelemahan *(security weaknesses)* sebuah komputer di jaringan komputer lokal *(local host)* ataupun aringan komputer dengan lokasi berjauhan *(remote host)*. Sehingga dengan menggunakan program ini maka seorang *hacker* yang mungkin secara phisik berada di Inggris dapat dengan mudah menemukan *security weaknesses* pada sebuah *server* di Amerika atau dibelahan dunia lainnya termasuk di Indonesia tanpa harus meninggalkan ruangannya!
- ***Sniffer*****,** adalah kata lain dari ***Network Analyser*** yang berfungsi sebagai alat untuk memonitor jaringan komputer. Alat ini dapat dioperasikan hampir pada seluruh tipe protokol omunikasi data, seperti: *Ethernet, TCP/IP, IPX* dan lainnya.

---

[111] Mayor Sus Ir. Rudy A.G. Gultom, M.Sc, Teknologi Militer CYBER TERRORISM (Sudah Siapkah Kita Menghadapinya)? http://www.tni.mil.id/images/gallery/cyber_terrorism.pdf

- ***Password Cracker***, adalah sebuah program yang dapat membuka enkripsi sebuah *assword* atau sebaliknya malah dapat mematikan sistim pengamanan *password* itu sendiri.
- ***Destructive Devices***, merupakan sekumpulan program-program virus yang dibuat khusus ntuk melakukan penghancuran data-data, diantaranya *Trojan horse, Worms, Email ombs, Nukes* dan lainnya.

Beberapa bentuk aksi CT yang pernah terjadi di manca Negara sebagai berikut : Amerika Serikat, pada bulan Februari 1998 terjadi serangan *(breaks-in or attack)* sebanyak 60 kali perminggunya melalui media *Internet* terhadap 11 jaringan komputer militer di Pentagon. Dalam *cyber attack* ini yang menjadi target utama para CT adalah Departemen Pertahanan Amerika Serikat *(DoD)*; Di Srilanka, pada bulan Agustus 1997, sebuah organisasi yang bernama *the Internet Black Tigers* yang berafiliasi kepada gerakan pemberontak Macan Tamil *(the Liberation Tigers of Tamil Eelam)* menyatakan bertanggung jawab atas kejahatan email *(email bombing, email harrasment, email spoofing, etc.)*[112] yang menimpa beberapa kedutaan serta kantor perwakilan pemerintah Srilanka di manca negara. Tujuan akhirnya adalah kampanye untuk melepaskan diri dari Srilanka dalam memperjuangkan kemerdekaan rakyat Tamil; Di Cina, pada bulan Juli 1998, sebuah perkumpulan CT

[112] Dr. Mudawi Mukhtar Elmusharaf Cyber Terrorism : The new kind of Terrorism http://www.crime research.org/articles/Cyber_Terrorism_new_kind_Terrorism

atau *crackers* terkenal berhasil menerobos masuk ke pusat komputer sistim kendali satelit Cina dan berhasil mengacaukan *"selama beberapa waktu"* sistim kendali sebuah satelit milik Cina yang sedang mengorbit di ruang angkasa. Tujuan utama dari aksi ini adalah untuk melakukan protes terhadap gencarnya investasi negara barat di Cina. Di Swedia, pada bulan September 1998, pada saat kegiatan pemilihan umum, sejumlah CT berhasil melakukan kegiatan sabotase yaitu merubah *(defaced)* tampilan website dari partai politik berhaluan kanan dan kiri. Dimana *Website links* partai politik tersebut dirubah tujuannya ke alamat situs-situs pornografi sehingga sangat merugikan partai karena kampanye partai secara elektronik melalui Internet menjadi terhambat.[113]

Ditemukan Virus "I Love You" dan "Love Bug" serta berbagai variasinya yang menyebar dengan cepat, diketahui berasal dari Filipina. Virus-virus tersebut sejauh ini menimbulkan kerusakan sangat besar dalam sejarah. Berdasarkan prakiraan, virus "I Love You" dapat merasuki 10 juta komputer dalam jaringan dunia dan menimbulkan kerugian finansial yang besar pada jaringan komputer di Malaysia, Jerman, Belgia, Perancis, Belanda, Swedia, Hongkong, Inggris Raya, dan Amerika Serikat. Virus ini menyebabkan ATM-ATM di Belgia tak berfungsi beberapa waktu, mengganggu sistem komunikasi internal Majelis

---

[113] http://www.symantec.com/avcenter/reference/cyberterrorism.pdf (cybernterrorism by sarah gordon)

Perwakilan Rendah (The House of Common) di Inggris, dan menghilangkan sistem surat elektronik (e-mail) pada Kongres Amerika Serikat.[114]

Di Indonesia sendiri, sekitar bulan Agustus 1997, CT atau *hackers* dari Portugal pernah merubah *(defacing)* tampilan situs resmi dari Mabes ABRI (TNI), walaupun dengan segera dapat diantisipasi. Kemudian pada bulan April 2004 situs resmi milik KPU (Komisi Pemilihan Umum) juga berhasil di *hack* dengan teknik *defacing*, namun dengan segera pelakunya yaitu seorang konsultan Teknologi Informasi suatu perusahaan di Jakarta dapat segera diamankan oleh pihak kepolisian. Namun sebenarnya masih banyak lagi aktivitas para CT di negara-negara lain yang masih berlangsung hingga saat ini.[115]

Pertengahan tahun 2006 pemerintah provinsi Distrik DIY dikejutkan akan adanya ancaman bom yang ditulis pengunjung Pemprov DIY meski ancaman itu tidak terbukti dan hanya omong kosong tetapi kejadian itu memberikan pelajaran bahwa internet adalah ruang terbuka bagi siapa saja. Sangat memungkinkan di tahun ini dan masa yang akan datang ancaman dari seseorang atau kelompok melalui jaringan internet akan terus bertambah meski kadang tujuan awal hanya untuk iseng.

---

[114] http://www.unisosdem.org/2009/06/13/kliping_detail.php?aid=2828&coid=1&caid=45

[115] http://www.symantec.com/avcenter/reference/cyberterrorism.and.home.user.pdf

Tetapi dari keisengan itu meningkat menjadi kenyataan jika ternyata pelaku CT bersinggungan dengan teroris asli yang notabene biasanya tidak paham akan jaringan internet, dan menemukan kesamaan visi dalam melakukan terror meski berbeda media. [116]

Tertangkapnya yazir bin baz alias faiz akhir april 2008 yang merupakan salah satu anak buah noordin m top beberapa waktu lalu membuktikan bahwa ketika seseorang yang sebenarnya tidak setuju dengan terror pengeboman tetapi sejalan dengan ideologis yang dianut membawa faiz ikut dalam kelompok noordin m top yang di tugasi untuk menterjemahkan buku buku jihad arab ke dalam Indonesia serta di minta untuk membuat website jihad yang didalamnya akan diisi oleh artikel dan ideologis jihad. Tujuan penerjemahan dan pembuatan website jelas untuk propaganda. Website adalah sarana publikasi ampuh ketika sebuah kelompok atau operasi radikal berhasil, maka biasanya dengan segera mereka akan memposting bahwa kejadian seperti pengeboman penyanderaan dan sebagainya adalah atas ulah mereka dan mereka berani bertanggung jawab terhadap apa yang telah di lakukannya. Pelaku CT paham betul bahwa memanfaatkan teknologi canggih digabung dengan internet akan dengan mudah melancarkan aksi aksinya ibaratnya dengan 2 hal tersebut otak teroris cukup duduk di depan komputer dan

---

[116] Cyber Terrorism August 13, 2008 by andreasbuvois, http://www.andreasbuvois.27/07/2009/blog. friendster.com

mencari dan mengetahui hasil-hasil capaian aksinya.[117]

Fakta lainya, yaitu terkait kasus terpidana mati Bom Bali, yaitu Iman Samudra yang melakukan *hacking, carding,* melakukan provokasi dan propaganda. Aksi *carding* dijumpai dengan ditemukannya situs *http/www.anshar.com* yang dibuat oleh Muhammad agung prabowo alias max fiderman alias ahmad kalingga dan agung setiyadi alias pak ne alias saiful jihad mahasiswa teknik elektro UNS yang merupakan kaki tangan pelaku Bom bali I imam samudera adalah bukti nyata bahwa telah terjadi pergeseran modus penggalangan dana pelaku teroris dengan memanfaatkan carding dan pemesanan alat terror melalui dunia maya di banding menunggu kiriman dari orangtua atau merampok.[118]

Bentuk aksi provokasi dan provaganda dan hacking deketahui melalui pernyataannya Iman Samudra sendiri yang dituangkan dalam bukunya yang berjudul Aku Melawan Teroris (I Fight terorists). Ia menyarankan kepada junior- juniornya untuk belajar internet, sehingga terampil seperti hacker. Bagi mereka, tujuan utama untuk berbagi

---

[117] http://www.thejakartapost.com/news/2006/09/14/cyberterrorism-creates-problems-real-world.htm...
"In his book Aku Melawan Teroris (I fight terrorists), Imam clearly stated that the Internet is the best tool to achieve his mission. He suggested that his juniors learn hacking skills. It would not be difficult for Muslim fundamentalists and the hackers to do that because both communities are anarchistic and anti-authority. To them, the primary motive of sharing their knowledge on hacking is political resistance.

[118] Cyber Terrorism August 13, 2008 by andreasbuvois, http://www.andreasbuvois.27/07/2009/blog. friendster.com

pengetahuan mereka mengenai hacking adalah sebagai perlawanan politik.[119]

*Hacking* yaitu memasukkan ke dalam sistem komputer dengan mengenalkan virus agar mudah kena serangan ke jaringan situs internet atau ancaman terroristik yang dilakukan melalui komunikasi elektronik.[120], *Hacking* dengan kata lain diartikan sebagai perusakan komputer jaringan pihak lain.[121]

*Hacking* merupakan salah satu kegiatan yang bersifat negatif, meskipun pada awalnya *hacking* memiliki tujuan mulia, yaitu untuk memperbaiki sistem keamanan yang telah dibangun dan memperkuatnya, tetapi dalam perkembangannya *hacking* digunakan untuk keperluan-keperluan lain yang bersifat merugikan. Hal ini tidak lepas dari penggunaan internet yang semakin luas sehingga penyalahgunaan kemampuan hacking juga mengikuti luasnya pemamfaatan internet

Dari hasil penelitian yang telah dijelaskan pada bagian sebelumnya, maka dapat disimpulkan beberapa tahap *hacking* yang

---

119 http://www.thejakartapost.com/news/2006/09/14/cyberterrorism-creates-problems-real-world.htm...
"In his book Aku Melawan Teroris (I fight terrorists), Imam clearly stated that the Internet is the best tool to achieve his mission. He suggested that his juniors learn hacking skills. It would not be difficult for Muslim fundamentalists and the hackers to do that because both communities are anarchistic and anti-authority. To them, the primary motive of sharing their knowledge on hacking is political resistance.

120 *Ibid*. http://en.wikipedia.org/wiki/Cyber-terrorism

121 Abdul Wahib dan Mohammad Labib, *Kejahatan Mayantara (Caber Crime),* Refika Aditama, Bandung, 2005, hal. 130

selanjutnya akan digunakan sebagai langkah untuk menentukan tahap-tahap *hacking* yang dapat dikonstruksikan sebagai kejahatan. Tahap-tahap *hacking* seperti yang dimaksud adalah :[122]

a. Mengumpulkan dan mempelajari informasi yang ada mengenai sistem operasi komputer atau jaringan komputer yang dipakai pada target sasaran;
b. Menyusup atau mengakses jaringan komputer target sasaran;
c. Menjelajahi sistem komputer (dan mencari akses yang lebih tinggi);
d. Membuat bacdoor dan menghilangkan jejak.

Cyber terrorism apabila tidak diamati secara teliti maka akan tampak sama dengan DDoS Attact, Hacking atau Cracking sebagai mana biasanya, namun ada beberapa perbedaan yang menonjol bila diteliti dari ciri-cirinya sebagai berikut;[123]

- Modal untuk menyerang relatif sangat murah, sebuah serangan yang besar/luas namun cukup dengan hanya mengunakan komputer dan modem yang sederhana.
- Dapat dilakukan oleh setiap individu, tidak perlu personil/unit yang besar.
- Rendahnya perkiraan terhadap resiko yang akan terjadi serta sangat sulit untuk melokalisir tersangka, bahkan kadang-kadang tidak menyadari sedang diserang.
- Tidak ada batasan waktu dan tempat, sangat memungkinkan diserang kapan saja (setiap saat) dan dari manapun.

---

[122] Agus Rahardjo, 2002, *Cyber Crime, Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi.* PT. Citra Adyta : Bandung, hal. 174-175

[123] Sabadan Daan dan Kunarto. *Kejahatan Berdimensi Baru.* Cipta Manunggal, Jakarta, 1999

- Kerugian akan sangat besar/mahal dan meluas apabila serangan tersebut berhasil.
- Motif untuk tujuan tertentu (bukan untuk tujuan keuntungan ekonomi saja).
- Sasaran terfokus (disengaja) pada infra struktur kritis.

Dapat disimpulkan perbedaannya adalah pada; motifnya, sasarannya serta dampak kerugian yang akan sangat besar serta fatal apabila serangannya berhasil.

Infrastruktur kritis adalah suatu institusi yang berperan sebagai sarana bagi masyarakat luas dalam menunjang kebutuhan hidupnya atau berfungsi melayani masyarakat luas agar kehidupannya dapat berjalan secara normal, artinya apabila institusi ini tidak berfungsi atau terganggu maka akan berakibat langsung pada kehidupan masyarat secara luas dan mereka tidak dapat melangsungkan kehidupannya secara normal. Adapun contoh dari infrastruktur kritis ini antara lain sebagai berikut;

- Jaringan Listrik, Pasokan Gas, Air & BBM .
- Jaringan Kominfo, Keuangan, Pelayanan kesehatan.
- Fasilitas Penerbangan, Kereta Api.
- Pelayanan Kepolisian, Kekuatan Pertahanan dan Pemerintahan.

*CIAO*(Critical Infrastructure Assurance Office)[124] di Amerika mendefinisikan infra struktur kritis adalah sebagai *"Those systems and assets---both physical and cyber---so vital to the Nation that their capacity*

[124] Satsuki Suwa. *Response of The National Police Agency in Japan in Dealing with Cyber Terrorism*. High-tech Crime Division NPA – Japan, unpublished, Tokyo - 2002

*or destruction would have a debilitating impact on national security, national economic security and/or national public health and safety"*, mengacu pada definisi ini dapat disimpulkan bahwa apabila salah satu atau sebagian dari infra struktur kritis tersebut menjadi target atau sasaran CT maka dampaknya akan sangat luas bagi masyarakat dan kerugiannya akan sangat besar, jadi pada tempatnya bila dalam ***draft Cyberlaw*** diberikan perlakuan khusus dalam hal perlindungan terhadap infrastruktur kritis serta hukuman yang lebih keras terhadap pelakunya.

## D. Kebijakan Kriminal dalam Kerangka Pembaharuan Hukum Pidana

Perkembangan masyarakat yang pesat di jaman modern ini sebagai akibat dari berkembangnya Ilmu Pengetahuan dan Teknologi (IPTEK), perlu diikuti dengan kebijakan di bidang hukum sebagai sarana untuk menertibkan dan melindungi masyarakat dalam mencapai kesejahteraannya.

Munculnya kejahatan-kejahatan dengan dimensi baru yang bercirikan modern yang merupakan dampak negatif dari perkembangan yang sangat cepat dibidang teknologi informasi, perlu pula ditanggulangi dengan berbagai upaya penanggulangan yang lebih efektif. Guna mengatasi kejahatan modern tersebut perlu adannya kerjasama antara

masyarakat dan aparat penegak hukum disamping juga perlu dilakukan pembenahan serta pembangunan hukum pidana yang menyeluruh baik dari segi struktur, substansi maupun budaya hukumnya.

Di Indonesia saat ini tengah berlangsung usaha untuk memperbaiki Kitab Undang-Undang Hukum Pidana (KUHP) sebagai bagian dari usaha pembaharuan hukum nasional yang menyeluruh. Usaha pembaharuan itu tidak hanya karena alasan bahwa KUHP yang sekarang diberlakukan dianggap tidak sesuai lagi dengan tuntutan perkembangan masyarakat khususnya karena perkembangan IPTEK, tetapi juga karena KUHP tersebut tidak lebih dari produk warisan penjajah Belanda, dan karenanya tidak sesuai dengan pandangan hidup bangsa Indonesia yang merdeka dan berdaulat.

Usaha pembaharuan hukum pidana di Indonesia tentunya tidak terlepas dari politik hukum yang bertugas untuk meneliti perubahan-perubahan yang perlu diadakan terhadap hukum yang ada agar dapat memenuhi kebutuhan-kebutuhan baru di dalam masyarakat. Politik hukum[125] tersebut meneruskan arah perkembangan tertib hukum, dari

---

[125] Menurut Sudarto dalam bukunya *Hukum dan Hukum Pidana*, (Alumni:Bandung),1997, halaman 159 dan dalam buku *Hukum Pidana Dan Perkembangan Masyarakat*, (Sinar Baru:Jakarta), 1983, halaman 20, bahwa "politik hukum" (*law policy/rechtspoltiek)* dapat diartikan sebagai: "usaha untuk mewujudkan peraturan-peraturan yang baik sesuai dengan keadaan dan situasi pada suatu saat; "kebijakan dari negara melalui badan-badan yang berwenang untuk menetapkan peraturan-peraturan yang dikehendaki yang diperkirakan bisa digunakan untuk mengekspresikan apa yang terkandung dalam masyarakat dan untuk mencapai apa yang dicita-citakan.

"*ius contitutum*' yang bertumpu pada kerangka landasan hukum yang terdahulu menuju pada penyusunan "*ius constituendum*" atau hukum pada masa yang akan datang.

Hal tersebut di atas sejalan dengan yang dikemukakan oleh **Barda Nawawi Arief**, yaitu :[126]

"Pembaharuan hukum pidana pada hakekatnya mengandung makna, suatu upaya untuk melakukan reorientasi dan reformasi hukum pidana yang sesuai dengan nilai-nilai sentral sosio-politik, sosio-filosofik, sosio-kultural masyarakat Indonesia yang melandasi kebijakan sosial, kebijakan kriminal dan kebijakan penegakan hukum di Indonesia".

Dari pendapat **Barda Nawawi Arief** tersebut dapat dilihat bahwa beliau merumuskan tiga latar belakang dan urgensi pembaharuan hukum pidana dengan meninjaunya dari aspek sosio-politik, sosio-filosofik, dan sosio-kultural. Sedangkan **Sudarto** menyebut ada tiga alasan mengapa KUHP perlu diperbaharui yakni alasan politik, sosiologis dan praktis.[127]

Jadi upaya pembaharuan hukum pidana Indonesia mempunyai suatu makna yaitu menciptakan suatu kodifikasi hukum pidana nasional untuk menggantikan kodifikasi hukum pidana yang merupakan warisan

---

[126] Barda Nawawi Arief, 2002, *Bunga Rampai Kebijakan Hukum Pidana*, (PT. Citra Aditya Bhakti:, Bandung), halaman 30-31

[127] Sudarto, 1983, *Hukum Pidana Dan Perkembangan Masyarakat*, (Sinar Baru:Bandung), halaman 66-68.

kolonial yakni *Wetboek van Strafrecht Nederlands Indie* 1915, yang merupakan turunan dari *Wetboek van Strafrecht* negeri Belanda tahun 1886.[128] Meskipun dalam KUHP sekarang ini telah dilakukan tambal sulam namun jiwanya tetap tidak berubah. **Sudarto**[129] mengatakan "*Wetboek van Starafrecht*" atau Kitab Undang-Undang Hukum Pidana yang disingkat W.v.S atau KUHP yang sehari-hari digunakan oleh para praktisi hukum Indonesia telah berusia lebih dari 50 tahun. Selama itu ia mengalami penambahan, pengurangan atau perubahan, namun jiwanya tidak berubah".

Upaya pembaharuan hukum di Indonesia yang sudah dimulai sejak lahirnya UUD 1945, tidak dapat dilepaskan pula dari landasan sekaligus tujuan yang ingin dicapai oleh bangsa Indonesia seperti telah dirumuskan dalam pembukaan UUD 1945 yaitu, "melindungi segenap bangsa Indonesia dan untuk mewujudkan kesejahteraan umum berdasarkan Pancasila".[130]

Tujuan pembangunan nasional yang terdapat dalam pembukaan UUD 1945 itu semata-mata demi terciptanya kesejahteraan bagi bangsa

---

[128] Muladi, *1984, Lembaga Pidana Bersyarat, (Alumni:* Bandung), halaman 10.

[129] Sudarto, 1974, *Suatu Dilema Dalam Pembaharuan Sistem Pidana Indonesia*, Pusat Study Hukum dan masyarakat, FH UNDIP Semarang, halaman 2

[130] Barda Nawawi Arief, 1994, *Beberapa Aspek Pengembangan Ilmu Hukum Pidana (Menyongsong Generasi Baru Hukum Pidana Indonesia)*, Pidato Pengukuhan Guru Besar FH UNDIP, Semarang, halaman 1.

Indonesia dan untuk mencapai semuanya itu maka dilakukan pembangunan. Adapun pembangunan yang dilakukan tidak hanya pada satu sisi kehidupan saja akan tetapi pada semua sisi kehidupan berbangsa dan bernegara termasuk didalamnya pembangunan hukum. Seiring dengan perkembangan pembangunan di Indonesia, berkembang pula bentuk-bentuk kejahatan ditengah-tengah masyarakat.[131] Dalam upaya menanggulangi kejahatan-kejahatan tersebut dilakukan suatu kebijakan kriminal/politik kriminal (*Criminal Policy*), yang meliputi kebijakan secara terpadu antara upaya penal dan non penal yang dapat diintegrasikan satu dengan yang lainnya.

Istilah kebijakan dalam hal ini ditransfer dari bahasa Inggris: "*policy*" atau dalam Bahasa Belanda: "*Politiek*" yang secara umum dapat diartikan sebagai prinsip-prinsip umum yang berfungsi untuk mengarahkan pemerintah (dalam arti luas termasuk pula aparat penegak hukum) dalam mengelola, mengatur, atau menyelesaikan urusan-urusan publik, masalah-masalah masyarakat atau bidang-bidang penyusunan peraturan perundang-undangan dan pengaplikasian hukum/peraturan, dengan suatu tujuan (umum) yang mengarah pada

[131] Kongres PBB ke IV tahun 1970 di Tokyo " *The Prevention of Crime And the Treatment of Offenders"* tidak dapat menetapkan dengan pasti hubungan antara kejahatan dan perkembangan (*development*), akan tetapi konggres mengakui bahwa beberapa aspek penting dari perkembangan masyarakat dianggap potensial sebagai kriminogen artinya mempunyai kemungkinan untuk menimbulkan kejahatan, aspek-aspek ini adalah urbanisasi, industrialisasi, mobilitas sosial dan sebagainya (Sudarto, *Hukum Pidana*, (Alumni: Bandung) Cetakan ke-2, 1981 halaman 102.)

upaya mewujudkan kesejahteraan atau kemakmuran masyarakat (warga negara).[132]

**Sutan Zanti Arbi** dan **Wayan Ardana**[133], menterjemahkan "*policy*" juga dengan kebijakan, yaitu suatu keputusan yang menggariskan cara yang paling efektif dan paling efisien untuk mencapai tujuan yang ditetapkan secara kolektif. Sementara itu **Barda Nawawi Arief**[134] mengatakan bahwa istilah "kebijakan" berasal dari kata "*politic", "politics"* dan "*policy"* (Inggris) atau "*politiek"* (Belanda). Politik berarti "*acting of judging wisely, prudent*", jadi ada unsur "*wise*" dan "*prudent*" yang berarti bijaksana. "*Politics*" berarti "*the science of the art of government*". *Policy* berarti a) *Plan of action*, suatu perencanaan untuk melakukan suatu tindakan dari negara, b) *art of government,* dan c) *wise conduct*.

---

[132] Lihat: Henry Campbell Black, et.al.,ed., *Black's Law Dictionary*, Fifth Edition, St. Paulminn West Publicing C.O., 1979, halaman 1041, antara lain disebutkan bahwa *Policy* merupakan : *The general principles by which a government is guided in its management of pullic affairs, or the legislature in its measures … this term, as applied to a law, ordinance, or rule of law, denotes, its general purpose or tendency considered as directed to the welfare or prosperity of the state community".*

[133] Dalam Barda Nawawi Arief, *Kebijakan Legislatif Dalam Penganggulangan Kejahatan dengan Pidana Penjara*, Badan Penerbit UNDIP Semarang, 1994, halaman 59

[134] Barda Nawawi Arief, *Kebijakan Kriminal (Criminal Policy)*, Bahan Penataran Kriminologi, FH Universitas Katolik Parahyangan , Bandung tanggal 9-13, halaman 780

Dalam Kamus Besar Bahasa Indonesia, istilah “Politik” diartikan sebagai berikut:[135]

1) pengetahuan mengenai ketatanegaraan atau kenegaraan (seperti sistem pemerintahan, dasar-dasar pemerintahan);
2) segala urusan dan tindakan (kebijakan, siasat dan sebagainya) mengenai pemerintahan negara atau terhadap negara lain;
3) cara bertindak (dalam menghadapi atau menangani suatu masalah), kebijakan .

Dari hal tersebut diperoleh gambaran bahwa di dalam istilah “*Policy*” akan ditemukan makna “Kebijaksanaan”. Makna kebijakan mempunyai kaitan yang erat dengan kebijaksanaan, dan di dalam kebijakan terkandung kebijaksanaan.

Arti politik kriminal, para pakar hukum pidana mempunyai berbagai ragam pendapat. **Marc Ancel** merumuskan politik kriminal sebagai *the rational organization of the control of crime by society* (usaha yang rasional dari masyarakat dalam menanggulangi kejahatan), sedangkan **G.P. Hoefnagels** yang bertolak dari pendapat **Marc Ancel** tersebut memberikan pengertian politik kriminal sebagai *the rational organization of the social reaction to crime*, disamping itu **G.P Hoefnagels** sendiri juga mengemukakan dengan berbagai rumusan seperti *criminal policy is the science of responses, criminal policy is the*

[135] Lihat *Kamus Besar Bahasa Indonesia*, edisi ketiga, 2002, (Pusat Bahasa Departemen Pendidikan Nasional, halaman 780

*science of crime prevention, criminal policy is a policy of designating human behaviour as crime dan criminal policy is rational total of the responses to crime*[136].

Menurut **G. Peter Hoefnagels**, kebijakan kriminal adalah merupakan ilmu kebijakan sebagai bagian dari kebijakan yang lebih luas yaitu kebijakan penegakan hukum (*criminal policy as a science of policy is part of a larger policy : the law enforcement policy)*; sedangkan kebijakan penegakan hukum juga bagian dari kebijakan sosial.

Sedangkan menurut **Sudarto**, definisi politik kriminal secara singkat sebagai usaha yang rasional dari masyarakat dalam menanggulangi kejahatan.[137] Pengertian tersebut diambil dari definisi yang dikemukakan oleh **Marc Ancel**. Selain itu beliau juga memberikan beberapa pengertian yaitu dalam arti sempit, dalam arti yang lebih luas dan dalam arti yang paling luas. Dalam arti sempit, politik kriminal adalah keseluruhan asas dan metoda yang menjadi dasar dari reaksi terhadap pelanggaran hukum yang berupa pidana. Dalam arti yang lebih luas, ia merupakan keseluruhan fungsi dari aparatur penegak hukum, temasuk di dalamnya cara kerja dari pengadilan dan polisi, sedangkan dalam arti yang paling luas politik kriminal merupakan keseluruhan

---

[136] Barda Nawawi Arief, 2002, *Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit*, halaman 2

[137] Sudarto, Hukum dan Hukum Pidana, (Alumni:Bandung), 1986, halaman 30

kebijakan yang dilakukan melalui perundang-undangan dan badan-badan resmi, yang bertujuan untuk menegakkan norma-norma sentral dalam masyarakat.[138]

Penegakan norma-norma sentral tersebut dapat diartikan sebagai penanggulangan kejahatan, melaksanakan politik kriminal berarti mengadakan pemilihan dari sekian banyak alternatif, mana yang paling efektif dalam usaha penanggulangan kejahatan.[139]

Politik kriminal menurut **Barda Nawawi Arief** merupakan bagian integral dari upaya perlindungan masyarakat (*social defence*) dan upaya untuk mencapai kesejahteraan masyarakat (*social welfare*). Oleh karenannya, tujuan akhir atau tujuan utama dari politik kriminal adalah "*perlindungan masyarakat untuk mencapai kesejahteraan masyarakat*".[140]

Kebijakan sosial sebagai kebijakan umum terdiri dari kebijakan dalam rangka mensejahterakan masyarakat (*social welfare policy*) dan kebijakan perlindungan masyarakat (*social defense policy*). Kebijakan perlindungan masyarakat dituangkan dalam kebijakan kriminal yang

---

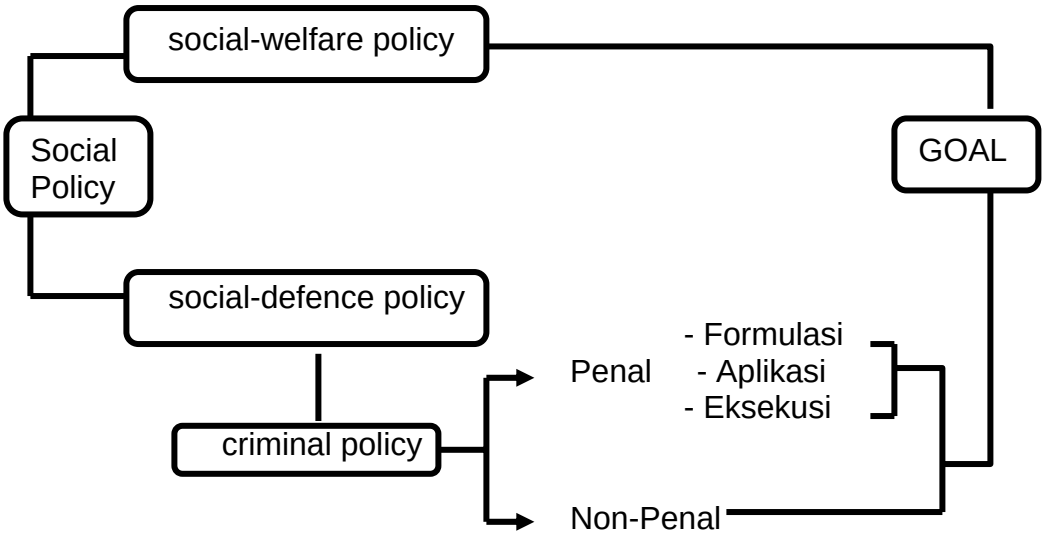
[138] Sudarto, *Kapita Selekta Hukum Pidana*, 1986, (Alumni:Bandung), halaman 113-114

[139] Sudarto, *Kapita Selekta Hukum Pidana*, 1986, (Alumni:Bandung), halaman 113-114

[140] Barda Nawawi Arief, 2002, *Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit*, halaman 2, lihat juga Muladi, *Kapita Selekta Sistem Peradilan Pidana*, 1995, Badan Penerbit UNDIP, Semarang, halaman 8

dalam upayanya untuk mencapai tujuan menggunakan sarana penal dan non penal, sehingga kebijakan penal dan non penal merupakan bagian yang tidak terpisahkan dari upaya perlindungan masyarakat dan upaya untuk mencapai kesejahteraan masyarakat atau dengan kata lain merupakan kebijakan integral.

Upaya penanggulangan kejahatan harus dilaksanakan secara sistematis dan integral, adanya keseimbangan antara upaya perlindungan masyarakat (*social defense*) serta upaya kesejahteraan masyarakat (*social welfare*). Dengan demikian dapat dikatakan bahwa politik kriminal pada hakekatnya juga merupakan bagian intergral dari politik sosial yaitu kebijakan atau upaya untuk mencapai kesejahteraan sosial. Hubungan tersebut secara skematis dapat digambarkan sebagai berikut :



Dari skema tersebut terlihat bahwa upaya penanggulangan kejahatan perlu ditempuh dengan pendekatan kebijakan, dalam arti ada ketepaduan antara politik kriminal dan politik sosial serta ada keterpaduan antara upaya penanggulangan kejahatan dengan penal dan non penal.[141]

Skema di atas juga mengambarkan bahwa pencegahan dan penanggulangan kejahatan harus menunjang tujuan (*goal) "social welfare*" dan "*social defence*". Kedua aspek tersebut yang sangat penting adalah aspek kesejahteraan/perlindungan masyarakat yang bersifat immaterial terutama nilai kepercayaan, kebenaran, kejujuran dan keadilan.[142]

Penegasan tentang perlunya upaya penanggulangan kejahatan diintergrasikan dengan keseluruhan kebijakan sosial dan perencanaan pembangunan terlihat juga dalam pernyataan **Sudarto** yang menyatakan bahwa apabila hukum pidana hendak digunakan sebagai sarana untuk menanggulangi kejahatan, maka penggunannya tidak terlepas dalam hubungan keseluruhan politik kriminal atau "*planning for*

---

[141] Barda Nawawi Arief, 2002, *Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit*, halaman 3

[142] Barda Nawawi Arief, 2001, *Masalah Penegakan Hukum dan Kebijakan Pengagulangan Kejahatan, (Citra Aditya Bhakti: Bandung), halaman* 74

*social defence". Social Defence Planning* ini pun harus merupakan bagian yang integral dari rencana pembangunan nasional.[143]

Beberapa kali konggres PBB mengenai *Prevention of Crime and the Treatment of Offender* juga mengisyaratkan hal yang sama tentang perlunya penanggulangan kejahatan diintegrasikan dengan keseluruhan kebijakan sosial dan perencanaan pembangunan nasional, sehingga kebijakan penanggulangan kejahatan tidak banyak artinya apabila kebijakan sosial atau kebijakan pembangunan itu sendiri justru menimbulkan faktor-faktor kriminogen dan viktimogen.[144]

Pernyataan yang hampir sama disampaikan oleh **Radzinowicz** sebagaimana dikutip oleh **Barda Nawawi Arief** yang menyatakan bahwa kebijakan kriminal harus mengkombinasikan bermacam-macam kegiatan preventif dan pengaturannya sedemikian rupa sehingga membentuk suatu mekanisme tunggal yang luas dan akhirnya mengkoordinasikan keseluruhannya itu kedalam suatu sistem kegiatan negara yang teratur.[145]

---

[143] Sudarto, *Hukum dan Hukum Pidana*, (Alumni:Bandung), 1986, halaman 96

[144] Barda Nawawi Arief, 2002, *Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit*, halaman 5-9. Pernyataan tersebut antara lain terlihat dalam konggres PBB ke-4 tahun 1970, Konggres PBB ke-5 tahun 1975, Konggres PBB ke-6 tahun 1980, Konggres PBB ke-7 tahun 1985 dan konggres PBB ke-8 tahun 1990 di Havana, Cuba, lihat juga Muladi, *Kapita Selekta Hukum Pidana*, Halaman 9-11

[145] Lihat Barda Nawawi Arief, *Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Pidana Penjara* (Semarang, Badan Penerbit UNDIP) 2000, halaman 34-35. Lihat juga Muladi dan Barda Nawawi Arief, 1992, *Teori-Teori dan Kebijakan Pidana,* (Alumni:Bandung),

Berkaitan dengan penggunaan hukum pidana sebagai sarana untuk penanggulangan kejahatan, **Muladi** menyatakan bahwa penegakan hukum pidana bukan merupakan satu-satunya tumpuan harapan untuk dapat menyelesaikan atau menanggulangi kejahatan secara tuntas. Hal ini wajar karena pada hakikatnya kejahatan itu merupakan "*masalah kemanusiaan*" dan *"masalah sosial*" yang tidak dapat diatasi semata-mata dengan hukum pidana sebagai suatu masalah sosial, kejahatan merupakan suatu fenomena kemasyarakatan yang dinamis, yang selalu tumbuh dan terkait dengan fenomena dan struktur kemasyarakatan lainnya yang sangat kompleks.[146]

Sejalan dengan pemikiran diatas, **Barda Nawawi Arief** menyatakan bahwa sehubungan dengan keterbatasan dan kelemahan yang dipunyai oleh hukum pidana antara lain karena penanggulangan atau "penyembuhan" lewat hukum pidana selama ini hanya merupakan penyembuhan/pengobatan simtomatik bukan pengobatan kausatif, dan pemidanaannya ("pengobatannya") hanya bersifat individual/personal,

---

halaman 159 disebutkan oleh Radzinowics bahwa *"criminal policy must combine the various preventive activities and adjust them so as to form a single comprehensive machine and finally coordinate the whole into an organized system of activity"*

[146] Muladi, *Kapita Selekta Sistem Peradilan Pidana*, *op.cit.* halaman 7

penggunaan atau intervensi "*penal*" seyogyanya dilakukan dengan lebih hati-hati, cermat, hemat, selektif dan limitatif.[147]

Dengan kata lain penggunaan sarana *penal* dalam hukum pidana pada suatu kebijakan kriminal memang bukan merupakan posisi strategis dan banyak menimbulkan persoalan. Persoalannya tidak terletak pada masalah "*eksistensinya*" tetapi terletak pada masalah kebijakan penggunaannya.[148]

Dilihat dari politik kriminal, usaha-usaha yang rasional untuk mengendalikan atau menanggulangi kejahatan, maka upaya penanggulangannya sudah barang tentu tidak hanya menggunakan sarana penal tetapi dapat juga dengan mengunakan sarana "non-penal", terlebih mengingat keterbatasan dari sarana penal itu sendiri. Upaya penanggulangan kejahatan melalui sarana non penal akan lebih mempunyai sifat pencegahan, sehingga yang menjadi sasaran utama penanganannya adalah mengenai faktor-faktor penyebab terjadinya kejahatan. Faktor-faktor tersebut adalah yang ditujukan terhadap kondisi-kondisi sosial yang secara langsung maupun tidak langsung dapat menimbulkan kejahatan atau tindak pidana. Usaha-usaha non

---

[147] Barda Nawawi Arief, 1998, *Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana*, (Citra Aditya Bhakti:Bandung), halaman 47-49

[148] Muladi dan Barda Nawawi Arief, *Teori-Teori dan Kebijakan Pidana*, (Alumni:Bandung), 1992, halaman 169

penal ini dapat meliputi bidang yang sangat luas sekali diseluruh sektor kebijakan sosial seperti misalnya penyantunan dan pendidikan sosial dalam rangka mengembangkan tanggung jawab sosial warga masyarakat, penggarapan kesehatan jiwa masyarakat melalui pendidikan moral, agama dan sebagainya. Tujuan utama dari usaha-usaha non penal ini adalah memperbaiki kondisi-kondisi sosial tertentu, namun secara tidak langsung mempunyai pengaruh preventif terhadap kejahatan. Dengan demikian dilihat dari sudut politik kriminal, keseluruhan kegiatan preventif yang non penal itu sebenarnya mempunyai kedudukan yang sangat strategis, memegang posisi kunci yang sangat diintensifkan dan diefektifkan.[149]

Ada dua masalah sentral dalam kebijakan/politik kriminal dengan menggunakan sarana penal (hukum) ialah masalah penentuan :

1. perbuatan apa yang seharusnya dijadikan tindak pidana, dan
2. sanksi apa yang sebaiknya digunakan atau dikenakan kepada si pelanggar.[150]

Dengan demikian dapat ditegaskan, bahwa masalah sentral hukum pidana mencakup tindak pidana, pertanggungjawaban pidana

---

[149] Muladi dan Barda Nawawi Arief, *Teori-Teori dan Kebijakan Pidana*, 1992, (Alumni:Bandung), halaman 159 Lihat pula Kebijakan Legisltif dalam Penanggulangan Kejahatan Dengan Pidana Penjara, 2000, (Badan Penerbit UNDIP:Semarang), halaman 33

[150] Barda Nawawi Arief, 2002, *Bunga Rampai Kebijakan Hukum Pidana*, *Ibid*.,halaman 29.

dan pidana. Kebijakan hukum pidana termasuk kebijakan dalam menanggulangi dua masalah sentral tersebut, yang harus pula dilakukan dengan pendekatan yang berorientasi pada kebijakan (*policy oriented approach*)[151] sehingga kebijakan hukum pidana (*penal policy)* dapat didefinisikan sebagai "usaha mewujudkan peraturan perundang-undangan pidana yang sesuai dengan keadaan dan situasi pada suatu waktu dan untuk masa yang akan datang[152].

Dari definisi tersebut sekilas terlihat bahwa "kebijakan hukum pidana" identik dengan "pembaharuan perundang-undangan hukum pidana" namun sebenarnya antara keduannya berbeda, dimana hukum pidana sebagai suatu sistem hukum yang terdiri dari budaya (culture), struktur dan substansi hukum, sehingga pembaharuan hukum pidana tidak sekedar memperbahaui perundang-undangan hukum pidana saja namun juga memperbaharui sektor-sektor lain seperti ilmu hukum pidana dan ide-ide hukum pidana melalui proses pendidikan dan pemikiran akademik.

---

[151] Muladi dan Barda Nawawi Arief, *Teori-Teori dan Kebijakan Pidana*, 1992, (Alumni:Bandung),, halaman 160-161

[152] Dalam hal ini Marc Ancel mendefinisikan *penal policy* sebagai "suatu ilmu sekaligus seni yang bertujuan untuk memungkinkan peraturan hukum positif (dalam hal ini hukum pidana) dirumuskan secara lebih baik". Lihat Barda Nawawi Arief, 2002, *Bunga Rampai Kebijakan Hukum Pidana*, (Citra Aditya Bakti:Bandung), halaman 21

Kebijakan hukum pidana dilaksanakan melalui tahap-tahap konkretisasi/operasionalisasi/fungsionalisasi hukum pidana yang terdiri dari tahap perumusan pidana (kebijakan formulatif/legislatif), tahap penerapan hukum pidana (kebijakan aplikatif/yudikatif), dan tahap pelaksanaan hukum pidana (kebijakan administratif/eksekutif)

Pembaharuan hukum pidana *(penal reform)* pada hakekatnya juga merupakan bagian dari kebijakan/politik hukum pidana *(penal policy)*, yang harus ditempuh dengan pendekatan yang berorientasi pada kebijakan (*policy-oriented approach)* dan pendekatan yang berorientasi pada nilai *(value-oriented approach)*[153] atau dengan kata lain upaya penanggulangan kejahatan perlu ditempuh dengan pendekatan kebijakan dalam arti ada keterpaduan (integrallis) antara politik kriminal dan politik sosial serta ada keterpaduan antara upaya penanggulangan kejahatan dengan penal dan non penal dan di dalam setiap kebijakan *(policy)* terkandung pula pertimbangan nilai.

Bertolak dari pendekatan kebijakan, **Sudarto** berpendapat bahwa dalam menghadapi masalah sentral dalam kebijakan kriminal terutama masalah pertama yang disebut juga masalah kriminalisasi, harus diperhatikan hal-hal yang pada intinya sebagai berikut :[154]

---

[153] Barda Nawawi Arief, 2002, *Bunga Rampai Kebijakan Hukum Pidana, Ibid*, halaman 28

[154] Barda Nawawi Arief, 2002, *Bunga Rampai Kebijakan Hukum Pidana*, *Ibid*, halaman 30

1. Penggunaan hukum pidana harus memperhatikan tujuan pembangaunan nasional yang mewujudkan masyarakat adil dan makmur yang merata, materiil, spirituil berdasarkan Pancasila; sehubungan dengan hal ini maka (penggunaan) hukum pidana bertujuan untuk menanggulangi kejahatan dan mengadakan pengugeran terhadap tindakan penangggulangan itu sendiri, demi kesejahteraan dan pengayoman masyarakat;
2. Perbuatan yang diusahakan untuk dicegah atau ditanggulangi dengan hukum pidana harus merupakan "perbuatan yang tidak dikehendaki", yaitu perbuatan yang mendatangkan kerugian (materiil dan atau spirituil) atas warga masyarakat;
3. Penggunaan hukum pidana harus pula memperhitungkan prinsip-prinsip biaya dan hasil (*cost and benefit principle*);
4. Penggunaan hukum pidana harus pula memperhatikan kapasitas atau kemampuan daya kerja dari bagian-bagian penegak hukum, yaitu jangan sampai ada kelampauan beban tugas (*overbelasting*)

Sejalan dengan yang dikemukakan Sudarto diatas, **Barda Nawawi Arief**[155] mengatakan bahwa menurut **Bassiouni** keputusan untuk melakukan kriminalisasi dan dekriminalisasi harus didasarkan pada faktor-faktor kebijakan tertentu yang mempertimbangkan bermacam-macam faktor, termasuk :

---

[155] Barda Nawawi Arief, 2002, *Bunga Rampai Kebijakan Hukum Pidana*, (Citra Aditya Bakti:, Bandung), halaman.32,. Mengenai pendapat M. Cherif Bassiuoni dalam bukunya *Substantive Criminal Law*, yang menyebutkan bahwa :

*The decision to sriminalize or decriminalize should be based on certain policy factor which take into account a variety of factor, including :*

*1. the proportionality of the means used in relationship to the outcome obtained;*

*2. the cost analysis of the outcome obtained in relationship to the objectives sought;*

*3. an appraisal of the objectives sought in relationship to other priorities in the allocation of human- power ; and*

*4. the social impact of criminalization and decriminalization in terms of its secondary effects*.

7) keseimbangan sarana-sarana yang digunakan dalam hubungannya dengan hasil-hasil yang ingin dicapai;
8) Analisis biaya terhadap hasil-hasil yang diperoleh dalam hubungannya dengan tujuan-tujuan yang dicari;
9) Penilaian atau penafsiran tujuan-tujuan yang dicari itu dalam kaitannya dengan prioritas-prioritas lainnya dalam pengalokasian sumber-sumber tenaga manusia;
10) Pengaruh sosial dari kriminalisasi dan dekriminalisasi yang berkenaan dengan atau dipandang dari pengaruh-pengaruh yang sekunder.

Hal lain yang perlu dikemukakan dari pendekatan kebijakan adalah yang berkaitan dengan nilai-nilai yang ingin dicapai atau dilindungi oleh hukum pidana. Menurut **Bassiouni**, tujuan-tujuan yang ingin dicapai oleh pidana pada umumnya terwujud dalam kepentingan-kepentingan sosial yang mengandung nilai-nilai tertentu yang perlu dilindungi. Kepentingan-kepentingan sosial tersebut menurut **Bassiouni** adalah :[156]

a. pemeliharaan tertib masyarakat;
b. perlindungan warga masyarakat dari kejahatan, kerugian atau bahaya-bahaya yang tidak dapat dibenarkan, yang dilakukan oleh orang lain;
c. memasyarakatkan kembali (rasionalisasi) para pelangar hukum;
d. memelihara atau mempertahankan integritas pandangan-pandangan dasar tertentu mengenai keadilan sosial, martabat kemanusiaan dan keadilan individu.

Kebijakan kriminal tidak dapat dilepaskan sama sekali dari masalah nilai karena seperti dikatakan oleh **Christiansen**, "*the*

[156] Muladi dan Barda Nawawi Arief, 2002, *Teori-Teori dan Kebijakan Pidana*, 1992, (Alumni:Bandung), halaman.166

*conseption of problem 'crime and punishment' is an essential part of the culture of any society*; begitu pula menurut **W. Clifford**, *the very foundation of any criminal justice system consists of the philosophy of given country.* Terlebih bagi Indonesia yang berdasarkan Pancasila dan garis kebijakan pembangunan nasionalnya bertujuan membentuk "manusia Indonesia seutuhnya".[157]

Kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana menjadi suatu tindak pidana. Pada hakikatnya, kebijakan kriminalisasi merupakan bagian dari kebijakan kriminal dengan menggunakan sarana hukum pidana, dan oleh karena itu termasuk bagian dari kebijakan hukum pidana.[158]

---

[157] Muladi dan Barda Nawawi Arief, 2002, *Teori-Teori dan Kebijakan Pidana*, 1992, (Alumni:Bandung), halaman.167

[158] Barda Nawawi Arief, 2002, *Bunga Rampai Kebijakan Hukum Pidana*, (Citra Aditya Bakti:Bandung), halaman.2-3

# BAB III

# HASIL DAN PEMBAHASAN

## A. Kebijakan Kriminal Saat ini dalam Menanggulangi Tindak Pidana *Cyber terrorism.*

### 1. Kebijakan Kriminalisasi atau Formulasi Tindak Pidana *Cyber Terrorism* di dalam Perundang-undangan di Indoensia.

*Cyber Terrorism* merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas di dunia internasional. A. Clem, MPH, memberikan isteilah CT sebagai *cyber ruang* dan *terrorisme,*[159] Beberapa sebutan lainya yang ”cukup keren” diberikan kepada jenis kejahatan baru ini di dalam berbagai tulisan, antara lain sebagai Terrorisme dunia maya.

Pertama-tama patut dikemukakan bahwa kebijakan penanggulangan CT dengan hukum pidana termasuk bidang *penal policy* yang merupakan bagian dari *criminal policy* (kebijakan penanggulangan kejahatan). Dilihat dari sudut *criminal policy,* upaya penanggulangan tindak pidana CT tidak dapat dilakukan semata-mata

---

[159] A. Clem, MPH, MSN Health Implications of Cyber-Terrorism Department of Environmental and Occupational Health, College of Public Health, University of South Florida, Tampa, Florida USA. http://www.mvhsmun.org/ConferenceSite/committees/specialized/CoT-Cyber-Terrorism_Synopsis.doc. Commission on Terror Komisi Terror

secara parsial dengan hukum pidana (sarana penal), tetapi harus ditempuh pula dengan pendekatan integral/sistemik. Sebagai salah satu bentuk *high tech crime*[160] yang dapat melampui batas-batas negara (bersifat *transnational*/transborder), merupakan hal yang wajar jika upaya penanggulangan CT juga harus ditempuh dengan pendekatan teknologi (*techno prevention*). Di samping itu, diperlukan pula pendekatan budaya/kultural, pendekatan moral/edukatif, dan bahkan pendekatan global (kerja sama internasional).[161]

Kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan yang dapat dipidana).

Kebijakan hukum pidana yang ditekankan pada penanggulangan kejahatan/penegakan hukum pidana/politik hukum pidana mengenai masalah CT pada penullsan ini adalah terbatas pada aspek/tahap kebijakan formulatif dari segi materiel, yaitu bagaimana formulasi perumusan suatu delik serta sanksi apa yang akan dikenakan terhadap pelanggarnya.

Berikut akan dilakukan pembahasan permasalahan pertama

---

[160] Australia High Tech Crime Centre 2003 membagi *high tech crime* Secara kasar dala dua kategori : (1) *crime commnited with or against computers or communication systems;* (2) *traditional crime which are largely facilitated by tehnology.* Dalam Barda Nawawi Arief, 2002, *Tindak Pidana Mayantara, Perkembangan Kajian Cyber Crime Di Indonesia.* PT. Raja Grafindo Persada : Jakarta. Hal, 90

[161] Lihat antara lain *Eighth UN Congress on the Prevention of Crime and the Treatment of Offender,* Reportm 1991, hlm.141 dst. Dan ITAC, *IIIC Common Views Paper on: Cyber Crime,* IIIC ITAC 2000 Millenium Congress, 19 September 2000, hlm. 5, dalam Barda Nawawi Arief, *Sari Kuliah Perbandingan Hukum Pidana* (Jakarta : PT Raja Grafindo, 2002) hlm 253-256

dalam tesis ini, dengan melakukan pengkajian apakah perundang-undangan tersebut dapat digunakan untuk menjangkau tindak pidana CT dengan melihat aspek sistem perumusan tindak pidananya, sistem pertanggungjawaban pidananya dan sistem perumusan sanksi pidananya, serta jenis-jenis saksi dan lamanya pidana.

Kebijakan formulasi hukum pidana yang berkaitan dengan masalah tindak pidana CT di bidang *cyber crime* dapat diidentifikasikan sebagai berikut :

**A. Kitab Undang-Undang Hukum Pidana Indonesia (KUHP)**

Kitab Undang-Undang Hukum Pidana Indonesia disingkat KUHP merupakan sistem induk bagi peraturan-peraturan hukum pidana di Indonesia. Meskipun KUHP ini merupakan buatan penjajah Belanda namun untuk saat ini karena belum ada perubahan atau penerimaan atas pembaharuan KUHP yang telah dilakukan oleh para ahli hukum pidana Indonesia yang telah diupayakan sejak tahun 1963 maka KUHP yang ada ini harus tetap dipergunakan demi menjaga keberadaan hukum pidana itu sendiri dalam masyarakat Indonesia.

Perumusan tindak pidana di dalam KUHP kebanyakan masih bersifat konvensional dan belum secara langsung dikaitkan dengan perkembangan CT yang merupakan bagian dari *cyber crime.* Di samping itu, mengandung berbagai kelemahan dan keterbatasan dalam mengahadapi perkembangan teknologi dan *high tech crime* yang sangat bervariasi.

Untuk menghadapi masalah pemalsuan kartu kredit dan transfer dana elektronik saja, KUHP mengalami kesulitan karena tidak ada ketentuan khusus mengenai perbuatan kartu kredit palsu. Ketentuan yang ada hanya mengenai : (a) sumpah/keterangan palsu, Bab IX Pasal 242; (b) pemalsuan mata uang dan uang kertas Bab X Pasal 244-252; (c) pemalsuan materai dan merek, Bab XI Pasal 253-262; (d) pemalsuan surat, Bab XII Pasal 263-276.[162]

Berkaitan dengan hal itu, apakah KUHP dapat digunakan dalam menanggulangi tindak pidana CT yang merupakan bagian dari *cyber crime,* berikut identifikasi penulis : (a) kejahatan terhadap ketertiban umum Bab V Pasal 168 ayat 1,2,dan 3; kejahatan terhadap nyawa Bab XIX Pasal 340; pencurian Bab XXII Pasal 362; pemerasan dan pengancaman Bab XXIII Pasal 368.

Berkaitan dengan permasalahan tersebut, jika KUHP ingin digunakan untuk menanggulangi tindak pidana CT haruslah diperhatikan terlebih dahulu batasan-batasan/ruang lingkup dan unsur-unsur/bentuk-bentuk CT yang telah penulis uraikan, sehingga dapat

[162] Barda Nawawi Arief, 2002, *Tindak Pidana Mayantara, Perkembangan Kajian Cyber Crime Di Indonesia.* PT. Raja Grafindo Persada : Jakarta. Hal, 90

dikatakan sebagai tindak pidana CT. Unsur-unsur tersebut antara lain :[163]

1. Serangannya melalui dunia maya bermotivasi politik yang dapat mengarah pada kematian luka-luka.
2. Menyebabkan ketakutan atau merugikan secara fisik atas tekhik serangan dari dunia maya tersebut.
3. Serangannya serius untuk melawan atau ditujukan ke infrastruktur informasi kritis seperti keuangan, energi, transportasi dan operasi pemerintah.
4. serangan yang mengganggu sarana yang tidak penting, bukan dikategorikan sebagai aksi cyber terrorism.
5. Serangan itu tidaklah semata-mata dipusatkan pada keuntungan moneter.

Jadi dari penjelasan di atas mengenai unsur-unsur/ bentuk-bentuk tindak pidana CT, maka penulis berkesimpulan bahwa KItab Undang-Undang Hukum Pidana, tidak dapat digunakan dalam menanggulangi tindak pidana CT.

## B. Undang-Undang di Luar KItab Undang-Undang Hukum Pidana

Dalam perkembangannya, saat ini telah ada perundang-undangan di Luar KUHP yang berkaitan dengan kejahatan teknologi canggih di bidang informasi, elektronik dan telekomunikasi yaitu sebagai berikut :

---

[163] The above definitions suggest that there are at least five elements which must be satisfied to construe cyberterrorism:
6. Politically motivated cyberattacks that lead to death or bodily injury;
7. Cause fear and/or physical harm through cyberattack techniques
8. Serious attacks against critical information infrastructure such as financial, energy, transportation and government operations;
9. Attacks that disrupt non-essential services are not considered as cyberterrorism;
10. Attacks that are not primarily focused on monetary gain.

*Ibid.* Cyberterrorism From Wikipedia, the free encyclopedia http://en.wikipedia.org/wiki/Cyber-terrorism

**1) Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektonik.**

Indonesia telah mensahkan salah satu Rancangan Undang-Undang yang berkaitan dengan kejahatan dunia maya (*cybercrime*) yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE). Undang-Undang ini bertujuan untuk mengharmonisasikan antara instrumen peraturan hukum nasional dengan instrumen-instrumen hukum internasional yang mengatur teknologi informasi diantaranya, yaitu: The United Nations Commissions on International Trade Law (UNCITRAL), World Trade Organization (WTO), Uni Eropa (EU), APEC, ASEAN, dan OECD. Masing-masing organisasi mengeluarkan peraturan atau model law yang mengisi satu sama lain. Dan juga instrument hukum internasional ini telah diikuti oleh beberapa negara, seperti: Australia (*The cyber crime act 2001*), Malaysia (*Computer Crime Act 1997*), Amerika Serikat (*Federal legislation: update April 2002 UNITED STATES CODE*), Kongres PBB ke 8 di Havana, Kongres ke X di Wina, kongres XI 2005 di Bangkok, berbicara tentang The Prevention of Crime and the Treatment of Offender. Dalam Kongres PBB X tersebut dinyatakan bahwa negara-negara anggota harus berusaha melakukan harmonisasi ketentuan ketentuan yang berhubungan dengan kriminalisasi, pembuktian dan prosedur (States should seek

harmonization of relevan provision on criminalization, evidence, and procedure)[164] dan negara-negara Uni Eropa yang telah secara serius mengintegrasikan regulasi yang terkait dengan pemanfaatan teknologi informasi ke dalam instrumen hukum positif (*existing law*) nasionalnya.[165]

UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik merupakan undang-undang yang mengatur tentang kejahatan-kejahatan yang berbasis teknologi (cyber crime), sedangkan tindak pidana CT merupakan bagian/jenis dari *cyber crime,* berikut identifikasi penulis :

**a. Sistem perumusan tindak pidana dalam UU ITE No. 11 Tahun 2008.**

Ketentuan pidana dalam UU ITE terdapat dalam Bab XI Pasal 45 sampai dengan Pasal 52. Berikut perumusan beberapa pasal dalam Bab XI mengenai ketentuan pidana :

---

[164] Prof. Barda Nawawi Arif. ***Tindak Pidana Mayantara***, *Perkembangan Kajian CyberCrime di Indonesia*. PT. Raja grafindo Persada : Jakarta, hal. v

[165] http://google.co.id/ *Naskah Akademik Rancangan Undang-Undang tentang informasi dan transaksi elektronik*

Pasal 45 UU No. 11 Tahun 2008

*(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) 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 memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau 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 memenuhi unsur sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).*

Pasal 52 UU No. 11 Tahun 2008

*(1) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 ayat (1) menyangkut kesusilaan atau eksploitasi seksual terhadap anak dikenakan pemberatan sepertiga dari pidana pokok.*
*(2) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik dipidana dengan pidana pokok ditambah sepertiga.*
*(3) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing-masing Pasal ditambah dua pertiga.*
*(4) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.*

Kualifikasi delik yang diatur dalam Undang-undang ITE tersebut diatur dalam Pasal 52 yang dikualifikasikan sebagai kejahatan.

Berdasarkan ketentuan pasal-pasal dalam Bab XI mengenai ketentuan pidana dalam UU ITE, maka dapat diidentifikasikan beberapa perbuatan yang dilarang (unsur tindak pidana) yang erat kaitannya dengan tindak pidana CT pada tiap-tiap pasalnya sebagai berikut :

Pasal 30 dengan unsur tindak pidana : megakses, menerobos, menjebol Sistem Komputer atau Sistem Elektronik milik orang lain secara illegal. (Terkait dengan aksi kejahatan CT yang berbentuk *unauthorized acces to computer system* dan *service*).

Pasal 31 dengan unsur tindak pidana : melakukan intersepsi/ penyadapan secara illegal atas Informasi Elektronik dan/atau Sistem Ellektronik dalam suatu komputer dan/atau Sistem Elektronik tertentu milik orang lain. (terkait dengan aksi kejahtan *Hacking*).

Pasal 32 dengan unsur tindak pidana : melakukan transmisi merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik dan/atau Dokumen Elektronik milik orang lain atau milik publik. (Terkait dengan aksi kejahatan CT yang berbentuk *cyber sabotage* dan *extortion*).

Pasal 33 dengan unsur tindak pidana : melakukan tindakan apa pun secara illegal yang berakibat terganggunya Sistem Elektronik menjadi tak bisa bekerja. (Terkait dengan aksi kejahatan CT yang berbentuk *unauthorized acces to computer system* dan *service*).

Pasal 34 dengan unsur tindak pidana : memperoduksi, menjual mengadakan untuk digunakan, mengimpor, menyediakan perangkat lunak komputer untuk tujuan kesusilaan atau eksploitasi seksual terhadap anak, penyadapan, merusak, dan

menghilangkan suatu Informasi Elektronik dan/atau Dokumen Elektronik dan/atau Dokumen Elektronik milik orang lain atau milik publik. (Terkait dengan aksi kejahatan CT yang berbentuk *Hackng, Cyber saborage* dan *extortion*).

Pasal 35 dengan unsur tindak pidana : melakukan perubahan, penciptaan, perusakan, penghilangan dan memanipulasi data Informasi Elektronik/ Dokumen Elektronik dengan tujuan Informasi dan/ atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik. (Terkait dengan aksi kejahatan *Hacking*).

Mengenai unsur sifat '*melawan hukum*', dalam undang-undang ITE tersebut disebutkan secara tegas, unsur 'sifat melawan hukum tersebut dapat dilihat pada perumusan "….*setiap orang dengan sengaja dan tanpa hak atau melawan hukum sebagaimana dalam pasal*…" seperti dirumuskan dalam Pasal 30 sampai dengan Pasal 37 tersebut di atas, sehingga dapat disimpulkan bahwa dengan disebutkannya secara tegas unsur '*sifat melawan hukum*' terlihat ada kesamaan ide dasar antara UU ITE dengan KUHP yang masih menyebutkan unsur sifat melawan hukumnya suatu perbuatan. Berbeda dengan Konsep KUHP baru yang sekarang tengah disusun yang menentukan bahwa meskipun unsur '*sifat melawan hukum*' tidak dicantumkan secara tegas, tetapi suatu delik harus tetap dianggap bertentangan dengan hukum.

Melihat berbagai ketentuan yang telah dikriminalisasikan dalam Undang-undang ITE tersebut, **nampak** adanya kriminalisasi terhadap perbuatan-perbuatan yang berhubungan dengan

penyalahgunaan penggunaan di bidang teknologi Infomasi dan Transaksi Elektronik, yang berbentuk tindak pidana CT.

Oleh karena itu, nampak bahwa perspektif Undang-undang Informasi dan Transaksi Elektronik adalah menekankan pada aspek penggunaan/keamanan Sistem Informasi Eleketronik atau Dokumen Elektronik, dan penyalahgunaan di bidang teknologi dan transaksi elektronik yang dilakukan oleh para pelaku CT.

**b. Sistem Perumusan Pertanggungjawaban pidana dalam Undang-Undang ITE**

Melihat perumusan ketentuan pidana dalam Undang-undang ITE sebagai mana diatur dalam Pasal 45 sampai dengan Pasal 52 maka dapat diidentifikasikan bahwa pelaku tindak pidana atau yang dapat dimintakan pertanggunjawaban pidana dalam undang-undang ITE adalah meliputi *individu/orang per orang* dan *korporasi*. Ini terbukti dari ketentuan pasal-pasal tersebut yang diawali dengan kata "*Setiap orang* …" dan "*korporasi*…".

Masalah pertanggungjawaban pidana berkaitan erat dengan pelaku tindak pidana. Pelaku yang dapat dipidana adalah orang dan korporasi, yang dijelaskan dalam Pasal 1 sub 21 dan dalam ketentuan pidana UU ITE tersebut.

UU ITE mengatur secara lanjut dan terperinci tentang ketentuan pertanggungjawaban pidana terhadap korporasi, karena UU ITE tersebut membedakan pertanggungjawaban pidana

terhadap individu dan korporasi, sebagaimana yang tercantum dalam Pasal 52 UU ITE.

**c. Sistem perumusan sanksi pidana, jenis-jenis sanksi dan lamanya pidana dalam UU ITE**

Sistem perumusan sanksi pidana dalam Undang-undang ITE adalah alternatif kumulatif. Hal ini bisa dilihat dalam perumusannya yang menggunakan kata "…*dan/atau*". Jenis-jenis saksi *(strafsoort)* pidana dalam Undang-undang ITE ini ada dua jenis yaitu pidana penjara dan denda. Sistem Perumusan lamanya pidana (*strafmaat*) dalam Undang-undang ITE ini adalah :

- Maxsimum khusus, pidana penjara dalam UU ITE paling lama 12 tahun.
- Maximum khusus pidana dendanya, paling sedikit sebanyak Rp 300.000.000,00 (tiga ratus juta rupiah), dan paling banyak Rp 12.000.000.000,00 (dua belas milyar rupiah).

Berdasarkan pembahasan di atas maka dapat diketahui bahwa Undang-undang Nomor 11 tahun 2008 tentang Informasi, dan Transaksi Elektronik dapat digunakan untuk menanggulangi jenis tindak pidana CT*,* sebagai suatu fenomena/bentuk baru *cyber crime* secara umum. Undang-undang ini menekankan pada pengaturan keamanan penggunaan Sistem Informasi Eleketronik atau Dokumen Elektronik, dan mengarah pada penyalahgunaan Informasi Eleketronik untuk tujuan perbuatan-perbuatan CT.

**2) UU No. 36 Tahun 1999 tentang Telekomunikasi**

Telekomunikasi terdiri dari kata ‘tele’ yang berarti jarak jauh (*at a distance*) dan ‘komunikasi’ yang berarti hubungan pertukaran ataupun penyampaian informasi, yang didefinisikan oleh UU Nomor 36 tahun 1999 sebagai setiap pemancaran, pengiriman informasi melalui medium apapun.

Undang-undang ini diundangkan pada tanggal 8 September 1999 dalam Lembaran Negara RI tahun 1999 Nomor 154, dengan Peraturan pelaksananya yaitu PP Nomor 52 tahun 2000 tentang Peraturan Pemerintah tentang Penyelenggaraan Telekomunikasi Indonesia dalam Lembaran Negara nomor 107 tahun 2000, TLN 3980. Salah satu pertimbangan dalam penyusunan Undang-undang telekomunikasi adalah bahwa pengaruh globalisasi dan perkembangan teknologi komunikasi yang sangat pesat telah mengakibatkan perubahan yang mendasar dalam penyelenggaraan dan cara pandang terhadap telekomunikasi. Penulis mencoba untuk mengkaji masalah CT ini dengan Undang-undang Telekomunikasi dengan pertimbangan bahwa jaringan internet merupakan salah satu alat atau sarana telekomunikasi yang dapat digunakan untuk memasukan dan menerima informasi, sehingga orang dapat saling melakukan komunikasi/hubungan walaupun berada di tempat yang berjauhan.

**a. Sistem perumusan tindak pidana dalam UU Telekomunikasi**

Ketentuan pidana dalam Undang-undang Nomor 36 tahun 1999 tentang Telekomunikasi terdapat dalam Bab VII Pasal 47 sampai dengan Pasal 57, berikut beberapa perumusan pasal dalam ketentuan pidananya :

Pasal 47 UU No. 36 tahun 1999:

*Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 11 ayat (1) dipidana dengan pidana penjara*

*paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah).*

Pasal 48 UU No. 36 tahun 1999:

*Penyelenggara jaringan telekomunikasi yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 19 dipidana dengan pidana penjara paling lama 1 (satu) tahun dan / atau denda paling banyak Rp 100.000.000,00 (seratus juta rupiah).*

Pasal 52 UU No. 36 tahun 1999:

*Barang siapa memperdagangkan, membuat, merakit, memasukkan, atau menggunakan perangkat telekomunikasi di wilayah Negara Republik Indonesia yang tidak sesuai dengan persyaratan teknis sebagaimana dimaksud dalam Pasal 32 ayat (1), dipidana dengan pidana penjara paling lama 1 (satu) tahun dan atau denda paling banyak Rp 100.000.000,00 (seratus juta rupiah).*

Pasal 59 UU No 36 tahun 1999

*Perbuatan sebagaimana dimaksud dalam Pasal 47, Pasal 48, Pasal 49, Pasal 50, Pasal 51, Pasal 52, Pasal 53, Pasal 54, Pasal 55, Pasal 56, dan Pasal 57 adalah kejahatan*

Kualifikasi delik yang diatur dalam Undang-undang Telekomunikasi tersebut diatur dalam Pasal 59 yang dikualifikasikan sebagai kejahatan.

Berdasarkan ketentuan pidana dari Pasal 47 sampai dengan Pasal 59 di atas, beberapa Pasal di antaranya dapat diidentifikasi unsur tindak pidananya sebagai berikut:

Pasal 47 dengan unsur tindak pidana: penyelenggaraan jaringan telekomunikasi yang tanpa izin dari menteri;

Pasal 50 dengan unsur tindak pidana: melakukan perbuatan tanpa hak, tidak sah atau memanipulasi, akses ke jaringan telekomunikasi dan/atau akses kejasa telekomunikasi

dan/atau akses ke jaringan ke telekomunikasi khusus;

Pasal 52 dengan unsur tindak pidana: memperdagangkan, membuat, merakit, memasukan dan/atau menggunakan perangkat komunikasi di wilayah Indonesia tanpa memenuhi syarat tekhnis dan ijin;

Pasal 53 dengan unsur tindak pidana: pengunaan spektrum frekwensi radio dan orbit satelit tanpa ijin pemerintah dan tidak sesuai dengan peruntukannya dan saling menganggu;

Pasal 55 dengan unsur tindak pidana: melakukan perbuatan yang menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi;

Pasal 56 dengan unsur tindak pidana: melakukan penyadapan informasi yang disalurkan melalui jaringan telekomunikasi; dan

Pasal 57 dengan unsur tindak pidana: tidak menjaga kerahasiaan infomasi yang dikirim dan/atau diterima oleh pelanggan.

Mengenai unsur sifat '*melawan hukum*', dalam undang-undang Telekomunikasi tersebut tidak disebutkan secara tegas, namun demikian unsur 'sifat melawan hukum' tersebut dapat dilihat pada perumusan "….*melanggar ketentuan sebagaimana dalam pasal*…" seperti dirumuskan dalam Pasal 47 sampai dengan Pasal 57 tersebut di atas, sehingga dapat disimpulkan bahwa dengan tidak disebutkannya secara tegas unsur '*sifat melawan hukum*' terlihat ada kesamaan ide dasar antara UU Telekomunikasi dengan Konsep KUHP baru yang sekarang tengah disusun yang menentukan bahwa meskipun unsur '*sifat melawan hukum*' tidak dicantumkan secara tegas, tetapi suatu delik harus tetap dianggap bertentangan dengan hukum. Disamping itu walaupun kata '*dengan sengaja*' tidak dicantumkan secara tegas, namun jika dilihat dari

unsur-unsur tindak pidana yang ada, maka tindak pidana yang dilakukan didasarkan pada unsur kesengajaan (*dolus*).

Jika dilihat dari unsur-unsur perbuatan yang dilarang seperti disebutkan di atas maka dapat diidentifikasikan perbuatan yang dilarang (unsur tindak pidana) yang erat kaitannya dengan penyalahgunaan internet untuk tujuan CT yaitu sebagaimana disebutkan dalam Pasal 22 berupa ’Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi: a). akses ke jaringan telekomunikasi; dan atau, b). akses kejasa telekomunikasi; dan atau, c). akses ke jaringan telekomunikasi khusus’, (Terkait dengan aksi kejahatan CT yang berbentuk *Unathorized acces to computer system and service*). Pasal 38 berupa ‘Setiap orang dilarang melakukan perbuatan yang dapat menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi’, (Terkait dengan aksi kejahatan *Cyber sabotaje and extortion*). Pasal 50 berupa ‘melakukan perbuatan tanpa hak, tidak sah atau memanipulasi, akses ke jaringan telekomunikasi dan/atau akses ke jasa telekomunikasi dan/atau akses ke jaringan ke telekomunikasi khusus’, (Terkait dengan aksi kejahatan *Unathorized acces to computer system and service*). dan Pasal 52 berupa ‘memperdagangkan, membuat, merakit, memasukan dan/atau menggunakan perangkat komunikasi

di wilayah Indonesia tanpa memenuhi syarat tekhnis dan ijin', (Terkait dengan aksi kejahatan *Carding*).

Melihat berbagai ketentuan yang telah dikriminalisasikan dalam Undang-undang Telekomunikasi tersebut, **nampak** adanya kriminalisasi terhadap perbuatan-perbuatan yang berhubungan dengan penyalahgunaan penggunaan internet, yang berbentuk tindak pidana CT.

Jika dicermati lebih lanjut, dalam UU Telekomunikasi tersebut ada pasal yang sebenarnya jika terjadi suatu pelanggaran dapat dikenai pidana tetapi hal tersebut justru tidak diatur secara lebih lanjut, yaitu pada Bagian Kelima tentang Hak dan Kewajiban Penyelenggara dan Masyarakat, yang dapat dilihat dalam perumusannya sebagai berikut:

Pasal 21 UU No. 36 tahun 1999:

*Penyelenggara telekomunikasi dilarang melakukan kegiatan usaha penyelenggaraan telekomunikasi yang bertentangan dengan* ***kepentingan umum****, kesusilaan,* ***keamanan, atau ketertiban umum.***

Terhadap pelanggaran Pasal 21 Undang-undang Telekomunikasi tersebut di atas, hanya dikenakan sanksi administratif saja sebagaimana disebutkan dalam Pasal 45 dan 46 UU Nomor 36 tahun 1999 tentang Telekomunikasi.

Pasal 45 UU No. 36 tahun 1999:

*Barang siapa melanggar ketentuan Pasal 16 ayat (1), Pasal 18 ayat (2), Pasal 19,* ***Pasal 21****, Pasal 25 ayat (2), Pasal 26 ayat (1), Pasal 29 ayat (1), Pasal 29 ayat (2), Pasal 33 ayat (1), Pasal 33 ayat (2), Pasal 34 ayat (1), atau Pasal 34 ayat (2) dikenai sanksi administrasi.*

Pasal 46 UU No. 36 tahun 1999:

*Sanksi administrasi sebagaimana dimaksud dalam Pasal 45 berupa pencabutan izin.*

*Pencabutan izin sebagaimana dimaksud pada ayat (1) dilakukan setelah diberi peringatan tertulis.*

Jika terjadi pelanggaran terhadap Pasal 21 tersebut di atas nampak tidak ada sanksi pidananya dan hanya sebatas sanksi administratif saja**,** yang juga tidak diatur dalam pasal-pasal yang lain. Padahal baik terhadap **kepentingan umum**, kesusilaan, **keamanan dan ketertiban umum** sebagaimana disebut dalam Pasal 21, kesemuanya memiliki kepentingan hukum yang juga harus senantiasa dilindungi dengan melalui hukum pidana.

Kaitannya dengan hal-hal yang bertentangan dengan kekepentingan umum keamanan, dan ketertiban umum dapat diidentifikasikan atau menunjuk pada perbuatan CT.

Seyogyanya jika terjadi pelanggaan terhadap ketentuan Pasal 21 Undang-undang Nomor 36 tahun 1999 tersebut harus disebutkan sebagai pelanggaran atau kejahatan terhadap **kepentingan umum**, kesusilaan, **keamanan, dan ketertiban umum** secara tegas, serta tersedia ancaman pidananya. Jika penyelenggara telekomunikasi dalam menjalankan usahanya ternyata bertentangan dengan kepentingan umum, kesusilaan, keamanan dan ketertiban umum maka hendaknya ditentukan bagaimana ancaman dan sanksi pidananya, tidak hanya sebatas sanksi administrasi aja, karena kepentingan umum, kesusilaan, keamanan dan ketertiban juga memiliki kepentingan hukum yang juga harus senantiasa dilindungi dengan melalui hukum pidana.

*Cyber terrorism* sebagai suatu fenomena kejahatan baru di dunia maya atau sebagai satu fenomena/bentuk baru dari *cyber crime* secara umum, yang dilakukan dengan menggunakan media internet sebagai salah satu sarana telekomunikasi, merupakan salah satu perbuatan berhubungan dengan **kepentingan umum, keamanan dan ketertiban umum**.

Hal tersebut juga dapat terlihat dalam kapasitas penyelenggara telekomunikasi, masalah telekomunikasi, alat telekomunikasi, perangkat telekomunikasi, maupun hal- hal yang memungkinkan di lakukannya perbuatan CT atau penggunaan internet sebagai salah satu sarana telekomunkasi untuk tujuan perbutan CT sebagai suatu hal yang menyangkut **kepentingan umum**, kesusilaan, **keamanan dan ketertiban umum**, seharusnya juga merupakan tanggung jawab penyelenggara telekomunikasi.

Namun demikian bagi penyelenggara telekomunikasi yang melakukan kegiatan usaha penyelenggaraan telekomunikasi yang bertentangan dengan **kepentingan umum**, kesusilaan, **ketertiban umum dan keamanan** tidak ada ancaman pidananya sama sekali, melainkan hanya dikenakan sanksi administratif saja sebagaimana disebutkan dalam Pasal 45.

Hal ini akan terlihat janggal dan tidak proporsional jika dibandingkan dengan ketentuan Pasal 47 yang menyebutkan bagi mereka yang melangar Pasal 11 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,- (enam ratus juta rupiah) hanya karena tidak mendapatkan izin dari menteri dalam penyelenggaraan telekomunikasi. Sementara pelanggaran atau kejahatan terhadap Pasal 21 yang menyangkut **kepentingan umum**, kesusilaan, **keamanan dan ketertiban umum** hanya dikenai sanksi

administratif saja. Apakah perlu ancaman pidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,- (enam ratus juta rupiah) bagi penyelenggara telekomunikasi yang tidak memenuhi kriteria Pasal 7, sementara bagi penyelenggara telekomunikasi yang melakukan kegiatan usaha penyelenggaraan telekomunikasi bertentangan dengan kepentingan umum, kesusilaan, keamanan dan ketertiban umum ternyata tidak ada ancaman pidananya sama sekali yang juga sebenarnya di dalamnya terkandung kepentingan hukum yang seyogyanya dilindungi dari sekedar penyelenggaraan telekomunikasi tanpa mendapatkan ijin dari menteri. Untuk lebih jelasnya lihat ketentuan Pasal 47, Pasal 11 dan Pasal 7 sebagai berikut:

Pasal 47 UU No. 36 tahun 1999:

*Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam **Pasal 11 ayat (1)** dipidana dengan pidana penjara paling lama 6 (enam) tahun dan / atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah).*

Pasal 11 UU Nomor 36 tahun 1999:

*Penyelenggaraan telekomunikasi sebagaimana dimaksud dalam **Pasal 7** dapat diselenggarakan setelah mendapat izin dan Menteri.*

*Izin sebagaimana dimaksud pada ayat (1) diberikan dengan memperhatikan :*

*a. Tata cara yang sederhana;*
*b. Proses yang transparan, adil dan tidak diskriminatif; serta*
*c. Penyelesaian dalam waktu yang singkat.*

*Ketentuan mengenai perizinan penyelenggaraan telekomunikasi sebagaimana dimaksud pada ayat (1) dan ayat (2) diatur dengan Peraturan Pemerintah.*

Pasal 7 UU No. 36 tahun 1999:

*(1) Penyelenggaraan telekomunikasi meliputi :*
*b. Penyelenggara jaringan telekomunikasi;*

*c. Penyelenggaraan jasa telekomunikasi;*
*c. Penyelenggaraan telekomunikasi khusus.*

*(2) Dalam penyelenggaraan telekomunikasi, diperhatikan hal-hal sebagai berikut :*
*a.Melindungi kepentingan dan keamanan negara;*
*b.**Mengantisipasi perkembangan teknologi dan tuntutan global**;*
*c.Dilakukan secara profesional dan dapat dipertanggungjawabkan;*
*d.Peran serta masyarakat.*

**b. Sistem perumusan pertanggungjawaban pidana dalam Undang-Undang Telekomunikasi**

Melihat perumusan ketentuan pidana dalam Undang-undang Telekomunikasi sebagai mana diatur dalam Pasal 47 sampai dengan Pasal 57 maka dapat diidentifikasikan bahwa pelaku tindak pidana atau yang dapat dimintakan pertanggunjawaban pidana dalam undang-undang Telekomunikasi adalah meliputi *individu/orang per orang* dan *korporasi*. Ini terbukti dari ketentuan pasal-pasal tersebut yang diawali dengan kata "*Barang siapa*…" dan "*Penyelenggara jasa telekomunkasi*…", terkecuali pada Pasal 48 yang diawali dengan kata "*Penyelenggaraan jaringan telekomunikasi…*".

Masalah pertanggungjawaban pidana berkaitan erat dengan pelaku tindak pidana. Untuk pasal yang diawali dengan kata "*Barang siapa*…", maka yang dimaksud pelaku dalam pengertian kalimat ini adalah individu dan badan hukum. Hal ini bisa dilihat

dalam ketentuan Pasal 1 angka 8 dan diatur lebih lanjut dalam Pasal 8 ketentuan tentang badan hukum yang disebut sebagai Penyelenggaraan jaringan telekomunikasi dan/atau penyelenggaraan jasa telekomunikasi serta Penyelenggaraan telekomunikasi khusus sebagaimana dimaksud Pasal 7 Undang-undang Telekomunikasi.

Pasal 1 angka 8 UU No.36 tahun 1999:

***Penyelenggara telekomunikasi*** *adalah : perseorangan, koperasi, badan usaha milik daerah, badan usaha milik negara, badan usaha swasta, instansi pemerintah, dan instansi pertahanan keamanan Negara*

Pasal 7 ayat (1) UU No.36 tahun 1999:

*Penyelenggaraan telekomunikasi meliputi :*

*a. Penyelenggaraan jaringan telekomunikasi;*
*b. Penyelenggaraan jasa telekomunikasi;*
*c. Penyelenggaraan telekomunikasi khusus*

Pasal 8 ayat (2) UU No. 36 tahun 1999:

*(1) Penyelenggaraan jaringan telekomunikasi dan / atau penyelenggaraan jasa telekomunikasi, sebagaimana dimaksud dalam Pasal 7 ayat (1) huruf a dan huruf b, dapat dilakukan oleh badan hukum yang didirikan untuk maksud tersebut berdasarkan peraturan perundang-undangan yang berlaku, yaitu:*

*a. Badan Usaha Milik Negara (BUMN);*
*b. Badan Usaha MiIik Daerah (BUMD);*
*c. Badan usaha swasta; dan*
*d. atau Koperasi.*

*(2) Penyelenggaraan telekomunikasi khusus sebagaimana dimaksud dalam Pasal 7 ayat (1) huruf c dapat dilakukan oleh :*

*Perseorangan;*
*Instansi pemerintah;*
*Badan hukum selain penyelenggara jaringan telekomunikasi dan/atau penyelenggara jasa telekomunikasi.*

Sementara dalam PP Nomor 52 tahun 2000 yaitu Peraturan Pemerintah tentang Penyelenggaraan Telekomunikasi Indonesia yang merupakan Peraturan pelaksana UU Telekomunikasi menyebutkan secara jelas bahwa Penyelenggaraan Jasa Telekomunikasi terdiri dari penyelenggaraan jasa teleponi dasar, penyelenggaraan jasa nilai tambah telepon dan penyelengaraan jasa multimedia yang diatur lebih lanjut dalam Keputusan Mentri, tetapi tidak disebutkan secara jelas apa yang termasuk dalam jasa multimedia tersebut.

Namun demikian Undang-undang Telekomunikasi tidak mengatur secara lanjut dan terperinci tentang ketentuan pertanggung jawaban pidana terhadap korporasi, karena ternyata dalam undang-undang tersebut tidak membedakan pertanggungjawaban terhadap individu dan korporasi bahkan aturan pemidanaan terhadap keduanya sama. Seharusnya jika suatu undang-undang menganggap korporasi sebagai dapat dipertanggungjawabkan dalam hukum pidana maka harus dijelaskan secara rinci kapan dan siapa yang dapat dipertanggungjawabkan serta bagaimana jenis dan ancaman pidannya. Hal ini untuk menghindari berbagai kemungkinan yang dapat terjadi dalam tahap aplikasinya. Terlebih dalam hal tidak

dapat terbayarnya denda yang dikenakan pada korporasi, karena selama masih menggunakan KUHP maka akan dikembalikan kepada sistem induknya yaitu KUHP, di mana jika denda tidak terbayar maka akan dikenakan kurungan pengganti yang tidak mungkin dikenakan pada korporasi, apalagi dalam Undang-undang tersebut juga tidak menjelaskan siapa yang dapat dimintakan pertanggungjawabannya dalam hal korporasi melakukan kejahatan/pelanggaran. Dapat disimpulkan pula bahwa dalam Undang-undang Telekomunikasi tidak ada ketentuan tentang pedoman pemidanaan atau cara bagaimana pidana tersebut dilaksanakan *(strafmodus)* sebagai pedoman bagi hakim.

**c. Sistem perumusan sanksi pidana, jenis-jenis sanksi dan lamanya pidana dalam UU Telekomunikasi**

Sistem perumusan sanksi pidana dalam Undang-undang Telekomunikasi adalah alternatif kumulatif. Hal ini bisa dilihat dalam perumusannya yang menggunakan kata "…*dan/atau*…", dengan pengecualian pada Pasal 53 yang mengancamkan sanksi pidana berupa pidana penjara secara tunggal sebagai pidana pokok yang dirumuskan secara tunggal.

Jenis-jenis saksi *(strafsoort)* pidana dalam Undang-undang Telekomunikasi ini ada dua jenis yaitu pidana penjara dan denda serta tindakan yang diatur dalam Pasal 58.

Pasal 58 UU No. 36 tahun 1999:

*Alat dan perangkat telekomunikasi yang digunakan dalam*

*tindak pidana sebagaimana dimaksud dalam Pasal 47, Pasal 48, Pasal 52, atau Pasal 56 dirampas untuk negara dan/atau dimusnahkan sesuai dengan peraturan perundang-undangan yang berlaku.*

Sistem Perumusan lamanya pidana (*strafmaat*) dalam Undang-undang Telekomunikasi ini adalah:

Maksimum khusus pidana penjara berkisar antara 1 tahun sampai dengan 15 tahun.

Maksimum khusus pidana denda berkisar antara Rp 100.000.000, (seratus juta rupiah) - sampai dengan Rp 600.000.000 ,(enam ratus juta rupiah).

Selain itu disebutkan pula sanksi administratif dalam Pasal 45 dan 46 sebagai sanksi administratif yang murni dan bukan merupakan sanksi pidana administratif.

Berdasarkan pembahasan di atas maka dapat diketahui bahwa Undang-undang Nomor 36 tahun 1999, ***dapat*** digunakan untuk menanggulangi jenis tindak pidana CT, sebagai suatu fenomena/bentuk baru *cyber crime* secara umum. Undang-undang ini menekankan pada pengaturan jaringan komunikasi.

**3) UU No. 15 Tahun 2003 jo. Perppu No. 1 Tahun 2002 tentang Tindak Pidana Terorisme.**

Berawal dari ledakan bom yang terjadi di Bali tanggal 12 Oktober 2002 yang meluluhlantahkan *Sari Cafe* dan *Paddy's Club,* dua tempat hiburan yang terletak di jalan Legian Kuta Bali telah menimbulkan korban ratusan jiwa melayang dan harta benda yang nilainya ratusan juta rupiah.

Pada dasarnya permasalahan ini bukan permasalahan yang luar biasa dari kaca mata hukum pidana karena hukum pidana yang ada (KUHP) dapat digunakan untuk menanggulangi serta membawa para pelaku pemboman ke muka pengadilan. Tetapi dibalik permasalahan itu muncul pemberian nama atas perbuatan itu dengan sebutan “terrorisme” sehingga menimbulkan persoalan hukum. Persoalan hukum yang timbul adalah bahwa perangkat hukum yang ada tidak dapat digunakan untuk menuntut para pelaku peledakan bom tersebut ke depan pengadilan, seolah-olah ada kekosongan hukum mengenai terrorisme.[166]

Kepentingan hukum yang dibahayakan oleh tindakan terrorisme tidak hanya berupa jiwa dan harta benda, tetapi juga rasa takut masyarakat, kebebasan pribadi, integritas nasional, kedaulatan negara, fasilitas international, instalasi publik, lingkungan hidup, sumber daya alam nasional, serta sarana transportasi dan komunikasi. Terrorisme dapat terjadi kapan saja dan dimana saja serta mempunyai jaringan yang sangat luas sehingga merupakan ancaman terhadap perdamaian dan keamanan, baik nasional maupun internasional.

---

[166] Nyoman Serikat Putra Jaya, *Beberapa Pemikiran Ke Arah Pengembangan Hukum Pidana.* PT. Citra Adtya Bakti: Bandung, 2008

Berkaitan dengan permasalahan terrorisme tersebut dibentuklah suatu Perpu Nomor 1 Tahun 2002 yang berlakunya tidak serta merta dan tidak secara otomatis. Sebagai pelaksana ketentuan Perpu Nomor 1 Tahun 2002, pemerintah mengerluarkan Perpu Nomor 2 Tahun 2002 tentang permberlakuan Perpu Nomor 1 Tahun 2002 pada peristiwa peledakan bom di Bali. Namun perkembanganya, saat ini Perpu Nomor 2 tahun 2002 ini dengan Undang-undang Nomor 16 Tahun 2003 ditingkatkan menjadi undang-undang, sedangkan Perpu Nomor 2 Tahun 2002 tentang Pemberantasan Tindak Pidana Terrorisme ditingkatkan menjadi Undang-undang Nomor 15 Tahun 2003 (selanjutnya disingkat UU terorisme).

**a. Sistem perumusan tindak pidana dalam UU Tindak Pidana Terrorisme**

Ketentuan pidana dalam Undang-undang Nomor 15 tahun 2003 jo Perpu Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terrorisme terdapat dalam Bab III Pasal 6 sampai dengan Pasal 19, berikut beberapa perumusan pasal dan ketentuan pidana tersebut :

Pasal 6

*Setiap orang yang dengan sengaja menggunakan kekerasan atau ancaman kekerasan menimbulkan suasana teror atau rasa takut terhadap orang secara meluas atau menimbulkan korban yang bersifat massal, dengan cara merampas kemerdekaan atau hilangnya nyawa dan harta benda orang lain, atau mengakibatkan*

*kerusakan atau kehancuran terhadap obyek-obyek vital yang strategis atau lingkungan hidup atau fasilitas publik atau fasilitas internasional, dipidana dengan pidana mati atau penjara seumur hidup atau pidana penjara paling singkat 4 (empat) tahun dan paling lama 20 (dua puluh) tahun.*

Pasal 9

*Setiap orang yang secara melawan hukum memasukkan ke Indonesia, membuat, menerima, mencoba memperoleh, menyerahkan atau mencoba menyerahkan, menguasai, membawa, mempunyai persediaan padanya atau mempunyai dalam miliknya, menyimpan, mengangkut, menyembunyikan, mempergunakan, atau mengeluarkan ke dan/atau dari Indonesia sesuatu senjata api, amunisi, atau sesuatu bahan peledak dan bahan-bahan lainnya yang berbahaya dengan maksud untuk melakukan tindak pidana terorisme, dipidana dengan pidana mati atau penjara seumur hidup atau pidana penjara paling singkat 3 (tiga) tahun dan paling lama 20 (dua puluh) tahun.*

*Pasal 11*

*Dipidana dengan pidana penjara paling singkat 3 (tiga) tahun dan paling lama 15 (lima belas) tahun, setiap orang yang dengan sengaja menyediakan atau mengumpulkan dana dengan tujuan akan digunakan atau patut diketahuinya akan digunakan sebagian atau seluruhnya untuk melakukan tindak pidana terorisme sebagaimana dimaksud dalam Pasal 6, Pasal 7, Pasal 8, Pasal 9, dan Pasal 10*.

Pasal 14

*Setiap orang yang merencanakan dan/atau menggerakkan orang lain untuk melakukan*
*tindak pidana terorisme sebagaimana dimaksud dalam Pasal 6, Pasal 7, Pasal 8, Pasal 9, Pasal 10, Pasal 11, dan Pasal 12 dipidana dengan pidana mati atau pidana penjara seumur hidup.*

Pasal 15

*Setiap orang yang melakukan permufakatan jahat, percobaan, atau pembantuan untuk melakukan tindak pidana terorisme sebagaimana dimaksud dalam Pasal 6, Pasal 7, Pasal 8, Pasal 9,*

*Pasal 10, Pasal 11, dan Pasal 12 dipidana dengan pidana yang sama sebagai pelaku tindak pidananya.*

Pasal 17

*(1) Dalam hal tindak pidana terorisme dilakukan oleh atau atas nama suatu **korporasi**, maka tuntutan dan penjatuhan pidana dilakukan terhadap korporasi dan/atau pengurusnya.*
*(2) Tindak pidana terorisme dilakukan oleh korporasi apabila tindak pidana tersebut dilakukan oleh orang-orang baik berdasarkan hubungan kerja maupun hubungan lain, bertindak dalam lingkungan korporasi tersebut baik sendiri maupun bersama-sama.*
*(3) Dalam hal tuntutan pidana dilakukan terhadap suatu korporasi, maka korporasi tersebut diwakili oleh pengurus.*

Pasal 18

*(1) Dalam hal tuntutan pidana dilakukan terhadap korporasi, maka panggilan untuk menghadap dan penyerahan surat panggilan tersebut disampaikan kepada pengurus di tempat tinggal pengurus atau di tempat pengurus berkantor.*
*(2) Pidana pokok yang dapat dijatuhkan terhadap korporasi hanya dipidana dengan pidana denda paling banyak Rp 1.000.000.000.000,- **(satu triliun rupiah**).*
*(3) Korporasi yang terlibat tindak pidana terorisme dapat dibekukan atau dicabut izinnya dan dinyatakan sebagai korporasi yang terlarang.*

Pasal 19

*Ketentuan mengenai penjatuhan pidana minimum khusus sebagaimana dimaksud dalam Pasal 6, Pasal 8, Pasal 9, Pasal 10, Pasal 11, Pasal 12, Pasal 13, Pasal 15, Pasal 16 dan ketentuan mengenai penjatuhan pidana mati atau pidana penjara seumur hidup sebagaimana dimaksud dalam Pasal 14, tidak berlaku untuk pelaku tindak pidana terorisme yang berusia di bawah 18 (delapan belas) tahun.*

Melihat berbagai ketentuan yang telah dikriminalisasikan dalam Undang-undang Pemberantasan Tindak Pidana Terrorisme tersebut, **nampak** adanya kriminalisasi terhadap perbuatan-

perbuatan yang berhubungan dengan penyalahgunaan penggunaan internet, yang berbentuk tindak pidana CT.

Bahkan jika dicermati dari kasus yang telah terjadi, seperti kasus ditemukannya situs *www.anshar.com* yang dibuat oleh Agung Prabowo dan Agung Setyadi kaki tangan Imam Samudera dijatuhi hukuman dengan menggunakan UU Terorisme tersebut.

**b. Sistem perumusan pertanggungjawaban pidana dalam Undang-Undang Pemeberantasan Tindak Pidana Terrorisme.**

Melihat perumusan ketentuan pidana dalam UUTerrorisme sebagai mana diatur dalam Pasal 6 sampai dengan Pasal 19 maka dapat diidentifikasikan bahwa pelaku tindak pidana atau yang dapat dimintakan pertanggunjawaban pidana dalam undang-undang pemberantasan tindap adalah meliputi *individu/orang per orang* dan *korporasi*. Ini terbukti dari ketentuan pasal-pasal tersebut yang diawali dengan kata "*Setiap orang*…" dan "*Koporasi*.

UU Terrorisme mengatur secara lanjut dan terperinci tentang ketentuan pertanggung jawaban pidana terhadap korporasi. Hal tersebut dapat terlihat dalam Pasal 17 danPasal 18.

Pasal 17

*(1) Dalam hal tindak pidana terorisme dilakukan oleh atau atas nama suatu **korporasi**, maka tuntutan dan penjatuhan pidana dilakukan terhadap korporasi dan/atau pengurusnya.*

*(2) Tindak pidana terorisme dilakukan oleh korporasi apabila tindak pidana tersebut dilakukan oleh orang-orang baik berdasarkan hubungan kerja maupun hubungan lain, bertindak dalam lingkungan korporasi tersebut baik sendiri maupun bersama-sama.*
*(3) Dalam hal tuntutan pidana dilakukan terhadap suatu korporasi, maka korporasi tersebut diwakili oleh pengurus.*

Pasal 18

*(1) Dalam hal tuntutan pidana dilakukan terhadap korporasi, maka panggilan untuk menghadap dan penyerahan surat panggilan tersebut disampaikan kepada pengurus di tempat tinggal pengurus atau di tempat pengurus berkantor.*
*(2) Pidana pokok yang dapat dijatuhkan terhadap korporasi hanya dipidana dengan pidana denda paling banyak Rp 1.000.000.000.000,-* ***(satu triliun rupiah)****.*
*(3) Korporasi yang terlibat tindak pidana terorisme dapat dibekukan atau dicabut izinnya dan dinyatakan sebagai korporasi yang terlarang.*

**c. Sistem perumusan sanksi pidana, jenis-jenis sanksi dan lamanya pidana dalam UU Pemberantasan Tindak Pidana Terorisme.**

Sistem perumusan sanksi pidana dalam UU Terrorime adalah tunggal. Hal ini bisa dilihat dalam perumusannya yang menggunakan kata mengancamkan sanksi pidana berupa pidana penjara secara tunggal sebagai pidana pokok yang dirumuskan secara tunggal.

Jenis-jenis saksi *(strafsoort)* pidana dalam UU Terrorime ini ada dua jenis yaitu pidana penjara dan denda. Ketentuan yang mengatur pidana denda khusus ditujukan kepada korporasi, di atur dalam Pasal 18 berupa

*(1) Dalam hal tuntutan pidana dilakukan terhadap korporasi, maka panggilan untuk menghadap dan penyerahan surat panggilan tersebut disampaikan kepada pengurus di tempat tinggal pengurus atau di tempat pengurus berkantor.*

*(2) Pidana pokok yang dapat dijatuhkan terhadap korporasi hanya dipidana dengan pidana denda paling banyak Rp 1.000.000.000.000,-* ***(satu triliun rupiah****).*

*(3) Korporasi yang terlibat tindak pidana terorisme dapat dibekukan atau dicabut izinnya dan dinyatakan sebagai korporasi yang terlarang.*

Sistem Perumusan lamanya pidana (*strafmaat*) dalam UU Terrorisme ini adalah:

1. Maksimum khusus pidana penjara berkisar sampai dengan 15 tahun.
2. Maximum umum pidana penjara 15 tahun.
3. Pidana denda yang hanya ditujukan kepada korporasi sebesar Rp 1. 000.000.000.000,- (satu triliun rupiah).

Berdasarkan pembahasan di atas maka dapat diketahui bahwa Undang-undang Nomor 15 Tahun 2003 jo Perpu Nomor 1 Tahun 2002, **dapat** digunakan untuk menanggulangi jenis tindak pidana CT, sebagai suatu fenomena/bentuk baru *cyber crime*. Hal tersebut dapat terlihat dalam ketentuan yang ada dalam Pasal 27 yang mengakui adanya Electronic Record sebagai alat bukti.

## C. Aspek Juridiksi

Sisi lain dari aspek/persyaratan objektif untuk

mempertanggungjawabkan CT merupakan masalah juridiksi, khususnya yang berkaitan dengan masalah ruang berlakunya hukum pidana menurut tempat. Dalam sistem hukum pidana yang berlaku saat ini, Hukum pidana pada umumnya hanya berlaku di wilayah negaranya sendiri (asas teritorial) dan untuk warga negaranya sendiri (asas personal/nasional aktif). Hanya untuk delik-delik tertentu dapat digunakan asas nasional pasif dan asas universal. Asas-asas ruang berlakunya hukum pidana menurut tempat yang konvensional/tradisional (juridiksi fisik) itu pun tentunya menghadapai tantangan sehubungan dengan masalah pertanggungjawaban CT.

Masalah juridiksi CT yang merupakan bagian dari jenis *cyber crime* tersebut termasuk yang sangat serius. Barbara Etter, didalam tulisannya berjudul *Critical Issues in High Tech Crime*[167] mengidentifikasi beberapa masalah kunci yang terkait atau yang menyebabkan timbulnya masalah juridiksi ini dalam konteks internasional antara lain :

1. Tidak adanya consensus global mengenai jenis-jenis CRC (Computer Related Crime), dan tindak pidana pada umumnya;
2. Kurangnya keahlian aparat penegak hukum dan ketidakcukupan hukum untuk melakukan investigasi dan mengakses sistem komputer.
3. Adanya sifat transnasional dan *computer crime;*

---

[167] *The lack of global consensus on what types of conduct should constitute a computer-related crime; The lack of global consensus on the the legal definition of criminal conduct; The lack of expertise on the part of police, prosecutors and the courts in this field; The inadequacy of legal powers for investigation and acces to computer system, including the inapplicability of seizure powers to intangibles such as computerized data the lack concerning the investigation of computer-related crime; The transnational character of many computer crime;and The lack of extradition and mutual assistance treaties and of synchronized law enforcement mechanisms that would permit international cooperation, or the inability of existing treaties to take into account the dynamics and special reguirements of computer crime investigation.* (bahan *Commonwealth Investigations Conference, Australia*, 10 September 2002). dalam **Barda Nawawi Arief**, ***Tindak Pidana Mayantara, Perkembangan Cyber Crime di Indonesia****,* PT. Raja grafindo Persada : Jakarta, 2005, hal. 107-108

4. Ketidakharmonisan hukum acara/procedural di berbagai Negara;
5. Kurang singkronisasi mekanisme penegakan hukum, bantuan hukum, ektradisi, dan kerja sama internasional dalam melakukan investigasi *cyber crime.*

Sehubungan dengan masalah juridiksi, UU di Australia memberi kewenangan untuk menuntut seseorang di mana pun berada yang menyerang komputer di wiliyah Aunstralia. Bahkan di USA, tidak hanya dapat menuntut setiap orang asing yang menyerang komputer-komputer di USA, tetapi juga orang Amerika yang menyerang komputer di Negara-negara lain.[168] Dari ketentuan demikian terlihat bahwa komputer dipandang sebagai kepentingan nasional dan sekaligus kepentingan international yang sepatutnya dilindungi, apalagi yang berkaitan dengan penyalahgunaan internet yang mengarah kepada perbuatan CT*,* tentunya juga akan sangat dilindungi sehingga terkesan dianut asas ubikuitas *(the principle of ubiquity)*[169] atau asas *omnipresence* (ada dimana-mana). Dianutnya asas ini tentunya harus didukung oleh kemampuan suatu Negara dan kerjasama international.

Sehubugan dengan masalah juridiksi tersebut, dalam Konsep RUU KUHP 2008 akan ada ketentuan mengenai perluasan asas berlakunya hukum pidana dan tempat terjadinya tindak pidana yang berorientasi pada “perbuatan” dan “akibat”, sehingga diharapkan dapat

---

[168] *Legal Frameworks For Combating Cyber Crime, Components of substantive Network Crime Laws: How to Criminalize Attacks on Computer Networks and Information,* bahan-bahan pelatihan tentang ”Cyber Crime Legislation and Enforsement Capacity Building”*,* Hanoy, Vietnam, 25-27 Agustus 2004. dalam **Barda Nawawi Arief**, ***Tindak Pidana Mayantara, Perkembangan Cyber Crime di Indonesia****,* PT. Raja grafindo Persada : Jakarta, 2005, hal.108

[169] Prinsip “ubikuitas” adalah prinsip yang menyatakan bahwa delik-delik yang dilakukan/terjadi sebagian diwiliyah territorial negara dan sebagian di luar territorial suatu negara, tetapi harus dapat di bawa ke dalam juridiksi setiap negara yang terkait.

menjaring tindak pidana (CT yang merupakan bagian dari *crime*) di luar territorial Indonesia yang akibatnya terjadi di Indonesia. Dalam Konsep RUU KUHP 2008 antara lain ada perumusan sebagai berikut :

Asas Wilayah atau Teritorial

**Pasal 3**

Ketentuan pidana dalam peraturan perundang-undangan Indonesia berlaku bagi setiap orang yang melakukan:

a. tindak pidana di wilayah Negara Republik Indonesia;
b. tindak pidana dalam kapal atau pesawat udara Indonesia; atau
c. tindak pidana di bidang teknologi informasi yang akibatnya dirasakan atau terjadi di wilayah Indonesia dan dalam kapal atau pesawat udara Indonesia.

Asas Nasional Pasif

Pasal 4

Ketentuan pidana dalam peraturan perundang-undangan Indonesia berlaku bagi setiap orang di luar wilayah Negara Republik Indonesia yang melakukan tindak pidana terhadap:

a. warga negara Indonesia; atau
b. kepentingan negara Indonesia yang berhubungan dengan :
    1. keamanan negara atau proses kehidupan ketatanegaraan;
    2. martabat Presiden dan/atau Wakil Presiden dan pejabat

Indonesia di luar negeri;
3. pemalsuan dan peniruan segel, cap negara, meterai, uang atau mata uang, kartu kredit, perekonomian, perdagangan, dan perbankan Indonesia;
4. keselamatan atau keamanan pelayaran dan penerbangan;
5. keselamatan atau keamanan bangunan, peralatan, dan aset nasional atau negara Indonesia;
6. keselamatan atau keamanan peralatan komunikasi elektronik;
7. tindak pidana jabatan atau korupsi; dan/atau
8. tindak pidana pencucian uang.

Tempat Tindak Pidana

Pasal 10

Tempat tindak pidana adalah:

a. tempat pembuat melakukan perbuatan yang dilarang oleh peraturan perundangundangan; atau
b. tempat terjadinya akibat yang dimaksud dalam peraturan perundang- undangan atau tempat yang menurut perkiraan pembuat akan terjadi akibat tersebut.

**2. Kebijakan Non Penal Saat ini dalam Mengatasi Tindak Pidana Cyber Terrorism**

konggres PBB ke-6 tahun 1980 di Caracas, Venezuela mengenai "*Crime Trends and crime prevention Strategis*" terlihat bahwa upaya non penal mempunyai kedudukan strategis, yang antara lain dinyatakan:[170]

[170] *Sixth UN Congress Report,* 1981, halaman 5,dalam Barda Nawawi Arief, 2002, *Bunga*

a. Bahwa masalah kejahatan merintangi kemajuan untuk pencapaian kualitas hidup yang pantas bagi semua orang;

(*The problem impedes progress towards the attainment of an acceptable quality of life for all people)*;

b. Bahwa strategi pencegahan kejahatan harus didasarkan pada penghapusan sebab-sebab dan kondisi-kondisi yang menimbulkan kejahatan;

(*Crime prevention strategis should be based upon the eliminatio of causes and conditions giving rise to crime)*;

c. Bahwa penyebab utama kejahatan dibanyak negara ialah ketimpangan sosial, diskriminasi rasial dan diskriminasi nasional, standar hidup yang rendah, penganguran dan kebutahurufan (kebodohan) diantara golongan besar penduduk;

*(The main causes of crime in many countries are social inequality, racial and national discrimination, low standar of living, unemployment and illiteracy among broad section of the population).*

*Cyber terrorism* sebagai bagian dari tindak pidana *cyber crime* atau perbuatan yang menyalahgunakan teknologi internet yang akibatnya dapat mengakibatkan kepanikan/ketakukan, kerugian secara fisik dan psikis terhadap individu maupun masyarakat dan menyerang sarana infrastrukstur penting suatu negara, sehingga mengakibatkan kerugian yang besar terhadap target sasarannya, untuk penanggulangannya pun harus diorientasikan pada pengaturan

---

*Rampai Kebijakan Hukum Pidana*, *Op.Cit*, hlm. 43

penggunaan teknologi internet itu sendiri seraya menanggulangi penyakit psikologis yang ditimbulkannya oleh provokasi ideology yang dilancarkan oleh para kaum terrorisme dalam merekrut dan menghegemony massanya.

Menyadari tentang pentingnya pengaturan mengenai CT ini sebagai salah bagian/jenis dari cyber crime yang memanfaatkan teknologi internet maka, pengaturan mengenai internetlah yang seharusnya dilakukan. Jika dilhat dari sudut metode **pendekatan teknologi (*techno prevention*)**[171] ini, untuk menahan gencarnya penyalahgunaan pemakain internet oleh para kaum hacker dan cracker/CT, Beberapa langkah yang dapat dilakukan dalam pengamanan sistem informasi berbasis interenet antara lain :[172]

**a. Mengatur akses *(access control)***

Salah satu cara yang umum digunakan untuk mengamankan informasi adalah dengan mengatur akses ke informasi melalui mekanisme *authentication* dan *access control.* Implementasi dari

---

[171] Pendekatan tekhnologi (pendekatan *techno-prevention*) yaitu upaya pencegahan/penanggulanga kejahatan dengan menggunakan tekhnologi. Perlunya penanggulangan kejahatan *cyber crime* secara tekhnologi diungkapkan oleh IIIC (*International Information Industry Congress*) yang mengakui bahwa tindakan pemerintah dan perjaanjian internasional untuk mengharmonisasikan hukum dan mengkordinasikan prosedur hukum merupakan kunci dalam upaya penanggulangan *cyber crime*, namun patut diingat bahwa hal ini janganlah diandalkan sebagai satu-satunya alat. *Cybercrime* dimungkinkan (terjadi) oleh tekhnologi dan (oleh karena itu) memerulukan suatu kepercayaan yang baik pada tekhnologi untuk pemecahannya. Dalam Barda Nawawi Arief, 2002, *Sari Kuliah Perbandingan Hukum Pidana*, Raja Grafindo Persada, Jakarta, hlm. 254-255.

[172] Budi Rahadjo, *op.cit,* hal. 51. Bandingkan dengan pendapat Arianto Mukti Wibowo yang terdapat dalam makalahnya berjudul *Keamanan Dalam Teknologi Informasi,* makalah pada seminar Nasional RUU Teknologi Informasi, Gradhika Bakti Praja, Semarang, 26 Juli 2001.

mekanisme ini antara lain dengan menggunakan *paswoord.* Di sistem UNIX dan Windows NT, untuk masuk dan menggunakan sistem komputer, pemakai harus melalui proses *authentication* dengan menuliskan *userid (user identification)* dan paswoord*.* Apabila keduanya valid, maka pemakai di perbolehkan untuk masuk dan menggunakan sistem, tetapi apabila diantara keduanya atau salah satunya tidak valid, maka akses akan di tolak. Penolakan ini tercatat dalam berkas *log* berupa waktu dan tanggal akses, asal hubungan *(connection)* berapa kali koneksi yang gagal itu. Setelah proses *authentication,* pemakai diberikan akses sesuai dengan level yang dimilikinya melalui sebuah *acsess 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 *supresure* yang memiliki kemampuan lebih dari grup lainnya. Pengelompokkan ini disesuaikan dengan kebutuhan dan penggunaan sistem yang ada.

**b. Menutup *service* yang tidak digunakan**

Sering kali 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. Dalam praktek pengelolaan situs, tidak semua service itu dipakai/dibutuhkan sehingga untuk mengamankan sistem *service* yang tidak diperlukan di *server* (komputer) tersebut sebaiknya dimatikan. Hal ini dilakukan karena banyak kasus terjadi yang menunjukkan *abuse* dari servis tersebut atau lubang kemanan dalam servis tersebut. Akan tetapi, administrator sistem tidak menyadari bahwa servis tersebut dijalankan di komputernya.

c. **Memasang proteksi**

Untuk lebih meningkatkan keamanan sistem informasi, proteksi dapat ditambahkan. Proteksi ini dapat berupa *filter* (secara umum) dan yag lebih spesifik adalah *firewall.* Filter dapat digunakan untuk memfilter e-mail, informasi, akses atau bahkan dalam level *packet* sebagai contoh, di sistem UNIX ada paket program *tcpwrapper* yang dapat digunakan untuk membatasi akses kepada service atau aplikasi tertentu. Misalnya, service untuk telnet dapat dibatasi untuk sistem yang memiliki nomor IP tertentu atau memiliki domain tertentu. Sementara *firewall* digunakan untuk melakukan filter secara tertentu. Sementara *firewall* digunakan untuk melakukan filter secara umum.

**d. Firewall**

*Firewall* merupakan sebuah perangkat yang diletakkan antara internal dengan jaringan internal. Informasi yang keluar atau masuk

harus melalui *firerwall* ini. Tujuan utama dar *firewall* adalah untuk menjaga *(prevent)* agar akses (ke dalam maupun ke luar) dari orang yang berwenang *(unauthorized acces)* tidak dapat dilakukan. Konfigurasi dari *firewall* bergantung kepada kebijaksanaan *(policy)* dari organisasi yang bersangkutan, yang dapat dibagi menjadi 2 (dua) jenis, yaitu :

1). Apa-apa yang tidak diperbolehkan secara ekplisit dianggap tidak diperbolehkan *(prohobitted); dan*

2). Apa-apa yang tidak dilarang secara ekplisit dengan diperbolehkan *(permitted).*

*Firewall* bekerja dengan mengamati paket *Internet Protocol* (IP) yang melewatinya. Berdasarkan konfigurasi dari *firewall,* maka akses dapat diatur berdasarkan *Internet Protocol* (IP) *andress, port* dan arah informasi. Detail dari konfigurasi bergantung kepada masing-masing *firewall.*

**e. Pemantau adanya serangan**

Sistem pemantau *(monitoring system)* digunakan untuk mengetahui adanya tamu tidak diundang *(intruder)* atau adanya serangan *(attack).* Nama lain 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 *Intuder,* baik yang sifatnya aktif maupun

pasif. *Intruder Detection Sistem* (IDS) cara yang paling pasif misalnya dengan monitor *log file.*

Ada beberapa contoh dari *Intuder Detection Sistem* (IDS), antara lain :

1). *Autobase*, mendeteksi *probing* dengan memonitor *log file.*
2). *Courtney* dan *portsentry,* mendeteksi *probing (port scanning)* dengan memonitor *packet* yang lalu lalang. *Portsentry* bahkan dapat memasukkan *internet Protocol* (IP) penyerang dalam *filter tcpwrapper.*
3). *Shadow* dan *SANS.*
4). *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 sistem**

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 database mengenai berkas-berkas atau direktori yang ingin kita amati beserta *signature* dari berkas, kapan dibuatnya, pemiliknya, hasil *checksum* atau *hash* dan sebagainya. Apabila ada perubahan pada berkas tersebut, maka keluaran dari *hush function* akan berbeda dengan yang ada di database 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 penyimpangan yang terjadi. Kegagalan untuk masuk ke sistem *(login)* misalnya tersimpan untuk rajin memlihara dan menganalisis berkas *log* yang dimilikinya.

**h. *Back up* secara rutin**

Sering kali masuk ke dalam sistem dan merusak sistem dengan menjebol sistem dan masuk sebagai *superesure,* maka ada kemungkinan dia dapat menghapus seluruh berkas. Untuk itu, adanya *back up* yang dilakukan secara rutin merupakan sebuah hal yang essential. Banyangkan jika yang berhasil dihapus oleh *intruder* itu adalah data-data rahasia apalagi data rahasia keamanan Negara.

**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 service di internet yang masih menggunakan *plain text* untuk *authentication* seperti penggunaan pasangan *userid* dan *password.* Informasi ini dapat dilihat dengan mudah oleh program penyadap atau penghapus *(sniffer).*

Untuk meningkatkan keamanan *server world wide web* dapat digunakan enkripsi pada tingkat *socket.* Dengan menggunakan enkripsi, orang tidak biasa 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.*

Secara umum seluruh pengguna internet hendaknya memahami etika penggunaan internet guna menghindari terjadinya penyalahgunaan terhadapnya. Pendekatan ini lebih dikenal dengan **pendekatan budaya/kultural** dalam kebijakan penanggulangan tindak pidana CT yang merupakan bagian/jenis dari *cybercime* yaitu membangun/membangkitkan kepekaan warga masyarakat termasuk di dalamnya orang tua serta aparat hukum terhadap masalah CT dan menyebarluaskan/mengajarkan etika penggunaan komputer melalui media pendidikan sebagaimana diamanatkan dalam salah satu butir dalam Resolusi Konggres PBB ke-8 di Havana Cuba yaitu memperluas *'rules of ethis'* dalam penggunaan komputer dan mengajarkannya melalui kurikulum informatika.

Selain itu juga terungkap dalam pernyataan *International information Industry Congres* tahun 2000 yang diselenggarakan oleh ITAC (*International Technology Association of Canada*, bahwa para anggota IIIC juga berpartisipasi dalam membangun atau

mengembangkan kode etik dan perilaku dalam menggunakan komputer dan internet, dan berkampanye mengenai perlunya perilaku yang etis dan bertanggungjawab. Untuk memberikan hasil/pencapaian upaya penanggulangan kejahatan internet secara internasional, maka para pengguna komputer dan internet seluruh dunia harus disadarkan akan perlunya standar/norma perilaku berkualitas tinggi (terpuji) diruang *cyber*.

Etika penggunaan internet ini dikenal dengan nama *cyber ethics*, yang berisi : [173]

Setiap orang harus bertanggungjawab terhadap perilaku sosial dan hukum tatkala menggunakan internet;

Tidak seharusnya ikut serta dalam berbagai bentuk saiber yang mengganggu;

---

[173] ***http//www.ParentNews Safety.com, cyber ethics:***

*Everyone should practice responsible social and legal behavior while on the Internet.*

*No one should participate in any form of cyber-bullying.*

*People should not say anything to anyone on the Internet that they would not say to them in person.*

*Copying or downloading copyrighted programs, games, or music without getting permission or paying for them is illegal*

*In order to avoid plagiarism, it is important to give credit to any Internet sites used for research.*

*Never hack into another person's computer, send e-mail from another persons account or read other people's mail..*

*Never intentionally spread computer viruses.*

*The Internet is not private and anything you do or say may come back to haunt you*

Seharusnya tidak bercakap-cakap tentang satu apapun kepada orang lain yang tidak dikenal di internet;

Mengcopy atau men-*download* program yang berhak cipta, *games* atau musik tanpa ijin atau tanpa membayar adalah perbuatan illegal;

Untuk menghindari plagiat '*plagiatism'* penting untuk memberi kredit terhadap situs yang digunakan untuk riset;

Tidak ada penggemar pada komputer pribadi yang berkirim surat satu sama lain atau saling membacanya;

Jangan pernah bermaksud menyebarkan virus komputer;

Internet tidak bersifat pribadi dan apa yang anda lakukan atau katakan akan kembali kepada anda.

Sejalan dengan yang dikemukankan oleh *International information Industry Congres* tahun 2000 yang diselenggarakan oleh ITAC (*International Technology Association of Canada),* maka hal-hal dapat diupayakan guna menanggulangi tindak pidana CT**,** yaitu : 1). pengenalan komputer dan internet kepada masyarakat, dan 2). peran serta masyarakat dalam bidang komputer dan internet .

1). Pengenalan komputer dan internet kepada masyarakat

Pengenalan yang dimaksud di sini adalah upaya sosialisasi komputer dan internet di tengah-tengah masyarakat. Upaya ini dapat ditempuh dengan jalan sebagai berikut :[174]

a) Pengenalan Komputer dan Internet Lewat Pendidikan

Penandatanganan nota kesepakatan antara PT Indosat dan Departemen Pendidikan Nasional (Depdiknas) tentang pengembangan *Cyber Education (CE),* di Malang Jawa Timur, merupakan salah satu upaya pengenalan komputer dan internet kepada masyarakat sejak usia dini.

Prinsip dasar *Cyber Education* cukup sederhana, yakni memamfaatkan teknologi *multimedia* internet untuk menyalurkan suatu materi dari satu tempat ke tempat lain. Untuk itu, tempat-tempat yang bersangkutan harus terhubung dalam jaringan komunikasi berbasis protokol internet. PT Indosat, melalui anak perusahaannya Indosat Multi Media, menyediakan infrastruktur sekaligus menyiapkan koneksi internet yang menghubungkan antar lokasi dalam satu jaringan. Depdiknas secara bertahap mengembangkan jaringan internet ke sekolah-sekolah di Kabupaten/Kota seluruh Indonesia.

---

[174] Sutarman, ***Cyber Crime, Modes Operandi dan Penanggulangannya,*** LaksBang PRESSindo, Jogjakarta, 2007, hal.101-102 *kata pengantar dari* Prof. Dr. M. Kholidin, S.H.,M.H.,C.n. (Guru Besar Ilmu Hukum Universitas Jember).

Pada tahap awal, jaringan sekolah dibentuk ditujuh kota sebagai proyek percontohan, yaitu Jakarta, Bandung, Surabaya, Malang, Yogjakarta, Solo dan Makasar. Di setiap kota disiapkan suatu jaringan yang disebut *Wide Area Network* (WAN) kota untuk menghubungkan sekolah satu dengan yang lainnya.

Dengan dibangunnya jaringan antar sekolah tersebut maka data pendukung, referensi, ataupun berbagai informasi lain yang relevan dapat diperoleh dengan cepat dan mudah. Selain itu, juga dapat dilakukan diskusi dan pengajaran jarak jauh.

b) Seminar Teknologi Informasi

Acara-acara seminar teknologi informasi sangat membantu pengenalan teknologi computer dan internet kepada mayarakat. Seminar yang dimaksudkan di sini dalam arti luas, di mana bisa juga dalam bentuk diskusi interaktif, bedah buku teknologi informasi, seminar dan lokakarya (SEMILOKA), *workshop* dan sebagainya. Misalnya arena konferensi, *workshop,* dan tutorial internet yang disponsori oleh Direktur PT Internetindo Data Centre Indonesia, Sri Handayani. Beliau juga bertindak sebagai selaku Ketua Panitia *Nice 2004* di Gedung

*Cyber* Jakarta. Pada kesempatan itu, Sri Handayani menyatakan pertemuan tersebut diproyeksikan sebagai ajang tahunan sekelas *Asia Pacific Regional Confrence on Operational Technologies* yang menjadi agenda wajib bagi para *netter* di kawasan Asia Pasifik.

Dalam acara tersebut pesertanya adalah kalangan akademisi dari Institut Teknologi Bandung, Universitas Indonesia, dan Univeersitas Brawijaya. Selain itu juga para operator dari berbagai penyedia jasa telekomunikasi, seperti Telkom, Satelindo, Exwlindo, perusahaan lain di bidang telekomunikasi. Sementara dari kalangan *vendor* hadir para profesional dari PT Cisco Sistem Indonesia, PT Multipolar, dan PT Sun Micosystem Indonesia turut memeriahkan acara.

Untuk memperkaya wawasan peserta, juga didatangkan para ahli dari institusi yang terkait erat dengan dunia internet, yaitu APNIC, IndoCISC, Polri, Kejaksaan, Kelompok Pengguna Linux Indonesia (KPLI), dan sebagainya.

2). Peran Serta Masyarakat dalam bidang komputer dan internet

Dalam konsep keamanan masyarakat modern, sistem keamanan bukan lagi tanggung jawab polisi semata, namun menjadi tanggung jawab bersama seluruh elemen masyarakat.

Dalam pandangan konsep ini, masyarakat di samping sebagai obyek juga sebagai subyek.

Sebagai subyek, masyarakat adalah pelaku aktivitas komunikasi antara yang satu dengan yang lain, serta pengguna jasa kegiatan internet dan media lainnya. Sebagai obyek, masyarakat dijadikan sasaran dan korban kejahatan bagi segenap aktivitas kriminalisasi internet.

Tanggung jawab bersama atas keamanan dan ketertiban di tengah masyarakat dalam konsep modern disebut *Community Policing.* Salah satu model pengamanan dan penegakan hokum yang professional di negara-negara maju. Semua elemen masyarakat dengan kesadaran penuh terpanggil dan bertanggung jawab atas keamanan dan ketertiban.

Dilibatkannya masyarakat dalam strategi pencegahan kejahatan mempunyai dua tujuan pokok, menurut Mohammad Kemal Dermawan adalah untuk :[175]

a. Mengeliminir faktor-faktor kriminogen yang ada dalam masyarakat.

b. Masyarakat potensi masyarakat dalam hal mencegah dan mengurangi kejahatan.

---

[175] Mohammad Kemal Dermawan, ***Strategi Pencegahan Kejahatan***, Citra Aditya Bakti, Bandung, 1994, h. 10

## B. Kebijakan Kriminal Yang Akan Datang dalam menanggulangi tindak pidana *cyber terrorism* di Indonesia.

### 1. Kebijakan Penal (Kebijakan formulasi hukum pidana) di masa yang akan datang untuk mengantisipasi tindak pidana *cyber terrorism* di Indonesia

Hukum dituntut peranannya dalam rangka mengantisipasi perubahan dan perkembangan yang terjadi dalam masyarakat, dengan menjamin bahwa pelaksanaan perubahan dan perkembangan tersebut dapat berjalan dengan cara yang teratur, tertib dan lancar. Bagaimanapun perubahan yang teratur melalui prosedur hukum dalam bentuk perundang-undangan/keputusan badan peradilan akan lebih baik dari pada perubahan yang tidak direncanakan. Pada perkembangannya, di Indonesia saat ini memang telah dibentuk peraturan perundang-undangan yang mengatur secara khusus tentang kejahatan komputer (*Cybercrime*), yaitu Undang-undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik disingkat ITE, yang mana pada uraian sebelumnya penulis berkesimpulan UU ITE ini tidak dapat digunakan dalam menanggulangi tindak pidana *cyebr terrorism.*

Dilihat dari sudut "*criminal policy*", upaya penanggulangan kejahatan CT yang merupakan bagian dari *Cybercrime* tentunya tidak dapat dilakukan secara parsial dengan hukum pidana (sarana *"penal")*, tetapi harus ditempuh pula dengan pendekatan integral/sistemik. Sebagai salah satu bentuk dari kejahatan tekhnologi tinggi "*hitech*

*crime*"[176], maka upaya penanggulangan CT juga harus ditempuh dengan pendekatan teknologi (*techno prevention*). Di samping itu diperlukan pula pendekatan budaya/ kultural, pendekatan moral/edukatif, dan bahkan pendekatan global (kerja sama internasional) karena kejahatan ini melampaui batas-batas negara (bersifat "*transnational/ transborder*")[177].

Dengan kata lain, proteksi terhadap *netizen/netter* (warga dunia maya-pengguna jasa internet) dari tindak kejahatan *cyber*, selain melalui perangkat teknologi dan berbagai pendekatan lain tersebut juga melalui sarana hukum, khususnya *cyber crime law* (hukum pidana siber). Namun membuat suatu ketentuan hukum terhadap bidang yang berubah cepat sungguh bukanlah suatu hal yang mudah, karena di sinilah terkadang hukum (peraturan perundang-undangan) tampak cepat menjadi usang manakala mengatur bidang-bidang yang mengalami perubahan cepat, sehingga situasinya seperti terjadi kekosongan hukum (*vaccum rechts*) termasuk terhadap CT ini. Di sisi lain, banyak negara yang telah melakukan pengembangan sistem hukum nasionalnya untuk menyikapi dan mengakomodir perkembangan internet, khususnya dengan membuat produk-produk legislatif yang baru yang berkaitan dengan keberadaan internet.

---

[176] Australian High Tech Crime Centre 2003 membagi "*Hitech crime*" secara kasar dalam dua kategori : (1) *crimes committed with or against computers or communication systems; (2) traditional crimes which are largely facilitated by technology*. Dalam Barda Nawawi Arief; Antisipasi Hukum Pidana Dan Perlindungan Korban *Cyber Crime* Di Bidang Kesusilaan, makalah pada Seminar "Kejahatan Seks melalui *Cyber Crime* dalam Perspktif Agama, Hukum, dan Perlidungan Korban", F.H UNSWAGATI, di Hotel Zamrud Cirebon, tanggal 20 Agustus 2005, hlm. 11

[177] Lihat antara lain *Eighth UN Congress on the Prevention of Crime and the Treatment of Offenders*, Report, 1991, hal. 141 dst. dan ITAC, *"IIIC Common Views Paper On: Cyber Crime"*, IIIC 2000 Millenium Congress, September 19th, 2000, p. 5, dalam Barda Nawawi Arief, *Sari Kuliah Perbandingan Hukum Pidana*, PT RajaGrafindo, Jakarta, 2002, hlm. 253 – 256.

Oleh karena itu pembaharuan hukum pidana (KUHP) merupakan suatu keharusan yang tidak dapat ditawar. Berbagai negara lain juga bahkan telah terlibat dalam usaha pembaharuan kodifikasi hukum pidana masing-masing, terutama setelah Perang Dunia II, baik negara-negara seperti Jerman, Polandia, Swedia, Jepang, Yugoslavia, maupun negara-negara yang baru tumbuh setelah perang dunia II seperti Korea Selatan, Mali dan lain sebagainya. Korea Selatan telah memberlakukan KUHP produk sendiri sejak tahun 1953 menggantikan warisan penjajahan sebelumnya. Sedangkan Mali mengesahkan KUHP sendiri tahun 1953. Karena itu Indonesia yang sudah memproklamirkan diri sebagai negara yang merdeka dan berdaulat pada tahun 1945, dalam hubungan ini dapat dianggap sebagai lambat dalam usaha pembaharuan KUHP-nya. Hingga kini KUHP warisan penjajahan Belanda yang diberlakukan belum juga kunjung digantikan dengan yang baru, meskipun Konsep Rancangan KUHP barunya telah dirumuskan berkali-kali.[178]

Tindak pidana pada hakikatnya merupakan "perbuatan yang diangkat" atau "perbuatan yang ditunjuk/ditetapkan" ("*benoemd gedrag*" atau "*designated behaviour*") sebagai perbuatan yang dapat dipidana oleh pembuat undang-undang. Secara singkat G.P. Hoefnagels menyatakan, "*crime is behavior designated as a punishable act*" [179].

---

**178** Jimly Asshidiqie, 1996, *Pembaharuan Hukum Pidana Indonesia*, *Study Tentang Bentuk-bentuk Pidana dalam Tradisi Hukum Fiqih dan Relevansinya bagi Usaha Pembaharuan KUHP Nasional*, (Angkasa:Bandung), hlm. 1

[179] G.P. Hoefnagels, *The Other Side of Criminology*, Kluwer-Deventer, Holland, 1973, p. 90.

Penentuan "*benoemd gedrag"/"designated behaviour*" ini merupakan bagian dari kebijakan kriminal (*criminal policy*). Oleh karena itulah, G. P. Hoefnagels juga menyatakan, bahwa *"criminal policy is a policy of desig-nating human behavior as crime*" [180] (kebijakan kriminal adalah suatu kebijakan dalam menetapkan perilaku manusia sebagai suatu kejahatan/tindak pidana)

Menurut **G.Peter Hoefnagels**, penanggulangan kejahatan dapat ditempuh dengan[181] :

a. Penerapan hukum pidana (*criminal law application*);
b. Pencegahan tanpa pidana (*prevention without punishment)*;
c. Mempengaruhi pandangan masyarakat mengenai kejahatan dan pemidanaan lewat media massa *(influencing views of society on crime and punishment/mass media*)

Dalam pembagian **Hoefnagels** tersebut , upaya yang disebut dalam butir (a) dapat dimasukan dalam kelompok *"penal"* sedangkan yang disebutkan dalam butir (b) dan (c) dapat dimasukan ke dalam kelompok *"non penal"*. Secara singkat dapatlah dibedakan, bahwa upaya penanggulangan kejahatan lewat jalur *penal* lebih menitikberatkan pada sifat "represif" (penindasan/penumpasan) sesudah kejahatan terjadi, sedangkan jalur *non-penal* lebih menitikberatkan pada tindakan preventif (pencegahan/pengendalian) sebelum kejahatan terjadi. Dalam tindakan represif juga di dalamnya

---

[180] Ibid., hlm. 100.

[181] Barda Nawawi Arief, 2002, *Bunga Rampai Kebijakan Hukum Pidana*, (Citra Aditya Bhakti:Bandung), hlm. 42

terkandung tindakan preventif dalam arti luas.[182]

Melaksanakan politik kriminal antara lain berarti membuat perencanaan untuk masa yang akan datang dalam menghadapi atau menanggulangi masalah-masalah yang berhubungan dengan kejahatan. Termasuk dalam perencanaan ini, di samping merumuskan perbuatan-perbuatan apa yang seharusnya dijadikan tindak pidana, juga menetapkan sanksi-sanksi apa yang seharusnya dikenakan terhadap si pelanggar.

Sementara itu Kebijakan hukum pidana yang dibuat juga harus berorientasi pada kemajuan teknologi, dimana hal ini sesuai dengan masukan dalam Konggres PBB ke-8 tahun 1990 di Havana, Cuba, antara lain disebutkan dalam Dokumen Konggres AA/CONF/144/L.11*),* sebagai berikut:[183]

a. *"The growing utilization of computer technology and world-ide computer and telecomunication networks as a integral part of contemperary international financial and banking operations can also create conditions tht greatly facilitate criminal operations within and between countries";*
b. *"the increases in the abuse of computers as a modality of economic crime and by difficlty of detecting computer-related crimes, especially in view of the rapidity with which they can be committed";*
c. *"the potential for links between oganized crime and computer-related abuses, and the fact that computers may often be used by*

[182] Sudarto, 1986, *Kapita Selekta Hukum pidana*, (Alumni:Bandung), hlm. 118

[183] Dokumen Seventh UN Congress AA/CONF/144/L.11*),*

*organized crime for purposes such as money lundering or in the management and transfer of illegally acquired assests.*

Berikut akan dilakukan kajian Kebijakan formulasi hukum pidana di masa yang akan datang *(ius costituendum)* untuk mengantisipasi perbuatan CT di Indonesia, dengan melihat berbagai aturan asing yang mengatur CT sebagai suatu perbuatan penyalahgunaan internet *(cyber crime).*

**a) Konsep KUHP 2008**

**KUHP merupakan induk dari berbagai ketentuan pidana yang ada di Indonesia. Sejak tahun 1977 telah dilakukan usaha pembaharuan KUHP dan telah mengalami kurang lebih 17 (tujuh belas) kali perubahan. Kosep KUHP baru hanya membagi KUHP dalam 2 (dua) Buku saja, berbeda dari KUHP WvS yang saat ini masih berlaku, di mana hanya meliputi Buku I tentang Ketentuan Umum dan Buku II tentang Tindak Pidana.**

**Sehubungan dengan kelemahan juridiksi di dalam KUHP dalam menghadapi masalah CT yang merupakan bagian/jenis *cyber crime,* dalam Konsep RUU KUHP 2008, dirumuskan perluasan asas territorial, dan perumusan delik tindak pidana di bidang teknologi informasi, yaitu sebagai berikut :**

Asas Wilayah atau Teritorial

**Pasal 3**

Ketentuan pidana dalam peraturan perundang-undangan Indonesia berlaku bagi setiap orang yang melakukan:

a. tindak pidana di wilayah Negara Republik Indonesia;
b. tindak pidana dalam kapal atau pesawat udara Indonesia; atau
c. tindak pidana di bidang teknologi informasi yang akibatnya dirasakan atau terjadi di wilayah Indonesia dan dalam kapal atau pesawat udara Indonesia.

**Seperti diketahui bahwa hukum pidana Indonesia (KUHP) tidak mengatur secara eksplisit tentang tindak pidana *cyeber terrorism*. Pengaturan mengenai Tindak Pidana terrorisme dalam Konsep KUHP Tahun 2008 ada dalam Bab 1 Buku Kedua Bagian Keempat, paragraf kesatu samapai dengan paragraph kelima yang diatur dalam Pasal 242 sampai dengan Pasal 251**

**Kaitannya dengan fenomena baru dalam Konsep mengenai tindak pidana CT, berikut identifikasi penulis terhadap beberapa ketentuan-ketentuan tindak pidana yang tercantum dalam Konsep.**

Ketentuan Tindak Pidana Mengenai Terrorisme, Beberapa pasal dalam Konsep yang terkait dengan permasalahan terorisme yaitu antara lain :

Pasal 242 diatur mengenai bentuk dan pengertian tindak pidana terorisme sebagai berikut :

*Setiap orang yang menggunakan kekerasan atau ancaman kekerasan menimbulkan suasana teror atau rasa takut terhadap orang secara meluas atau menimbulkan korban yang bersifat massal, dengan cara merampas kemerdekaan atau hilangnya nyawa dan harta benda orang lain, atau mengakibatkan kerusakan atau kehancuran terhadap objek-objek vital yang strategis atau lingkungan hidup atau fasilitas umum atau fasilitas internasional, dipidana karena melakukan terorisme dengan pidana mati atau penjara seumur hidup atau pidana penjara paling singkat 5 (lima) tahun dan paling lama 20 (dua puluh) tahun.*

Pasal 244 konsep dikategorikan sebagai tindak pidana terorisme yang mengatur tentang terrorisme yang menggunakan bahan kimia, berbunyi :

*Setiap orang yang menggunakan bahan-bahan kimia, senjata biologis, radiologi, mikroorganisme, radioaktif atau komponennya untuk melakukan terorisme dipidana dengan pidana mati atau penjara seumur hidup atau pidana penjara paling singkat 5 (lima) tahun dan paling lama 20 (dua puluh) tahun.*

Pasal 245 yang oleh Konsep dikategorikan sebagai tindak pidana pendanaan untuk terorisme menyatakan sebagai berikut :

*Setiap orang yang menyediakan atau mengumpulkan dana dengan tujuan akan digunakan atau patut diketahuinya akan digunakan sebagian atau seluruhnya untuk melakukan tindak pidana terorisme sebagaimana dimaksud dalam Pasal 242, Pasal 243, dan Pasal 253, dipidana dengan pidana penjara paling singkat 3 (tiga) tahun dan palinglama 15 (lima belas) tahun.*

Dengan melihat pada isi pasal 242 Konsep dapat dipahami bahwa unsur tindak pidananya dapat menunjuk pada aksi kejahatan CT, artinya Ketentuan mengenai Tindak Pidana Terrorisme dalam

Konsep tersebut dapat digunakan dalam menanggulangi tindak pidana CT.

Sedangkan untuk ketentuan yang berkaitan dengan tindak pidana terhadap Informatika dan Telematika di dalam Konsep KUHP 2004/ 2005 di atur dalam pasal 373 sampai dengan 379. Berikut identifikasi beberapa pasal dalam ketentuan pidana tersebut di atas:

Bagian Kelima
Tindak Pidana terhadap Informatika dan Telematika

Paragraf 1

Penggunaan dan Perusakan Informasi Elektronik dan Domain

Pasal 373

*Dipidana dengan pidana penjara paling lama 4 (empat) tahun dan pidana denda paling banyak Kategori IV, setiap orang yang menggunakan dan/atau mengakses komputer dan/atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud untuk memperoleh, mengubah, merusak, atau menghilangkan informasi dalam komputer dan/atau sistem elektronik.*

Paragraf 2

Tanpa Hak Mengakses Komputer dan Sistem Elektronik

Pasal 376

*Dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan pidana denda paling banyak Kategori IV setiap orang yang :*

*a. menggunakan, mengakses komputer, dan/atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud memperoleh, mengubah, merusak, atau menghilangkan informasi pertahanan nasional atau hubungan internasional yang dapat menyebabkan gangguan atau bahaya terhadap negara dan/atau hubungan dengan subjek hukum internasional;*

*b. melakukan tindakan yang secara tanpa hak yang menyebabkan transmisi dari program, informasi, kode atau perintah komputer dan/atau sistem elektronik yang dilindungi Negara menjadi rusak;*

*c. menggunakan dan/atau mengakses komputer dan/atau sistem elektronik secara tanpa hak atau melampaui wewenangnya, baik dari dalam maupun luar negeri untuk memperoleh informasi dari komputer dan/atau sistem elektronik yang dilindungi oleh negara;*

*d. menggunakan dan/atau mengakses komputer dan/atau sistem elektronik milik pemerintah yang dilindungi secara tanpa hak;*

*e. menggunakan dan/atau mengakses tanpa hak atau melampaui wewenangnya, komputer dan/atau sistem elektronik yang dilindungi oleh negara, yang mengakibatkan komputer dan/atau sistem elektronik tersebut menjadi rusak;*

*f. menggunakan dan/atau mengakses tanpa hak atau melampaui wewenangnya, computer dan/atau sistem elektronik yang dilindungi oleh masyarakat, yang mengakibatkan computer dan/atau sistem elektronik tersebut menjadi rusak;*

*g. mempengaruhi atau mengakibatkan terganggunya komputer dan/atau sistem elektronik yang digunakan oleh pemerintah;*

*h. menyebarkan, memperdagangkan, dan/atau memanfaatkan kode akses (passwod) atau informasi yang serupa dengan hal tersebut, yang dapat digunakan menerobos komputer dan/atau sistem elektronik dengan tujuan menyalahgunakan komputer dan/atau sistem elektronik yang digunakan atau dilindungi oleh pemerintah;*

*i. melakukan perbuatan dalam rangka hubungan internasional dengan maksud merusak komputer atau sistem elektronik lainnya yang dilindungi negara dan berada di wilayah yurisdiksi Indonesia dan ditujukan kepada siapa pun; atau*

*j. melakukan perbuatan dalam rangka hubungan internasional dengan maksud merusak komputer atau sistem elektronik lainnya yang dilindungi negara dan berada di wilayah yurisdiksi Indonesia dan ditujukan kepada siapa pun.*

Pasal 377

*Dipidana dengan pidana penjara paling singkat 3 (tiga) tahun dan paling lama 15 (lima belas) tahun dan pidana denda paling sedikit Kategori IV dan paling banyak Kategori VI, setiap orang yang menggunakan dan/atau mengakses komputer dan/atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud memperoleh, mengubah, merusak, atau menghilangkan informasi milik pemerintah yang karena statusnya harus dirahasiakan atau dilindungi.*

Pasal 378

*Dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan pidana denda paling banyakKategori VI, setiap orang yang :*

*a. menggunakan dan/atau mengakses komputer dan/atau sistem elektronik secara tanpa hak atau melampaui wewenangnya dengan maksud memperoleh keuntungan atau memperoleh informasi keuangan dari Bank Sentral, lembaga perbankan atau lembaga keuangan, penerbit kartu kredit, atau kartu pembayaran atau yang mengandung data laporan nasabahnya;*

*b. menggunakan data atau mengakses dengan cara apapun kartu kredit atau kartu pembayaran milik orang lain secara tanpa hak dalam transaksi elektronik untuk memperoleh keuntungan;*

*c. menggunakan dan/atau mengakses komputer dan/atau sistem elektronik Bank Sentral, lembaga perbankan dan/atau lembaga keuangan yang dilindungi secara tanpa hak atau melampaui wewenangnya, dengan maksud menyalahgunakan, dan/atau untuk mendapatkan keuntungan daripadanya; atau*

*d. menyebarkan, memperdagangkan, dan/atau memanfaatkan kode akses atau informasi yang serupa dengan hal tersebut yang dapat digunakan menerobos komputer dan/atau sistem elektronik dengan tujuan menyalahgunakan yang akibatnya dapat mempengaruhi sistem elektronik Bank Sentral, lembaga perbankan dan/atau lembaga keuangan, serta perniagaan di dalam dan luar negeri.*

**Berikut dapat diidentifikasikan unsur-unsur tindak pidananya yang erat kaitannya dengan tindak pidana CT sebagai berikut:**

**Pasal 373 dengan unsur tindak pidana : mengakses komputer dan/atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud untuk memperoleh, mengubah, merusak, atau menghilangkan informasi dalam komputer dan/atau sistem elektronik; (terkait dengan aksi kejahatan CT yang berbentuk *Unauthorized***

***acces computer system and sevice, Hacking, dan Cyber sabatoge dan extortion*).**

Pasal 376 dengan unsur tindak pidana : mengakses komputer, dan/atau sistem elektronik tanpa hak, yang menyebabkan gangguan atau bahaya terhadap negara dan/atau hubungan dengan subjek hukum internasional; (Terkait dengan aksi kejahatan *Unauthorized acces computer system and service*).

Pasal 377 dengan unsur tindak pidana : mengakses komputer dan/atau sistem elektronik tanpa hak memperoleh, mengubah, merusak, atau menghilangkan informasi milik pemerintah yang karena statusnya harus dirahasiakan atau dilindungi; (terkait dengan aksi kejahatan CT yang berbentuk *Unauthorized acces computer system and sevice, Hacking, dan Cyber sabatoge dan extortion*).

Pasal 378 dengan unsur tindak pidana : mengakses komputer dan/atau sistem elektronik tanpa hak dengan maksud memperoleh keuntungan atau memperoleh informasi keuangan dari Bank Sentral, lembaga perbankan atau lembaga keuangan, penerbit kartu kredit, atau kartu pembayaran atau yang mengandung data laporan nasabahnya; (terkait dengan aksi kejahatan CT yang

berbentuk *Unauthorized acces computer system and sevice,* dan *Carding*).

**Jika dicermati isi pasal-pasal tersebut, secara jelas dan terinci adanya kriminalisasi terhadap perbuatan CT, pasal-pasal tersebut mengarah kepada kriminalisasi terhadap tindak pidana CT.**

**b) Dalam Kajian Perbandingan**

Untuk mengantisipasi perbuatan CT di Indonesia, seyogyanya para legislator juga melakukan perbandingan dengan negara lain yang telah terlebih dahulu memiliki peraturan yang berkaitan dengan penggunaan tekhnologi informasi dengan melihat berbagai aturan asing yang mengatur perbuatan *cyber crime* sebagai suatu perbuatan penyalahgunaan internet untuk tujuan perbuatan CT.

Indonesia dapat mengikuti perkembangan munculnya berbagai jenis kejahatan tekhnologi informasi serta merupakan salah satu upaya harmonisasi eksternal. Perkembangan hukum di negara lain terhadap efek negatif dari kontent internet telah melahirkan perdebatan antara pemerintah dan pengguna jasa internet tentang pengaturan kontent internet (*Internet content regulations*).

Setelah dikaji, belum ditemukan negara yang mencantumkan CT sebagai satu tindak pidana secara khusus. Formulasi kejahatan CT hanya dimasukan dalam pengaturan mengenai *cyber crime*. Kejahatan CT pun pada umumnya merupakan bagian dari *cyber crime.* Untuk jelasnya akan disajikan berbagai pengaturan kejahatan CT di berbagai negara asing.

Namun demikian, dengan melakukan perbandingan hukum

tidak berarti Indonesia harus menyusun Undang-undang yang sama dengan salah satu negara tersebut, seyogyanya perumus kebijakan legislatif di Indonesia dapat melakukan pilihan sesuai dengan perkembangan nilai budayanya. Penyusunan undang-undang harus tetap memperhatikan nilai-nilai sosial budaya bangsa, sebagaimana hal tersebut telah dilakukan pula oleh konsep. Soerjono Soekanto mengemukakan perbandingan hukum mungkin diterapkan dengan memakai unsur-unsur sistem hukum sebagai titik tolak perbandingan, sistem hukum mencakup tiga unsur pokok, yaitu:[184]

a. Struktur hukum yang mencakup lembaga-lembaga hukum;
b. Substansi hukum yang mencakup perangkat kaidah atau perilaku teratur, dan
c. Budaya hukum yang mencakup perangkat nilai-nilai yang dianut.

Menurut Soerjono Soekanto, perbandingan dapat dilakukan terhadap masing-masing unsur atau dilakukan secara kumulatif terhadap semuanya. Dengan metode perbandingan hukum dapat dilakukan penelitian terhadap perbagai subsistem hukum yang berlaku di suatu masyarakat tertentu atau secara lintas sektoral terhadap sistem-sistem hukum perbagai masyarakat yang berbeda-beda.

Computer Crime Research Center (CCRC) menyatakan bahwa CT diartikan sebagai suatu tindakan direncanakan terlebih dahulu, bermotivasi politik serangan terhadap informasi, sistem komputer, program komputer, dan data yang mengakibatkan kekerasan terhadap sasaran oleh kelompok atau sub-nasional agen rahasia. Sejak saat itu kata cyber-terorisme telah dimasukkan ke dalam kamus IT pakar keamanan dan teroris ahli dan daftar kata media massa "profesional", sehingga pengaturan CT masuk dalam pengaturan penyalahgunaan

---

[184] Barda Nawawi Arief, *Perbandingan Hukum Pidana*, Raja Grafindo Persada, Jakarta, 1998, hlm. 11

internet *(cyber crime).*

Berikut adalah pengaturan dalam undang-undang beberapa negara asing yang mengatur delik *cyber crime* yang erat kaitannya dengan CT sebagai suatu perbuatan penyalahgunaan internet.

**1) SINGAPURA**

Penggunaan media internet oleh para teroris di Asia Tenggara menunjukan peningkatan yang signifikan, kelompok yang sering dituding oleh dunia barat sebagai ekstrimis itu menggunakan ranah maya untuk menyebarkan ide radikal, merekut serta melatih para anggotanya. Temuan yang dilakukan oleh Sekolah Internasional S Rajaratnam Singapura dan Institut Strategi Kepolisian Australian memberitahu kalau, banyak pihak keamanan di Asia Tenggara yang sukses bisa mendeteksi keberadaan sebuah bom, tapi mereka tidak mengerti bagaimana bom itu dibuat.

Indikasi yang menunjukan kalau peningkatan ini terjadi salah satunya adalah, makin banyaknya kelompok ekstrimis mengunggah video melalui internet mengenai cara membuat dan menggunakan bom," terang juru bicara Sekolah Rajaratman, seperti yang dilansir *AFP*, Senin (20/4/2009).

Menurut data yang mereka himpun, hingga 2008 lalu sudah ada 117 situs tentang kelompok radikal ini. Padahal, pada 2007 sebelumnya, situs seperti ini hanya berjumlah tidak kurang dari 15 saja. Dan kebanyakan dari situs tersebut, berbasis di Indonesia dan Filipiina" Kita harus memperhatikan dengan serius

pertumbuhan dan pergerakan kelompok radikal online tersebut," tandas juru bicara tersebut.[185]

Di Singapura pengaturan mengenai penyalahgunaan internet/computer crime yang mengarah kepada tindak pidana CT di atur khusus di dalam undang-undang di luar KUHP nya. Beberapa ketentuan dalam perundang-undangan Negara Singapura berkaitan dengan perbuatan CT.

(Chapter 50A;Com*puter missue Act)*
*Unauthorized access to computer material.*

*Section 3-(1) any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offense and shall be liable on conviction to a imprisonment for a term not exceeding 2 years or to both and, in case of a second or subsequent for a term not exceeding 3 years or to both.*

*(1) If any damage is caused as a restut of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50.000 or to imprisonment for a term not exceeding 7 years or to both.*

*Section 4: Accesswith intent to commit or facilitate commission of offence.*

*(1) Any person who causes a computer to perform any function for the purpose of securing access to any computer with intent to commit this section applies, shall be guilt of an offence.*

*(2) This section shall apply to an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than 2 years.*

---

[185] *Informasi lebih lengkap dapat diakses di http://techno.okezone.com/index.php/ReadStory/2009/04/20/55/212093/makin-canggih-terorisasia- tenggara-gunakan-internet/makin-canggih-teroris-asia-tenggara-gunakan-internet*

*(3) Any person guilty of an offence under this section shall be liable on conviction to a not exceeding $50.000 or to imprisonment for a term not exceeding 10 years pr to both.*

Dari ketentuan di atas dapat disimpulkan bahwa setiap orang yang mengakses komputer yang tanpa hak/secara illegal yang dapat mengarah kepada perbuatan CT dipidana penjara paling sedikit 2 (dua) sampai dengnan 3 (tiga) tahun, kemudian apabila menyebabkan program dan data komputer terganggu di pidana penjara selama 7 (tujuh) sampai dengan 10 tahun penjara dan denda $50.000

**2) Di Belgium**

Di Belgia pengaturan mengenai penyalahgunaan internet *(cyber crime)* diatur dalam *penal code* atau KUHP. Ketentuan-ketentuan yang berkaitan dengan *cyber crime* yang merujuk pada aksi kejahatan CT ditambahkan pasal baru dalam KUHP Belgia yang berlaku efektif tanggal 13 2001. Bentuk CT yang diatur yaitu mengenai aksi kejahatan *Hacking.*

*IV. COMPUTER HACKING*
*Article 550 (b) of the Criminal Code :*

*Section 1. Any person who, aware that he is not authorized, accesses or maintains his acces to computer system, may be sentencedto a term of imprisonment of 3 months to 1 years and to a fine of (Bfr 5,200-5m) or to one of these sentences. If the offences specified in section 1 above is committed with intention of defraud, the term of imprisonment may be from 6 months to years.*

*Section 2. Any person who, with the intention to defraud or with the intention to cause harm, exceeds his power of access to a*

*computer system, may be sentenced to term of imprisonment of 6 months to 2 years and to a fine of (BFr 5, 200-20m) or to one of these sentences.*

*Section 3. Any person finding himself in one of the situations specified in saction 1 and 2 who either: accesses data which is stored, processed or transmitted by a computer system, or procures such data in any way whatsoever, or makes any use whatsoever, or couse any damage, even unintentionally, to a computer system, or data which is stored, processed or transmitted by such a system may be sentenced to term of imprisonment of 1 to 3 year and to a fine of (BFr 5, 200-10m) or to one of these sentenced.*

Pasal tersebut menegaskan setiap orang yang tanpa hak atau secara illegal mengakses sistem informasi diancam pidana 3 (tiga) tahun penjara dan denda 5 (lima) milyar, jika melakukan penipuan terhadap sistem informasi tersebut dipidana penjara 3 (tiga) bulan hingga 1 (satu) tahun, jika menyebabkan kerusakan terhadap data dalam komputer atau sistem informasi di ancam pidana penjara 1 (satu) sampai dengan 3 (tiga) tahun dan denda 10 (sepuluh) milyar.

***2.*** **Kebijakan Non Penal Yang Akan Datang dalam mengatasi tindak pidana *cyber terrorism.***

Secara sederhana dapatlah dibedakan, bahwa upaya penanggulangan kejahatan lewat jalur *penal* lebih menitikberatkan pada sifat "*represif*" (penindasan/pemberantasan/penumpasan) sesudah kejahatan terjadi, sedangkan jalur *non-penal* lebih menitikberatkan pada tindakan *preventif* (pencegahan/pengendalian) sebelum kejahatan terjadi, namun dalam tindakan represif juga di dalamnya terkandung tindakan preventif dalam arti luas.[186]

---

[186] Sudarto, 1986, *Kapita Selekta Hukum pidana*, (Alumni:Bandung), hlm. 118

Meskipun hukum pidana digunakan sebagai *ultimatum remedium* atau alat terakhir apabila bidang hukum yang lain tidak dapat mengatasinya, tetapi harus disadari bahwa hukum pidana memiliki keterbatasan kemampuan dalam menanggulangi kejahatan. Keterbatasan-keterbatasa tersebut sebagaimana dikekmukakan oleh **Barda Nawawi Arief** adalah sebagai berikut :[187]

a. Sebab-sebab kejahatan yang dimiliki komplek berada di luar jangkuan hukum pidana;
b. Hukum pidana hanya merupakan bagian kecil (subsistem) dari sarana kontrol sosial yang tidak mungkin mengatasi masalah kejahatan sebagai masalah kemanusiaan dan kemasyarakatan yang sangat kompeks (sebagai masalah sosio-psikologis, sosio-politik, sosio-ekonomi, sosio-kultural dan sebagainya);
c. Pengguanaan hukum pidana dalam menanggulangi kejahatan hanya merupakan ”*kurieren am symtom”,* oleh karena itu hukum pidana hanya merupakan ”pengobatan simptomatk” dan bukan ”pengobatasn 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/berfungsinya hukum pidana memrlukan sarana pendukung yang lebih bervariasi dan lebih menuntut ”biaya tinggi”.

konggres PBB ke-6 tahun 1980 di Caracas, Venezuela mengenai “*Crime Trends and crime prevention Strategis*” terlihat bahwa upaya non penal mempunyai kedudukan strategis, yang antara lain dinyatakan:[188]

---

[187] Barda Nawawi Arief, Batas-batas Kemampuan Hukum Pidana Dalam Penanggulangan Kejahatan, dalam Barda Nawawi Arief, *Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana,* PT Citra Aditya Bakti, Bandung, 1998, hal. 46-47

[188] *Sixth UN Congress Report,* 1981, halaman 5,dalam Barda Nawawi Arief, 2002, *Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit*, hlm. 43

a. Bahwa masalah kejahatan merintangi kemajuan untuk pencapaian kualitas hidup yang pantas bagi semua orang;

(*The problem impedes progress towards the attainment of an acceptable quality of life for all people)*;

b. Bahwa strategi pencegahan kejahatan harus didasarkan pada penghapusan sebab-sebab dan kondisi-kondisi yang menimbulkan kejahatan;

(*Crime prevention strategis should be based upon the eliminatio of causes and conditions giving rise to crime)*;

c. Bahwa penyebab utama kejahatan dibanyak negara ialah ketimpangan sosial, diskriminasi rasial dan diskriminasi nasional, standar hidup yang rendah, penganguran dan kebutahurufan (kebodohan) diantara golongan besar penduduk;

*(The main causes of crime in many countries are social inequality, racial and national discrimination, low standar of living, unemployment and illiteracy among broad section of the population).*

*Cyber terrorism* sebagai bagian dari tindak pidana *cyber crime* atau perbuatan yang menyalahgunakan teknologi internet yang akibatnya dapat mengakibatkan kepanikan/ketakukan, kerugian secara fisik dan psikis terhadap individu maupun masyarakat dan menyerang sarana infrastrukstur penting suatu negara, sehingga mengakibatkan kerugian yang besar terhadap target sasarannya, untuk penanggulangannya pun harus diorientasikan pada pengaturan penggunaan teknologi internet itu sendiri seraya menanggulangi

penyakit psikologis yang ditimbulkannya oleh provokasi ideology yang dilancarkan oleh para kaum terrorisme dalam merekrut dan menghegemony massanya.

Menyadari tentang pentingnya pengaturan mengenai CT yang memanfaatkan teknologi internet di dalam melakukan aksinya maka, pengaturan mengenai internetlah yang seharusnya dilakukan.

Ada beberapa pendekatan (*'approach')*[189] yang dilakukan oleh berbagai negara di dunia untuk mengatasi persoalan penyalahgunaan internet ini, termasuk di dalamnya adalah CT.

*The Constitutional approach*

Pendekatan ini membuat konstitusi negara sebagai faktor penentu dari apa yang bisa diterima di Internet. Negara yang telah melakukan adalah Amerika Serikat dengan mengaturnya secara umum dalam konstitusinya, sehingga sering terjadi konflik antara Konstitusi Amerika dengan UU yang dibuat Kongres.

*The State Control approach*

Pendekatan ini diadopsi oleh pemerintahan yang percaya bahwa mereka berhak dan bahkan bertanggung jawab untuk campur tangan secara langsung dan menempatkan kendali teknis atas isi yang dapat diakses oleh warganegaranya. Negara yang

---

[189] Roger Darlington, *Should The Internet be Regulated* ?, http://www.rogerdarlington.co.uk/regulation.html

melakukan adalah Arab Saudi dan negara-negara sekitarnya. Negara diyakini memiliki hak dan tanggungjawab atas warganya agar tidak diintervensi oleh pihak luar. Saudi Arabia yang memiliki 30 penyedia jasa intenet, yang semuanya harus terpusat di mana pemerintah dapat menghalangi akses ke arah tujuan perbuatan CT.

Di China, semua cafe Internet (warnet) harus menyimpan arsip lokasi/situs yang dikunjungi, dengan tujuan mencegah akses ke penyusupan, perusakan, dan, penghilangan data-data penting pemerintah dan perbuatan yang merugikan kesatuan nasional, kedaulatan dan integritas teritorial *(terkait dengan tindak pidana CT)*. Pada konggres komunis Cina November 2002, penguasa menghalangi semua akses kepada *Google* sebagai mesin pencari untuk sementara waktu. Selain itu di negara lain, yang sedang mencoba untuk membatasi akses Internet warganya antara lain Algeria, Yemen, Bahrain, Uni Emirat Arab, Korea Utara, Vietnam, Iran, Maldives dan Singapura.

*The Statutory approach*

Pendekatan ini membuat suatu bagian yang spesifik tentang perundang-undangan baru sebagai faktor penentu yang utama tentang apa yang bisa diterima di Internet. Negara yang melakukannya adalah Australia dengan diterbitkannya *Broascasting Services Amandement Act* Tahun 1999, yang

mengatur secara khusus tentang isi internet. Undang-Undang ini menghendaki Jasa Pelayanan Internet Australia untuk tidak mengakses material ke atau memindahkan dari lokasi web mereka yang dinilai terlarang (X).

*The Self Regulation approach*

Pendekatan ini dilakukan atas prakarsa sukarela dari penyedia jasa internet/*provider.* Pendekatan ini dipakai di Inggris karena tidak ada undang-undang tertulis dan pemerintah tidak menunjukkan kehendak untuk membuat undang-undang. Sebagai gantinya di tahun 1996, Industri penyedia jasa Internet '*Internet Service Providers Industry*' Inggris mendirikan *Internet Watch Foundation.*

*Rating and Filtering Techniques*.

Dalam hal ini para pengguna internet menggunakan perangkat lunak untuk menyaring dan membatasi akses internet yang berpotensi merusak.

Setiap pemerintah mempunyai *policy* yang berbeda-beda, tapi pada umumnya *policy* yang dianut akan sangat tergantung dari tingkat adopsi demokrasi di negara-negara tersebut. Beberapa model kebijakan yang dilakukan oleh berbagai negara untuk mengatasi maraknya CT yang masuk melalui penyalahgunaan internet menunjukkan persamaan sikap, yaitu menyadari bahwa teknologi

internet disamping membawa perubahan kearah yang lebih baik tapi juga berpotensi membawa perubahan kepada hal-hal yang tidak baik.

Di dalam menanggulangi kejahatan ini perlu dilakukan kerjasama dengan para pihak. Negara bukanlah satu-satunya pihak yang dituntut untuk melakukan penanggulangan kejahatan ini. Para pihak yang dapat memberikan kontribusi nyata untuk penanggulangan kejahatan ini adalah:

*Negara dengan peraturan perundangan dan aparaturnya.*

*Korporasi atau industri jasa internet atau ISPs (Internet Service Providers)*

*Orang tua, Pemuda dan bahkan sekolah.*

Kebijakan non penal/*non penal policy* dapat dilakukan dengan meningkatkan peran serta penggunaan alat dan teknologi modern yang berfungsi sebagai penyaring atau filter yang umumnya berupa *software protection*, karena kebijakan penanggulangan bisa diterima jika dikombinasikan dengan menyaring perangkat lunaknya. Dari sudut **pendekatan teknologi (*techno prevention*)**[190], guna mengatasi

[190] Pendekatan tekhnologi (pendekatan *techno-prevention*) yaitu upaya pencegahan/penanggulanga kejahatan dengan menggunakan tekhnologi. Perlunya penanggulangan kejahatan *cyber crime* secara tekhnologi diungkapkan oleh IIIC (*International Information Industry Congress*) yang mengakui bahwa tindakan pemerintah dan perjaanjian internasional untuk mengharmonisasikan hukum dan mengkordinasikan prosedur hukum merupakan kunci dalam upaya penanggulangan *cyber crime*, namun patut diingat bahwa hal ini janganlah diandalkan sebagai satu-satunya alat. *Cybercrime* dimungkinkan (terjadi) oleh tekhnologi dan (oleh karena itu) memerulukan suatu kepercayaan

penyalahgunaan pemakain internet oleh para kaum hacker dan cracker/CT, maka perlu dapat ditingkatkan sistem pengaman pada sistem komputer dan jaringan internet. Disamping beberapa langkah yang telah ditempuh dengan menggunakan metode pendekatan teknologi *(techno prevention)* seperti yang telah penulis uraikan sebelunya di dalam kebijakan non penal yang ada saat ini, beberapa langkah lain juga dapat dilakukan dalam pengamanan sistem informasi jaringan global, antara lain :[191]

1. Isi substansi data dan/atau informasi yang merupakan input dan output dari penyelenggara sistem informasi dan disampaikan ke pada publik atau disebut juga dengan *content.* Dalam hal penyimpanan data dan/atau informasi tersebut akan disimpan dalam bentuk data *bases* dan dikomunikasikan dalam bentuk *data messages;*
2. Sistem pengolahan informasi *(Computing and/or information system)* yang merupakan jaringan sistem informasi *(computer network)* organisasional yang efisien, efektif dan legal. Dalam hal suatu sistem informasi merupakan perwujudan penerapan perkembangan teknologi informasi ke dalam suatu bentuk organisasional/organisasi perusahaan (bisnis).
3. Sistem komunikasi *(comunication)* perwujudan dari sistem keterhubungan *(interconnection)* dan sistem pengoperasian global *(interoperational)* antar sistem informasi/jaringan komputer *(computer network)* maupun penyelenggara jasa dan/jaringan telekomunikasi; dan

---

yang baik pada tekhnologi untuk pemecahannya. Dalam Barda Nawawi Arief, 2002, *Sari Kuliah Perbandingan Hukum Pidana*, Raja Grafindo Persada, Jakarta, hlm. 254-255.

[191] Danrivanto Budjijant, *Asek-aspek Hukum Dalam Perniagaan Secara Elektronik (E-Commerce),* Makalah pada Seminar Nasional Aspek Hukum Transaksi Perdagangan via Internet di Indonesia (E-Commerce) diselenggarakan FH UNPAD, Bandung, 22 Juli 2000. Hal.11. lihat juga Edmon Makarim, *Telematics Law, Cyberlaw, Media, Communication & Information Technologies,* Makalah pada Seminar tentang Cyber Law, diselenggarakan Yayasan Cipta Bangsa di Bandung. 29 Juli 2000, hal.4

4. Masyarakat *(community)* yang merupakan perangkat intelektual *(brainware),* baik dalam kedudukannya sebagai pelaku usaha, professional penunjang maupun pengguna.

Menjaga keempat aspek itu merupakan bagian dari kebijakan keamanan informasi keamanan. Keamanan sistem informasi berbasis internet merupakan suatu keharusan yang harus diperhatikan karena jaringan computer internet yang sifatnya publik dan global pada dasarnya tidak aman. Sistem keamanan jaringan komputer terhubung ke internet harus direncanakan dan dipahami dengan baik agar informasi yang berharga itu dapat terlindungi secara efektif. Untuk mencapai semua itu, jaringan komputer harus dianalisis untuk mengetahui apa yang harus dan untuk apa diamankan, serta besar nilainya. Keamanan komputer *(computer security)* meliputi 4 (empat) aspek yaitu : *privacy, integrity, authentication* dan *availability.* Selain keempat aspek itu masih ada 2 (dua) aspek lain yang sering dibahas dalam kaitannya dengan *electronic commerce,* yaitu *access control* dan *non repudiation.*[192]

Aspek utama dari ***privacy*** atau ***confidentially*** adalah usaha untuk menjadi informasi dari orang yang tidak berhak mengakses. *Privacy* lebih ke arah data-data yang sifatnya privat, sedangkan

---

[192] Simon Garfingkel Sebagaimana dikutip oleh Budi Rahardjo, 2002, *Implikasi Teknologi dan Internet Terhadap Pendidikan, Bisnis dan Pemerintahan, Siapkah Indonesia?.* PT. Insan komunikasi/Infonesia: Bandung, hal. 11-14

*confidentiality* biasanya berhubungan dengan data yang diberikan untuk keperluan tertentu tersebut. Contoh hal yang berhubungan dengan *privacy* adalah e-mail seorang pemakai *(user)* tidak boleh dibaca oleh administrator, sedangkan contoh *confidentiality* information adalah data-data yang sifatnya pribadi dan merupakan data-data yang diproteksi penggunaan dan penyebarannya. Serangan terhadap aspek *privacy* ini misalnya adalah usaha untuk melakukan penyadapan *(sniffing).* Usaha yang dapat dilakukan untuk menigkatkan *privacy* dan *confidentiality* adalah dengan menggunakan tehnologi *kriptografi* (enkripsi dan dekripsi).

Beberapa kategori yang termasuk *privacy* yaitu :[193]

1. Protection from intrusion;
2. Protection from the public disclosure of embarrassing private facts;
3. Protection from publicity that places the individual in a false light and;
4. Protection from the use of a person's name or likeness

Setiap kebudayaan mengakui beberapa bentuk dari *privacy, privacy,* yang diikuti untuk menunjukkan rasa hormat pada orang lain *(immunity from intrusion)* dan pengertian pada diri sendiri *(according a sphere of autonomy).* Ada yang berpendapat bahwa *privacy* harus

[193] Ann K. Moceyunas,*On-line Privacy : the Push and Pull of Self-Regulation and law.* Net Law News, Oct-Nov-Dec 1999

dilindungi dan ditempatkan tersembunyi pada koleksi data, tetapi ada juga yang berpendapat perlu adanya masyarakat yang teransparan *(transparent society)* dimana akan ada terbuka keseimbangan di antara kekuatan individu dan kekuatan institusi. *The United States Federal Trade Commision* dalam sebuah studinya dari tahun 1995-1998 menentukan bahwa Asosiasi Industri Amerika Serikat menentukan 5 (lima) prinsip pokok dari koleksi data individual yang perlu dilindungi, yaitu *notice, choice, access, security and enforcement mechanism.*[194]

Aspek ***integrity*** menekankan bahwa informasi tidak boleh di ubah tanpa seizing pemilik informasi. *Virus Trojan horse* atau pemakai lain yang mengubah informasi tanpa izin merupakan contoh masalah yang harus di hadapi pada aspek ini. Sebuah e-mail dapat saja ditangkap (*intercept)* di tengah jalan, diubah isinya *(altered, tampered, modified),* kemudian diteruskan kealamat yang dituju. Dengan kata lain, integritas dari informasi sudah tidak terjaga. Penggunaan *enkripsi* dan *digital signature*, misalnya dapat mengatasi masalah ini.

Aspek ***authentication*** berhubungan dengan metode untuk menyatakan bahwa informasi betul-betul asli atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud. Masalah pertama membuktikan keaslian dokumen, dapat dilakukan dengan teknologi *watermaking* dan *digital signature*. *Watermaking* juga dapat digunakan untuk menjaga *intellectual property,* yaitu dengan menandai dokumen atau hasil karya dengan tanda tangan pembuat. Masalah kedua biasanya berhubungan dengan *access control,* yaitu berkaitan dengan pembatasan orang yang dapat

---

[194] Bandingkan dengan persyaratan *privacy* yang dinyatakan dalam *The Children's Online Privacy Protection Act 1998* yang menentukan ada 5 (lima) prinsip, yaitu *notice,consent, disclosure, collection, and security of personally identiable data. ibid*

mengakses informasi. Dalam hal ini pengguna harus menunjukkan bukti bahwa memang dia adalah pengguna yang sah, misalnya dengan menggunakan *password, biometric* (ciri-ciri khas orang) dan sejenisnya. Pengguna teknologi *smart coord* saat ini kelihatannya dapat meningkatkan keamanan aspek ini. Secara umum proteksi authentication dapat menggunakan *digital certificates.*

Aspek ***availability*** atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadaan akses ke informasi. Contoh hambatan adalah serangan yangsering disebut dengan *Denial of Service attack* (DoS attack), di mana *server* dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang di luar perkiraan sehingga tidak dapat melayani permintaan lain atai bahkan sampai *down, hang, crach.* Contoh lain adalah adanya *mailbomb,* di mana seorang pemakai dikirimi e-mail bertubi-tubi (katakanlah ribuan e-mail) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka e-mailnya. Serangan terhadap *availability* dalam bentuk *Denial of Service* (DoS attack) merupakan yang terpopuler saat ini. Contoh serangan *Denial of Service* (DoS attack yaitu pada bulan Februari 1998 terjadi serangan *(breaks-in or attack)* sebanyak 60 kali perminggunya melalui media *Internet* terhadap 11 jaringan komputer militer di Pentagon. Dalam *cyber attack* ini yang menjadi target utama para *cyber terrorist* adalah Departemen Pertahanan Amerika Serikat *(DoD)*;

***Access control*** berhubungan dengan cara pengaturan akses pada informasi. Hal ini biasanya berhubungan dengan masalah *aunthentication* dan juga *privacy. Access control* sering kali di lakukan dengan menggunakan kombinasi *userid/password* atau dengan menggunakan mekanisme lain. Aspek ***non-repudiation*** ini menjaga

agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Contohnya jika seseorang/CT mengirim e-mail untuk memesan barang, tidak dapat menyangkal bahwa dia telah mengirimkan e-mail tersebut. Aspek ini sangat penting dalam hal *electronic commerce.* Penggunaan *digital signature, certificate*s dan teknologi *kriptografi* secara umum dapat menjaga aspek ini, tetapi masih harus didukung oleh hukum, sehigga statusnya dar i*digitas signature* itu jelas legal.

Dari sudut **pendekatan moral/edukatif**, usaha yang dapat dilakukan yaitu, dengan pemberian pendidikan/pelatihan khususnya pendidikan kewarganegaraan, pelatihan-pelatihan komputer dengan misi teknologi untuk membantu masyarakat, dan lebih khususnya lagi dalam hal agama, karena perbuatan CT, bukan untuk berkompetisi/mengadu kepintaran dengan menggunakan teknologi informasi, dan bukan semata-mata mencari keuntungan materi, tetapi lebih kepada ideologi. Ideologi tersebut bisa berbentuk ideologi jihad, ideologi untuk kepentingan kelompok tertentu dan ideologi untuk menunjukkan keesistensiannya di panggung politik dunia.

Bentuk upaya yang dapat dilakukan dengan pendekatan mora/edukatif ini, misalnya dengan melakukan pencerahan oleh pemimpin agama, tokoh berkhsarisma untuk mengeliminasi pemahaman radikalisme ajaran agama kelompok-kelompok fundalimentalis garis keras, dialog, negosiasi serta konsensi politik bagi kelompok-kelompok bawah tanah menjadi gerakan formal secara

konstitusional, melibatkan parpol dan organisasi kemasyarakatan untuk berdialog dengan kelompok-kelompok radikal, menetapkan organisasi-organisasi mana yang terlarang dan membubarkannya, melaksanakan program ekonomi dan sosial budaya seperti pemerataan hasil pembangunan, pengentasan kemiskinan, penciptaan lapangan kerja dan pendidikan agama dan Pancasila agar tidak disusupi ideology ektrim radikal.

Dari segi ***pendekatan budaya/kultural*** dalam kebijakan penanggulangan tindak pidana CT yang ada sebelumnya guna menanggulangi tindak pidana CT**,** langkah yang telah ditempuh yaitu : 1). pengenalan komputer dan internet kepada masyarakat, dan 2). peran serta masyarakat dalam bidang komputer dan internet.

Tugas masyarakat di atas seyogyanya harus tetap ditingkatkan *(continue)* tidak hanya sebatas mengurangi angka kejahatan semata, mealinkan juga harus ikut serta dalam proses menganalisis, megenal dan memahami ancaman kejahatan-kejahatan di bidang teknologi informasi, yang lebih khususnya berkaitan dengan masalah CT. Upaya lainya yang dapat dilakukan dengan menggunakan metode pendekatan budaya/kultural guna menanggulangi tindak pidana CT di masa yang akan datang, yaitu dengan melakukan pencerahan oleh pemimpin agama, tokoh berkharisma untuk mengeliminasi pemahaman radikalisme ajaran agama kelompok-kelompok

fundamentalisme garis keras, dialog, negosiasi serta konsensi politik bagi kelompok-kelompok bawah tanah menjadi gerakan formal secara kontitusional,e melibatkan parpol dan tanah dan organisasi kemasyarakatan untuk berdialog dengan kelompok-kelompok radikal, melaksanakan program ekonomi dan sosial budaya seperti pemerataan hasil pembangunan, pengentasan kemiskinan, penciptaan lapangan kerja dan pendidikan agama dan pancasila agar tidak didudupi idologi ektrim radikal.

Hal ini sejalan dengan berbagai seminar-seminar (pembangunan) hukum nasional yang diadakan, mulai dari seminar ke-1 tahun 1963 sampai seminar ke-8 tahun 2003, yang sarat dengan amanat nasional untuk melakukan “pendekatan  kultural dan religius”. Dalam seminar nasional ke-8 tahun 2003 ditegaskan, agar nilai-nilai religius dijadikan sebagai sumber motivasi, sumber inspirasi, sumber muatan substantif, dan sumber evaluasi, dalam kebijakan pembangunan hukum nasional.

Dalam forum-forum seminar baik Nasional maupun Internasional yang menghasilkan kesimpulan dan rekomendasi akan

perlunya pengkajian dan penggalian hukum agama dan hukum adat dalam pembaharuan hukum pidana antara lain tertuang dalam:[195]

Kesepakatan Pertemuan Ilmiah Nasional (antara lain dalam seminar hukum Nasional) I/1963; IV/1979; VI/1995; VIII/2003; dan Simposium Pembaharuan Hukum Pidana Nasional 1980);

Kebijakan Legislatif Nasional (antara lain dalamUU No.1 Drt 1951dan UU No 14 tahu 1970 jo UU No 35 tahun 1999 jo UU No 4 tahun 2004).

Laporan Konggres PBB mengenai "*The Prevention of crime and the tratment of Offenders*", (antara lain konggres V/1975; VI/1980; VII/1985; dan VIII/1990)

Seminar Pembangunan Hukum Nasional VIII tahun 2003 di Kuta Denpasar, Bali, memberikan kesimpulan dan rekomendasi (saran pemecahan masalah) antara lain: "Menjadikan ajaran agama sebagai sumber motivasi, sumber inspirasi dan sumber evaluasi, yang kreatif dalam membangun insan hukum yang berakhlak mulia, sehingga wajib dikembangkan upaya-upaya kongkrit dalam muatan kebijakan pembangunan hukum.

Memperkuat landasan budaya keagamaan yang sudah berkembang dalam masyarakat;

Memfasilitasi perkembangan keberagaman dalam masyarakat dengan kemajuan bangsa

Mencegah konflik sosial antar umat beragama dan meningkatkan hubungan antar umat beragama".[196]

---

[195] Barda Nawawi Arief, *Pokok-Pokok Pemikiran (Ide Dasar) Asas-asas Hukum Pidana Nasional*, Makalah pada seminar Nasional ,"Asas-Asas Hukum Pidanan Nasional", Kerjasama BPHN dan HAM dengan FH UNDIP, Semarang, 26-27 April 2004, hlm. 4-7.

[196] Barda Nawawi Arief, *Pokok-Pokok Pemikiran (Ide Dasar) Asas-asas Hukum Pidana Nasional*, Makalah pada seminar Nasional ,"Asas-Asas Hukum Pidanan Nasional", Kerjasama BPHN dan HAM dengan FH UNDIP, Semarang, 26-27 April 2004, hlm. 4-7.

Sila Ketuhanan Yang Maha Esa dari Pancasila yang telah menjadi dasar bagi ketentuan Pasal 29 UUD 1945, telah melegitimasi bahwa kehidupan agama telah merasuk dalam kalbu bangsa Indonesia. Rasa keagamaan ini sangat sensitif dan sangat mudah tergerak dalam kesempatan-kesempatan tertentu dan semuanya itu memberikan landasan yang kuat bagi unsur-unsur agama bagi tata hukum di Indonesia, termasuk di dalamnya dalam delik-delik CT yang dilakukan para kaun terrorisme.[197] Bahkan seperti yang dikatakan oleh **Alfred Denning**, *"Without religion there can be no morality, and without morality there can be no law*".

Sementara itu dilihat dari sudut **pendekatan global** (kerja sama internasional), Kebijakan global yang berkaitan dengan kebijakan kriminal terlihat di dalam berbagai pertemuan Internasional, terutama dalam laporan Kongres PBB mengenai *"The Prevention of Crime and the Treatment of Offenders"* (yang pada kongres terakhir ke-XI/2005 diubah menjadi *"Prevention of Crime and Criminal Justice*"). Berbagai hasil pertemuan Kongres PBB itu juga sering menghimbau untuk dilakukan "pendekatan filosofik/kultural", "pendekatan moral religius", dan "pendekatan humanis" yang diintegrasikan ke dalam pendekatan rasional yang berorientasi pada kebijakan *("policy oriented approach"*).

Berbagai pernyataan (*statement*) Kongres PBB itu, antara lain sebagai berikut :

a. Laporan Kongres ke V (1975) :

> *".... it was necessary, in the long term, to rethink the whole of criminal policy in a spirit of rationalization, planning and democratization. ..... the criminal justice system should be transformed so as to be more responsive to contemporary social necessities, the aspirations of the*

---

[197] Ibid, hlm. 48

*whole population and the demands of a scientific evaluation of needs and means in preventing and containing criminality"*;

*"It was important that traditional forms of primary social control should be revived and developed"*.

b. Laporan Kongres ke VI (1980) :

*"... development (berarti termasuk pembangunan di bidang hukum, pen.) was not criminogenic per se, but could become such if it was not rationally planned, disregarded cultural and moral values, and did not include integrated social defence strategies"*;

*"... the importation of foreign cultural patterns which did not harmonize with the indigenous culture had had a criminogenic effect;*

*Often, lack of consistency between laws and reality was criminogenic; the farther the law was removed from the feeling and the values shared by the community, the greater was the lack of confidence and trust in the efficacy of the legal system.*

c. Laporan Kongres ke VII (1985) :

*"Crime prevention and criminal justice should not be treated as isolated problems to be tackled by simplistic, fragmentary methods, but rather as complex and wide-ranging activities requiring systematic strategies and differentiated approaches in relation to : The socio-economic, political and cultural context and circumstances of the society in which they are applied; The developmental stage, .....; The respective traditions and customs, making maximum and effective use of human indigenous options"*;

*"The conflicts existing in many countries between indigenous and traditions for the solution of socio-legal problems and the frequently imported or super-imposed foreign legislation and codes should be reviewed with a view to assuring that official norms appropriately reflect current societal values and structures*";

*"When new crime prevention measures are introduced, necessary precautions shoul be taken not to disrupt the smooth and effective functioning of traditional systems, full*

*attention being paid to the preservation of cultural identities and the protection of human rights"*.

d. Laporan Kongres ke VIII (1990) :

*"The trial process should be consonant with the cultural realities and social values of society, in order to make it understood and to permit it to operate effectively within the community it serves. Observance of human rights, equality, fairness and consistency should be ensured at all stages of the process*".

Sebagaimana ditulis Barda Nawawi Arief,[198] berbagai "statement" Kongres PBB di atas, pada intinya menyatakan :

Perlu ada harmonisasi/sinkronisasi/konsistensi antara pembangunan/ pembaharuan hukum nasional dengan nilai-nilai atau aspirasi sosio-filosofik dan sosio-kultural.

Sistem hukum yang tidak berakar pada nilai-nilai budaya dan bahkan ada "diskrepansi" dengan aspirasi masyarakat, merupakan faktor kontribusi untuk terjadinya kejahatan (*"a contributing factor to the increase of crime*").

Kebijakan pembangunan yang mengabaikan nilai-nilai moral dan kultural, dapat menjadi faktor kriminogen.

Ketiadaan konsistensi antara undang-undang dengan kenyataan merupakan faktor kriminogen;

---

[198] Barda Nawawi Arief, *Kriminalisasi Kebebasan Pribadi Dan Pornografi/Pornoaksi Dalam Perspektif Kebijakan Hukum Pidana*, Makalah pada Seminar "KRIMINALISASI ATAS KEBEBASAN PRIBADI DAN PORNOGRAFI/ PORNOAKSI", yang diselenggarakan atas kerja sama FH UNDIP dengan KOMNAS HAM, di Hotel Graha Santika Semarang, 20 Desember 2005.hlm 8-10

Semakin jauh UU bergeser dari perasaan dan nilai-nilai yang hidup di dalam masyarakat, semakin besar ketidakpercayaan akan keefektifan sistem hukum .

Dalam "*background paper*" lokakarya "*Measures to Combat Computer-related Crime"* Kongres PBB XI tahun 2005 di Bangkok dinyatakan, bahwa "teknologi baru yang mendunia di bidang komunikasi dan informasi memberikan "bayangan gelap" (*a dark shadow)* karena memungkinkan terjadinya bentuk-bentuk eksploitasi baru, kesempatan baru untuk aktivitas kejahatan, dan bahkan bentuk-bentuk baru dari kejahatan".[199]

Adanya kebijakan yang integral yang dilakukan oleh semua pihak yang peduli terhadap bahaya penyalahgunaan internet ini akan memberikan sumbangan besar untuk penanggulangan kejahatan yang dilakukan melalui internet, khususnya kejahatan CT sebagai bentuk baru dari *cybercrime*.

Indonesia sebagai salah satu negara yang ada dalam pentas pergaulan dunia juga tidak dapat berlepas diri dari ancaman kejahatan CT ini. Pengalaman yang telah dilakukan oleh negara-negara lain di

---

[199] Dokumen United Nations A/CONF.203/14, Eleventh United Nations Congress on Crime Prevention and Criminal Justice, Bangkok, 18-25 April 2005, Background paper, Workshop 6: Measures to Combat Computer-related Crime : *"The worldwide multiplication of new information and communication technologies also casts a dark shadow: it has made possible new forms of exploitation, new opportunities for criminal activity and indeed new forms of crime".*

dunia dapat menjadi pelajaran yang berharga, bahwa penanggulangan kejahatan CT sebagai salah satu bentuk kejahatan terrorisme dengan sarana teknologi informasi dalam dimensinya yang baru tidak dapat ditanggulangi hanya dengan kebijakan penal semata. Namun, harus melibatkan kebijakan non penal pula dengan berbagai pendekatan yang dilakukan secara intergral.

Bentuk upaya kerjasama internasional/pendekatan global yang dapat dilakukan guna mengatasi masalah CT, antara lain :

- Bekerjasama dengan Pemerintahan Malaysia dengan bergabung pada Koalisi Melawan *Cyber-Terrorism* yang didirikan di Malaysia.[200]

  International Multilateral Partnership Against *Cyber-Terrorism* (IMPACT), sebuah kerjasama global public-private ini bertujuan untuk menyatukan pemerintah, para pemimpin industri, dan ahli pengaman cyber dalam usahanya bertarung melawan ancaman online.

  Bertempat di kawasan 'panas' perkembangan teknologi infomasi di Malaysia, fasilitas seluas tujuh hektar ini memiliki empat divisi kunci, yaitu: respon global, kebijaksanaan dan kerjasama internasional, pelatihan dan pengembangan kemampuan, juga

[200] http://www.sda-indo.com/sda/features/psecom,id,2068,nodeid,1,_language,Indonesia.html

asuransi keamanan dan outreach. Front ini juga didukung oleh dewan penasehat yang didalamnya terdapat tokoh terkemuka dari bidang industri dan akademis. Salah satunya adalah "bapak internet" Dr Vinton Cerf dan pendiri White House Security Advisor, Howard Schmidt.

IMPACT telah menjalin kerjasama dengan International Telecomunication Union (ITU) PBB. Kerjasama ini diharapkan dapat memainkan peran besar dalam agenda ITU Global Cybersecurity, yang akan mendorong kerjasama internasional untuk membuat cyberspace lebih aman digunakan oleh para pengguna berat jaringan saat ini.

Kemitraan ini bertujuan untuk membangun analisis real-time, agregat, dan penyebaran informasi ancaman cyber global, juga termasuk didalammya, saluran sistem peringatan dini yang mampu menyediakan respon darurat untuk ancaman cyber global *(terkait juga masalah CT)*. Mitra kunci lainnya yang tergabung dalam dewan penasehat adalah penyedia solusi keamanan seperti Cisco, Kapersky Lab, dan Symantec.

- Kerjasama lainnya, yaitu melakukan upaya ***resosialisasi*** dan ***rehabilitasi*** antara lain dilakukan dengan merosialisasikan anggota kelompok melalui pergaulan sosial yang normal. Sedangkan rehabilitasi korban dilakukan dengan mendirikan lembaga

konpensasi korban terrorisme dan juga asuransi seperti yang diperaktikkan oleh Amerika Serikar melalui *the September 11th Victim' Conpensation Fund* data *the Terrorism Risk Insurance Act of 2002.* Tindakan lain yang dilakukan pemerintah Amerika adalah mendirikan *Office for Victis Of Crime (OVC)* untuk melayani warga Amerika Serikat yang menjadi korban kejahatan di luar negeri atau warga negara asing yang menjadi korban kejahatan di Amerika Serikat termasuk korban kejahatan terrorisme. Kewenangan OVC dedasarkan atas *the Antiterrorism and Effective Death Penalty Act* 1996.[201]

- Dalam sistem hukum Indonesia, pengaturan mengenai pemulihan atau reparasi korban terrorisme di atur dalam pasal 36, 38, 39, 40, dan 41 Undang-undang No.15 Tahun 2003. Namun Undang-undang ini hanya mengatur hak korban atas konpensasi dan hak restitusi, sedangkan hak rehabilitasi korban tidak diatur dalam undang-undang. Undang-undang hanya mengatur mengenai hak-hak rehabilitasi bagi orang-orang yang diputus bebas atau lepas dari segala tuntutan hukum melalui putusan hakim yang memiliki kekuatan hukum tetap sesuai dengan ketentuan pasal 37. Kelemahan lain undang-undang ini adalah konpensasi dan/atau

[201] *Officefor Victims of Crime International Aktivities, OVC Fact Sheet, U.S. Departement of justice,* Washington D.C., Juli 1999 atau buka web site <http://www.ojp.usdoj.gov/ovc/>

restitusi diberikan dan dicantumkan dalam amar putusan pengadilan. Rumusan ini melemahkan hak-hak reparasi korban karena tergantung putusan hakim, apabila terdakwa dibebaskan atau dilepaskan maka hal tersebut tidak dapat dijalankan.

Upaya pengembangan infrastruktur pendukung antara lain dengan memberikan dukungan berupa bantuan internasional untuk pengadaan peralatan dan teknologi bagi Polri, Intelejen, TNI dan fasilitas koordinasi (Desk KPT), peningkatan satuan-satuan pelaksanaan lapangan dan jajaran penegak hukum, pendirian organisasi lembaga koordinasi, pengembangan jaringan kerjasama melalui kemitraan antara instansi pemerintah dengan lembaga non-pemerintah terkait, termasuk lembaga akademik, pembentukan *cyber task force* di Mabes Polri dan jajarannya, membentuk *task force IT security nasional,* memasang *real time intrusion detection system,* membentuk *cyber patrol* dan membentuk Tim Koordinasi Perlindungan Keamanan dan Penanggulangan Infrastruktur Strategis Berbasis Teknologi Informasi.

- National Police Agency of Japan (NPA) telah membentuk ***Cyber Taskforce***[202] untuk menjawab tantangan ini, dikombinasikan

---

[202] Satsuki Suwa. *Response of The National Police Agency in Japan in Dealing with Cyber Terrorism*. High-tech Crime Division NPA – Japan, unpublished, Tokyo - 2002 .

dengan membangun suatu instalasi berupa sistem pemantau gangguan secara cepat yang dapat memberikan peringatan dini serta informasi lokasi korban penyerangan juga lokasi darimana penggangu berasal, sistim ini disebut *Real time Intrusion Detection System Network* (Real time IDS Network). Di Amerika pada bulan Februari 2003 diluncurkan The Nation Strategy for The Physical Protection of Critical Infrastructures and Key Assets serta The National Strategy to Secure Cyberspace, kita sekarang sudah perlu untuk mengadopsi sistem ini dan Mabes Polri akan mengembangkan serta membangunnya.

***Cyber taskforce*** adalah suatu gugus tugas yang dirancang untuk menghadapi aspek-aspek tehnis serta respon darurat bila terjadi serangan cyber (tindak pidana biasa di Internet *terutama* **(CT*)***, dengan peran mulai dari ***pencegahan kerusakan*** yang lebih meluas, ***assitensi dan recovery*** korban serta ***penyidikan*** untuk mengungkap pelakunya. *Cyber Taskforce* Center berada di ***Mabes Polri*** serta ada pada setiap Polda, didukung dan terkordinasi dengan komponen / institusi di bidang tehnologi Informasi diluar Polri antara lain; Kampus, Departemen terkait (Birokrat), Icon-icon

tehnologi informasi (Id-Cert,Id-First, dsb) serta Industri di bidang Tehnologi Informasi (APJII, AWARI, dsb).

Misi dan peranan *Cyber Taskforce* adalah ***"mencegah serta merespon keadaan darurat agar kerugian / resiko akibat serangan pada sistim Informasi terhadap infra struktur kritis seminimal mungkin serta melakukan tindakan hukum yang diperlukan"***, dengan peran sebagai berikut ;

- Pusat komando & informasi,
- Membangun hubungan kerja yang baik dengan infrastruktur kritis,
- Mengumpulkan/menganalisa informasi,
- Merespon segera situasi darurat untuk memperkecil kerusakan,
- Intrusion Detection Sistem.

Cyber Taskforce melakukan kegiatan-kegiatan yang spesifik dalam upaya untuk merealisasikan peran-nya, antara lain sebagai berikut ;

- Mendeteksi secara dini dan memberikan bantuan untuk meminimalkan kerawanan-kerawanan pada infrastruktur kritis,
- Merespon secara cepat keadaan darurat agar kerusakannya minim,
- Menyediakan bimbingan & bantuan investigasi serta melakukan investigasi secara langsung.

***Cyber Taskforce*** Center multak diperlukan dan harus segera diwujudkan, tentunya dengan dukungan dan keterlibatan dari berbagai pihak karena bagaimanapun juga Polri tidak dapat berdiri

sendiri menghadapi fenomena ***Hightech crime*** yang sarat atau penuh dengan disiplin ilmu diluar Ilmu Kepolisian, juga sarat dengan sarana (hardware & software) yang pengadaannya ada pada industri-industri diluar institusi Kepolisian. Adapun beberapa pertimbangan atau alasan kuat perlunya Cyber Taskforce dibentuk adalah sebagai berikut ;

- Indonesia akan menuju e-Government, artinya Infrastruktur kritis akan semakin bertambah.
- Kejadian - kejadian Web page defacement dari e-Government di Indonesia sudah sering terjadi oleh Hacker terorganisasi dari luar negeri (Perang Cyber).
- Bukti-bukti pada kasus ***Imam Samudra*** yang membuktikan bahwa CT sekarang ini sudah pada tahap ***"clear and present danger"*** walaupun masih belum berupa electronic attack.
- IP Address Indonesia diblokir di beberapa negara, akibat dari kelemahan dalam pencegahan tindak pidana di bidang tehnologi informasi dan kelemahan penegakan hukumnya.
- Sangat diperlukan untuk upaya preventif dan memperkecil kerusakan serta mengorganisasikan staff yang telah terlatih dibidang tehnis.
- Sebagai saluran keluhan dan pengaduan yang selama ini selalu dicari-cari oleh masyarakat, terutama para korban TPTI.

*Cyber Taskforce* Center ini hanya dapat berfungsi dengan baik apabila telah dibangun (installed) ***Real time IDS Network***, atau harus dibangun keduanya secara bersamaan.

Konsep ini berasal dari NPA-Japan yang dijelaskan Mr. Satsuki Suwa, Assistant Director CT Technology Office pada pertemuan tahunan CTINS (***Computer crime & Technology***

***Information Network System***) di Tokyo 26 – 29 Maret 2002, ***Real time IDS Network*** merupakan instalasi dari berbagai komponen yang terintegrasi guna menciptakan sistim peringatan dini dari gangguan / serangan elektronik serta agar tercipta suatu rekasi yang cepat untuk menanggulangi gangguan atau serangan tersebut. Komponen-komponen sistem ini membentuk suatu jaringan kerja (network) yang melakukan tugas sesuai peran dan fungsinya masing-masing namun terintegrasi sehingga laporan dapat cepat disampaikan, demikian juga dalam menanggulangi gangguan atau serangan yang terjadi komponen inipun berfungsi dan berperan secara proposional /tidak terjadi duplikasi tetapi saling mengisi dan terkordinir dengan baik.

Contoh di Negara lainnya lagi adalah dibentuknya unit khusus komputer dalam sistem penegakan hukumnya seperti yang dioeraktikkan oleh Jepang dengan mendirikan the HITEC *(HI-tech crime Tehnical Expert Center)* yang khusus berfungsi sebagai pasukan polisi *cyber ("cyber police force").*[203] Korea mendirikan *the Korean National Police Agency's Cyber Terrorism Response Center*

[203] http://www.npa.go.jp/higtech/jyu_prog_eng.htm

dan *General Investigation Center of Computer Crimes Under the Prosecutor-General's Office.*[204]

# BAB IV

# PENUTUP

## A. SIMPULAN

Dari hasil dan pembahasan, dapatlah ditarik simpulan sebagai berikut :

1. Kebijakan kriminal yang ada di Indonesia saat ini dalam menanggulangi tindak pidana CT, baik dari segi aspek kebijakan formulasi/penal yang menjadi kajian khusus dalam penulisan ini, yang merupakan tahap pertama dalam penegakan hukum pidana/politik hukum pidana, dan kebijakan non penal yang ada saat ini, dapat digunakan dalam menanggulangi tindak pidana CT.
2. Kebijakan kriminal yang akan datang dalam menanggulangi tindak pidana CT, baik dari aspek kebijakan

---

[204] Urbas, Regor, *CyberCrimeLegislation in the Asia-Pasific Region, revisi paper* pada *the First Asia CyberCrime, the Center for Criminology at the of hongkong,* 25-26 April 2001*, Australian Institute of Criminology,* 2001, hlm. 15-16 atau buka *web site* http://www.hku.hk/crime/

formulasi/penal, dan non penal yang akan datang, seyogyanya perlu ada suatu peningkatan dan perubahan sebagai berikut :

- dari segi aspek kebijakan legislatife/formulasi/perundang-undangan di Indonesia yang akan datang, seyogyanya perlu ada konektifitas antara Sistem induk hukum pidana, yaitu KUHP dengan undang-undang di luar KUHP, artinya perlu dilakukan perubahan terhadap sistem induk KUHP Indonesia yang berlaku saat, agar sesuai dengan kondisi masyarakat Indonesia saat ini. Untuk itu Konsep KUHP secapatnya perlu disyahkan. Disamping itu juga harus memperhatikan kajian komparatif terhadap undang-undang di berbagai negara asing lainnya, yang terkait dengan tindak pidana CT agar lebih memaksimalkan dalam menanggulangi tindak pidana CT tersebut.
- dari segi kebijakan non penal yang akan datang dalam menanggulangi tindak pidana CT*, seyogyanya* perlu dilakukan peningkatan-peningkatan dari kebijakan non penal yang sudah dilakukan sebelumnya. Peningkatan tersebut dapat dilakukan dari berbagai segi pendekatan,

antara laian : ***Pendekatan Teknologi (Techno Prevention)***, dengan melakukan peningkatan dalam hal : Mengatur akses (access control), Menutup service yang tidak digunakan Memasang proteksi, Firewall, Pemantau adanya serangan, Pemantau integritas sistem, Audit: mengamati berkas log, Back up secara rutin, dan Penggunaan enkripsi untuk meningkatkan keamanan; ***Pendekatan Moral/Edukatif,*** dapat dilakukan dengan pemberian pendidikan/pelatihan khususnya pendidikan kewarganegaraan, pelatihan-pelatihan komputer dengan misi teknologi untuk membantu masyarakat, dan lebih khususnya lagi dalam hal agama, karena perbuatan CT, bukan untuk berkompetisi/mengadu kepintaran dengan menggunakan teknologi informasi, dan bukan semata-mata mencari keuntungan materi, tetapi lebih kepada ideologi. ***Pendekatan Budaya Kultural,*** hal-hal yang dapat dilakukan yaitu, Pengenalan komputer dan internet kepada masyarakat, dan peran serta masyarakat dalam bidang komputer dan internet. ***Pendekatan Global*** *(kerjasama internasional)****,*** upaya yang dapat dilakukan yaitu melakukan kerjasama-kerjasama dengan negara-negara lain guna mengatasi tindak pidana CT, seperti

bekerjasama dengan Pemerintahan Malaysia dengan bergabung pada Koalisi Melawan *Cyber-Terrorism* yang didirikan di Malaysia.

## B. **Saran**

Berkaitan dengan hasil penelitian dan pembahasan yang telah diuraikan, maka penulis menyarankan :

1. Sehubungan dengan *penal reform,* maka seyogyanya perlu secepatnya mengesahkan/melegitimasi Konsep KUHP 2008. Agar sistem induk dalam hukum pidana tersebut dapat sesuai dengan perkembangan masyarakat Indonesia saat ini.
2. Sehubungan dengan hal-hal yang perlu ditinjau kembali dalam kebijakan non penal guna mengatasi tindak pidana CT*,* maka seyogyanya perlu ditingkatkan kembali kebijakan/usaha-usaha yang sudah ada sebelumnya secara menyeluruh, baik peningkatan dengan menggunakan pendekatan Teknologi *(Techno Prevention),* pendekatan Moral/Edukatif, pendekatan Budaya/Kultural, dan pendekatan Global.

## DAFTAR PUSTAKA


A.Lewis, James, *Assesing the Risk Of Cyber Terrorism, Cyber War and Other Cyber Threats, Center For Strategic and International Studies,* Washington D.C.

Adolf Huala, 1996**,** *Aspek-Aspek Negara dalam Hukum Internasional*, Rajawali Pers Jakarta,

Asshidiqie Jimly, 1996, *Pembaharuan Hukum Pidana Indonesia*, *Study Tentang Bentuk-bentuk Pidana dalam Tradisi Hukum Fiqih dan Relevansinya bagi Usaha Pembaharuan KUHP Nasional*, (Angkasa:Bandung)

Ann K. Moceyunas,*On-line Privacy : the Push and Pull of Self-Regulation and law.* Net Law News, Oct-Nov-Dec 1999

Dermawan Mohammad Kemal, *Strategi Pencegahan Kejahatan*, Citra Aditya Bakti, Bandung, 1994

Danrivanto Budjijant, *Asek-aspek Hukum Dalam Perniagaan Secara Elektronik (E-Commerce),* Makalah pada Seminar Nasional Aspek Hukum Transaksi Perdagangan via Internet di Indonesia (E-Commerce) diselenggarakan FH UNPAD, Bandung, 22 Juli 2000. Hal.11. lihat juga Edmon Makarim, *Telematics Law, Cyberlaw, Media, Communication & Information Technologies,* Makalah pada Seminar tentang Cyber Law, diselenggarakan Yayasan Cipta Bangsa di Bandung. 29 Juli 2000

Hoefnagels. G.P, 1973. *The other side of criminolgy*, Kluwer B.V. Deventer.

Hadisuprapto, Paulus, 2008. *Delikuensi Anak, Pemahaman dan Penaggulangannya.* Bayumaedia, Malang.

Hirst, Paul dan Grahame Thompson, 2001, *Globalisasi Adalah Mitos.* Jakarta, Yayasan Obor.

……, 2004, *Pager Gunung*, Indra Apiadi,

Henry Campbell Black, M.A. Fifth Edition, St. Paul Minn, West Publishing Co, 1979 page 766

Muladi, *1984, Lembaga Pidana Bersyarat, (Alumni:* Bandung)

--------, 2002, *Kapita Selekta Sistem Peradilan Pidana*, cetakan ke-2, Badan Penerbit UNDIP, Semarang

--------, 2002, *Demokratisasi, HAM dan Reformasi Hukum di Indonesia,* The Babibie Center, Jakarta

Muladi dan Barda Nawawi Arief, 2002, *Bunga Rampai Hukum Pidana,* Penerbit Alumni, Bandung

....., 2005, *Teori-Teori dan Kebijakan Pidana.* P.T. Alumni, Bandung

M. Arief, Dikdik Mansur, 2005, *Cyber Law, Aspek Hukum Teknologi Informasi*. Refika Aditama, Bandung

Nawawi Arief, Barda, 1994, *Beberapa Aspek Pengembangan Ilmu Hukum Pidana (Menyongsong Generasi Baru Hukum Pidana Indonesia)*, Kumpulan Pidato Pengukuhan Guru Besar FH UNDIP, Semarang.

....., 1996, *Kebijakan Legislatif, dalam Penanggulangan Kejahatan dengan Pidana Penjara,* Badan Penerbit UNDIP Semarang

....., 1998, *Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana*, (Citra Aditya Bhakti:Bandung)

....., 2001, *Masalah Penegakan hukum dan Kebijakan Penanggulangan Kejahatan.* PT. Citra Aditya Bakti : Bandung.

....., 2002, *Bunga Rampai Kebijakan Hukum Pidana*, Citra Aditya Bakti, Bandung

....., 2002, *Sari Kuliah Perbandingan Hukum Pidana*, PT RajaGrafindo, Jakarta,

....., 2003, *Kapita Selekta Hukum Pidana*, Citra Aditya Bhakti, Bandung.

....., 2004, *Pokok-Pokok Pemikiran (Ide Dasar) Asas-asas Hukum Pidana Nasional*, Makalah pada seminar Nasional ,"Asas-Asas Hukum Pidanan Nasional", Kerjasama BPHN dan HAM dengan FH UNDIP, Semarang, 26-27 April 2004

......, 2005, *Tindak Pidana Mayantara*, *Perkembangan Kajian CyberCrime di Indonesia*. PT. Raja grafindo Persada : Jakarta

....., 2005, *Pembaharuan Hukum Pidana, Dalam Persepektif Kajian Perbandingan.* PT.Citra Aditya Bakti, Bandung.

----------, 2008, *Bunga Rampai Kebijakan Hukum Pidana Perkembangan Penyusunan Konsep KUHP Baru*, Kencana, Jakarta

----------, 2005, *Antisipasi Hukum Pidana Dan Perlindungan Korban Cyber Crime di bidang Kesusilaan*, Makalah pada Seminar "Kejahatan Seks melalui *Cyber Crime Dalam Perspektif Agama, Hukum, Dan Perlindungan korban,* F.H UNSWAGATI, Hotel Zamrud Cirebon, tanggal 22 Agustus 2005

.....,2005*, Kriminalisasi Kebebasan Pribadi Dan Pornografi/Pornoaksi Dalam Perspektif Kebijakan Hukum Pidana*, Makalah pada Seminar "KRIMINALISASI ATAS KEBEBASAN PRIBADI DAN PORNOGRAFI/ PORNOAKSI", yang diselenggarakan atas kerja sama FH UNDIP dengan KOMNAS HAM, di Hotel Graha Santika Semarang, 20 Desember 2005

……, *Kebijakan Kriminal (Criminal Policy)*, Bahan Penataran Kriminologi, FH Universitas Katolik Parahyangan , Bandung tanggal 9-13

Nyoman Serikat Putra Jaya, 2007, *Makalah Pembaharuan Hukum Pidana.* Program Magister Ilmu Hukum UNDIP, UNSOED, dan UNTAG

Pollitt Mark, Weimann, Gabriel (2006). *Terror on the Internet: The New Arena, the New Challenges*. United States Institute of Peace,U.S.. I

Raharjo, Agus, 2002, *Cybercrime, Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi,* Citra Aditya Bahkti : Bandung

Rahardjo, Budi, 2002, *Implikasi Teknologi dan Internet Terhadap Pendidikan, Bisnis dan Pemerintahan, Siapkah Indonesia?.* PT. Insan komunikasi/Infonesia: Bandung

Ramli, Ahmad M, 2004. *Cyber Law dan HAKI dalam Sistem Hukum di Indonesia*

Ronny Rahman Nitibaskara, 2001, *Ketika Kejahatan Berdaulat*, (Peradaban : Jakarta),

Rian Ahmed, *Aturan Dunia Maya Langgar HAM,* Media 28 Januari 2008 | 1058 kata*, Journal*, Daniel Pearl, pada Februari 2002, di kota pelabuhan Pakistan, Karachi, berkomunikasi melalui email

The White House. *Defending America's Cyberspace – National Plan For Information Systems Protection V.1 – An Invitation to a Dialogue*. Washington DC – 2000.

Tien S. Saefullah, *Yurisdiksi Sebagai Upaya Penegakan Hukum Dalam Kegiatan Cyberspace*, artikel dalam *Cyber Law :Suatu Pengantar*, (ELIPS: Jakarta), 2002

Tien S. Saefullah, *Yurisdiksi Sebagai Upaya Penegakan Hukum Dalam Kegiatan Cyberspace*, artikel dalam *Cyber Law :Suatu Pengantar*, (ELIPS: Jakarta), 2002

Sitompul, Asril, 2004, *Hukum Internet, Pengenalan Mengenai Masalah Hukum Cyberspace*, Citra Aditya Bhakti, Bandung

Sutanto, Hermawan Sulistyo, dan tjuk Sugiarto (Ed), *Cyber Crime Motif dan Penindakan,* Pensil 324, Jakarta,

Sutarman, H, 2007, Kata Pengantar dari Prof. Dr. M. Khoiden, S.H, M.H., C.N (Guru Besar universitas Jember ), *Cyber Crime, Modus Operandi dan Penangulangannya*. LeksBang komputer PRESSindo Jogjakarta.

Sudarto, 1974, *Suatu Dilema Dalam Pembaharuan Sistem Pidana Indonesia*, Pusat Study Hukum dan masyarakat, FH UNDIP Semarang

....., 1981, *Hukum dan Hukum Pidana*, Sinar Baru, Bandung

....., 1983, *Hukum Pidana Dan Perkembangan Masyarakat*, Sinar Baru, Bandung.

......, 1986, *Kapita Selekta Hukum Pidana,* , Penerbit Alumni, Bandung

……., 1990, *Hukum Pidana I*, Cetakan ke-2, Yayasan Soedarto, Semarang

Urbas, Regor, *CyberCrimeLegislation in the Asia-Pasific Region, revisi paper* pada *the First Asia CyberCrime, the Center for Criminology at the of hongkong,* 25-26 April 2001

Wahid, Abdul dan Moh.Labib, 2005, *Kejahatan Mayantara (Caber Crime),* Refika Aditama, Bandung

Wisnubroto, Al, 1999, Kata Pengantar Prof. DR. Barda Nanawi Arief, SH., *Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer,* Universitas Atma Jaya Yogyakarta.

Sabadan Daan Drs. dan Drs. Kunarto. *Kejahatan Berdimensi Baru. Cipta Manunggal,* Jakarta, 1999.

Suwa satsuki. *Response Of The National Police Agency in Japan in Dealing with Cyber Terrorris.* High-tech Crime Division NPA – Japan, unpublished, Tokyo - 2002

Swetman, Yonah Alexander, , Michael S. (2001). *Cyber Terrorism and Information Warfare: Threats and Responses*. Transnational Publishers Inc.,U.S..

**Website**

A. Clem, MPH, MSN Health Implications of Cyber-Terrorism Department of Environmental and Occupational Health, College of Public Health, University of South Florida, Tampa, Florida USA. http://www.mvhsmun.org/ConferenceSite/committees/specialized/CoT-Cyber-Terrorism_Synopsis.doc. Commission on Terror Komisi Terror

Art Bowker and Michael Gray*, An Introduction to the Supervision of the Cybersex Offender,* www.uscourts.gov Publishing Information:

Berinato S: The truth about cyber-terrorism (2002). Available at www.cio.com/archive/031502/truth.html. Accessed 25 June 2003

CBN Newsletter, Edisi 9/II Februari 2003Terroris Di Dunia Maya, http://library.monx007.com/computer/terorismaya/2)

Cyberterrorism From Wikipedia, the free encyclopedia http://en.wikipedia.org/wiki/Cyber-terrorism.

*Cyber Terrorism*, August 13, 2008 by Andreasbuvois, http://www.andreasbuvois.blog. friendster.c. 27/07/2009

*Cyber Crime dan Cyber-Terrorism*, *Manfaatkan Perkembangan Teknologi* http://www.unisosdem.org/2009/06/13/kliping_detail.php?aid=2828&coid=1&caid=4,5

*Cyber terrorism creates problem,* http://www.thejakartapost.com/news/2006/09/14/cyberterrorism-creates-problems-real-world.htm

Denning DE: Cyber-terrorism (2000). Available at www.cs.georgetown.edu/~denning/infosec/cyberterror.html. Accessed 25 June 2003

Dorothy Denning, defined cyber-terrorism. http://www.crime-research.org/library/Cyber-terrorism.htm

Dorothy. E. Dening, *Social After Sep 11, Is Cyber Terror Next?, Sosial Science research counsil.* http:// www.ssrc.org/sept11/essays/dening_next_only.htm

Darrel Menthe, *Jurisdiction in Cyberspace : A Theory of International Space*, available at http:/www.mttlr.org/vlogfour/menthe.html

Dr. Mudawi Mukhtar Elmusharaf Cyber Terrorism : The new kind of Terrorism http://www.crime research.org/articles/Cyber_Terrorism_new_kind_Terrorism

http://www.npa.go.jp/higtech/jyu_prog_eng.htm

http://en.wikipedia.org/wiki/Cyber-terrorism

http//www.ParentNews Safety.com, cyber ethics

http://www.directionsmag.com/article.php?article_id=432

http://www.sda-indo.com/sda/features/psecom,id,2068,nodeid,1,_language,Indonesia.html

http://www.unisosdem.org/2009/06/13/kliping_detail.php?aid=2828&coid=1&caid=45

http://www.symantec.com/avcenter/reference/cyberterrorism.and.home.user.pdf

http://google.co.id/ *Naskah Akademik Rancangan Undang-Undang tentang informasi dan transaksi elektronik*

http://techno.okezone.com/index.php/ReadStory/2009/04/20/55/212093/makin-canggih-terorisasia- t

*My Pesonal Library Online, Cyber Crime*. Dapat dijumpai pada situs internet :http://dhani.singcat.com/internet/modul/php.

Muhammad Aulia Adnan, *Tinjauan Hukum Hukum dala E Business* *Olyx76@yahoo.com*.

Mauria, Bisma. *Tindak Pidana Terorisme Dalam Dunia Maya (Cyber Terrorism*) Undergraduate Theses of Airlangga University Created: 2008-12-01, with 1 file(s),

http://adln.lib.unair.ac.id/go.php?id=gdlhub-gdl-s1-2008-mauriabism

Mayor Sus Ir. Rudy A.G. Gultom, M.Sc. *Teknologi Militer, Cyber Terrorism, Sudah Siapkah Kita Menghadapinya?*

http://www.tni.mil.id/2009/06/22/images/gallery/cyber_terrorism.pdf

Naavi in All News, Country News, India News Read 1,092 times. http://www.bloggernews.net/118946 bna 30-4-2009, *How Do We Define "Cyber Terrorism",*

Naskah Akademik Rancangan Undang-Undang tentang informasi dan transaksi elektronik, http://google.co.id/

*Officefor Victims of Crime International Aktivities, OVC Fact Sheet, U.S. Departement of justice,* Washington D.C., Juli 1999 atau buka web site <http://www.ojp.usdoj.gov/ovc/>

The National Police`s Criminal Investigation Department, Commissioner General Makbul Padmanagara. *case cyber terrorism in Kuta Bali,*

http://www.antara.co.id/en/arc/2006/9/13/police-uncover-their-first-cyber-terrorism-case

The National Conference of State Legislatures (NCSL), *Cyberterrorism*, http://en.wikipedia.org/wiki/Cyber-terrorism bna, 30-4-2009

*Terroris di Dunia Maya*, CBN Newsletter, Edisi 9/II Februari 2003, http://library.monx007.com/2009/06/9computer/terorismaya/2

Rattray G J: Chapter 5. The cyber-terrorism threat. Available at www.securityunit. com/asale/inss/terrchp5.html. Accessed 25 June 2003.

Roger Darlington, *Should The Internet be Regulated ?*, http://www.rogerdarlington.co.uk/ regulation.html

Sarah Gordon, *cybernterrorism.* http://www.symantec.com/avcenter/reference/cyberterrorism.pdf

**Dokumen :**

Dokumen United Nations A/CONF.187/10, (*Tenth United Nations Conggress on The Prevebtion of Crime and the Treatment of Offender)* di Wina (Vienna) pada tanggal 10-17 April 2000, halaman 4

Dokumen United Nations A/CONF.203/14, Eleventh United Nations Congress on Crime Prevention and Criminal Justice, Bangkok, 18-25 April 2005, Background paper, Workshop 6: Measures to Combat Computer-related Crime : *"The worldwide multiplication of new information and communication technologies also casts a dark shadow: it has made possible new forms of exploitation, new opportunities for criminal activity and indeed new forms of crime".*

Dokumen Seventh UN Congress AA/CONF/144/L.11

Dalam Kongres XI, judul kongres berubah menjadi *Congress on Crime Prevention and Criminal Justice*

General Assembly Resolution GA-Res. 34/145; Security Council Resolution 635 (1989) Declaration on Measure to Eliminate International Terrorisme

Organization of American States (OAS) dengan Convention to Prevent and Punish the Acts of Terrorism Taking the Forms of Crimes Againts Persons and Related Extrortion That are of International Significance 1971

Tempo Interaktif, diakses pada 13/04/2009

**Kamus :**

Kamus Besar Bahasa Indonesia, 1997, edisi kedua, Departemen Pendidikan Nasional, (Balai Pustaka: Jakarta),

*Kamus Besar Bahasa Indonesia*, edisi ketiga, 2002, (Pusat Bahasa Departemen Pendidikan Nasional

**Undang-undang:**

Moeljatno, KUHP : *Kitab Undang-Undang Hukum Pidana*, 2001, Cet.21, (PT. Bumi Aksara:Jakarta),

Undang- Undang RI Nomor 11 Tahun 2008, *Informasi dan Transaksi Elektronik*

Suara Merdeka edisi 24 juli 2002.