YURISDIKSI BERDASARKAN *CONVENTION ON CYBERCRIME*

SKRIPSI

AFITRAHIM M.R
050400007Y

FAKULTAS HUKUM
UNIVERSITAS INDONESIA
PROGRAM STUDI ILMU HUKUM S1 REGULER
DEPOK
JULI 2009

YURISDIKSI BERDASARKAN *CONVENTION ON CYBERCRIME*

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana

AFITRAHIM M.R
050400007Y

FAKULTAS HUKUM
UNIVERSITAS INDONESIA
PROGRAM STUDI ILMU HUKUM S1 REGULER
KEKHUSUSAN HUKUM TENTANG HUBUNGAN TRANSNASIONAL
DEPOK
JULI 2009

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Afitrahim M.R

NPM : 05400007Y

Tanda Tangan :

Tanggal : 13 Juli 2009

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh :
Nama : Afitrahim M.R
NPM : 050400007Y
Program Studi : Ilmu Hukum
Judul Skripsi : Yurisdiksi Berdasarkan *Convention on Cybercrime*

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Hukum pada Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Indonesia

DEWAN PENGUJI

Pembimbing	: Adijaya Yusuf,S.H.,LL.M.	( )
Pembimbing	: Hadi R. Purnama S.H.,LL.M	( )
Penguji	: Prof.Dr.R.D.Sidik Suraputra,S.H.	( )
Penguji	: Prof.Dr.Sri Setianingsih Suwardi,S.H.,M.H.	( )
Penguji	: Prof.A.Zen Umar Purba,S.H.,LL.M.	( )
Penguji	: Prof.Hikmahanto Juwana,S.H.,LL.M.,Ph.D.	( )
Penguji	: Adolf Warrouw,S.H.,LL.M.	( )
Penguji	: Emmy Juhassarie Ruru,S.H.,LL.M.	( )
Penguji	: Melda Kamil Ariadno,S.H.,LL.M.	( )

Ditetapkan di : Depok
Tanggal : 14 Juli 2009

KATA PENGANTAR

Puji syukur ke hadairat Allah SWT, bahwa dengan rahmat dan hidayahNya, penulis dapat menyelesaikan Skripsi ini. Selanjutnya penulis ingin mengucapkan terimakasih pada :

1. Bapak Dr. M. Fadil Rasad Sp. THT, M.kes dan Ibu Dr. Siti Andriani Gazali yang telah dengan sabar membersarkan penulis sehingga dapat mencapai keadaan yang sekarang, untuk adikku Siti Rahmadini, uda doakan semoga bisa mengikuti jejak uda di UI (Amiiin).
2. Bapak Adjiaya Yusuf S.H., LL.M selaku pembimbing I yang telah meluangkan waktunya untuk membimbing penulis dari segi materi dan substansi (maaf bapak saya terlalu lama memberikan tiap bab).
3. Bang Hadi Rahmat Purnama S.H, LL.M selaku pembimbing II yang setia mengkoreksi tulisan penulis dari segi penulisan (maaf bang kalau saya baru tahu penulisan yang baik dan benar).
4. Bapak Prof. Hikmahanto Juwana S.H., LL.M, Ph.D selaku pembimbing akademis untuk pujian dan omelannya yang membuat penulis semangat dalam menjalani studi di FHUI.
5. Rendhy Febryanto, sahabat penulis yang suaraya tambah merdu dari hari ke hari (kapan rekaman Ren).
6. Teman-teman "*genk* Onta, Ibnu, Refan (tambah ganteng aja lo), Hizbul (kapan bikin law firm Onta), Ana, Real (semoga sukess di Malaysia), Haekal (bahagia selalu), Wahyu, dan Bundo, Qory, Rila, Aida, Devin (selamat akan menempuh hidup baru), Sandra, Anggi, Pinka, Citra, Windy, Keket yang selalu berbagi suka dan duka dengan penulis.
7. Teman-teman PK VI 2004 baik yang sudah lulus maupun akan lulus, Ncil (pembuka jalan angkatan 10), Willy (calon diplomat), Aji (kapan jadi petinggi negara?), Arimbi (selesaikanlah skripsimu, jangan ngajar melulu), Luis (Ciao men), Sandi (magang lagi di LPHI?), Sandra, Vareta, Keke, Setiafitri, Desi (duluan lo des), Rey, Ricky, Adhi (good luck di ekstensi bro), Josua (banyak gaya lo jos), Nyoman (makin cinta sama Arsenal nih kayaknya), Theo, Fitria, Donny (kapan masuk DPR?), Mimi.
8. Teman-teman FHUI angkatan 2004 yang lain yang sudah maupun akan lulus. Bersama-sama kita wujudkan angkatan yang kompak selamanya
9. Teman-teman angkatan 2004 SMAN 4 Jakarta yang sangat kompak dan tanggap terhadap keadaan angkatan maupun sekolah.

10. Teman-teman angkatan 2001 SMPN 1 Jakarta.
11. Teman-teman angkatan 1998 SDN Godangdia 01 Pagi Jakarta.
12. Anggota dan Pengurus *Indonesia Flag Football Association* (IFFA) terutama dari tim Pioneers, Bombshell, Spartans, Phoenix. Juga untuk senior senior (CK, PT, ST, Bang Soljah, Erkep) yang selalu bersedia untuk melatih adik-adiknya.
13. Anggota dan Pengurus United Indonesia yang sudah susah payah mengurusi tiket MU Tour dan Keanggotaan.

Dan berbagai pihak telah membantu penulis untuk menyelesiakan skripsi ini. Penulis merasa skripsi ini jauh dari sempurna, maka dari itu diperlukan saran dan kritik yang membangun. Pada akhir kata moga moga skripsi ini dapat berguna bagi ilmu pengetahuan pada umumnya terutama pada bidang hukum pada khususnya.

Jakarta, 7 Juli 2009

(Afitrahim M.R)

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini:

Nama	: Afitrahim M.R
NPM	: 050400007Y
Program Studi Kekhususan	: Hukum Tentang Hubungan Transnasional
Fakultas	: Hukum
Jenis karya	: Skripsi

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul :

"Yurisdiksi Berdasarkan *Convention on Cybercrime*"

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.
Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok
Pada tanggal : 14 Juli 2009

Yang menyatakan

(Afitrahim M.R)

Abstrak

Nama : Afitrahim M.R.

Program Studi : Ilmu Hukum/Hukum Transnasional.

Judul : Yursidiksi Negara Berdasarkan *Convention on Cybercrime*.

Perkembangan teknologi yang begitu pesat memunculkan berbagai permasalahan di masyarakat. Salah satu akibatnya tersebut adalah terciptanya sebuah media baru untuk berinteraksi yang disebut cyberspace. Di cyberspace orang bebas melakukan apapun tanpa diketahui oleh orang lain karena tidak diketahui asal-usul maupun kewarganegaraan asli seseorang. Hal ini dimanfaatkan oleh sebagian orang untuk melakukan suatu kejahatan yang disebut cybercrime. Telah banyak usaha untuk melakukan pengaturan di cyberspace untuk mencegah terjadinya cybercrime baik oleh hukum internasional maupun hukum nasional. Salah satunya adalah dengan lahirnya Convention on Cybercrime yang dibuat oleh Dewan Eropa (European Council), aspek yang menjadi perhatian khusus dalam konvensi ini adalah masalah yurisdiksi sebuah negara dalam menangani kasus cybercrime karena semua negara tidak senang yurisdiksi negaranya di lampaui oleh negara lain, termasuk Indonesia. Di Indonesia sendiri perngaturan mengenai cybercrime diatur dalam Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Kata Kunci :

Hukum Internasional Yurisdiksi, Cybercrime, Dewan Eropa

Abstract

Name : Afitrahim M.R

Study Program : Law/Transnational Law

Title : State Jurisdiction According To *Convention on Cybercrime*.

Massive techology development brings various problems in the society. One of the impact is an invention of a new interactve media called *cyberspace*. In *cyberspace* people is free to do anything anonymuously because no one knows your actual profile and citizenship. This is used by a certain people to commit such crime called *cybercrime*. There are many attempt to regulate a rules in *cyberspace*, weather from internatonal law or national law. One of the attempts is created by *Council of Europe* who produce *Convention on Cybercrime* with jurisdiction as one special aspect that is important because none of the country in the world like their jurisdiction violated by other country, inculding Indonesia. In Indonesia *cybercrime* regulation enacts in Law number 11 Year 2008 regarding Information and Electronic Transaction.

Keywords:

International Law, Jurisdiction, *Cybercrime*, Council of Europe

DAFTAR ISI

BAB 1
Pendahuluan

1.1. Latar Belakang

Perkembangan teknologi dewasa ini menyebabkan kita tidak bisa lepas dari sebuah perangkat elektronik yang bernama komputer, istilah komputer yang diambil dari bahasa latin yaitu *computare* yang artinya menghitung pada mulanya diciptakan untuk melakukan penghitungan yang kompleks.

Awal mula komputer yang sebenarnya dibentuk oleh seorang profesor matematika Inggris, Charles Babbage (1791-1871). Tahun 1812, Babbage memperhatikan kesesuaian alam antara mesin mekanik dan matematika:mesin mekanik sangat baik dalam mengerjakan tugas yang sama berulangkali tanpa kesalahan; sedang matematika membutuhkan repetisi sederhana dari suatu langkah-langkah tertenu. Masalah tersebut kemudian berkembang hingga menempatkan mesin mekanik sebagai alat untuk menjawab kebutuhan mekanik. Usaha Babbage yang pertama untuk menjawab masalah ini muncul pada tahun 1822 ketika ia mengusulkan suatu mesin untuk melakukan perhitungan persamaan diferensial. Mesin tersebut dinamakan Mesin Diferensial. Dengan menggunakan tenaga uap, mesin tersebut dapat menyimpan program dan dapat melakukan penghitungan serta mencetak hasilnya secara otomatis. Setelah bekerja dengan Mesin Diferensial selama sepuluh tahun untuk menyempurnakan penemuannya Babbage membuat komputer general-purpose yang pertama, yang disebut *Analytical Engine*[1].

Saat ini komputer mengalami perkembangan yang sangat pesat, hal ini ditandai dengan munculnya penelitian yang dilakukan oleh Joshepson Junction[2] , dalam penelitiannya tersebut Joshepson mencoba untuk menggantikan bahan dasar prosesor yang ada saat ini dengan helium cair yang telah didinginkan mendekati nol derajat absolut (sekitar minus 200 derajat celcius), penggantian bahan ini dapat meningkatkan kemampuan memproses (*processing ability*) prosesor tersebut dari miliyar per detik menjadi triliyun perdetik. Joshepson

[1] Ivan Sudirman & Romi Satria Wahono;*Sejarah Komputer*, Makalah disampaikan pada Training Ilmu Komputer,bahan didownload dari www.ilmukomputer.com, hal 2

[2] Edmon Makarim;*Kompilasi Hukum Telematika*, cet kedua, hal 59

mengambil ide dari novel fiksi karya Arthur .C. Clarke yang berjudul 2001: Space Odyssey[3], dalam novel tersebut ada komputer bernama HAL 9000, komputer tersebut menampilkan seluruh fungsi yang diinginkan dari sebuah komputer generasi kelima. Dengan kecerdasan buatan (*artificial intelligence*), HAL memiliki nalar yang cukup untuk melakukan percakapan dengan manusia, menggunakan masukan visual, dan belajar dari pengalamannya sendiri.

Seiring dengan perkembangan komputer ternyata terdapat pula perkembangan yang sangat signifikan dibidang piranti lunak (*software*) maupun jaringan (*network*) yang digunakan untuk melengkapi fungsi komputer. Salah satu perkembangan tersebut adalah dengan ditemukannya internet yang sudah tentu pada saat ini merupakan teknologi yang sudah sangat luas dipakai oleh orang banyak, kata internet sendiri memiliki 2 arti yaitu :[4]

a. Jaringan internet (huruf "i" kecil sebagai huruf awal) adalah suatu jaringan komunikasi yang mana komputer-komputer terhubung dapat berkomunikasi walaupun perangkat keras dan perangkat lunaknya berlainan (sering disebut *internet- working*).

b. Jaringan Internet (huruf "I" besar sebagai huruf awal) adalah jatingan dari sekumpulan jaringan (*networks of networks)* yang terdiri dari jutaan komputer yang dapat berkomunikasi satu sama lain dengan menggunakan sauatu aturan komunikasi jaringan komputer (protokol) yang sama. Protokol yang digunakan tersebut adalah *Transsmission Control Portoco/InternetProtocol* (TCP/IP).

Sedangkan *The Council Networking Council* (FNC) memberikan definisi mengenai internet dalam resolusinya tanggal 24 Oktober 1995. Definisi yang diberikan adalah sebagai berikut[5]:

---

[3] Sudirman, *op.cit*, hal 9

[4] Francisca Haryanti Chandra, *Internet:Information Superhighway*, Makalah pada Penataran Kualitas Dosen di Bidang Pengolahan Data dan Penyusunan Presentasi Melalui Media Komputer bagi Dosen PTS Kopertis Wilayah V1 di Semarang, 4-8 September 1995, hal 1-2

[5] Agus Raharjo, *Cybercrime :Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, hal 60

Internet refers to the global information system that --

(i) is logcally linked toghether by a globally unique addresses space based in the Internet Protocol (IP) or its subsequent extensions/follow-ons;

(ii) is able to support communications using the Transsmission Control Protocol/Internet Protocol (TCP/IP) suite or it's subsequent extension/follow-ons, and/other Internet Protocol (IP)-compatible protocols; and

(iii) Providers, uses or makes accessible, either publicly or privately, high level services layered on the the communicatons and related infrastructure described herein

Sejarah internet dimulai ketika perang dingin antara Amerika Serikat (AS) dan Uni Soviet (USSR) dimulai dengan diluncurkannya satelit buatan pertama milik Uni Soviet, *Sputnik* pada tahun 1957. Sebagai respons atas perbuatan Uni Soviet, AS membentuk *Advance Reseach Project Agency* (ARPA) pada tahun 1958 yang berada dibawah *Departement of Defense* (DoD), lalu untuk melindungi data-data dan arsip rahasia yang penting. Tugas pertama ARPA adalah membangun sebuah jaringan untuk melindungi data dan arsip tersebut, untuk itu ditunjuklah J.C.R Licklider, seorang ahli komputer dari *Massachusetts Institute of Technlogy* (MIT) untuk menjadi ketua program *Computer Research* di *Defense Advance Reseach Project Agency* (DARPA), bagian dari ARPA yang mengkhususkan diri untuk mengembangkan program-program yang berkaitan dengan pertahanan dan keamanan. Hasilnya teciptalah sebuah jaringan komputer yang disebut ARPANET

Komersialisasi ARPANET pertama kali di lakukan oleh salah satu kontraktornya, yaitu *Bolt, Beranet & Newman* (BBN) yang membuka layanan paket data pertama bagi publik yang di sebut *telnet*, istilah internet baru populer pada tahun 1982 dimana ARPANET tidak lagi berfungsi sebagai host utama yang menghubungkan setiap komputer didunia, sebagai penggantinya digunakanlah *Transsmission Control Portocol/InternetProtocol* (TCP/IP) sebagai protokol universal yang megizinkan pengguna komputer agar dapat terhubung ke sebuah host tanpa mengetahui jalur pasti ke host tersebut.

Setelah menggunakan TCP/IP, pada kurun waktu 1980-1990, Tim Berners-Lee seorang kontraktor di *European Organization on Nuclear Research* (CERN) Swiss ,mengembangkan ENQUIRE, sebuah database bagi karyawan CERN, dia memakai konsep *hypertext* yang dipoulerkan oleh Ted Nelson pada tahun 1965[6]. *Hypertext* adalah teknologi yang memungkinkan setiap halaman (*page)* langsung terhubung dengan sebuah link tanpa harus mengetik alamat *page* tujuan, lalu Berners-Lee dan partnernya Robert Cailliau menggabungkan konsep *hypertext* dengan internet, hasilnya pada 1990 terciptalah halaman web pertama didunia, yang kita kenal dengan nama *World Wide Web* (disingkat www). Pada tahun 1994-1996 dimulai komersialisasi www, dimana ide Berners-Lee dan Cailliau di ambil oleh DARPA dan mereka mendirikan *World Wide Web Consortium* (W3C), saat ini internet sudah memasuki masa apa yang disebut dengan web 2.0[7], dimana tampilan dan bahasa programnya semakin kompleks dan rumit.

Perkembangan internet yang sangat pesat melahirkan konsep-konsep baru dalam dunia informasi teknologi salah satu teori yang berkembang adalah teori *cyberspace* sebagai sebuah "dunia baru atau rumah baru"[8], istilah *cyberspace* pertama kali dipopulerkan oleh William Gibson dalam novel *science fiction* yang berjudul *Neuromancer* [9] . Secara singkat *cyberspace* dapat didefinisikan didefinisikan sebagai suatu tempat yang tidak berbatas dimana data-data diorganisir sedemikian rupa kedalam suatu lintas media[10].Sementara definisi yang lain mengatakan bahwa *cyberspace* adalah fenomena dunia digital yang telah merasuki segala segi dari kehidupan manusia.[11]

Dibalik kegunaan internet sebagai media penyampai informasi yang lebih cepat, ada juga kekurangan dari internet, kekurangannya adalah dari segi keamanan. Meskipun sampai saat ini telah banyak ditemukan program-program untuk melindungi data-data penting di internet *(firewall*), masih saja ada segelintir

---

[6] Sejarah Internet, www.id.wikipedia.org/wiki/sejarah_internet, diakses tanggal 15 Maret
[7] History of The World Wide web, www.en.wikipedia.org/wiki/history_of_the_world_wide_web, diakses tanggal 16 Maret
[8] Yang dimaksud dengan dunia baru yaitu dunia yang bersifat viritual (maya) dimana belum ada seperangkat aturan yang berlaku dan masih perlu dijelajahi lagi (Abdul Wahid & Muhammad Labib, *Kejahatan Mayantara (cyber crime), hal 3*)
[9] Makarim, *op.cit*, hal 5
[10] .*Ibid*
[11] .*Ibid*, hal 13

orang yang memanfaatkannya sebagai media kejahatan, kejahatan yang dilakukan pada awalnya hanya sebatas menembus *firewall* jaringan sebagai hobi, mereka ini dikenal dengan sebutan *cracker*[12]. Selain *cracker* ada pula segelintir orang yang tidak hanya sekedar menembus *firewall,* tapi juga menyalahgunakan informasi bahkan mengubah informasi tersebut untuk hal-hal yang melanggar hukum (penipuan, pencurian, pencemaran nama baik, dan lain-lain), golongan ini dikenal dengan sebutan *hacker*[13], mereka bebas beroperasi dari berbagai belahan dunia untuk masuk ke jaringan yang bersifat rahasia.

Untuk menangkal mereka (baik *cracker* maupun *hacker*) maka dibutuhkan sebuah hukum yang tegas dan mengikat bagi semua orang yang menggunakan internet, namun yang menjadi permasalahan utama adalah tentang yurisdiksi negara, apakah setiap negara berhak mengadili pelaku *cybercrime* yang berasal dari negara lain? Untuk mengatasi permasalahan ini, banyak negara-negara yang mencoba untuk membahas *cybercrime.* Salah satu usaha yang terlihat jelas adalah Dewan Eropa (*Council of Europe)* membahas dan mengkaji masalah *cybercrime*, Dewan Eropa telah menghasilkan suatu konvensi internasional tentang *cybercrime* yang dikenal dengan nama The *Council of Europe Convention on Cybercrime* yang dikenal dengan sebutan *Convention on Cybercrime*, konvensi ini di tandatangani di Budapest, Hungaria pada tanggal 23 November 2001. Masalah yang diatur dalam konvensi tersebut meliputi segala aspek yang menyangkut kepentingan negara termasuk masalah yurisdiksi, yang menjadi bahasan utama tulisan ini. Hingga tanggal 16 Maret 2009,negara yang telah meratifikasi konvensi ini berjumlah 24 Negara dengan Jerman menjadi negara terbaru yang meratifikasi konvensi ini pada tanggal 9 Maret 2009[14].

Saat ini sudah banyak pembicaraan mengenai permasalahan *cybercrime* baik secara bilateral mau pun multilateral, contohnya perjanjian bilateral antara

---

[12] Definisi *cracker* yang umum adalah *"a person who breaks security, encryption, or digital rights management schemes — a software cracker or password cracker"*, http://en.wikipedia.org/wiki/Cracker

[13] Definisi *hacker* yang umum adalah *" hacker is a person who breaks into computers."*, http://en.wikipedia.org/wiki/Hacker_(computer_security)

[14] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG, diakses tanggal 10 Maret

Jepang dan Prancis[15] yang dilakukan di sela-sela konfrensi G8 pada tahun 2008. Pasca *cybercrime convention 2001*, negara-negara Eropa juga tengah membicarakan untuk membuat sebuah peraturan mengenai penanganan terhadap serangan *denial-of-services* (DOS-attack) dan *hacking*[16]

Saat ini dunia interasional sedang hangat membicarakan tentang kasus *cybercrime* yang diduga dilakukan oleh negara China yaitu, kasus mata-mata melalui internet (*cyberspy*). Kasus ini pertama kali di ketahui oleh para aktivis pro Tibet yang merasa data-data penting seputar Dalai Lama dan orang-orang dalam di pemerintahan pengasingan Tibet, telah di *hack* dan diunduh (*download*) secara ilegal oleh orang yang tidak dikenal. Bekerja sama dengan ahli komputer dari Jerman dan Kanada, mereka menelusuri asal muasal jaringan tersebut, hasilnya sangat mengejutkan ditemukan bahwa sekitar 1300 komputer di seluruh dunia, khususnya milik pemerintah di 103 negara telah diawasi (*spy*) oleh pemerintah China, termasuk Indonesia[17]

Perkembangan hukum yang mengatur mengenai *cybercrime* di indonesia dimulai pada tahun 1998-1999 dengan di keluarkannya Undang-Undang No 36 Tahun 1999 tentang telekomunikasi, dalam undang-undang ini meskipun tidak secara jelas di sebutkan mengenai *cybercrime*, namun sudah memuat pengaturan tentang perbuatan yang digolongkan sebagai cikal-bakal *cybercrime*, yaitu *Illegal Access*[18] . Perkembangan yang terbaru mengenai peraturan perundang-undangan yang mengatur tentang *cybercrime*, adalah dengan dikeluarkannya Undang-Undang no 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), pada awal pemberlakuannya undang-undang ini menuai kontroversi dari berbagai kalangan, namun lambat laun meski belum efektif, keberadaan undang-undang ini semakin mempertegas bahwa Indonesia sudah tidak ketinggalan zaman dalam mengatasi segala bentuk kejahatan yag berhubungan dengan teknologi.

---

[15] Secara garis besar dalam perjanjian tersebut disebutkan yang termasuk *cybercrime* adalah pornografi anak (*child pornography*), pelecehan melalui internet (*internet harassment*), dan masalah hak cipta yang dilakukan melalui jaringan komputer (*copyright crimes through in peer-to-peer networks)*, selain itu juga dijalin kerjasama dalam bentuk pertukaran informasi oleh kepoilisian antar kedua negara, < www.crime-research.org/news/26.06.2008/3428/>, diakses tanggal 4 April

[16] http://news.zdnet.co.uk/security/0,1000000189,39156968,00.htm, diakses tanggal 5 April

[17] Selain Indonesia, negara-negara yang diduga diawasi adalah Bangladesh, Bhutan, Filipina, Korea Selatan, www.independent,co.uk , diakses tanggal 3 April

[18] Undang-Undang no 36 tahun 1999, pasal 22

1.2. Pokok Permasalahan

Tulisan ini mengangkat permasalahan yurisdiksi negara dalam menangani kasus *cybercrime* yang dilakukan lintas negara. Seiring dengan kemajuan teknologi internet berdampak makin beragamnya jenis *cybercrime*, contoh yang paling aktual adalah berkembangnya suatu jenis *cybercrime* baru yaitu *cyberterrorism*, yang merupakan kombinasi antara *cybercrime* dalam *cyberspace* dan terrorisme.[19]

Untuk membatasi pembahasan yang terlalu kompleks maka peneliti akan mebatasi pada masalah yang akan dibahas yaitu :

1.Bagaimana pengaturan tentang yurisdiksi negara dalam menangani kasus *cybercrime* berdasarkan ketentuan hukum internasional yang berlaku?

2.Bagaimana pengaturan mengenai yurisdiksi dalam menangani kasus *cybercrime* di Indonesia sebelum dan sesudah berlakunya Undang-Undang Informasi dan Transaksi Elektronik No 11 Tahun 2008?

3.Bagaimana kemungkinan hukum Indonesia memandang kasus *cyberspy*?

1.3.Tujuan Penelitian

1.3.1. Tujuan Umum

Tujuan umum dari penulisan ini adalah memberikan gambaran tentang pengaturan mengenai yurisdiksi *cybercrime* di Indonesia dan bagaimana instrumen hukum internasional, dalam hal ini *the Europe Council Convention on Cybercrime* mengatasi masalah yurisdiksi suatu negara dalam menangani kasus *cybercrime*.

[19] Barry Colin, *the Future of Cyberterrorism*, Crime and Justice International, March 1997, hal 15-18

1.3.2. Tujuan Khusus

Selain tujuan umum penulisan ini juga memiliki tujuan khusus yang berfungsi untuk menjelaskan hal-hal yang spesifik diluar tujuan umum, adapun yang menjadi tujuan khusus penulisan ini adalah :

A.Mengetahui bagaimana pendefinisian *cybercrime* dan jenis-jenis *cybercrime* yang diatur dalam *cybercrime convention 2001*.

B.Mengetahui bagaimana negara-negara peserta konvensi mengatur tentang *cybercrime* dalam hukum nasionalnya.

C.Membandingkan pengaturan mengenai yurisdiksi indonesia dalam menangani kasus *cybercrime* sebelum dan sesudah di sahkannya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE).

1.4.Kerangka Konsepsional

Untuk membatasi bahasan yang bergitu luas, penulis hanya menfokuskan pembahasan tulisan ini pada masalah yurisdiksi yang terkait dengan negara sebagai subjek hukum Internasional dan juga hubungan antara warganegara dengan negara pada umumnya, teori-teori yang dipakai adalah teori-teori tentang yurisdiksi yang berkembang dalam hukum Internasional. Teori-teori tersebut adalah :

1) Subjective Territoriality
2) Objective Territoriality
3) Nationality
4) Passive Nationality
5) Protective Principle
6) Universality

Istilah-istilah yang akan sering ditemui pada tulisan ini adalah istilah di bidang komputer, untuk memudahkan pembaca memahami tulisan ini, maka akan diuraikan beberapa istilah yang sering ditemui :

1) *Hacking* adalah penggunaan kemampuan dalam bidang komputer untuk mendapatkan akses tidak sah pada suatu jaringan atau mendapatkan data secara tidak sah[20]

[20] "American heritage dictionary of the English language,fourth editionwww.referance.com/browse/wiki/hack(technologyslang), diakses tanggal 20April

2) *Carding* adalah kejahatan yang dilakukan dengan cara mencuri informasi dari credit card dan mengunakan informasi tersebut untuk tujuan transaksi ilegal tanpa sepengetahuan pemiliknya[21]

4) *Defacing* adalah tindakan mengubah tampilan dari suatu website dengan tampilan yag diinginkan si pelaku[22]

5) *Spamming* adalah menggunakan segalamacam media komunikasi elektronik untuk mengirimkan pesan yang tidak diinginkan dalam julah yang banyak, tanpa pandang bulu, tidak seperti pengiriman pesan kepada kelompok tertentu sebagaimana terjadi pada pemasaran normal,spam berbentu email berisi iklan[23]

6) Phreaking adalah kejahatan yang menggunakan jaringan telepon untuk menggunakan hubunga komuikasi yang lebih lama dengan cara yang ilegal.[24]

1.5. Metodologi Penelitian

Metodologi penelitian yang digunakan dalam penelitian ini adalah studi normatif. Dalam studi kepustakaan ini penulis berusaha untuk mendapatkan data-data yang ada hubungannya dan dapat mendukung permasalahan yang dibahas. Bahan pustaka yang dipergunakan antara lain:

1.Bahan Hukum *primer*, yaitu bahan hukum yang mempunyai kekuatan mengikat yang berhubungan dengan penulisan ini yaitu, *The Council of Europe Convention on Cybercrime*, Undang-Undang Telekomunikasi, Undang-Undang Penyiaran, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Keterbukaan Informasi Publik.

---

[21] "*Wikipedia, the free online dictionary*", www.referance.com/browse/wiki/carder, diakses tanggal 20 April

[22] "*Merriam-Websters Dictionary of Law*"www.dictionary.reference.com/search?q--defacing, diakses taggal 21 April

[23] Wikipedia The Free Online Dictionary 2001-2006 <www.refernce.com/browse/wiki/spam%28electronic%29>, diakses tanggal 21 April

[24] Dennis Howe, "*the free online dictionary of computing*" www.dictionary.reference.com/search?q--phreaking, diakses tanggal 21 April

2.Bahan Hukum *sekunder*, yaitu bahan hukum yang berupa buku-buku teks, penelusuran internet, artikel ilmiah, jurnal, majalah dan surat kabar, makalah dan skripsi.

3.Bahan Hukum *tertier*, yaitu bahan hukum yang memberikan petunjuk maupun penjelasan terhadap bahan hukum *primer* dan *sekunder*, yaitu kamus.

Penelitian ini termasuk penelitian deskriptif yang memberikan gambaran yang jelas mengenai *cybercrime* dalam penerapan perangkat hukum internasional, teori-teori dan prinsip-prinsip umum terkait, dan peraturan-peraturan nasional Indonesia. Tujuan dari penelitian ini adalah penelitian hukum yang normatif dimana tidak terlalu diperlukan perumusan hipotesa.

1.6. Sistematika Penulisan

Sistematika disajikan untuk mempermudah pembaca dalam memahami materi yang akan dibahas selanjutnya dalam skripsi ini. Dengan adanya sistematika ini diharapkan pembaca dapat mengetahui secara garis besar skripsi ini. Penulisan ini dapat dibagi dalam 5 bab sebagaimana diuraikan berikut ini :

Bab pertama berisikan pendahuluan, yang menjelaskan mengenai latar belakang permasalahan yang berisi tentang sejarah komputer, internet dan perkembangan terkini mengenainya yang membuat penulis tertarik untuk menjadikan topik ini sebagai tulisan, lalu dijelaskan pula apa yang menjadi masalah yang akan dibahas dalam tulisan ini agar tidak terlalu luas pembahasannya, selanjutnya diternagkan juga dalam bab ini tentang tujuan umum dan khusus yang ingin dicapai penulis dengan penulisan ini dan diterangkan pula metodologi (cara-cara penulis mendapatkan dan menganalisis data) untuk tulisan ini agar pembaca memahami tulisan ini, pada akhirnya di bab ini diterangkan mengenai sistematika penulisan yang dimaksudkan untuk memandu pembaca mengikuti jalan pikiran penulis dalam mengupas topik ini.

Bab kedua berisikan tentang tinjauan umum tentang *cybercrime*. Pada bab ini dijelaskan terlebih dahulu mengenai *cyberspace* sebagai media terjadinya *cybercrime*, karena antara *cyberspace* dan *cybercrime* mempunyai ikatan yang sangat dekat, lalu dijelaskan pula pendefinisian *cybercrime* menurut berbagai

sumber baik itu dari ahli hukum maupun ahli komputer. Pada bab ini juga dijelaskan kejahatan atau perbuatan apa yang dapat digolongkan sebagai *cybercrime* dan juga dijelaskan mengenai sasaran dari *cybercrime* tersebut.

Bab ketiga berisikan mengenai teori-teori umum tentang yurisdiksi yang berlaku dan berkembang dalam hukum internasional, pengaturan mengenai yurisdiksi berdasarkan *cybercrime convention 2001*, serta perbandingan pengaturan tentang *cybercrime* dalam hukum nasional beberapa negara peserta *cybercrime convention 2001*.

Bab keempat adalah inti dari semua permasalahan yang sudah bersifat khusus bab ini berisikan pembahasan mengenai pengaturan mengenai yurisdiksi dalam penanganan kasus *cybercrime* di Indonesia. Pada bab ini akan dibandingkan bagaimana yurisdiksi dalam menangani kasus *cybercrime* sebelum berlakunya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang kala itu masih berlaku Undang-Undang Penyiaran dan Undang-Undang Telekomunikasi, dan setelah diberlakukannya UU ITE, sebagai tambahannya penulis memasukkan juga Undang-Undang Keterbukaan Informasi Publik karena Undang-Undang ini berkaitan dengan UU ITE, lalu penulis juga membahas kasus *cyberspy* yang dilakukan oleh pemerintah China dan menganalisisnya dari prespektif hukum nasional Indonesia

Bab kelima berisi kesimpulan dari seluruh pembahasan yang telah diuraikan pada bab-bab sebelumnya, kesimpulan ini adalah merupakan jawaban atas pokok permasalahan yang penulis ajukan dalam bab pertama, selain itu bab ini juga berisi saran-saran yang penulis buat untuk permasalahan yang dibahas.

Bab 2
TINJAUAN UMUM TENTANG CYBERCRIME

2.1.Cyberspace Sebagai Media Cybercrime

Kelahiran internet diikuti juga dengan munculnya penggunaan istilah baru, salah satunya adalah *cyberspace* (dunia maya). Istilah *cyberspace* pertama kali dipopulerkan oleh William Gibson dalam novel *science fiction* yang berjudul *Neuromancer*[1] pada tahun 1980-an, *cyberspace* didefinisikan sebagai suatu tempat yang tidak berbatas dimana data-data diorganisasikan sedemikian rupa ke dalam suatu lintas media[2]. Sementara definisi dari Ian J. Lloyd mengatakan bahwa *cyberspace* adalah fenomena dunia digital yang telah merasuki segala segi dari kehidupan manusia.[3]

Cyberspace dan *cybercrime* merupakan dua hal yang tak terpisahkan. Korelasi keduanya apabila dianalogikan seperti hubungan antara bumi dan aktifitas manusia, yaitu hubungan antara media dan aktifitas yang berlangsung di atasnya. *Cybercrime* sebagai suatu aktifitas tidak akan terjadi jika tidak ada medianya, yaitu *cyberspace*. Namun penanalogian diatas akan menjadi tidak tepat jika kita kaitkan dengan permasalahan batas teritorial atau wilayah, maksudnya jika di dunia nyata, kita dengan mudah dapat mengidentifikasian tempat (lokasi) berlangsungnya suatu aktifitas seseorang. Maka hal yang sama tidak berlaku di *cyberspace*, karena aktifitas di media terebut tidak seperti yang terjadi di dunia nyata, terlepas dari isu batas wilayah. Permasalahan batas wilayah ini dalam konteks dunia nyata mempunyai arti yang penting, khususnya dalam hal menentukan hukum mana atau hukum apa yang seharusnya diterapkan terhadap suatu peristiwa.[4]

---

[1] Mark D.Rasch,*CriminalLaw and The Internet*, www.cybercrime.net, diakses tanggal 20 April 2009, Lihat juga di buku *Kompilasi Hukum Telematika* karya Edmon Makarim, hal 59
[2] *Ibid.*,
[3] *Ibid.*, hal 13, lihat juga di artikel Ian J.Lloyd, *Information and Technology Law*, third edition, London, Butterworths, 2000
[4] UNESCO, *The International Demension of Cyberspace Law*, (England: Ashgate Publishing Ltd., 2000), hal 128

Secara umum *cyberspace* memiliki sejumlah karakteristik yang unik, dimana beberapa diantaranya mempunyai pengaruh besar bagi dunia hukum. Karakterisitik yang dimaksud antara lain sebagai berikut:[5]

1) Tidak ada batasan wilayah (*No geoghraphic limitation/no boundaries*)

Karakteristik dari *cyberspace* yang paling khas adalah tidak adanya batasan wilayah (*no boundaries*). Karakteristik ini muncul dengan didasari argument yang memandang bahwa segala yang terjadi di *cyberspace* merupakan suatu interaksi secara elektronik yang dapat melewati batas negara.[6] Sebagai salah satu contoh dalam hal ini adalah *chatting*, dimana aktifitas tersebut tidak mengenal adanya batasan wilayah. Artinya tidak ada suatu ketentuan yang menyatakan bahwa setiap orang hanya dapat *chatting*[7] dengan orang lain yang masih berada di negara yang sama. Karena pada kenyataannya sesorang yang berasal dari negara Indonesia bebas melakukan *chatting* dengan siapapun dari negara manapun. Berkaitan dengan prinsip *no baoundaries* tersebut, pandangan yang paling ekstrim yang berkembang menyatakan bahwa *cyberspace* tidak terkait dengan multi yurisdiksi, melainkan berkaitan dengan tidak ada yurisdiksi.[8]

Mengingat keberadaan yurisdiksi selalu dikaitkan dengan keberadaan suatu hukum, maka pendapat yang diuraikan pada paragraf diatas kurang lebih dapat diartikan bahwa di *cyberspace* pada dasarnya tidak ada hukum yang mengatur (*lawless paradise)*[9] . Munculnya pendapat tersebut dan jika di kaitkan karakteristik dari *cyberspace* yaitu *no baoundaries*, maka dapat dikatakan bahwa keberadaan *cyberspace* bersama dengan karakteristiknya telah menyimpang dari konsep penerapan hukum yang umumnya didasarkan kondisi fisik dan wilayah.[10]

---

[5] *Ibid.*, hal 14
[6] *Ibid.*
[7] Online-chat adalah suatu bentuk komunikasi melalui internet dengan cara mengetik teks (*text-based*) dimana dua orang atau lebih saling melakukan percakapan dan balasan yang didapatkan secara langsung seperti sedang berbicara secara langsung, kenyataan yang sebenarnya bahwa orang tersebut berada di tempat yang jauh, biasanya chatting dilakukan melaui sebuah media seperti Internet Relay Chat (IRC) , Yahoo Messangers dan lain lain
[8] David G.Post, "Anarchy, State and The Internet: An Essay on Law Making in Cyberspace", (*Journal of Online Law*, 1995), hal 2
[9] UNESCO, *.op. cit*, hal 219
[10] *Ibid.*, hal 15

2) Penyembunyian Identitas (*Anonymity*)

Karakteristik *cyberspace* yang lain adalah diperkenankannya seseorang memasuki *cyberspace* untuk menyembunyikan identitas aslinya. Dalam hal ini pengguna internet umumnya menyembunyikan identitas aslinya dengan nama samaran (*nickname).*[11] Bahkan tidak hanya nama saja yang dapat disembunyikan di *cyberspace*, tempat asal dan umur adalah hal-hal yang lain yang dapat dimanipulasi di *cyberspace*. Sebagai contoh misalnya Udin seorang warganegara Indonesia berusia 45 tahun tengah melakukan *chatting* dengan pengguna lainnya, dalam kesempatan ini Udin bisa saja mengaku bernama John yang berkewarganegaraan Australia berusia 20 tahun.

Karakteristik *cyberspace* yang satu ini memang memungkinkan setiap orang berimajinasi sepuasnya dalam menentukan identitas yang akan diguakan saat beraktifitas di *cyberspace*. Namun disamping itu, keberadaan karakteristik ini juga mempunyai dampak negatif secara hukum yaitu, setiap orang yang melakukan pelanggaran atau kejahatan di *cyberspace* dapat saja lolos dari jeratan hukum hanya dengan memanipulasi identitas dirinya.

3) Flekisbilitas (*mobilitas*)

Karakteristik selanjutnya adalah aktifitas di *cyberspace* merupakan aktifitas yang sangat fleksibel dalam hal ruang gerak (mobilitas).[12] Dengan adanya karakteristikini maka pengguna *cyberspace* dengan bebas dapat memilih tempat dimana ia akan melanjutkan aktifitasnya.

Fleksibilitas ini dapat terjadi karena aktifitas di *cyberspace* yang mengedepankan konsep *online*, tidak harus dilakukan di suatu komputer tertentu secara tetap. Apalagi jika dikaitkan dengan perkembangan jenis komputer yang, semakin canggih, yang ditandai dengan kemunculan *Laptop* yang diikuti dengan komputer saku (*pocket computer*) yang memiliki kelebihan dari segi mobilitas.

---

[11] *Ibid.*
[12] *Ibid.*, hal 16

Dampaknya secara hukum adalah dengan sifat fleksibilitas tersebut, pelaku kejahatan di *cyberspace* dapat saja lolos dari jeratan hukum hanya dengan memindahkan lokasi tempat aktifitas *cybercrime* berlangsung dari satu yurisdiksi ke yurisdiksi yang lain. Mereka dapat pula memilih yurisdiksi suatu negara yang kondisi penegakkan hukumnya lemah, sehingga semaikin membuka peluang untuk lolos dari jeratan hukum.

2.2. Perbedaan Cyber-related Crimes dengan Cybercrime

Ilmu pengetahuan dan teknologi telah menghasilkan prasarana yang memudahkan manusia. Salah satu produk dari ilmu pengetahuan dan teknologi adalah teknologi informasi atau yang lebih dikenal dengan teknologi telekomunikasi. Telekomunikasi telah membantu umat manusia berinteraksi dengan sesama umat manusia dengan mudah. Munculnya komputer dan internet membuat komunikasi tidak dibatasi dengan sekat-sekat territori suatu negara.

Perkembangan teknologi terutama internet membuat banyak dampak positif bagi kemjuan umat manusia,ini ditandai dengan munculnya berbagai layanan yang dilakukan via internet seperti e-*commerce, e-banking, e-goverment dan e-learning*. Selain dampak positif perkembangan tekologi juga memiliki dampak negatif, dalam hal ini dikaitkan dengan dunia kejahatan, para pelaku biasanya menggunakan intenet untuk melakukan kejahatan yang berhubungan dengan komputer seperti, penipuan kartu kredit dan bursa efek, pornografi anak dan terrorisme, selain itu juga ada kejahatan yang menjadikan komputer sebagai targetnya seperti, *defacing*, *cracking* dan *phreaking*.[13]

---

[13] Heru Sutadi, "Cybercrime, apa yang bisa diperbuat?", <http://www.sinarharapanbaru.co.id/berita/0304/05/op01.html>, diakses tanggal 15 april . sebagaimana dirujuk oleh Abdul Wahid dan Mohammad Labib *.op.cit.*, hal 27

Beberapa pengertian dalam kalimat diatas (diambil dari Kamus Komputer dan Teknologi Informasi karangan Jack Febrian, Penerbit Informatika tahun 2007)

Defacing adalah melakukan perubahan pada halaman web depan pada situs-situs tertentu, biasanya aktifitas ini dilakukan oleh para *hacker* atau *cracker* dengan gerakan undergroundnya sebagai sebuah *cyber gang fight* untuk mengganggu informasi yang dimunculkan pada halaman situs yang dimaksud.

Cracking adalah proses menemukan kata kunci rahasia dari data yang telah disimpan dan atau dikirim oleh sistem komputer. Pendekatan umumnya dengan secara terus-menerus menebak password yang ingin di-*crack*. Tujuan password *cracking* adalah untuk membantu user memperoleh kembali password yang hilang/lupa, untuk mendapatkan hak-hak akses ke sebuah sistem, atau sebagai ukuran pencegahan oleh administrator

2.2.1. Cyber-related Crime (Kejahatan komputer)

Beberapa ahli telah mencoba mendefinisikan pengertian dari kejahatan komputer, baik dalam suatu literatur (pengertian kriminologis) atau dalam undang-undang/rancangan undang-undang (pengertian yuridis, sehingga muncul berbagai definisi tentang kejahatan komputer, sesuai dengan kepentingan dan sudut pandang masing-masing). Berikut ini penulis mencoba untuk menguraikan beberapa pengertian mengenai kejahatan komputer sebagai gambaran.

1) Pengertian kejahatan komputer menurut Kadish Sanford dan Morrison (guru besar di *Law University of California*) :

Service.When people gain unauthorized access to a computer and use the service for their own purpose, the crime is also often describe as theft of computer crime. If the unauthorized use continue for the exteded period, if can result in a conciderable less in term of service value without permission from the employer, employees have established own companies and have used the employers computer for the new company seometimes the employers existing data and programs have been used.[14]

2) Pengertian kejahatan komputer menurut IBM. Inc. Japan (perancangan dan specialis komputer) :[15]

a. *Crime using computer as a tool of theft, fraud, embezzlement and so forth*

b. *Crime through computer system, such at tempering stealing, and elimination of the data and programs.*

3) Pengertian kejahatan komputer meurut *Organization of European Community a Development : Any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of data*.[16]

---

sistem untuk mengecek password-password yang dapat *di-crack* dengan mudah. Istilah password cracking terbatas untuk menemukan kembali satu atau lebih plaintext password dari password yang *di-hack*.

Phreaking adalah proses *hacking* dengan menggunakan telefon

[14] Kadish Sanford and May T Morrison, ed., "*Encyclopedia of Crime and Justice*",Law University of California, Berkeley, Volume I, hal 220.

[15] Djoko Sarwoko "Computer Crime sebagai Dimensi Baru Tindak Pidana Ekonomi", *Varia Peradilan Nomor 21 Tahun II*, (Juni 1987), hal 150, tampaknya IBM. Inc. menganut konsep *Computer* dan *Computer System* yang terpisah.

Dari definisi yang bermacan-macam tersebut bahwa pada dasarnya ada perumusan definisi mengenai kejahatan komputer secara luas yaitu, perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain; dan perumusan secara sempit yaitu perbuatan melawan hukum yang dilakukan dengan menggunakan teknologi komputer yang canggih.[17]

Berdasarkan beberapa pendapat diatas dapat ditarik suatu gambaran secara umum mengenai ciri-ciri dari kejahatan komputer:[18]

1). Merupakan kejahatan atau berkaitan dengan komputer dan/atau sistem komputer.

2). Merupakan kejahatan dengan modus operandi dengan cara memperdaya komputer.

3). Perbuatan itu dilakukan secara ilegal, tanpa hak atau tidak etis.

4). Perbuatan tersebut membuat komputer tidak dapat berfungsi secara benar.

5). Perbuatan tersebut mengakibatkan kerugian materiil amupun kerugian imateriil (waktu, nilai, jasa,pelayanan).

Para ahli berusaha membatasi perumusan kejahatan komputer sedemikian rupa agar tidak mengaburkan batas-batas dari kejahatan komputer itu sendiri. Sebab jika kurang hati-hati dalam merumuskan definisi kejahatan komputer, misalnya memberikan rumusan yang sedemikian luasnya agar mampu mencakup seluruh permasalahan kejahatan komputer yang cukup kompleks tanpa memberikan batasan-batasan yang pasti, maka hal itu justru akan mengaburkan pengertian dari kejahatan komputer .

Seandainya kejahatan komputer diartikan sebagai kejahatan yang menyangkut komputer dan peralatan-peralatan yang berhubungan dengan sarana-sarana penunjangnya,

---

[16] Eddy Djunaidi Karnasudirja, *Yurisprudensi Kejahatan Komputer*, (Jakarta : CV. Tanjung Agung, 1993), hal 3

[17] A.L Wisnubroto, *Kebijakan HukumPidana dalam Penanggulangan Penyalahgunaan Komputer*, (Yogyakarta: Penerbitan Universitas Atma Jaya, 2001), hal 4

[18] *Ibid.*

maka sebenarnya tidak semua kejahatan yang biasanya disebut kejahatan komputer merupakan kejahatan komputer. Sebagai ilustrasi ketika seseorang mencuri *harddisk* yang kosong (tidak memuat data atau program) dan bermaksud untuk dimilikinya sendiri atau dijual ke orang lain, maka perbuatan orang tersebut belumdapat digolongkan sebagai kejahatan komputer. Perbuatan tersebut lebih tepat disebut sebagai pencurian biasa seperti yang diatur dalam pasal 362 KUHP. Berbeda ketika seseorang tersebut mencuri *harddisk* itu dengan mengetahui atau setidak-tidaknya menduga bahwa di dalam *harddisk* tersebut terdapat program atau data komputer dan orang tersebut bermaksud memiliki atau menjual kepada orang lain data atau program yang terdapat dalam *disk* tersebut (jadi bukan *harddisk* itu sendiri) atau punya maksud lain misalnya untukbalas dendam atau memperoleh imbalan yang tidak wajar dengan menyandera benda-benda vital tersebut agar suatu pusat komputer tidak dapat menjalankan operasinya, maka perbuatan ini baru bisa disebut sebagai kejahatan komputer.[19]

Berikut beberapa klasifikasi atau kategorisasi mengenai kejahatan komputer dari berbagai pendapat. Jongerius membagi kejahatan komputer dalam kategori sebagai berikut:[20]

1). Manipulasi komputer;

2). Spionase komputer;

3). Sabotase komputer dengan (dengan merusak atau menghancurkan peralatan dan atau sistem jaringan komputer);

4). *Unauthorized Use* (pemakaian secara tidak sah) *Computer*;

5). *Unauthorized Access* (memasuki secara tidak sah sistem komputer.

Dalam suatu studi dari kongres Amerika Serikat terdapat empat kategori kejahatan komputer yaitu :

1) Pemasukan data yang tidak benar (*fraudulent*) kedalam komputer;

2) Pemakaian fasilitas-fasilitas yang berhubungan dengan komputer;

3) Merubah atau merusak informasi atau arsip;

---

[19] A.L Wisnubroto, *.op.cit*, hal 25 dengan modifikasi kasus oleh penulis.

[20] Andi Hamzah, *Aspek-aspek Pidana di Bidang Komputer*, (Jakarta: Sinar Grafika, 1990), hal 23-24

4) Pencurian apakah secara elektronis atau dengan cara-cara lain terhadap uang, fasilitas-fasilitas, dan data yang berharga.

Selanjutnya ada klasifikasi lain yang meletakkan sebagaian besar dari kejahatan komputer ke dalam empat kategori:

1). Sabotase dan vandalisme sistem komputer;

2). Penggunaan fasilitas-fasilitas komputer tanpa wewenang sebagai pencurian;

3). Kejahatan terhadap barang (pencurian melalui penggunaan komputer); dan

4) Kejahatan terhadap data (pencurian informasi)

Dalam ensiklopedia tentang kejahatan dan keadilan (*The Encyclopedia of Crime and Justice*) dikemukakan mengenai kategorisasi kejahatan komputer sebagai berikut :

> *It has two main categories. In the first, the computer is a tool of a crime, such as fraud, emblezzement, and theft of property, or is used to plan manage a crime. In a second, the computer is a object of a crime, such as sabotage, theft or alteration of storage data, or theft of it services.*[21]

Andi Hamzah mengklasifikasikan kejahatan komputer berdasarkan tugas-tugas yang dibebankan dengan sifat kecuragan di bidang komputer, yaitu:[22]

1). Kejahatan terhadap sistem komputer:

a. Pada masukan (*input*), dengan penghapusan, penambahan bahan-bahan masukan;
b. Pada pengolahan data, dengan perubahan, pengerusakan;
c. Pada program komputer, dengan pencurian dan penjualan program, pengerusakan program, memasukkan instruksi yang bersifat curang; dan
d. Pada keluaran (*output*), dengan pemalsuan.

2). Kejahatan terhadap peralatan komputer

[21] *The Encyclopedia of Crime and Justice, edition 2*,edited by Joshua Dressler, October 2001, Macmillian Reference.
[22] Andi Hamzah,. *Op. Cit.*

Perbuatan yang dapat dimasukkan disini misalnya, kecurangan pada dana pembelian peralatan komputer, disamping kecurangan yang dilakukan dengan merusak peralatan komputer (*hardware*) dengan tujuan penghancurkan prestasi dan reputasi pihak lawan.

Dari beberapa pandangan mengenai klasifikasi kejahatan komputer yang telah diuraikan diatas, dapat ditarik kesimpulan bahwa ternyata kejahatan komputer dapat dilihat dari banyak segi. Ternyata antara klasifikasi satu dengan yang lain terdapat kesamaan dalam beberapa hal, oleh karena itu untuk memudahkan klasifikasi kejahatan komputer maka beberapa klasifikasi diatas dapat dirangkum sebagai berikut :

1). Kejahatan-kejahatan yang menyangkut data atau informasi komputer;

2). Kejahatan-kejahatan yang menyangkut program atau *software* komputer;

3). Pemakaian fasilitas-fasilitas komputer tanpa wewenang untuk kepetingan-kepentingan yang tidak sesuai dengan tujuan pengelolaan atau operasinya;

4). Tindakan-tindakan menggangu operasi komputer; dan

5). Tindakan-tindakan merusak peralatan komputer atau peralatan-peralatan yang berhubungan dega komputer atau sarana-sarana peunjangnya.

Tampak bahwa klasifikasi atau kategorisasi kehajatan komputer cenderung bersifat luas, sehingga dalam *The International Handbook on Computer Crime* yang diproduksi pada tahun 1986 menganjurkan untuk membuat kategorisasi kejahatan komputer sebagai berikut:[23]

1). Computer-related Economic Crime.

a. *Fraud by computer manipulation.*
b. *Computer espionage and software piracy.*
c. *Computer sabotage.*
d. *Theft of service.*
e. *Unauthorized access to DP system and hacking.*

[23] The Hon.. Adrian Roden Q.C., *Computer Crime and The Law*, dalam Criminal Law Journal, 1991, hal 339.

f. *The computer is a tool for traditional business offences.*

2). Computer-related Infringements of Privacy

g. *Use of incorrect data.*

h. *Illegal collection and storage of correct data.*

i. *Illegal disclosure and misuse of data.*

j. *Infringements of formalities of privacy laws.*

3). *Further Abuses*

a. *Offences against state and political interest.*

b. *The extension to offences against personal integrity.*

Dari klasifikasi atau kategorisasi tersebut tampak bahwa sebagian besar dari kejahatan komputer sebenarya merupakan perbuatan kejahatan biasa dengan melibatkan peranan komputer, baik sebagai sarana atau alat maupun sebagai objek, misalnya pencurian dengan komputer, sabotase terhadap komputer. Hanya sebagia kecil dari perbuatan itu yang benar-benar bersifat khas sebagai kejahatan komputer, misalnya *hacking*.

2.2.2.Pengertian Cybercrime

Belum terdapat definisi final mengenai *cybercrime*. *Convention on Cybercrime* tidak menganggap terminologi "*cybercrime*" sebagai kata yang urgen untuk didefinisikan. Hanya ada 4 kata yang didefinisikan dalam konvensi tersebut, yaitu "computer system", "computer data", "service provider" dan "traffic data"[24]

Namun jika dilihat dari asal katanya , *cybercrime* secara harafiah berasal dari kata *cyber* dan *crime*. *Cyber* berasal dari kata *cybernetics* yang di dalam *Encyclopedia of Knowledge*, sebagaimana yang dikutip oleh Edmon Makarim[25] adalah :

"…is a term formerly used to describe an interdisciplinary approach to the study ofcontrol and communication in animals, humans, machines and orgaizations. The Word…"

[24] Convention on Cybercrime Article 1
[25] Makarim,.*op. cit*, hal 6

Sedangkan crime memiliki arti kejahatan. Secara sederhana definisi kejahatan adalah suatu tindakan yang anti sosial. J.M. Bemmelen memandang kejahatan sebagai suatu tindakan yang menimbulkan kerugian, ketidakpatutan dalam masyarakat, sehingga dalam masyarakat terdapat kegelisahan, dan untuk menentramkan masyarakat. Karena itu negara harus menjatuhkan hukuman terhadap si pelaku.

Sementara berdasarkan Edwin H Sutherland dalam bukunya 'Principle of Criminology,' menyebutkan terdapat beberapa unsur kejahatan yang saling bergantung dan saling mempengaruhi. Di antaranya, pertama, terdapat akibat-akibat tertentu yang nyata atau kerugian, dan kedua, kerugian tersebut melanggar undang-undang yang berlaku dan ketiga, dilakukan secara sengaja.[26] Sedangkan definisi dari kejahatan secara internasional adalah :

> *…an "international crime" is an act that is defined as criminal under international law. In most instances, this will be done through international agreements, but customary international law also plays a role. Normally, an act will initially be defined as a crime by an international agreement and then, after the agreement has been ratified by a large number of states and generally accepted even by those states who do not become parties, the act may be regarded as a crime under customary international law. If an act is defined as an international crime under customary*.[27]

Berbagai pihak telah mencoba untuk memberikan definisi tentang *cybercrime*. Ada yang mendefinisikan bahwa *cybercrime* adalah suatu aktivitasbyang dilakukan dengan sebuah alat (*PC, laptop, notebook, handphone*) yang terhubung dengan jaringan internet dan aktivitas tersebut melanggar undang undang.[28]

---

[26] Muhammad Istijar, Korupsi Kejahatan Luar Biasa, www.hokionline, diakses pada 30 Juni 2009
[27] John F Murphy," *Civil Liability for the Commision of International Crimes as an Alternative to Criminal Prosecution"*, Harvard Human Rights Journal
[28] Sutanto, Hermawan Sulistyo, Tjuk Sugiarso,Ed.,*Cybercrime: Motif dan Penindakan*,Cet. 1, (Jakarta:Pensil-324,2005), hal 20.

Sedangkan menurut Goodman & Brenner[29], istilah "*cybercrime*", "*computer crime*", dan "*high-tech-crime*" seringkali digunakan secara bergantian untuk merujuk kepada 2 kategori, dimana suatu perbuatan telah dianggap melawan hukum. Dua kategori itu adalah, pertama, komputer merupakan target bagi perbuatan pelaku. Dalam hal ini pelaku bisa melakukan akses secara illegal, penyerangan kepada jaringan (pembobolan) dan lain lain yang terkait dengan sistem pengamanan jaringan (*networking*). Kategori kedua adalah bahwa perbuatan tersebut mengandung maksud dan tujuan seperti layaknya kejahatan konvensional, misal pencurian, pemalsuan.

Lastwoka dan Hunter mendefinisikan *cybercrime* sama degan apa yang biasanya disebut sebagai *viritual crime* (kejahatan maya), yaitu suatu kejahatan yang dilakukan terhadap komputer atau dengan alat bantu komputer.[30]

Sebuah komite yang dibentuk oleh Parlemen Australia (*Parlimentary Joint Commite on The Australian Crime Commision*) dalam laporannya yang dirilis pada tahun 2004 menyatakan bahwa tidak (belum) ada perundang-undangan yang secara tegas mendfinisikan *cybercrime*.[31] Sinyalmen ini barangkali bisa dibenarkan, karena di dalam *Convention on Cybercrime* memang tidak memberikan definisi khusus mengenai *cybercrime*.

Oleh karena itu, komite tersebut menampung beberapa masukan untuk mencari gambaran yang lebih tepat mengenai *cybercrime*. Beberapa masukan yang berhasil dijaring antara lain menyebutkan:

A term that encompasses a variety of offence associated with the use of technology. The use of the term Cybercrime is synonymous with the term electronic crime (e-crime). [definisi oleh Attorney General's Departement]

---

[29] Marc D. Goodman dan Susan W. Brenner, *The Emerging Consensus On Criminal Conduct in Cyberspace*, hal 10. Diakses melalui situs <http://www.lawtechjournal.com/articles/2002/03_020625_goodmanberner.php>, pada tanggal 1 April 2009.

[30] F.Gregory Lastwoka dan Dan Hunter, *Virtual Crime*, didownload dari situs <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=564801>, pada tanggal 5 Maret 2009.

[31] Parliament of the Commonwealth of Australia, *Parlimentary Joint Commite On The Australian Crime Commission*,diakses melalui <http://www.aph.gov.au/senate_acc> , diakses pada 10 Maret 2009.

A cybercrime is any crime effected or progressed using a public or private telecommunication service. [definisi oleh Australian Bankers Association]

[E-Crime includes] offences where a computer is used as tool in the commission of an offence, as the target of an offence, or used as a storage device in the commission of an offence. [definisi oleh Australian Crime Commission]

Selain itu ada juga survey mengenai *cybercrime* oleh Goodman dan Brenner.[32] Survey ini menujukkan bahwa di negara-negara yang relatif maju teknologi informasinya *cybercrime* dapat dibedakan ke dalam delapan kategori, yaitu :

a. Akses secara tidak sah;

b. Merubah dan memanipulasi data pada komputer secara tidak sah;

c. Sabotase terhadap komputer;

d. Pemanfaatan sistem informasi secara melawan hukum;

e. Penipuan dengan komputer (*computer fraud*);

f. Spionase (industrial, keamanan dan lain lain); dan

g. Pelanggaran privasi.

Meskipun gambaran mengenai *cybercrime* cukup beragam, namun pada dasarnya terdapat karakteristik tertentu yang dapat digunakan untuk mengenali *cybercrime*. Menurut Freddy Harris[33], pada umumnya *cybercrime* memiliki ciri-ciri sebagai berikut :

a. *non-violence* (tanpa kekerasan)

b. sedikit melibatkan kontak fisik (*minimum of physical contact*)

c. menggunakan peralatan dan teknologi;

d. Memanfaatkan jaringan telematika global

Berdasarkan ciri-ciri tersebut, terutama cirri yang terakhir, menunjukkan bahwa *cybercrime* dapat terjadi denga mengaitkan beberapa wilayah hukum atau beberapa negara sekaligus. Hal ini sesuai dengan rekomendasi yang dikeluarkan oleh negara-negara G-8 yang menyatakan bahwa *high-tech* dan *computer-related crimes* termasuk ke dalam

[32] Goodman and Brenner, *.op. cit.*, hal 79

[33] Dikdik M.Arief Mansur dan Elisatris Gultom, *Cyber Law-Aspek Hukum Teknologi Informasi*, Cet.1 (Bandung: PT Refika Aditama,2005), hal 27

transnational crime.[34] Masuknya *cybercrime* kedalam kategori *transnational crime* berarti bahwa *cybercrime* melibatkan lintas yurisdiksi.

Sedangkan situs wikipedia menyamakan *cybercrime* dengan *computer crime*, *high tech crime*, menurut situs tersebut *cybercrime* adalah aktivitas criminal dimana komputer atau jaringan (*network*) menjadi sumber, alat, target atau tempat dimana kejahatan tersebut dilakukan.[35]

2.3. Jenis-jenis Cybercrime

Seperti pengertian *cybercrime*, jenis-jenis *cybercrime* juga berbeda-beda, karena setiap ahli hukum memiliki pandangan yang berbeda-beda, selain itu juga belum ada kesepakatan yang seragam mengenai pengertian *cybercrime* membuat banyaknya perbedaan tersebut. Menurut *Convention on Cybercrime*, tindak pidana yang dapat digolongkan sebagai *cybercrime* diatur dalam pasal 2-5, adapun jenis tindak pidana tersebut adalah :

1. *Illegal Access*[36]

Illegal access melingkupi pelanggaran dasar dari ancaman-ancaman yang berbahaya dari serangan terhadap keamanan data dan sistem komputer.[37] Perlindungan terhadap pelanggaran *illegal access* ini merupakan gambaran dari kepentingan organisasi atau kelompok dan orang-orang yang ingin mengatur, menjalankan dan mengendalikan sistem mereka berjalan tanpa ada ganguan dan hambatan.

---

[34] G8 Recommendations on Transnational Crime, diaksess melalui internet dengan alamat <http://www.justice.gc.ca/en/news/g8/doc1.html#4d>, pada April 2009

[35] Cybercrime, <www.cybercrime.net>, diakses pada 1 Juli 2009.

[36] Diatur dalam pasal 2 *Convention on Cybercrime*, yang berbunyi :

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."

[37] Council of Europe, *Explanatory Report To The Convention on Cybercrime* (ETS No 185), poin ke 44.

Pasal ini merupakan ketentuan pertama yang mengatur mengenai masalah *cybercrime*. Sebagai contoh dari kejahatan ini adalah *hacking, cracking* atau *computer trespassing*.Gangguan jenis ini memberikan akses kepada pelaku terhadap data-data penting (termasuk *password* atau informasi sistem) dan rahasia-rahasia, yang mungkin digunakan untuk membeli barang dengan menggunakan informasi kartu kredit milik orang lain atau mendorong pelaku untuk melakukan bentuk pelanggaran berkenaan dengan komputer yang lebih berbahaya, seperti pemalsuan atau penipuan dengan komputer.[38]

Pemahaman mengenai *access* sebagaimana disebut dalam ketentuan pasal ini, terdiri dari memasuki seluruh atau sebagian dari suatu sistem komputer (*hardware*, bagian-bagian, data yang tersimpan pada sistem yang terpasang, direktori-direktori, lalu-lintas data-data dan data yang berkenaan dengan isi). Namun demikian aksesk yang dilakukan ini tidak termasuk didalamnya dengan kegiatan mengirimkan *email* atau *file* ke sistem tersebut. *Access* yang dimaksud meliputi kegiatan memasuki sistem komputer lainnya baik yang terkoneksi melalui jaringan komunikasi umum, tatu terhadap suatu sistem komputer pada jaringan yang sama seperti pada suatu *Local Area Network* (LAN) atau *intranet* dalam suatu organisasi. Cara komunikasi yang dilakukan baik dari satu lokasi tertentu dengan cara *remote* maupun dengan penghubung *wireless* pada jarak yang dekat tidak masalah.[39]

Ketentuan pasal ini juga menerangkan mengenai pentingnya permasalahan tanpa hak yang harus ada pada suatu pelanggaran yang dilakukan . Bukanlah suatu pelanggaran pidana terhadap akses yang disetujui oleh pemilik atau pemegang hak dari suatu sistem atau bagian dari pemilik atau pemegang hak tersebut.[40] Kondisi ini dapat terjadi apabila dibutuhkan pengujian terhadap keamanan suatu sistem.

---

[38] Mike Keyser, "The Council of Europe Convention on Cybercrime", (*Journal of Transnational Law and Policy*, volume 12, 2003), hal 300.
[39] Council of Europe, *.op cit.*, poin ke 46
[40] Council of Europe,*.op cit.*, poin ke 47

2. *Illegal Interception*[41]

Menyatakan tidak sah tindakan pencegatan atau menahan tanpa hak bentuk pemindahan data komputer yang dilakukan secara pribadi yang dilakukan melalui faximile, *email*, atau pemindahan *file*. Tujuan dari pasal ini adalah perlindungan atas hak atas kebebasan dalam komunikasi data. Pelanggaran ini hanya ditujukan terhadap pemindahan pribadi dari data komputer.

Pengertian *interception* secara teknis dijleaskan dalam *Explanatory Report To The Convention on Cybercrime* yaitu,

"*Interception by techincal means relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or undirectly through the use of electronic eavesdropping or taping devices.Interception may also involving recording."*[42]

Salah satu bagian dari pelanggaran yang dimaksud dari ketentuan pasal ini adalah melakukan penahanan komunikasi atau menghambat proses komunikasi dengan menggunakan perangkat elektronik untuk mendengarkan pembicaraan orang lain atau menggunakan peralatan untuk menyadap komunikasi. Klasifikasi ini hanya berlaku pada komunikasi data komputer yang dilakukan secara pribadi, klasifikasi ketentuan ini mengacu pada sifat pemindahan dan sifat dari data yang dipindahkan. Komunikasi yang terjadi dapat melalui hubungan dari komputer ke *printer*, antara dua komputer atau dari orang ke komputer itu sendiri (seperti mengetik dengan keyboard).[43]

---

[41] Diatur dalam pasal 3 *Cybercrime Convention*, yang berbunyi :

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system."

[42] Council of Europe,.*op cit.*, poin ke 53

[43] Keyser, .*loc cit*., hal 301.

3. *Data Interception*[44]

Ketentuan pengerusakan data menjadi tindak pidana bertujuan untuk memberikan perlindungan yang sama terhadap data komputer dan program komputer sebagaimana dengan benda-benda berwujud. Sebagai contoh adalah memasukan kode-kode jahat (*malicous codes*), *Viruses*, dan *Trojan Horse* ke suatu sistem komputer merupakan pelangagaran menurut ketentuan pasal ini.[45]

Berdasarkan Pasal 4 ayat 1 merupakan tindak pidana apabila dilakukan dengan terencana tindakan merusak, menghapus, memperburuk, mengubah atau mengembangkan suatu data komputer tanpa hak.[46] Ketentuan yang diatur dalam pasal ini berusaha untuk memberi jaminan bahwa data yang dikirimkan melaui jaringan internet atau pemindahan data yang dilakukan melaui suatu jaringan adalah sama dengan data yang dikirimkan oleh si pengirim. Kepentingan perlindungan hukum dalam pasal ini adalah keutuhan dan berfungsi sebagaimana mestinya penggunaan data komputer yang tersimpan atau program-program komputer.[47]

4.*System Interference* [48]

Dalam Pasal 5 konvensi ini disebutkan bahwa *system interference* ditetapkan sebagai pelanggaran pidana apabila *"... when committed intentionally, the serious hindering without right of the functioning of a computer system…"*, harus dilakukan dengan memasukkan, menyebarkan, merusak, menghapus atau menyembunyikan data komputer.[49]

---

[44] Diatur dalam pasal 4 *Cybercrime Convention* yang berbunyi :

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

[45] Keyser, .*loc cit*., hal 302

[46] The Convention on Cybercrime.23. November 2001.

[47] Council of Europe,.*op cit.*Poin ke 60

[48]Diatur dalam pasal 5 *Cybercrime Convention* berbunyi

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data."

[49] Council of Europe,.*op cit*, poin 66

Pengganguan terhadap sistem dijadikan sebagai tindak pidana bertujuan untuk mencegah *"…the serious hindering without right of the functioning of a computer system…"*[50]

Sebagai contoh adalah serangan *denial-of-service* yang dilakukan dengan teknik *hacking*, pembuatan kode jahat seperti virus. Contoh tersebut dapat memperlambat penggunaan sistem komputer yang mengakibatkan pengguna tidak dapat mengakses suatu *website*.

Menurut Dr Adam Graycar, Direktur Australian Institute of Crminology (AIC) yang termasuk ke dalam kategori *cybercrime* adalah:[51]

1). Theft of telecomminication services;

2). Communications in furtherance of criminal conspiracies;

3). Telecommunication piracy;

4). Disemination of offensive materials;

5). Electronic money laundering and tax evasion;

6). Electronic vandalism, terrorism and extortion;

7). Sales and investment fraud

8). Illegal interception of telecommunications;

9). Electronic funds transfer fraud.

Berdasarkan survey yang dilakukan oleh Ekaterina Drozova terhadap 50 Undang-Undang dari negara-negara di dunia sedikitnya 30 negara memiliki hukum yang berkenaan dengan *cybercrime* yang mengatur tentang:[52]

1). Unauthorized acess;

2). Illicit tampering with files or data;

3). Computer or network sabotage;

4). Use of information systems to commit or advance traditional crime;

5). Computer-mediated espionage;

---

[50] Keyser, *.loc cit*., hal 303

[51] "Cybercrime: Old Wine in New Bottles?", Makalah disampaikan di Centre for Crimnology, The University of Hongkong, tanggal 24 Februari 2000

[52] Johanna Granville, "The Transnational Dimension of Cybercrime and Terrorism", *British Journal of Criminology volume .43*, (2003), hal 452-453

6). Violation against privacy in the acquisition or use of personal data;

7). Theft or damage of computer hardware or software.

Menurut Global Internet Policy Initiative (GIPI), ada empat kategori dari pelanggaran yang dikategorikan sebagai *cybercrime*, yaitu:[53]

1). Data iterception;

2). Data interference;

3). System interference;

4). Illegal access.

Pembagian oleh GIPI ini sama dengan jenis-jenis *cybercrime* yang diatur di *Convention on Cybercrime*. Jenis-jenis *cybercrime* yang telah dipaparkan telah menjadi bentuk yang dikenal oleh masyarakat seiring dengan perkembangan teknologi informasi. Berdasarkan jenis-jenis *cybercrime* tersebut dapat dilakukan pembagian atas tiga kategori[54], yaitu

1). Cyberpiracy;

2). Cybertersspass;

3). Cybervandalism.

Dalam penelitian yang dilakukan oleh Capitol College menyimpulkan bahwa yang termasuk sebagai *cybercrime* adalah:[55]

1) .Unauthorized access by insiders (such as employees)

2). System penetration by outsiders (such as hackers)

3). Theft of proprietary information (

4). Financial fraud using computers

5). Sabotage of data or networks

6). Disruption of network traffic (e.g., denial of service attacks)

---

[53] Gobal Internet Policy Initiative, Trust and Security in Cyberspace :The Legal and Policy Framework for Adressing Cybercrime, 2005

[54]"Cybercrime and Cybercriminals", http://www3.interscience.wiley.com:8100/legacy/college/0471249661/presentation/ch07.ppt, diakses pada tanggal 10 April

[55] Cybercrime, <faculty.capitol-college.edu/~dward/MSIA%20711%20upload/MSIA711.02.ppt>, diakses pada tanggal 2 Mei 2009.

7). Creation and distribution of computer viruses

8). Software piracy

8). Identity theft

9). Hardware theft (e.g., laptop theft).

10). Terrorists that target critical infrastructures, such as the PSTN, power grid, and the air traffic control system.

Sedangkan menurut divisi *cybercrime* kepolisian Mumbai, India (sering disebut Mumbaicell) yang termasuk *cybercrime* adalah :[56]

1). Hacking;

2). D-Dos attack;

3). Virus dessemination;

4). Software piracy;

5). Pornography;

6). IRC crime;[57]

7). Credit card fraud;

8). Net extortion;

9). Phising[58];

10). Spoofing[59];

11). Cyber defamation[60];

12). Threatening;

13). Salami attack[61] ;

---

[56]Cybercrime Awareness, Mumbai Police Cybercrime Branch, www.cybercellmumbai.com/files/Types%20of%20cyber%20crime.pdf, pada tanggal 20 Mei 2009

[57] IRC (Internet Relay Chat) sebuah ruang chatting dapat dimanfaatkan untuk:
-Merencanakan suatu kejahatan
-Para Hacker menggunakannya untuk saling berbagi informasi
-Pedofill menggunakannya untuk menarik perhatian anak-anak

[58] *Phising* artinya mengambil data penting dari bank atau lembaga keuangan dengan cara membuat halaman yang mirip dengan web bank atau lembaga keuangan tersebut

[59] *Spoofing* artinya, menyamarkan identitas sebuah komputer seolah-olah itu adalah komputer lain, kejahatan ini biasanya dilakukan dalam satu network dan dilakukan oleh orang yang mempunyai akses khusus (adiministrator,webmaster)

[60] *Cyber Defamation*, menjelek-jelekan seseorang atau suatu badan di internet yang berujung pada fitnah (biasanya dilakukan oleh mantan karyawan yang dipecat tidak hormat, mantan pacar, atau mantan istri.suami)

Dari sekian banyak pengertian *cybercrime* yang diuraikan diatas, dapat ditarik gambaran secara umum bahwa yang termasuk ke dalam jenis-jenis *cybercrime* adalah :[62]

1). *Unauthorized Access to Computer System and Service*

Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (*hacker*) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukannya hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi.

2). *Illegal Contents*

Merupakan kejahatan dengan memasukkan data atau informasi ke Internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya, pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah dan sebagainya.

3). *Data Forgery*

Merupakan kejahatan dengan memalsukan data pada dokumen dokumen penting yang tersimpan sebagai *scripless document* melalui Internet. Kejahatan ini

---

[61] Korupsi jenis baru, yang dilakukan dengan cara memodifikasi suatu sistem yang menangani keuangan (contoh seorang nasabah bank menghack sistem bank dan memodifikasi sistem agar mentransfer sejumlah uang yang kecil jumlahnya dari rekening nasabah lain ke rekeningnya, jumlah uang yang kecil ini jika dijumlahkan akan menjadi besar)

[62] Petrus Reinhard Golose, *Perkembangan Cybercrime dan Penanganannya di Indonesia oleh POLRI*, makalah disampaikan pada seminar nasional mengenai "Penanganan *Cybercrime* di Indonesia ke Arah Pengembangan Kebijakan Menyeluruh dan Terpadu", tanggal 10 Agustus 2006

biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi "salah ketik", yang pada akhirnya akan menguntungkan pelaku karena korban akan memasukkan data pribadi dan nomor kartu kredit yang dapat saja disalah gunakan.

4). *Cyber Espionage*

Merupakan kejahatan yang memanfaatkan jaringan Internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data pentingnya (*data base*) tersimpan dalam suatu sistem yang *computerized* (tersambung dalam jaringan komputer).

5). *Cyber Sabotage and Extortion*

Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan Internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku.

6). *Offense against Intellectual Property*

Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di Internet. Sebagai contoh, peniruan tampilan pada *web page* suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di Internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.

7). *Infringements of Privacy*

Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara *computerized*, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

.

2.4.Sasaran Cybercrime

Susan W Brenner, *Professor of Law and Technology* dari *University of Dayton School of Law* mempunyai pendapat untuk menggambarkan bentuk-bentuk *cybercrime*. Brenner mengatakan bahwa terdapat berbagai pendekatan dalam merespon *cybercrime* antara lain ada yang menggunakan hukum pidana tradisional, ada yang memodifikasi hukum pidana tradisional dan ada pula yang membutuhkan perumusan suatu hukum pidana yang benar-benar baru.[63] Akan tetapi Brenner mengelompokkan kejahatan-kejahatan tersebut ke dalam kategori : *crimes against persons, crimes against property, crimes against state* dan *crimes against morality*.[64]

Menurut Brenner, empat kategori ini merupakan pembidangan yang lebih tepat untuk menggolongkan kejahatan-kejahatan yang dilakukan dengan cara-cara yang baru tersebut. Pembidangan tersebut adalah sebagai berikut :

2.4.1. *Crimes Against Persons* (kejahatan tehadap orang)

Kejahatan ini oleh Brenner dibedakan menjadi dua yaitu, kejahatan seksual dan non-seksual. Kejahatan seksual disini antara lai adalah pornografi. Barangkali pornografi mempunyai intrepretasi yang berbeda-beda di tiap negara, tetapi pornografi yang melibatkan anak dibawah umur (*child pornography)* pada dasarnya telah dikriminalisasi di hampir semua negara.

[63]G8 Reccomendation, *.op. cit.*, poin ke 14
[64] G8 Reccomendation, *.op. cit*, poin ke15

Sedangkan kejahatan non-seksual terhadap orang dapat terjadi melalui media *cyber*, antara lain berupa *homicide* (menimbulkan kematian bagi orang lain) dan *assault* (menyebabkan cedera atau celaka bagi orang lain). Contoh tersebut antara lain dapat diilustrasikan mengenai seorang hacker yang mampu membobol sistem computer sebuah rumah sakit, dan kemudian memanipulasi daftar obat-obatan berbahaya yang ada di *database* agar dikonsumsikan kepada pasien-pasien yang tidak mengkonsumsi obat-obat berbahaya tersebut. Dengan begitu akan semakin bertambah parah bahkan bisa berakibat tewasnya para pasien tersebut.[65]

2.4.2. *Crimes Against Property* (kejahatan terhadap hak milik)

Kejahatan terhadap hak milik seseorang merupakan kejahatan yang paling popular, bahkan merupakan kejahatan yang paling umum bila dilihat dari prespektif kejahatan konvensional sekalipun. Namun kali ini cara yang dilakukan oleh pelaku adalah dengan memanfaatkan teknologi internet.

Kejahatan terhadap hak milik ini ada beberapa jenis. Brenner memfokuskan tipe kejahatan ini kedalam 3 jenis yaitu *hacking* (pembobolan), *theft* (pencurian) dan *forgery* (pemalsuan)

2.4.3. *Crimes Against State* (kejahatan terhadap negara)

Menurut Brenner, kejahatan terhadap Negara pada dasarnya telah dikriminalisasi oleh berbagai peraturan perundang-undangan pidana yang ada disetiap negara. Bentuk-bentuk kejahatan semacam ini antara lain perbuatan yang secara langsung dapat menghancurkan kekuatan militer Negara (missal sabotase), diarahkan kepada infrastruktur Negara (missal sarana kesehatan, sarana komunikasi), dapat menggangu stabilitas sistem fiskal nasional (missal pemalsuan uang atau surat-surat berharga). Bahkan kejahatan terhadap agama juga dapat dikategorikan ke dalam kejahatan ini.

[65] G8 Reccomendation, *.op. cit*, poin ke 17

Kemajuan teknologi komputer, telah meningkatkan jumlah dokumen rahasia yang disimpan dalam format komputer. Dengan demikian, kejahatan terhadap negara semakin mudah dilakukan dengan adanya bantuan teknologi informasi sekarang.

2.4.3. *Crimes Against Morality* (kejahatan terhadap moral)

Brenner beranggapan bahwa teknologi computer telah memberikan peluang yang cukup besar bagi tindakan-tindakan yang dapat dianggap bertentangan dengan moralitas. Walaupun pada dasarnya kejahatan terhadap moral ini telah dikriminalisasi oleh undang-undang pidana tradisional, tetapi dengan fasilitas teknologi komputer, perbuatan a moral semakin mudah dilakukan.Oleh Brenner tindakan-tindakan a moral itu diberi contoh antara lain perjudian *on-line*, iklan dan perdagangan prostitusi, penyebarluasan materi-materi pornografi.

BAB 3
YURISDIKSI NEGARA DALAM MENANGANI KASUS *CYBERCRIME*

3.1.Penerapan Hukum di *Cyberspace*

Sebelum memasuki bahasan utama mengenai yurisdiksi, penulis merasa perlu diulas mengenai penerapan hukum di *cyberspace*. Di dalam penerapan hukum ini terdapat perdebatan yang alot antara ide kebebasan di dalam *cyberspace* dengan desakan perlunya pengaturan (hukum) di dalam *cyberspace*. Pertentangan kedua kubu ini menjadi cikal-bakal perdebatan mengenai penerapan yurisdiksi di *cyberspace*. Pertentangan kedua kubu ini menjadi cikal-bakal perdebatan mengenai penerapan yurisdiksi di cyberspace.

3.1.1.Kebebasan Kontra Pengaturan

Kemuculan teknologi komputer yang diikuti dengan lahirnya internet telah membawa sejumlah konsekuensi, salah satunya adalah berupa terbentuknya suatu komunitas atau kelompok sosial baru.[1] Sementara itu seiring dengan perkembangan teknologi komputer (internet) yang begitu pesat, jumlah komunitas tersebut semakin hari semakin bertambah. Akibatnya aktifitas yang terjadi di *cyberspace* yag melibatkan individu-individu yang biasa di sebut *Netizen*[2] pun semakin meningkat, baik itu aktifitas yang bersifat positif maupun aktifitas yang bersifat negatif

Berangkat dari fenomena ini, maka sejumlah kalangan menganggap perlu segera diadakannya pengaturan terhadap *cyberspace* beserta aktifitas-aktifitas yang terjadi disana. Dasar pemikirannya adalah hukum, sebagaimana kodratnya diperlukan di *cyberspace* agar aktifitas-aktifitas yang terjadi diatasnya dapat teratur dan terkontrol[3], sehingga tidak terjadi *radikalisme* di *cyberspace*.

---

[1] Gede Artha A.P, *op.cit*, hal 16

[2] Vivek Sood, *Cyber Law Simplified*, (New Delhi: Tata McGraw-Hill Publishing Co.Ltd, 2001), hal 38, kata netizen ini berasal dari gabungan antara kata internet dan citizen

[3] UNESCO, *The International Dimension of Cyberspace Law* (England: Ashgate Publishing Ltd., 2000), hal 19

Kekhawatiran tersebut memang cukup beralasan mengingat akan konsep kebebasan (free access) yang berlaku di *cyberspace*.[4]

Ide yang diuraikan diatas secara tegas ditentang oleh kalangan, umumya adalah aktivis *cyberspace* yang menjunjung tinggi konsep kebebasan di internet (*cyberspace*).[5] Mereka bahkan memandang *cyberspace* sebagai sesuatu yang berada di luar jangkauan negara, maka dari itu negara tidak dapat memberlakukan hukum di *cyberspace*.[6] Konsep kebebasan di *cyberspace* memungkinkan penggunanya dapat mengakses, menyimpan andakan, mengirim informasi atau aktifitas lainnya secara bebas di internet.[7] Pandangan ini berlawanan dengan pendapat sebelumnya yang menganggap *cyberspace* "hanyalah[8]" media biasa yang digunakan oleh manusia untuk berkomunikasi, berinteraksi dan berbisinis.[9]

3.1.2.Kondisi Empiris

Walaupun tidak ada kesepakatan yang secara jelas mengakhiri perseteruan antara dua pendapat diatas, namun kondidi empiris yang ada sekarang setidaknya telah menggambarkan kearah mana masyarakat hukum internasional berpihak. Sebagian besar cenderung menyetujui gagasan yang mengehendaki adanya pengaturan atau penerapan hukum terhadap *cyberspace* beserta aktifitas-aktifitas yang berlangsung disana. Keberpihakan ini antara lain ditandai dengan kemunculan sejumlah ketentuan hukum mengenai *cyberspace*, baik itu yang berlaku secara internasional maupun nasional. Ketentuan hukum mengenai *cyberspace* atau yang biasa disebut *cyberlaw* diterbitkan oleh sejumlah negara sebagai reaksi dan atisipasi terhadap ancaman keamanan yang muncul sebagai konsekuensi dari perkembangan teknologi yang beitu pesat.

Secara umum, negara-negara yang telah memiliki *cyberlaw* dapat diklasifikasikan menjadi dua, Kelompok pertama adalah negara-negara yang memutuskan untuk membuat *cyberlaw* khusus. Beberapa negara yang termasuk

---

[4] Juliet M, Oberding and Treje Norderhaug, *"A Separate Jurisdiction for Cyberspace"*, www.cyberjurisdiction.net , diakses pada 16 Mei 2009
[5] Vivek Sood, *op.cit*, hal 275
[66] UNESCO, *op.cit*, hal 219
[7] Vivek Sood, *op.cit*, hal 276
[8] Maksud dari pendapat ini adalah *cyberspace* dianggap sama dengan media penyampai informasi umum, seperti media cetak
[9] *Ibid.*

dalam kelompok ini antara lain Amerika Serikat (Computer Fraud and Abuse Act), Inggris (Theft/Forgery and Counterfeiting Act), dan Singapura (Computer Misuse Act).[10]

Sementara kelompok kedua adalah negara-negara yang hanya menyisipkan ketentuan mengenai *cyberspace* atau merevisi undang-undang pidana biasa yang ada. Belanda dan Prancis adalah contoh negara yang termasuk dalam kelompok negara kedua ini.[11] Keberpihakan ini semakin diperkuat dengan adanya sejumlah ketentuan yang dikeluarkan beberapa organisiasi internasional seperti PBB, Council of Europe, dan OECD (Organization for Economic Co-Operation Development).

3.2.Perdebatan Mengenai Konsep Yurisdiksi di Cyberspace

Salah satu masalah paling krusial yang diminculkan oleh *cybercrime* adalah masalah yurisdiksi yang berkaitan dengan sejauh mana suatu negara dapat menerapkan kedaulatan hukumnya atau dengan kata lain sejauh mana kemampuan suatu negara menyidangkan suatu perkara bernuansa internasional.

Permasalahan yurisdiksi di suatu negara dapat menerapkan kedaulatan hukumnya atau dengan kata lain sejauh mana kemampuan suatu negara menyidangkan suatu perkara bernuansa internasional.

Permasalahan yurisdiksi di *cybercrime* ini selajutnya memunculkan perbedaan pendapat antara dua kubu, perdebatan tersebut pada pertanyaan mengenai bagaimana seharusnya *cyberspace* diatur termasuk juga konsep yurisdiksi yang seharusnya berlaku di *cyberspace*. Kubu pertama menganggap bahwa *cyberspace* cukup diatur dengan hukum serta konsep yang selama ini ada dan digunakan dalam dunia nyata (kubu ini selannjutnya disebut dengan konsep analogi). Sementara kubu kedua mempunyai pandangan bahwa *cyberspace* itu dunia yang khas, unutuk itu perlu ada hukum serta konsep tersendiri yang diberlakukan di *cyberspace*. Pandangan ini mencoba memisahkan *cyberspace* dengan dunia nyata (kubu ini selajutnya disebut dengan konsep pemisahan).

---

[10] A.L Wisnubroto, *Kebijakan Hukum Pidana Dalam Penyalahgunaan Komputer*, cet.1, (Yogyakarta: Penerbit Univ. Atmajaya, 1999), hal 26

[11] *.Ibid*

Ditengah perdebatan yang alot mengenai hal ini, David R. Johnson mencoba menawarkan empat model yang patut dipertimbangkan sebagai solusi, keempat model tersebut antara lain:[12]

a. Pelakasanaan kontrol dilakukan oleh badan-badan peraadilan yang saat ini ada;

b. Mengadakan kesepakatan internasional mengenai pengaturan *cybespace*;

c. Membentuk organisasi internasional yang khusus mengatur *cyberspace*;

d. Pegaturan sendiri oleh pengguna internet (*self-governance*).

Salah satu tawaran dari Johnson yang cukup menarik adalah ide pembentukan organisasi internasional yang khusus mengatur segala aspek tetang *cyberspace*. Gagasan ini bisa jadi adalah solusi terbaik bagi masalah ”ketidakjelasan” pengaturan di *cyberspace*. Berkaitan dengan gagasan tersebut, UNESCO dalam terbitannya berjudul *“The International Dimensions of Cyberspace Law”* berpendapat bahwa tidak dapat dipungkiri bahwa keberadaan sebuah organisasi internasional akan mempunyai peran yang penting dalam perkembangan *cyberspace*[13]. Alasan yang mendasari gagasan ini adalah bahwa dengan adanya organisasi internasional ini semua negara dapat menyesuaikan atau menyeragamkan peraturan mengenai segala sesuatu yang berkaitan dengan *cyberspace*. Namun UNESCO dalam hal ini mengingatkan bahwa pembentukan organisasi internasional baru juga memiliki permasalahan-permasalahan yang harus dijawab. Beberapa permasalahan yang dimaksud antara lain berkaitan dengan dasar kewenangan, jaminan obyektifitas, jaminan perlindungan terhadap golongan minoritas, dan sebagainya.[14]

Terlepas dari permasalahan yang disebutkan diatas, penulis secara pribadi setuju dengan pendapat UNESCO, pembentukan organisasi internasional merupakan sesuatu yang paling memungkinkan, dengan begitu setidaknya ada otoritas tunggal yang mengatur segala aspek di *cyberspace*. Selain itu menurut

---

[12] David R. Johnson and David G. Post, *“And How Should The Internet Be Governed?”*, www.itworld.com, diakses tanggal 13 Mei 2009

[13] UNESCO, *op.cit*, hal 42

[14] *Ibid.*

hemat penulis organisasi ini dapat dijadikan sebuah *platform* menuju sebuah penyeragaraman peraturan di *cyberspace*, namun keberadaan organisasi ini hanyalah bersifat sementara dan dapat dibubarkan jika semua negara telah mengikuti pedoman-pedoman yang dihasilkan oleh orgainsiasi ini.Lebih jauh lagi, organisasi ini dapat diberikan kewenangan dalam bidang-bidang tertentu, misalnya dalam proses penyidikan hingga peradilan. Tentu saja gagasan ini masih perlu dikembangkan dengan penelitian khusus yang mendalam dan komprehensif.

3.2.1.Konsep Berdasarkan Analogi

Konsep ini pada intinya ingin menekankan bahwa sebenarnya *cyberspace* hanyalah merupakan bentuk elektronik dari ruang biasa yang kita kenal selama ini.[15] Dengan kata lain golongan ini berpandangan bahwa *cyberspace* adalah dunia biasa sebagaimana halnya dengan dunia nyata, karena analogi ini maka di *cyberspace* dapat diterapkan aturan atau konsep yurisdiksi yang selama ini berkembang dalam hukum internasional, terutama dalam hal penanganan tindak pidana

Menurut hukum internasional yang selama ini berlaku, suatu negara memiliki batasan-batasan tertentu dalam hal penerapan yurisdiksi terhadap kasus yang melibatkan kepentingan negara lain.[16] Salah satu batasan yang dimaksud misalnya saja berupa kewajiban setiap negara untuk berhati-hati dan sedapat mungkin menghnidari munculnya gangguan terhadap negara lain dalam upaya penerapan yurisdiksinya. Meskipun begitu, pada prakteknya hukum internasional tidak dapat memaksakan suatu negara untuk menerapkan suatu konsep yurisdiksi tertentu, bahkan dalam konteks ini setiap negara cenderung diberikan kebebasan dalam menentukan konsep mana yang akan digunakan. Kebebasan tentu saja akan diberikan sepajang tidak mengancam ketertiban internasional.[17] Secara umum yurisdiksi dibedakan menjadi tiga jenis, yaitu:[18]

---

[15] Rene L. Pattiradjawane, *"Cyberlaw: Apakah bisa Melindungi Pribadi Pengguna Iternet?"*, 2000, www.kompas.com, diakses tanggal 23 Mei 2009

[16] Stephen Wilske and Teresa Schiller, *"International Jurisdiction in Cyberspace: Which States May Regulate The Internet,"*www.cyberjurisdiction.net , diakses tanggal 23 Mei 2009

[17] *Ibid.*

[18] *Ibid.*

1) Yurisdiksi legislatif (*Jurisdiction to prescribe*)

Secara umum yurisdiksi legislatif merupaka kemampuan suatu negara untuk menerapkan hukum nasionalnya terhadap individu dan peristiwa tertentu.[19] Kemampuan ini pada prinsipnya dapat terwujud selama peristiwa yang dimaksud terjadi di wilayahnya atau peristiwa tersebut dilakukan oleh warganegaranya yang berada diluar batas wilayah negara tersebut. Selain itu jenis yurisdksi ini juga dapat dikatakan sebagai titik tolak dalam menetukan penerapan jenis yurisdiksi yang yang lainnya. Artinya untuk menerapkan yurisdiksi yudikatif, maka harus diawali dengan menganalisa yurisdiksi legislatif terlebih dahulu, namun ini tidak perlu dilakukan jika pihak yang bertindak sebagai negara forum berkenan mempergunakan hukum asing. Persyaratan yang sama berlaku juga bila ingin menerapkan yurisdiksi eksekutif.

Dalam menentukan yurisdiksi legislatif , maka terhadap seseorang maupun suatu peristiwa, terdapat 6 (enam) prinsip lain yang dapat dijadikan acuan. Prinsip-prinsip tersebut antara lain :[20]

1. Subjective territoriality (territorial subjektif)
2. Objective territoriality (territorial objektif)
3. Nationality (nasionalitas aktif)
4. Passive Nationality (nasionalitas pasif)
5. Protective Principle (prinsip perlindungan)
6. Universality (universalitas)

2) Yurisdiksi yudikatif (*Jurisdiction to adjudicate*)

Yurisdiksi yudikatif merupakan kewenangan suatu negara untuk melakukan proses peradilan terhadap individu atau peristiwa yang mempunyai hubungan yang cukup dengan negara tersebut.[21] Sebagaimana yang disebutkan sebelumnya, penerapan yurisdiksi yudikatif hampir selalu dengan penerapan yurisdiksi legislatif. Hal ini sangat masuk akal mengingat hampir tidak ada pengadilan yang rela memakai hukum pidana negara lain.[22] Dalam kasus

[19] *Ibid.*
[20] *Ibid.*
[21] *Ibid.*
[22] *Ibid.*

kejahatan internasional, penerapan yurisdiksi yudikatif secara normative sangat bergantung pada dimana pelaku kejahatan tersebut berada.

2) Yurisdksi eksekutif (*Jurisdiction to enforce*)

Yurisdiksi eksekutif mempunyai makna sebagai kewenangan negara untuk meningkatkan kepatuhan terhadap hukum dan kewenangan negara untuk menjatuhkan hukuman bagi yang melanggar hukum. Jenis yurisdiksi ini memiliki kaitan erat dengan yurisdiksi legislatif, maksudnya suatu negara tidak dapat menegakkan hukum nasionalnya begitu saja kecuali negara tesebut memiliki yuirsdiksi legislatif atas seseorang atau suatu peristiwa.

Yurisdiksi legislatif terkadang juga menjadi dasar pembenar bagi suatu negara untuk mengambil langkah-langkah yang dianggap perlu dalam rangka penerapan yurisdiksi eksekusinya diwilayah negara lain dengan syarat ada persetujuan dari negara tersebut. Persetujuan yang dimaksud disini adalah persetujuan yang diberuikan oleh pejabat resmi dari negara yang bersangkutan dan langkah-langkah yang dapat diambil antara lain : penahanan, pengiriman surat, pelayanan dokumen, dan penyelidikan.[23]

Sehubungan dengan belum adanya titik temu antara dua kubu yang saling berseteru mengenai konsep yurisdiksi yang akan digunakan terhadap *cyberspace*, khususnya mengenai *cybercrime*. Maka dengan kondisi tersebut, praktis konsep tradisional seperti yang disebutkan diatas yang selama ini berlaku dalam menentukan yurisdiksi terhadap kasus-kasus kejahatan komputer yang bernuansa internasional. Setidaknya konsep yang tercantum dalam peraturan nasional khusus tentang kejahatan komputer di beberapa negara, yang merupakan dasar hukum yang selama ini digunakan sebelum adanya ketentuan yang bersifat internasional.

3.2.2.Konsep Berdasarkan Pemisahan

Konsep ini diperjuangkan oleh kubu yang sebagian besar terdiri dari para akitvis *cyberspace* atau sekumpulan orang yang sehari-harinya memiliki kegiatan yang tidak lepas dari komputer (internet), beberapa diantaranya adalah *hacker*. Dengan melihat komposisi golongan yang mendukung konsep ini, maka dapat

[23] *Ibid.*

dimaklumi kiranya jika mereka secara terang-terangan menolak segala upaya untuk menyamaratakan *cyberspace* dengan dunia biasa atau dengan kata lain mereka merasa dunia mereka terusik dengan keberadaan konsep analogi.

Pemikiran yang menjiwai konsep ini pada dasarnya berangkat dari beberapa teori yag mereka yakini sebagai kekhasan dari *cyberspace* itu sendiri, seperti :[24]

a. Bahwa *cyberspace* adalah media yang terletak tidak di suatu lokasi tertentu.

b. Aktifitas di *cyberspace* tidak ada kaitannya suatu lokasi.

c. *Cyberspace* merupakan sesuatu yang jelas berbeda dengan dunia nyata.

Berangkat dari butir-butir diatas kalangan yang menawarkan konsep pemisahan berpendapat bahwa tidak satu pun organisasi atau negara yang pantas mengatur aktifitas di *cyberspace*. Lebih jauh lagi mereka berpandangan bahwa yang berhak mengatur *cyberspace* hanyalah pengguna *cyberspace* itu sendiri.[25] Argumen tersebut muncul berdasarkan dua asumsi sebagai berikut:[26]

1. Menurut mereka keberadaan *cyberspace* tidak secara serta-merta menyakiti seseorang di wilayah tertentu.

2. Segala upaya untuk mengontrol aktifitas *cyberspace* akan menjadi sia-sia, karenadegan mudah aktifitas tersebut akan berpindah-pindah dari suatu wilayah ke wilayah yang lain.

Pandangan ini mendapat kritikan dari beberapa kalangan, misalnya yang dikemukakan oleh Lawrence Lessig. Beliau berpendapat bahwa alasan-alasan yang dikemukakan oleh penganut konsep pemisahan lebih merupakan alasan dari prespektif normative serta emosional belaka, bukanlah suatu alasan yag bersifat

---

[24] Dan L. Burk, "*Jurisdiction in a World Without Border*," www.cyberjurisdiction.net , diakses tanggal 5 Mei 2009

[25] *Ibid.*

[26] *Ibid.*

analitis.[27] Contohnya pandangan mereka yang menganggap bahwa *cyberspace* beserta aktifitasnya harus dipisahkan dari dunia nyata.

Jika pandangan ini diasumsikan benar maka orang yang berhubungan di *cyberspace* adalah bukan orang sungguhan, bahkan benda pun adalah benda fiktif. Hal ini jelas seuatu yag masuk akal menurut Lessig karena menurut beliau orang adalah tetap orang baik sebelum atau sesudah ia menjauh dari komputer.[28] Secara eksterem Lessig selanjutnya menyatakan bahwa *cyberspace* bukanlah suatu "wilayah aman diluar bumi" (*extra terrestrial safety zone*), para penjahat komputer tidaklah aman dari tuntutan pengadilan.[29]

Kritikan lain datang dari Misaki Hamano yang menyatakan bahwa ide pemisahan *cyberspace* dengan dunia nyata dan ide *self-governance* terhadap *cyberspace*, bukan sesuatu yang realistis saat ini. Karena sekalipun kejahatan di *cyberspace* terus menigkat, namun negara-negara cenderung memilih menggunakan konsep lama dibandingkan membuat ketentuan yang baru. Selanjutnya Masaki menambahkan bahwa memang benar jika dikatakan bahwa ada keterbatasan negara untuk mengatasi problem yurisdiksi di *cyberspace*, akan tetapi bukan berarti pengguna *cyberspace* bebas dari hukum di dunia nyata.[30]

Salah satu gagasan yang ditawarkan oleh kubu ini adalah dengan menempatkan *cyberspace* sebagai **The 4th International Space** disamping zona Antartika, ruang angkasa (*outer space*), dan zona laut.[31] Degan menempatkan *cyberspace* setara dengan zona-zona khusus lainnya, maka bagi *cyberspace* perlu juga diadakan pengaturan khusus yang didalamnya termasuk juga konsep yurisdiksi khusus yang berlaku di khusus yang berlaku di *cyberspace*. Berkaitan dengan gagasan ini UNESCO dalam terbitannya yang berjudul "The International Dimensions of Cyberspace Law" berpendapat bahwa *cyberspace* dapat mengambil pengalaman yang berharga dari praktek pengaturan di ruang angkasa (outer space), dimana banyak kalangan yang menganggap bahwa pengaturan di

---

[27] Barda Nawawi Arief, "*Kebijakan Kriminalisasi dan Masalah Yurisdiksi Tidak Pidana Maya Antara*." Makalah pada seminar nasional dalam rangka penyusunan RUU teknologi informasi, hal 12

[28] *Ibid.*

[29] *Ibid.*

[30] Masaki Hamano, "*Comparative Study I The Approach to Jurisdiction in Cyberspace*", www.cyberjurisdiction.net, diakses tanggal 13 Mei 2009

[31] UNESCO, *op.cit*, hal 38

ruang angkasa terbilang berhasil, khususnya dalam hal menertibkan upaya pengeksplorasian di zona tersebut.[32]

3.3.Yurisdiksi Berdasarkan Hukum Internasional

Begitu banyak pendapat-pendapat tentang yurisdiksi yang berkembang dan dilontarkan oleh berbagai ahli, namun sedikit sekali yang akhirnya diterima oleh hukum internasional sebagai prinsip. Prinsip-prinsip tersebut adalah :

3.3.1. Subjective Territoriality (territorialitas subjektif)

Subjective territoriality adalah prinsip yang terpenting di dalam hukum internasional.[33] Menurut prinsip ini, keberlakuan hukum ditentukan berdasarkan tempat perbuatan dilakukan dan penyelesaian tindak pidananya dilakukan di negara lain. Mayoritas negara-negara di dunia, mengadopsi prinsip ini ke dalam perundang-undangan pidananya.[34]

Namun demikian J.G Starke, sebenarnya asas ini bukan merupakan asas umum hukum internasional, tetapi penggunaannya yang khusus sudah menjadi bagian hukum internasional, sebagai akibat dari dua konvensi yang penting yaitu *Geneva Convention for Supression of Counterfeiting Currency* (1929) dan *Geneva Convention of the Illicit Drug Traffic* (1930).[35]

3.3.2.Objective Territoriality (territorialitas objektif)

Objective Territoriality digunakan pada saat suatu tindakan dilakukan oleh pelaku yang berada di luar wilayah suatu negara, akan tetapi justru akibat paling serius yang timbul karena peristiwa itu berada di dalam wilayah negara yang dimaksud.[36] Asas ini dirumuskan oleh Prof. Hyde, sebagaimana dikutip oleh J.G Starke[37], sebagai berikut :

---

[32] *Ibid.*, hal 143
[33] Derrel Menthe, *Jurisdiction in Cyberspace : A Theory of International Spaces*, didownload melalui www.mttlr.org/volfour/menthe_art.html , pada tanggal 20 April 2009
[34] *Ibid.*
[35] J.G Starke, *Introduction to International Law*, 9th ed, (London: Butterworths), hal 184
[36] Darrel Menthe, *op.cit*, nomor 8
[37] J.G Starke ,*op.cit*, hal 187

> "*Menggerakkan suatu kekuatan diluar wilayah suatu negara, kekuatan tersebut menimbulkan akibat yang berbahaya, maka hal ini membenarkan yang berdaulat dalam wilayah itu untuk menuntutunya jika si pelaku memasuki wilayahnya*."

Sebagai contoh, misalnya orang yang sedang berada di perbatasan suatu negara kemudian menembak seseorang yang berada di wilayan negara lain.

3.3.3.Nationality (nasionalitas aktif)

Nationality adalah prinsip yang didasarkan kepada status kewarganegaraan seseorang.[38]Prinsip ini oleh Starke disebut juga prinsip nasionalitas aktif[39], yaitu negara tidak wajib menyerahkan warganegaranya yang melakukan pelanggaran di luar negeri. Artinya, negara dianggap lebih berwenang mengadili daripada negara lain tempat terjadinya kejahatan.

Sebagai ilustrasi, apabila seorang WNI berada di luar negeri, kemudian melakukan hubungan denga negara asing dan kemudian meggerakkan kekuatan asing agar melakukan peyerangan kepada Indonesia, maka berdasarkan pasal 111 ayat (1) KUHP, orang tersebut dapat diadili atau dituntut di pengadilan Indonesia.

3.3.4.Passive Nationality (nasionalitas pasif)

Prinsip ini sedikit berbeda dengan prinsip *nationality*. Jika prinsip *nationality* melihat status kewarganegaraan pelaku kejahatan sebagai dasar kewenangan melakukan penuntutan, maka prinsip *Passive Nationality* melihat status kewarganegaraan korban.[40]

Pembenaran terhadap prinsip ini adalah bahwa setiap negara berhak melindungi warganegaranya di luar negeri, dan apabila negara territorial tempat pelanggaran itu terjadi tidak menghukum orang yang menimbulkan kerugian itu, maka negara dari korban itu berweang menghukum pelanggar tersebut jika pelaku memasuki wilayahnya.[41] Keberatan terhadap prinsip ini adalah bahwa

---

[38] Darrell Menthe,*op.cit*, nomor 9
[39] J.G Starke,*op.cit*, hal 211
[40] Darrel Menthe,*op.cit*, nomor 10
[41] J.G Starke,*op.cit*, hal 211

kepentingan umum negara tidak serta merta terganggu hanya karena salah seorang warganegaranya telah dirugikan.[42]

Prinsip nasionalitas pasif ini antara lain termuat dalam undang-undang pidana Mexico, Brazil, Itali dan Indonesia. Sedangkan Inggris dan Amerika Serikat tidak mengadopsi prinsip ini ke dalam undang-undang pidananya.[43]

3.3.5.Protective Principle (prinsip perlindungan)

Hukum Internasional mengakui bahwa setiap negara berwenang menangai kejahatan yang berkaitan dengan keamanan dan integritas, serta kepentingan ekonomi yang cukup vital.[44]*Protective Principle* inilah yang digunakan sebagai dasar memanifestasikan kewenangan tersebut. Prinsip ini biasanya diterapkan gua melindungi kepentingan negara dari kejahatan yang dilakukan diluar wilayahnya, terutama apabila korban adalah negara atau pemerintah.[45]

Ada dua alasan yang mendasari prinsip ini, yaitu, *pertama*, akibat kejahatan sangat besar bagi negara yang dirugikan . *Kedua*, jika kewenangan tidak diterapkan oleh negara yang dirugikan, maka pelaku kejahatan bisa lolos karena di negara tempat perbuatan dilakukan, perbuatan yang dimaksud belum tentu merupakan tindak pidana serta ekstradisi juga ditolak karena alasan-alasan politis.[46]Kelemahan terbesar yang menimbulkan penolakan terhadap *protective principle* ini, yaitu negara (korban) itu sendiri yang menentukan perbuatan mana yang membahayakan keamanan, sehingga dapat menimbulkan kesewenang-wenangan.

3.3.6.Universality (universalitas)

Asas ini seringkali juga dusebut sebagai asas "*universal interest jurisdiction*".[47] Dahulu asas ini digunakan sebagai dasar kewenangan untuk menangkap dan menghukum para pelaku bajak laut dan kejahatan perang akan

---

[42] *Ibid.*
[43] *Ibid.*
[44] *Ibid.*
[45] Darrel Menthe,*op.cit*, Nomor 11
[46] J.G Starke,*op.cit*, hal 212
[47] Ahmad M.Ramli, *Cyberlaw dan HaKI Dalam Sistem Hukum Indonesia*, cet-1 (Bandung: PT Refika Aditama, 2004), hal 20

tetapi kemudian asas ini telah diperluas sehingga termasuk pula penyiksaan, genosida, dan pembajakan pesawat udara.[48]

Asas *universal interest jurisdiction* ini selayaknya memperoleh perjatian khusus guna penanganan dan penegakkan hukum kasus-kasus *cybercrime*.[49]Hal ini disebabkan karena asas ini memandang kewenangan untuk menangani kejahatan lebih kepada perlindungan terhadap kepentingan-kepentingan tertentu dari negara-negara yang ada di dunia, tanpa perlu mempersoalkan *locus delicti* dan kewarganegaraan pelaku.[50]

3.4.Yurisdiksi Negara Dalam Menangani Kasus Cybercrime

Masalah yurisdiksi merupakan masalah yang pelik dan seringkali menimbulkan konfilik kepentingan antar dua negara. Untuk membantu pembaca memhami lebih dalam mengenai yurisdiksi, maka pembahasan akan dibagi menjadi dua bagian yaitu :

1. Yurisdiksi menurut Convention on Cybercrime
2. Perbandingan pengaturan mengenai cybercrime di beberapa negara

3.4.1.Yurisdiksi Menurut Convention on Cybercrime

Permasalahan yurisdiksi dalam *Convention on Cybercrime* yang dibuat oleh Dewan Eropa, secara khusus ditempatkan pada pasal tersendiri yakini pada pasal 22. Pasal yang terdiri dari lima ayat tersebut antara lain berbunyi sebagai berikut[51] :

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a in its territory; or

b on board a ship flying the flag of that Party; or

c on board an aircraft registered under the laws of that Party; or

---

[48] Menthe,*op.cit*, nomor 12
[49] M. Ramli,*loc.cit*
[50] E.Y Kanter dan S.R Sianturi, *Asas-asas Hukum Pidana Di Indonesia Dan Penerapannya*, Cet.2 (Jakarta: Storia Grafika, 2002), hal 111
[51] European Committee on Crime Problems (CDPC), "Final Draft Convention on Cybercrime", Strasbourg, 25 Mei 2001

d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.[52]

---

[52] Terjemahan bebas dari pasal 22 ini adalah :

1) Setiap Negara yang menjadi peserta dalam konvensi ini sebaiknya mengambil langkah-langkah di bidang legislasi dan bidang lainnya yang dianggap perlu untuk menerapkan yurisdiksinya terhadap kejahatan-kejahatan yang tercantum dalam pasal 2-11 konvensi ini, dalam hal kejahatan tersebut berlangsung di :

a. Di wilayah negara tersebut,

b. Diatas kapal berbendera negara tersebut,

c. Diatas pesawat yang terdaftar menurut hukum negara tersebut,

d. Kejahatan yang dilakukan oleh warganegaranya, dalam hal perbuatan yang dilakuakan tersebut dikategorikan sebagai tindak kejahatan menurut hukum pidana dimana perbuatan itu terjadi atau jika perbuatan tersebut berlangsung di luar wilayah yurisdiksi negara.

2) Setiap negara berhak untuk memilih apakah akan menerapkan atau tidak ketentuan yurisdiksi dalam bagian 1b-1ds diatas dengan mempertimbangkan kondisi serta kasus tersebut.

3) Setiap peserta dalam konvensi ini sebaiknya mengambil langkah-langkah yang dianggap perlu untuk menerapkan yurisdiksinya terhadap kejahatan-kejahatan berdasarkan pasal 24 bagian pertama konvensi ini, dalam hal tersangka berada di wilayahnya dan tidak dilakukan ekstradisi atas dirinya dengan pertimbangan status kewarganegarannya.

Dewan Eropa melalui *Commitee of Experts on Crime in Cyberspace* (PC-CY) sebagai panitia perumus konvensi ini menerbitkan penjelasan resmi mengenai pasal-pasal dalam konvensi tersebut. Penjelasan tersebut dimuat dalam suatu dokumen yang dinamakan *Expalanatoty Report of The Draft Convention on Cybercrime* yang telah disetujui pada bulan November 2001. Pasal 22 ini memuat sejumlah kritreria yang mewajibkan setiap pihak dalam konvensi ini untuk menerapkan yurisdiksinya terhadap kejahatan-kejahatan yang disebutkan mulai dari pasal 2 hingga pasal 11 dalam konvensi ini. Kejahatan-kejahatan tersebut antara lain :

1) Penyadapan secara tidak sah (*illegal interception*),
2) Memasuki suatu sistem komputer secara tidak sah (*illegal access*),
3) Intervensi terhadap data (*data intervention*),
4) Intervensi terhadap sistem (*system interference*),
5) Penyalahgunaan alat (*misuse of device*),
6) Pemalsuan melalui komputer (*computer related forgery*),
7) Penipuan melalui komputer (*computer realted fraud*),
8) Kejahatan pornografi anak (*offences related to child pornography*),
9) Pelanggaran hak cipta dan hak-hak lainnya yang terkait (*offences related to infringements of copyright and related rights*),
10) Segala bentuk percobaan, pembantuan, dan persekongkolan yang berkaitan dengan kejahatan-kejahatan tersebut diatas.[53]

Ayat pertama dalam pasal ini menganut prinsip teritorial, artinya setiap negara yang menjadi pihak dalam konvensi ini berhak mengadili terhadap kejahatan-kejahatan yang tercantum dalam konvensi ini yang dilakukan di wilayahnya. Sebagai contoh misalnya suatu negara dapat menerapkan yurisdiksi teritorialnya jika baik pelaku maupun sistem komputer yang diserang berada di wilayahnya atau jika sistem komputer yang diserang berada di wilayahnya, tetapi

---

4) Keberadaan konvensi ini tidak mengenyampingkan penerapan yurisdiksi kriminal berdasarkan hukum nasional suatu negara.

5) Apabila lebih dari satu pihak mengkalim yurisdiksi atas suatu kejahatan yang terdapat dalam konvensi ini, maka para pihak yang terlibat sebaiknya mengadakan konsultasi dalam menentukan yurisdiksi yang tepat.

[53] "Expalantory Report of Convention on Cybercrime",Adopted November 2001. www.coe.net

pelakunya tidak berada di wilayahnya.[54] Pada awal perumusannya, dalam pasal ini juga dipertimbangkan untuk memasukkan klausul yang memungkinkan suatu negara perserta konvensi menerapkan yurisdiksinya berdasarkan jenis kejahatan dalam konvensi ini yang melibatkan satelit yang terdaftar pada negara tersebut. Namun tim perumus konvensi pada akhirnya menganggap hal ini tidak perlu mengingat kejahatan yang melibatkan satelit bagaimanapun juga selalu berasal dari bumi dan tertuju ke bumi. Dalam hal ini, salah satu dasar penentuan yurisdiksi yang tercantum dalam ayai (1) butir (a) hingga (c) dapat diterapkan oleh suatu negara jika transmisi melalui satelit tersebut berasal atau dilakukan di luar wilayahnya. Sementara ayat (1) butir (d) dapat diterapkan jika kejahatan tersebut dilakukan oleh warganegara yang bersangkutan dan dilakukan di luar wilayah yurisdiksi negara tersebut. Selanjutnya sempat dipertanyakan juga apakah tepat jika menempatkan negara dimana satelit tersebut terdaftar sebagai penentuan yurisdiksi kriminal, mengingat dalam banyak kasus sebenarnya tidak ada hubungan yang berarti antara kejahatan yang dilakukan dengan negara tempat satelit tersebut terdaftar karena pada dasarnya fungsi satelit hanya sebagai pengirim.[55]

Pasal 22 Ayat 1 butir b dan c menganut prinsip teritorial yang diperluas, dimana dimungkinkan setiap negara menrapkan yurisdiksinya terhadap kejahatan yang dilakukan di kapal laut yang mengibarkan bendera atau pesawat yang terdafatar menurut hukum negara tersebut. Prinsip ini secara praktek telah dikenal luas dan tercantum dalam beberapa hukum nasional sejumlah negara, khususnya semenjak kapal laut dan pesawat dianggap sebagai perluasan dari yurisdiksi suatu negara. Penerapan ini hanya akan berguna jika kapal laut atau pesawat tersebut berada diluar yurisdiksi negara yang dimaksud.[56] Pasal Ayat (1) butir (d) berisi prinsip nasionalitas yang banyak oleh negara-negara penganut sistem *civil law*. Prinsip ini memungkinkan seorang warganegara diproses menurut hukum

[54] *Ibid.*
[55] *Ibid.*
[56] *Ibid.*

negaranya atas suatu perbuatan yang dilakukan diluar wilayah yurisdiksi negara yang bersangkutan.[57]

Ayat (2) memuat ketentuan yang memungkinkan negara peserta konvensi untuk melakukan pengecualian (persyaratan) terhadap ayat (1) butir (b), (c), dan (d). Sementara pengecualian tersebut tidak diperkenankan terhadap pemberlakuan yurisdiksi teritorial seperti yang tercantum dalam butir a, atau terhadap penerapan yurisdiksi berdasarkan prinsip *aut dedere aut judicare* (pengekstradisian atau penuntutan) seperti yang tercantum dalam ayat 3 yakni dalam hal suatu negara menolak untuk mengekstardisi seorang pelaku kejahatan karena status kewarganegaraannya serta pelaku berada di wilayah negara tersebut. Ketentuan ayat 3 tersebut perlu untuk menjamin bahwa negara peserta konvensi yang menolak mengekstradisi tetap mempunyai kewenangan untuk melakukan penyelidikan dan prosedur hukum lainnya terhadap warganegaranya, jika ekstradisi tersebut diminta oleh negara peserta konvensi lainnya berdasarkan syarat-syarat dalam Pasal 24 ayat (6), yang berbunyi bahwa jika permintaan ekstradisi terhadap pelaku kejahatan-kejahatan dalam konvensi ini ditolak dengan alasan status kewarganegaraanya atau pihak yang diminta menganggap mereka mempunyai yurisdiksi terhadap kejahatan tersebut, maka negara yang menolak tersebut harus menyampaikan kepada pihak yang meminta serta memberikan laporan hasil proses yang dilakukan.[58]

Dasar penerapan yurisdiksi yang tercantum dalam ayat 1 tidak bersifat baku, karena dalam ayat (4) disebutkan bahwa negara peserta konvensi diperkenankan untuk mempergunakan jenis yurisdiksi lainnya yang didasarkan pada hukum nasionalnya masing-masing.[59] Dalam hal kasus kejahatan yang melibatkan sistem komputer, terdapat kemungkinan dimana lebih dari satu negara peserta yang mengklaim mempunyai yurisdiksi terhadap kejahatan tersebut. Misalnya, banyak kejahatan seperti serangan virus, penipuan, atau pelanggaran hak cipta yang dilakukan lewat internet dengan korban lebih dari satu negara. Oleh karena itu untuk menghindari persaingan antar negara dalam hal penegakan hukum, maka negara peserta yang terlibat dalam situasi tersebut dapat

[57] *Ibid.*
[58] *Ibid.*
[59] *Ibid.*

mengadakan perundingan untuk menentukan yurisdiksi yang tepat terhadap kejahatan yang dimaksud. Perundingan yang dimaksud tidak bersifat wajib, melainkan hanya dilakukan jika dianggap perlu. Sebagai contoh misalnya salah satu pihak yang memiliki kepentingan atas suatu kejahatan yang melibatkan lebih dari suatu negara telah mendapat pemberitahuan bahwa pihak lain yang juga memiliki kepentingan tidak akan mengajukan tuntutan apa-apa.[60]

Berdasarkan uraian mengenai Pasal 22 beserta penjelasannya diatas, dapat dilihat bahwa *Convention on Cybercrime* ciptaan Dewan Eropa ternyata masih menggunakan konsep yurisdiksi yang selama ini dikenal dan dipergunakan secara internasional. Selain itu, meskipun tidak secara tegas menyatakan dukungan terhadap konsep analogi, konvensi ini cenderung 'melepaskan' diri dari konsep pemisahan. Sikap ini dimaklumi, mengingat desakan untuk menciptakan hukum tersendiri terhadap *cyberspace* selama ini masih sebatas wacana yang terus berkembang dan praktis belum ada konsep yang jelas mengenai hal ini. Sementara disisi lain, intensitas kejahatan komputer yang merupakan dampak negatif dari kecanggihan komputer terus meningkat. Kondisi ini akan berbahaya dan dapat menimbulkan 'anarkisme' di *cyberspace* jika tidak segera dibuat suatu produk legislasi yang natinya berfungsi menertibkan segala aktivitas di *cyberspace*.[61] Lebih jauh lagi, dengan adanya ketentuan mengenai yurisdiksi yang tercantum dalam Pasal 22, maka negara peserta konvensi mempunyai 'sandaran' hukum yang pasti dalam menerapkan yurisdiksinya terhadap *cybercrime* sehingga konflik yang potensial terjadi karena perebutan penerapan yurisdiksi dapat dihindari.

3.4.2.Perbandingan Pengaturan Mengenai *Cybercrime* di Beberapa Negara

Seperti yang sudah dijelaskan sebelumnya, bahwa negara-negara didunia menanggapi isu *cybercrime* dengan cara yang berbeda-beda, begitupun dengan pengaturannya, ada yang membuat aturan khusus mengenai *cybercrime*, dan ada pula yang hanya mengamandemen dan menambahkan peraturan perundang-undangan yang sudah ada. Dalam sub topik ini penulis akan menguraikan secara singkat pengaturan *cybercrime* di beberapa negara yang juga peserta *Convention on Cybercrime* maupun negara-negara yang bukan peserta *Convention on*

[60] *Ibid.*
[61] Mark D. Rasch, *loc.cit*

Cybercrime sebagai perbandingan dengan peraturan perundang-undangan Indonesia.

1) Amerika Serikat

Ketika kita membicarakan mengenai pengaturan *cybercrime* di Amerika Serikat, kita akan menemukan berbagai peraturan yang menyangkut *cybercrime*. Selain karena ada dua hukum yang berlaku (federal dan negara bagian) juga dikarenakan banyaknya teori-teori mengenai yurisdiksi di *cyberspace* yang berkembang, menurut Darrel Menthe teori-teori tersebut adalah[62]:

a) *The Theory of The Uploader and The Downloader*

Berdasarkan teori ini, *uploader* adalah pihak yang memasukkan informasi ke dalam suatu lokasi di *cyberspace*, sedangkan *downloader* adalah pihak yang mengakses informasi dalam *cyberspace*. Pada umumnya yurisdiksi mengenai perbuatan-perbuatan perdata dan tindak pidana tidak ada kesulitan. Suatu negara dapat melarang, dalam wilayahnya, kegiatan *uploading* dan *downloading* yang diperkirakan dapat bertentangan dengan kepentingan negaranya. Misalnya, suatu negara dapat melarang setiap orang untuk *uploading* kegiatan perjudian dan melarang setiap orang dalam wilayahnya untuk *downloading* kegiatan perjudian tersebut.

Beberapa negara bagian di Amerika Serikat telah menggunakan teori ini, baik yurisdiksi untuk *uploaders* maupun *downloaders* di luar wilayah negara-negara bagian tersebut. Minnesota adalah salah satu negara bagian pertama yang menerapkan yurisdiksi ini. Jaksa Agung Minnesota, Hubert Humphrey III telah mengeluarkan suatu memorandum yang menyatakan:

"person outside of Minnesota who transmit information via the internet knowing that information will be diseminated in Minnesota are subject to jurisdiction in Minnesota courts for violation of state criminal and civil laws".

Pendapat ini digunakan juga dalam kasus *Minnesota v. Granite Gate Resort*[63] berdasarkan fakta bahwa *"during a two week period in February and*

[62] Darrel Menthe, *op.cit*, hal 3-4, lihat juga di tulisan Ny Tien Saefullah "*Yurisdiksi Sebagai Alat Untuk Menegakkan Hukum di Cyberspace"* dalam kumpulan tulisan "Cyberlaw: Suatu Pengantar"(2002,Bandung : ELIPS), hal 102-104

[63]Kasus ini bermula ketika Granite Gate Resort berlokasi di Belize membuat suatu *webpage* tentang judi online yang sasarannya adalah warga Minnesota, karena judi online di larang di

March 1996, at least 248 Minnesota computers accessed and received transmission from appelant's websites". Akan tetapi pendekatan yang dilakukan oleh Minnesota ini menimbulkan beberapa masalah, antara lain bahwa Minnesota telah mengabaikan *the presumption against extraterriotorial in application of US laws*. Alasannya karena Minnesota sebagai negara bagian tidak memiliki kedaulatan sehingga tidak memiliki yurisdiksi ekstrateritorial, yang memiliki yurisdiksi hanyalah negara federal dan bukan negara bagian.

b) *The Theory of The Law of The Server*

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

c) *The Theory of International Space*

Dalam kaitan dengan teori ini, Menthe mengusulkan agar *cyberspace* menjadi *the fourth space*. Yang menjadi dasar analogi tidak terletak pada kesamaan fisik, melainkan pada sifat internsional yakini *soverignless quality*. Dalam hukum intenasional dikenal ruang dimensi keempat, yaitu ruang angkasa. Ruang angkasa merupakan ruang bebas yang tidak tunduk pada kedualtan negara manapun. Hukum yang mengatur kegiatan di ruang angkasa adalah hukum internasional, yaitu berupa perjanjian antara negara-negara. Maksud dari teori *internasional space* ini bahwa kegiatan dalam ini bahwa kegiatan dalam *cyberspace* dianalogikan dengan kegiatan di ruang angkasa. Semua kegiatan di sana diatur secara bersama-sama oleh negara-negara. Dari teori Menthe ini dapat disimpulkan bahwa Menthe lebih condong kepada kubu yang mendukung konsep pemisahan.

Minnesota, maka Granite Gate dituntut berdasarkan peraturan *cybercrime* yang berlaku di Minnesota, dalam pembelaannnya kuasa hukum Granite Gate menyatakan, Minnesota tidak berhak menghukum kliennya karena bukan yurisdiksinya, alasan tersebut ditolak sehingga Granite Gate dinyatakan besalah

Terlepas dari teori yurisdiksi yang diterapkan, ternyata Amerika Serikat sudah memulai sebuah studi mengenai perlunya pengaturan tentang *cybercrime* di Amerika. Pada tahun 1977 seorang senator Amerika yang juga ketua tim studi mengenai *cybercrime* bernama Ribicoff, mengajukan proposal undang-undang tentang *Unauthorized Access* , proposal ini kemudian disetujui dan dikenal dengan nama *Ribicoff Bill*.[64] Sampai sekarang sudah banyak peraturan federal yang mengatur tentang *cybercrime* atau setidaknya mengandung unsur *cybercrime*, peraturan-peraturan itu antara lain[65] :

1.Access Device Fraud. (18 U.S.C. § 1029), mengatur tentang penipuan dengan menggunakan alat penghubung ;
2.Computer Fraud and Abuse Act (18 U.S.C. § 1030), mengatur tentang penipuan yang berkaitan dengan konektivitas komputer;
3. CAN-SPAM Act (15 U.S.C. § 7704), mengatur tentang pengawasan material yang berbau pornografi sekaligus sebagai Undang-Undang Pemasaran;
4. Extortion and Threats (18 U.S.C. § 875), mengatur tentang ancaman dan pemerasan melalui komunikasi antar negara bagian;
5. Identity Theft and Assumption Deterrence Act (18 U.S.C. § 10286.), mengatur mengenai penipuan indentitas;
6. Wire Fraud (18 U.S.C. § 1343), mengatur tentang penipuan yang dilakukan melalui kabel, televisi, radio;
7. No Electronic Theft ("NET") Act (17 U.S.C. § 506), mengatur tentang kejahatan yang berhubungan dengan hak cipta;
8. Digital Millennium Copyright Act (DMCA) (17 U.S.C. § 1201), mengatur tentang perlindungan hak cipta elektronik;
9. Electronic Communications Privacy Act (18 U.S.C. § 2701, et seq), mengatur tentang perlindungan terhadap penyimpanan data yang berhubungan dengan perbankan;
10. Trade Secrets Act (18 U.S.C. § 1832), mengatur tentang perlindungan rahasia dangang;

[64] www.cybercrime.com/history, diakses pada tanggal 5 Juni 2009
[65]

11. Economic Espionage Act (18 U.S.C. § 1831), mengatur tentang spionase ekonomi.

2) Negara-Negara Asia

Baru sedikit negara-negara di Asia yang memiliki peraturan yang khusus mengatur tentag *cybercrime* dan hanya Jepang yang baru masuk menjadi peserta *Cybercrime Conventio 2001*. Penelitian yang dilakukan oleh Galexia, sebuah lembaga riset internasional mencoba mengambil sampel empat negara Asia, yaitu Jepang, Hongkong, Korea Selatan sebagai objek penelitian dalam bidang *cybercrime*. Masalah khusus yang diteliti oleh Galexia adalah peraturan tentang konten dewasa dan judi. Ringkasan dari penelitian tersebut adalah :[66]

a. Hongkong

Ada tiga kategori yang diatur dalam *Control of Obscene and Indecent Articles Ordinance* untuk mengelompokkan konten dewasa, yang dimaksud dengan konten dewasa disni adalah segala senuatu yang berbau pornografi dalam bentuk gambar maupun artikel, kategori tersebut adalah :

1. Class 1 articles (neither obscene nor indecent) which will not be subject to any restriction.
2. Class 2 articles (indecent) which may only be published to persons over 18 years old and must carry a prescribed warning
3. Class 3 articles (obscene) which are banned from publication.

Kategorisasi dan pengawasan untuk hal ini di buat oleh suatu badan yang disebut *Obsence Article Tribunal* . Setiap pelanggaran akan berkaibat pada pengenaan denda dan pidana penjara. Sementara untuk pengaturan mengenai perjudian Hongkong menerapkan aturan yang sangat ketat, temasuk untuk judi *online*, semua perizinan bagi lembaga yang akan melakukan kegiatan judi harus mengajukan izin ke *Television and Licensing Authority* (TELA) . Selain itu juga ada peraturan lain yang mengatur tentang internet, yaitu *The Hongkong Internet*

[66] Chris Conolly, An Introduction to Internet Content Regulation in Asia and the Pacific (Galexia intelligence reports, articles, papers, conferences and seminars

Service Provider Association (HKISPA) *code*. *Code* ini mengatur tentang pembatasan konten dewasa, setiap anggota HKISPA harus melakukan :

a. Mengambil tindakan yang diperlukan untuk mencegah pengguna internet untuk memasang atau mentransmisikan konten *Class* 3;

b. Menghimbau kepada pengguna agar setiap akses ke internet yang dilakukan oleh orang yang berusia dibawah 18 tahun harus didampingi oleh orang dewasa;

c. Menginformasikan kepada pengguna agar segala konten yang termasuk *Class 2* agar di non-aktifkan atau di blok dari orang yang berusia dibawah 18 tahun; dan

d. Menghimbau kepada penyedia konten agar setiap konten yang termasuk *Class* 2 sebelum bisa diakses harus di beri peringatan di layar komputer.

b. Jepang

Di Jepang ada semacam *Guidelines* untuk melakukan kegiatan yag berhubungan dengan internet yang disebut *General Ethical Guidelines for Running Online Srevices* yang disusun oleh *Electronic Network Consortium* (ENC). Dalam *Guidelines* tersebut harus meyetujui klausa dalam *Guidelines* tersebut yang meliputi :[67]

a. Kewajiban untuk mengawasi;

b. Hal yang dilarang; dan

c. Penanggulangan

Selain itu setiap pihak harus mengorganisasikan sebuah *Help Desk and Management System* yang meliputi :

a. *Help Desk* untuk mengurusi masalah permohonan dan komplain;

b. Prosedur internal untuk mengatasi komplain; dan

c. Setiap ISP harus mempublikasikan langkah penaggulangan.

Sayangnya meskipun telah mengeluarkan peraturan yang begitu banyak berdasarkan Laporan dari Soros pada tahun 1998, tidak ada sensor terhadap

[67] *Ibid.*

konten internet.[68] Untuk pengawasan terhadap perjudian di Jepang telah dikeluarkan peraturan yang disebut *Law on Control and Improvement of Amusement Business* yang diamandemen pada tahun 1999, dalam peraturan ini selain mengatur tentang perjudian juga mengatur apa yang disebut dengan '*image transmission type sex-oriented special amusement business'*, yaitu bisnis yang menggunakan material yang berbau sex, seperti *Host Club*, Pachinko.

c. Korea Selatan

Di Korea Selatan konten internet di atur dalam *Electronic Communication Business Law* and the *Telecommunication Business Act*. Dalam *Act* ini diatur mengenai pembentukan kantor etika informasi dan telekomunikasi (*Information and Telecommunication Ethics Office*) yang berada dibawah Kementrian Telekomunikasi. Tugas dari kantor ini adalah mengatur segala sesuatu yang berhubungan dengan *online services*. Kantor ini juga mengeluarkan semacam rating untuk membedakan konten dewasa, selain itu kantor ini juga memiliki kewenangan untuk memerintahkan sebuah ISP untuk memblok penggunanya untuk mengakses situs yang memiliki server di luar negeri.

Mengenai perjudian di Korea Selatan tidak ada peraturan perundang-undangan khusus yang mengatur. Hal ini merupakan kewenagan kantor etika informasi dan telekomunikasi, selain itu kitab undang-undang hukum pidana Korea Selatan juga berlaku baik untuk pelanggaran konten dewasa maupun perjudian.

3) Negara-Negara Eropa

Untuk negara-negara eropa, penulis tidak akan menjelaskan terlalu dalam karena sebagian besar negara-negara di Eropa adalah peserta dari *Cybercrime Convention*. Otomatis negara-negara tersebut peraturan perundang-undangannya sudah sesuai dengan yang diatur dalam *Convention on Cybercrime* baik dengan cara ratifikasi maupun adopsi.

[68] *Ibid.*

BAB 4
PENGATURAN MENGENAI *CYBERCRIME* DI INDONESIA

Apabila kita berbicara mengenai peraturan perundang-undangan yang mengatur tentang *cybercrime* di Indonesia, bisa dibilang kita masih sangat tertinggal karena baru satu peraturan yang mengatur secara spesifik mengenai *cybercrime*, yaitu Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE). Pada awalnya hanya ada pengaturan mengenai telekomunikasi melalui Undang-Undang No 3 tahun 1989 yang kemudian diamandemen dengan dikeluarkannya Undang-Undang No 36 Tahun 1999 tentang hal yang sama. Setelah itu perkembangan peraturan yang mengatur mengenai *cybercrime* terus berkembang.

Untuk memudahkan pemahaman maka penulis membagi pembahasan mengenai perkembangan peraturan perundang-undangan yang mengatur tentang *cybercrime* menjadi dua bagian yaitu :

1. Sebelum berlakunya UU ITE
2. Sesudah berlakunya UU ITE

4.1. Sebelum Berlakunya Undang-Undang Informasi dan Transaksi Elektronik

Pada pembahasan ini penulis akan fokus kepada Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi. Alasan kenapa penulis hanya akan fokus kepada satu undang-undang karena undang-undang ini adalah merupakan undang-undang pertama yang mengatur tentang *cybercrime*.

4.1.1 Undang-Undang Telekomunikasi

Undang-undang ini mengatur tentang segala hal mengenai telekomunikasi. Hal yang pertama kali diatur dalam undang-undang ini adalah tentang siapa saja yang berhak menyelenggarakan telekomunikasi sesuai dengan peruntukkannya, pihak-pihak yang berhak menyelenggarakan komunikasi adalah :[1]

[1] Indonesia, Undang Undang No 3 tahun 1999 Tentang Telekomunikasi Lembaran Negara RI No 154 Tambahan Lembaran Negara RI No 3881 , Pasal 8-10

1. Penyelenggara Jasa Telekomunikasi

Penyelenggara jasa telekomunikasi adalah penyelenggaraan telekomunikasi untuk memenuhi kebutuhan masyarakat. Badan penyelenggara untuk jasa telekomunikasi dalam negeri (domestik) adalah PT. Telkom dan Badan Penyelenggara untuk jasa telekomunikasi luar negeri (internasional) adalah PT. Indosat. Badan Usaha Milik Negara tersebut diberi wewenang untuk yang menyelenggarakan jasa telekomunikasi, seperti telepon, telex, faksimili, dan sebagainya, maupun jasa telekomunikasi berupa jasa-jasa nilai tambah (*value added service*). Badan lain di luar badan penyelenggara, baik dalam bentuk Badan Usaha Milik Swasta (BUMS), Badan Usaha Milik Daerah (BUMD) maupun Koperasi juga berhak untuk menyelenggarakan jasa telekomunikasi non dasar. Sedang untuk menyelenggarakan jasa telekomunikasi dasar, badan lain dapat bekerjasama dengan PT Telkom dan atau PT Indosat. Bentuk kerjasama antara badan penyelenggara dan badan lain ini telah diatur dalam Peraturan Pemerintah Nomor 8 tahun 1993, yaitu dapat berbentuk Kerjasama Operasi (KSO), usaha patungan dan kontrak manajemen.

2. Penyelenggaraan Telekomunikasi untuk Keperluan Khusus

Penyelenggaraan telekomunikasi untuk keperluan khusus adalah penyelenggaraan telekomunikasi yang dilakukan oleh instansi pemerintah tertentu, perorangan atau badan hukum untuk keperluan khusus atau untuk keperluan sendiri.Telekomunikasi khusus dapat dilakukan oleh instansi pemerintah tertentu atau badan hukum (perseroan terbatas atau koperasi) yang ditentukan berdasarkan hukum. Telekomunikasi khusus diselenggarakan berdasarkan ijin yang ditetapkan oleh Direktur Jenderal Pos dan Telekomunikasi.
Ijin penyelenggaraan telekomunikasi khusus hanya diberikan Badan Hukum apabila wilayah tersebut belum tersedia atau belum terjangkau fasilitas telekomunikasi yang dapat disediakan oleh badan penyelenggara atau badan lain.Telekomunikasi untuk keperluan khusus hanya dapat diselenggarakan dengan mempertimbangkan kerahasiaan dan jangkauan atau pengoperasiannya perlu bentuk sendiri. Penyelenggara telekomunikasi untuk keperluan khusus adalah : Instansi pemerintah

tertentu untuk pelaksanaan tugas khusus, perseorangan atau , Badan hukum.

3. Penyelenggaraan Telekomunikasi untuk Keperluan Pertahanan dan Keamanan

Berdasarkan Peraturan Pemerintah Nomor. 4 tahun 1992 tentang Penyelenggaraan Telekomunikasi untuk Keperluan Pertahanan dan Keamanan Negara diatur bahwa penyelenggaraan telekomunikasi untuk keperluan pertahanan dan keamanan negara(Hankamneg) diselenggarakan oleh Dephankam dan/atau ABRI. Penyelenggaraan diperuntukan bagi pertahanan keamanan negara bukan merupakan penyelenggaraan jasa telekomunikasi.

Undang-undang ini merupakan amandemen dari undang-undang sebelumnya, yaitu UU No 3 tahun 1989 dan menjadi undang-undang pertama yang memasukkan *cybercrime* sebagai salah satu pelanggaran di dalam bidang telekomunikasi. Pengaturan mengenai *cybercrime* pada undang-undang ini diatur dalam Pasal 38 dan Pasal 40 yang berbunyi[2] :

Pasal 38

"Setiap orang dilarang melakukan perbuatan yang dapat menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi".

Pasal 40 :

"*Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melaiui jaringan telekomunikasi dalam bentuk apapun*"

Berdasarkan penjelasan Pasal 38 perbuatan yang dapat digolongkan sebagai perbuatan yang dapat menyebabkan ganguan telekomunikasi adalah :[3]

a. Tindakan fisik yang dapat menimbulkan kerusakan suatu jaringan telekomunikasi sehingga jaringan tersebut tidak dapat berfungsi sebagaimana mestinya;

[2]*Ibid.*, Pasal 38 dan 40
[3]*Ibid.*, Penjelasan Pasal 38

b. Tindakan fisik yang menyebabkan hubungan telekomunikasi tidak berjalan sebagaimana mestinya;

c. Penggunaan alat telekomunikasi yang tidak sesuai dengan persyaratan teknis yang berlaku;

d. Penggunaan alat telekomunikasi yang bekerja dengan gelombang radio yang tidak sebagaimana mestinya sehingga menimbulkan gangguan terhadap penyelengaraan telekomunikasi lainnya;

e. Penggunaan alat bukan telekomunikasi yang tidak sebagaimana mestinya sehingga menimbulkan pengaruh teknis yang tidak dikehendaki suatu penyelenggaraan telekomunikasi.

Sedangkan menurut penjelasan Pasal 40 yang dimaksud dengan *Cyberspy* adalah "**kegiatan memasang alat atau perangkat tambahan pada jaringan telekomunikasi untuk tujuan mendapatkan informasi dengan cara tidak sah**"[4]

Dari penjelasan pasal 38 dan 40 tersebut dapat kita simpulkan bahwa yang diatur dalam undang-undang ini adalah salah satu perbuatan yang termasuk dalam kategori *cybercrime* yaitu *illegal interception*[5] terhadap kegiatan telekomunikasi yang mengakibatkan proses telekomunikasi menjadi terhambat.

Mengenai pengaturan tentang yurisdiksi dalam undang-undang ini tidak disebutkan secara gamblang pada pasal tertentu, namun dari pengaturan Pasal 44 dapat disimpulkan bahwa apabila terjadi pelanggaran terhadap gangguan telekomunikasi maka yang diterapkan adalah hukum Indonesia. Bunyi Pasal 44 adalah :[6]

(1) Selain Penyidik Pejabat Polisi Negara Republik Indonesia, juga Pejabat Pegawai Negeri Sipil tertentu di Iingkungan Departemen yang Iingkup tugas dan tanggung jawabnya di bidang telekomunikasi, diberi wewenang khusus sebagai penyidik sebagaimana dimaksud dalam Undang-undang Hukum Acara Pidana untuk melakukan penyidikan tindak pidana di bidang telekomunikasi.

(2) Penyidik Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) berwenang :

---

[4] *Ibid.*, Penjelasan Pasal 40.

[5] Cybercrime Convention , Article 3, lihat juga pendapat dari Goodman & Brenner, GIPI dalam Bab 2 tulisan ini.

[6] Indonesia, *loc.cit*, Pasal 44.

a. melakukan pemeriksaan atas kebenaran laporan atau keterangan berkenaan dengan tindak pidana di bidang telekomunikasi;

b. melakukan pemeriksaan terhadap orang dan atau badan hukum yang diduga melakukan tindak pidana di bidang telekomunikasi;

c. menghentikan penggunaan alat dan atau perangkat telekomunikasi yang menyimpang dari ketentuan yang berlaku;

d. memanggil orang untuk didengar dan diperiksa sebagai saksi atau tersangka;

e. melakukan pemeriksaan alat dan atau perangkat telekomunikasi yang diduga digunakan atau diduga berkaitan dengan tindak pidana di bidang telekomunikasi;

f. menggeledah tempat yang diduga digunakan untuk melakukan tindak pidana di bidang telekomunikasi;

g. menyegel dan atau menyita alat dan atau perangkat telekomunikasi yang digunakan atau yang diduga berkaitan dengan tindak pidana di bidang telekomunikasi;

h. meminta bantuan ahli dalam rangka pelaksanaan tugas penyidikan tindak pidana di bidang telekomunikasi;

i. mengadakan penghentian penyidikan

(3) Kewenangan penyidikan sebagaimana dimaksud pada ayat (2) diliaksanakan sesuai dengan ketentuan undang-undang Hukum Acara Pidana

Dari pengaturan tentang yurisdiksi diatas maka dapat disimpulkan bahwa undang-undang ini menganut prinsip *objective territoriality* (teritorial objektif), hal ini bisa dilihat dari perumusan Pasal 38 yang menyatakan bahwa setiap orang dilarang untuk melakukan perbuatan yang dapat menggangu komunikasi. Berarti yang dilihat dari Pasal ini adalah akibat dari perbuatan yang dapat mengakibatkan terganggunya komunikasi tanpa melihat tempat dilakukannya kejahatan tersebut.[7]

[7] J.G Starke, .*op cit*, hal 184

4.2. Sesudah Berlakunya Undang-Undang Informasi dan Transaksi Elektronik

Dalam sub-bab ini dijelaskan mengenai peraturan yang mengatur mengenai *cybercrime* sesudah berlakunya UU ITE. Secara spesifik akan difokuskan pada pembahasan terhadap dua undang-undang, yaitu :

1. Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
2. Undang-Undang No 14 Tahun 2008 tentang Keterbukaan Informasi Publik

4.2.1. Undang-Undang Informasi dan Transaksi Elektronik

Secara umum Undang-Undang ini mengatur tentang segala sesuatu mengenai data elektronik dan pemanfaatannya untuk kepentingan umum. Pada awal pembentukkannya undang-undang ini menuai banyak kontroversi karena dianggap akan mematikan kebebasan untuk mengekspresikan diri di *cyberspace*.

Dalam undang-undang ini secara rinci dijelaskan mengenai segala perbuatan yang digolongkan sebagai *cybercrime*, jenis-jenis perbuatan ini di atur dalam Pasal 27 sampai Pasal 37. Hanya saja untuk pembahasan ini akan dijelaskan beberapa pasal yang terkait dengan *Covention on Cybercrime*. Pasal-pasal tersebut berbunyi :

Pasal 27

(1) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.

(2)Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.

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

(4) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

Pasal 27 memiliki tiga unsur yang sama yaitu unsur setiap orang, unsur dengan sengaja dan tanpa hak, dan unsur mendistribusikan dan/atau mentransmisikan

dan/atau membuat dapat diaksesnya Informasi Elektronik dan atau Dokumen Elektronik. Ayat yang perlu diperhatikan adalah ayat (3) karena hal ini bisa mengakibatkan seorang pengguna internet atau Blogger dapat dituduh mencemarkan nama baik.[8] Seperti yang dialami oleh seorang ibu rumah tangga bernama Prita Mulyasari yang sempat ditahan hanya gara-gara menuliskan sebuah surat pembaca di salah satu forum di internet.[9] Karena surat pembaca ini Prita dilaporkan ke polisi karena dituduh mencemarkan nama baik Rumah Sakit OMNI Internsional dalam dakwaan yang dibacakan di Pengadilan Negeri Tangerang Jaksa penuntut umum membidik Prita dengan tiga dakwaan alternatif. Pertama, Prita dijerat dengan Pasal 45 Ayat (1) jo Pasal 27 Ayat (3) UU ITE.[10]Sementara untuk dakwaan kedua dan ketiga, jaksa menggunakan KUHP, yaitu Pasal 310 Ayat (2) dan 311 Ayat (1). Ketiga pasal dalam dakwaan itu mengatur masalah pencemaran nama baik dan penghinaan.[11] Kelanjutan dari kasus ini adalah hakim telah menerima eksepsi dari pihak Prita dan membebaskan Prita dari segala tuntutan.

Pasal 28

(1) Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.

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

---

[8] Anggara, UU ITE merupakan ancaman bagi bloger indonesia, http://anggara.org/2008/03/26/uu-informasi-dan-transaksi-elektronik-adalah-ancaman-serius-bagi-bolger-indonesia/, diakses tanggal 1 Juli 2009

[9] http://suarapembaca.detik.com/read/2008/08/30/111736/997265/283/rs-omni-dapatkan-pasien-dari-hasil-lab-fiktif , diakses tanggal 25 Juni 2009

[10] Pasal 45 ayat UU ITE berbunyi :
(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).

[11]Prita Mulyasari Hari Ini Didakwa , www.hukumonline.com, diakses pada tanggal 29 Juni 2009.

Pasal 28 memiliki unsur setiap orang, unsur dengan sengaja, unsur tanpa hak, unsur menyebarkan. Sama seperti pasal sebelumnya, yang membedakannya hanyalah isi dari apa yang disebarkan. Pada ayat (1) yang disebarkan adalah informasi yang dapat mengakibatkan kerugian konsumen, sedangkan pada ayat (2) yang disebarkan adalah informasi yang berisi SARA dengan tujuan untuk menimbulkan kebencian atau permusuhan. Pasal ini juga krusial bagi seorang pengguna internet karena dengan mudahnya seorang pengguna internet melakukan tindakan tersebut baik secara langsung maupun tidak langsung.[12]

Pasal 30

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.

(2)Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik

(3)Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Pasal ini memiliki unsur setiap orang, unsur dengan sengaja, unsur tanpa hak, dan unsur mengakses komputer atau sistem elektronik. Dapat disimpulkan bahwa Pasal ini mengatur tentang larangan setiap orang untuk tidak melakukan *illegal access* dengan cara apapun (*hacking, cracking* maupun *cyber trespassing*). Sama seperti yang diatur dalam *Convention on Cybercrime* dalam pasal 2[13] yang dimaksud dengan *access* yang dimaksud meliputi kegiatan memasuki sistem komputer lainnya baik yang terkoneksi melalui jaringan komunikasi umum, tatu terhadap suatu sistem komputer pada jaringan yang sama seperti pada suatu *Local Area Network* (LAN)

[12] Anggara, *op.cit*

[13] Pasal 2 *Convention on Cybercrime*, yang berbunyi :

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."

atau *intranet* dalam suatu organisasi. Cara komunikasi yang dilakukan baik dari satu lokasi tertentu dengan cara *remote* maupun dengan penghubung *wireless* pada jarak yang dekat tidak masalah.[14]

Pasal 31

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.

(3) Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang - undang.

(4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Pasal ini memiliki unsur setiap orang, unsur dengan sengaja, unsur tanpa hak, dan unsur melakukan intersepsi atau penyadapan atas sebuah komputer atau sistem elektronik. Dapat disimpulkan bahwa pasal ini melarang setiap orang untuk melakukan *illegal interception*. Maksud dari Pasal ini sama dengan yang diatur dalam Pasal 3 *Convention on Cybercrime*.[15] Salah satu bagian dari pelanggaran yang dimaksud dari ketentuan pasal ini adalah melakukan penahanan komunikasi atau menghambat proses komunikasi dengan menggunakan perangkat elektronik untuk

[14] Council of Europe, *.op cit*., Poin 46.

[15] Pasal 3 *Cybercrime Convention*, yang berbunyi :

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system."

mendengarkan pembicaraan orang lain atau menggunakan peralatan untuk menyadap komunikasi. Klasifikasi ini hanya berlaku pada komunikasi data komputer yang dilakukan secara pribadi, klasifikasi ketentuan ini mengacu pada sifat pemindahan dan sifat dari data yang dipindahkan. Komunikasi yang terjadi dapat melalui hubungan dari komputer ke *printer*, antara dua komputer atau dari orang ke komputer itu sendiri (seperti mengetik dengan *keyboard*).[16]

Pasal 32

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

Pasal ini memiliki unsur setiap orang, unsur dengan sengaja, unsur tanpa hak, unsur mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik. Dapat disimpulkan bahwa pasal ini mengatur tentang larangan untuk melakukan *data interception* seperti yang diatur dalam Pasal 4 *Convention on Cybercrime*.[17] Ketentuan yang diatur dalam pasal ini berusaha untuk memberi jaminan bahwa data yang dikirimkan melaui jaringan internet atau pemindahan data yang dilakukan melaui suatu jaringan adalah sama dengan data yang dikirimkan oleh si pengirim. Kepentingan perlindungan hukum dalam pasal ini adalah keutuhan dan berfungsi sebagaimana mestinya penggunaan data komputer yang tersimpan atau program-program komputer.[18]

Mengenai yurisdiksi dalam undang-undang ini diatur dalam pasal 2, yang berbunyi :

---

[16] Keyser, .*loc cit*., hal 301

[17] Pasal 4 *Cybercrime Convention* yang berbunyi :

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

[18] Council of Europe,.*op cit.* Poin 60

"Undang-Undang ini berlaku untuk setiap Orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang - Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia"

Dari perumusan pasal diatas dapat disimpulkan bahwa undang-undang ini menganut prinsip *objective territoriality* (teritorial objektif) karena yang lebih dilihat adalah akibat dari perbuatan yang ditimbulkan karena perbuatan yang di sebutkan dalam pasal-pasal tersebut

4.2.2. Undang-Undang Keterbukaan Informasi Publik

Undang-undang No 14 Tahun 2008 ini mengatur tentang penyampaian informasi untuk kepentingan publik. Undang-undang ini akan efektif berlaku pada tanggal 30 April sesuai dengan pengaturan dalam pasal 64.[19] Penulis merasa perlu untuk membahas undang-undang ini karena pengertian informasi mencakup juga informasi secara elektronis yang salah satu media penyebarannya melalui *cyberspace*.[20]

Dalam undang-undang ini terdapat ketentuan yang dapat dilihat sebagai suatu *cybercrime*. Hal ini berlaku apabila sebuah informasi publik di sebarkan melalui publik di sebarkan melalui *cyberspace*. Pasal-pasal tersebut adalah :[21]

Pasal 54
(1) Setiap Orang yang dengan sengaja dan tanpa hak mengakses dan/atau memperoleh dan/atau memberikan informasi yang dikecualikan sebagaimana diatur dalam Pasal 17 huruf a, huruf b, huruf d, huruf f, huruf g, huruf h, huruf i, dan huruf j

---

[19]Indonesia UU No 14 Tahun 2008 pasal 64 yang berbunyi

(1) Undang-Undang ini mulai berlaku 2 (dua) tahun sejak tanggal diundangkan.

(2) Penyusunan dan penetapan Peraturan Pemerintah, petunjuk teknis, sosialisasi, sarana dan prasarana, serta hal-hal lainnya yang terkait dengan persiapan pelaksanaan Undang-Undang ini harus rampung paling lambat 2 (dua) tahun sejak Undang-Undang ini diundangkan.

[20] *Ibid.*, pasal 1 angka 1 yang berbunyi :

(1) Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasisecara elektronik ataupun nonelektronik.

[21] *Ibid.*, pasal 54-55

dipidana dengan pidana penjara paling lama 2 (dua) tahun dan pidana denda paling banyak Rp10.000.000,00 (sepuluh juta rupiah).
(2) Setiap Orang yang dengan sengaja dan tanpa hak mengakses dan/atau memperoleh dan/atau memberikan informasi yang dikecualikan sebagaimana diatur dalam Pasal 17 huruf c dan huruf e, dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan pidana denda paling banyak Rp20.000.000,00 (dua puluh juta rupiah).

Pasal 55
Setiap Orang yang dengan sengaja membuat Informasi Publik yang tidak benar atau menyesatkan dan mengakibatkan kerugian bagi orang lain dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau denda paling banyak Rp5.000.000,00 (lima juta rupiah).

Dalam pasa-pasal ini jika kita kaitkan dengan jenis-jenis *cybercrime* menurut *Convention on Cybercrime* maka terdapat dua perbuatan yaitu, *illegal access*[22] yang terdapat dalam pasal 54 yang melarang setiap orang yang tanpa hak mengakses informasi publik yang tidak seharusnya dia peroleh. Perbuatan selanjutnya yang termasuk *cybercrime* adalah *data interception*[23] yang diatur dalam pasal 55 yang melarang setiap orang untuk membuat sebuah informasi publik yang tidak benar dengan cara apapun.

4.3. Tinjauan Kasus *Cyberspying* Dari Prespektif Hukum Indonesia

Kasus ini bermula dari adanya temuan dari aktivis Tibet yang menemukan dugaan bahwa komputer mereka telah di sadap secara elektronik, lalu mereka meminta kepada Information Warfare Monitor (IWM) untuk mengadakan suatu

[22]Pasal 3 *Cybercrime Convention*, yang berbunyi :
"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system."

[23] Pasal 4 *Cybercrime Convention* yang berbunyi :
1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

penelitian.[24] Hasilnya sungguh mengejutkan dimana diduga sekitar 1300 komputer di 103 negara, kebanyakan merupakan komputer di kedutaan besar telah disadap.[25]

Dalam laporannya yang berjudul *Tracking GhostNet : Investigating a Cyber Espionage Network*, IVM mengklaim bahwa dari 1300 komputer yang disadap 30% (tiga puluh persen) diantaranya dapat dikategorikan sebagai jaringan komputer yang bernilai tinggi karena merupakan jaringan komputer yang dimiliki oleh Kementrian Luar Negeri Iran, Banglades, Latvia, Indonesia, Filipina, Brunei, Barbados dan Bhutan; Kedutaan Besar India, Korea Selatan, Indonesia, Romania, Siprus, Malta, Thailand, Taiwan, Portugal, Jerman dan Pakistan. Selain itu *Cyberspy* tersebut juga terjadi pada jaringan komputer milik sekreatariat ASEAN (*Association of East Asian Nation*) SAARC (*South Asian Association for Regional Cooperation*), ADB (*Asian Development Bank*), beberapa kantor berita dan komputer rahasia yang ada di markas NATO.[26] Cara *Cyberspy* ini dilakukan dengan cara memasukan sebuah program (*Malware*) yang bernama *GhostNet* dalam kurun waktu 2007-2008.[27]

Dalam melakukan penelitiannya IWM melakukan dua metode. Metode yang pertama adalah dengan melakukan penelitian lapangan di India, Eropa dan Amerika Utara dengan fokus di Dharmsala, India, tempat pemerintahan pengasingan Tibet berada[28]. IWM melakukan wawancara dengan staf-staf pemerintahan pengasingan Tibet sehubungan dengan dugaan *Cyberspy* ini. Metode yang kedua adalah dengan melakukan pemantauan secara viritual dengan menggunakan empat *server* serta menggunakan metode *IP lookup*[29] dan menggunakan sebuah *software* yang bernama *GhostRat*.

Kesimpulan dari penelitian yang dilakukan oleh IWM menunjukkan bahwa dari 986 *Internet Protocol* (*IP*) yang di teliti Taiwan memiliki jumlah komputer terbanyak yang diduga ternifeksi *malware* ini yaitu sebanyak 148 komputer diikuti

---

[24] Major Cyberspy Network Uncovered, http://news.bbc.co.uk/2/hi/americas/7970471.stm ,d iakses tanggal 25 Juni 2009

[25] Chinese Cyberspy Networks Hacks into 103 Nations, www.independent.co.uk/.../**chinese-cyber-spy**-network-hacks-into-103-nations-1657045.html ,diakses tanggal 10 Juni 2009

[26] Information Warfare Monitor, *Tracking GhostNet : Investigating a Cyber Espionage Network*, 29 March 2009, hal 5

[27] *Ibid.*, hal 44

[28] *Ibid.*, hal 14

[29] *IP Lookup* adalah metode untuk mengetahui lokasi sebuah komputer dengan cara melihat *Internet Protocol* (IP) tempat komputer tersebut berada, data yang dihasilkan cukup lengkap mulai dari negara tempat komputer tersebut berada sampai siapa yang menggunakan komputer tersebut

oleh Amerikas Serikat sebanyak 113 komputer, sementara Indonesia sendiri diduga sebanyak 13 komputer telah terinfeksi dimana infeksi yang terbanyak terdapat di Departemen Luar Negeri dan sekretariat ASEAN dan oleh IVM komputer-komputer tersebut diklasifikasikan sebagai *High Confidentiality* .[30]

Jika dikaitkan dengan hukum Indonesia, maka pelaku *cyberspy* dapat diadili di Indonesia, tidak perlu mempermasalahkan status kewarganegaraan si pelaku karena perbuatannya telah merugikan Indonesia. Hal ini diatur dalam pasal 2 UU ITE mengenai yurisdiksi berlakunya hukum Indonesia.[31] Jika dilihat dari perbuatannya yang diatur dalam *Convention on Cybercrime* maka *cyberspy* termasuk ke dalam golongan *illegal access* dan *data interception.*

Penjelasan dari pernyataan diatas adalah ketika seseorang memasuki sebuah komputer atau jaringan komputer yang sebenarnya dia tidak berhak maka ia telah melakukan sebuah *illegal access*, dalam hal *cyberspy* si pelaku untuk melaksanakan niatnya, yaitu melakukan penyadapan, harus terlebih dahulu menembus sebuah komputer atau jaringan komputer yang sebenarnya si pelaku tidak mempunyai hak untuk mengaksessnya. Sedangkan penyadapan (*spying*) terhadap sebuah komputer atau jaringan komputer termasuk ke dalam jenis *data interception.*[32]

Apabila hukum Indonesia yang diberlakukan kepada pelaku *cyberspy*, maka pasal yang dapat didakwakan kepada si pelaku adalah :

1. Pasal 56 *jo.* Pasal 40 Undang-Undang Telekomunikasi
2. Pasal 46-47 *jo.* Pasal 30-31 Undang-Undang Informasi dan Transaksi Elektronik
3. Pasal 54-55 Undang-Undang Keterbukaan Informasi Publik.

Jadi kesimpulan yang dapat ditarik adalah jika kasus *cyberspy* terjadi dan perbuatannya merugikan Indonesia, maka hukum Indonesia dapat diterapkan berdasarkan ketentuan perundang-undangan yang berlaku.

---

[30] *Ibid.*, hal 41-43

[31] Pasal 2 UU ITE Berbunyi :

Undang-Undang ini berlaku untuk setiap Orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang - Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia

[32] Convention on Cybercrime, pasal 3

BAB 5
PENUTUP

5.1. Kesimpulan

Setelah melakukan penelitian yang telah dijabarkan pada bab-bab sebelumnya, maka penulis berkesimpulan sebagai berikut :

1. Pengaturan terhadap yurisdiksi dalam hukum internasional khusus mengenai *cybercrime* diatur dalam *Convention on Cybercrime*. Permasalahan yurisdiksi dalam *Convention on Cybercrime* yang dibuat oleh Dewan Eropa, secara khusus ditempatkan pada pasal tersendiri yakini pada pasal 22. Pasal yang terdiri dari lima ayat tersebut antara lain berbunyi sebagai berikut :

Berdasarkan uraian mengenai Pasal 22 beserta penjelasannya diatas, dapat dilihat bahwa *Convention on Cybercrime* ciptaan Dewan Eropa ternyata masih menggunakan konsep yurisdiksi yang selama ini dikenal dan dipergunakan secara internasional. Selain itu, meskipun tidak secara tegas menyatakan dukungan terhadap konsep analogi, konvensi ini cenderung 'melepaskan' diri dari konsep pemisahan. Sikap ini dimaklumi, mengingat desakan untuk menciptakan hukum tersendiri terhadap *cyberspace* selama ini masih sebatas wacana yang terus berkembang dan praktis belum ada konsep yang jelas mengenai hal ini. Sementara disisi lain, intensitas kejahatan komputer yang merupakan dampak negatif dari kecanggihan komputer terus meningkat. Kondisi ini akan berbahaya dan dapat menimbulkan 'anarkisme' di *cyberspace* jika tidak segera dibuat suatu produk legislasi yang natinya berfungsi menertibkan segala aktivitas di *cyberspace*. Lebih jauh lagi, dengan adanya ketentuan mengenai yurisdiksi yang tercantum dalam Pasal 22, maka negara peserta konvensi mempunyai 'sandaran' hukum yang pasti dalam menerapkan yurisdiksinya terhadap *cybercrime* sehingga konflik yang potensial terjadi karena perebutan penerapan yurisdiksi dapat dihindari.

2. Sebelum berlakunya Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pengaturan mengenai *cybercrime* diatur dalam Undang-Undang No 36 Tahun 1990 tentang Telekomunikasi. Mengenai pengaturan tentang yurisdiksi dalam undang-undang ini tidak disebutkan secara gamblang pada pasal tertentu, namun dari pengaturan pasal 44 dapat disimpulkan bahwa apabila terjadi pelanggaran terhadap gangguan telekomunikasi maka yang diterapkan adalah hukum Indonesia.

Dari pengaturan tentang yurisdiksi diatas maka dapat disimpulkan bahwa undang-undang ini menganut prinsip *objective territoriality* (teritorial objektif), hal ini bisa dilihat dari perumusan pasal 38 yang menyatakan bahwa setiap orang dilarang untuk melakukan perbuatan yang dapat menggangu komunikasi. Berarti yang dilihat dari Pasal ini adalah akibat dari perbuatan yang dapat mengakibatkan terganggunya komunikasi tanpa melihat tempat dilakukannya kejahatan tersebut.

Setelah berlakunya Undang-Undang No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik ,maka pengaturan yurisdiksi diatur secara spesifik dalam pasal 2. Dari perumusan Pasal 2 dapat disimpulkan bahwa undang-undang ini menganut prinsip *objective territoriality* (teritorial objektif) karena yang lebih dilihat adalah akibat dari perbuatan yang ditimbulkan karena perbuatan yang di sebutkan dalam pasal-pasal tersebut. Kesimpulan akhir yang dapat ditarik adalah tidak adanya perubahan cara pandang mengenai pengaturan yurisdiksi baik dalam UU Telekomunikasi dengan UU ITE, kedua UU tersebut menganut prinsip *objective territoriality* (teritorial objektif) yang lebih mengutamakan akibat dari perbuatan daripada tempat dilakukannya perbuatan tersebut.

3. Kasus *cyberspy* bermula dari adanya temuan dari aktivis Tibet yang menemukan dugaan bahwa komputer mereka telah di sadap secara elektronik, lalu mereka meminta kepada Information Warfare Monitor (IWM) untuk mengadakan suatu penelitian. Hasilnya sungguh mengejutkan dimana diduga sekitar 1300 komputer di 103 negara, kebanyakan merupakan komputer di kedutaan besar telah disadap.Kesimpulan dari penelitian yang dilakukan oleh IWM menunjukkan bahwa dari 986 *Internet Protocol* (*IP*) yang di teliti Taiwan memiliki jumlah komputer terbanyak yang diduga ternifeksi *malware* ini yaitu sebanyak 148 komputer diikuti oleh Amerika Serikat sebanyak 113 komputer, sementara Indonesia sendiri diduga sebanyak 13 komputer telah terinfeksi dimana infeksi yang terbanyak terdapat di Departemen Luar Negeri dan sekretariat ASEAN dan oleh IVM komputer-komputer tersebut diklasifikasikan sebagai *High Confidentiality* .

Jika dikaitkan dengan keberlakuan hukum indonesia, maka perbuatan pelaku *cyberspy* dapat di dakwa dengan menggunakan ketentuan yang ada di Indonesia. Hal ini disebabkan bahwa setiap Pasal yang mengatur tentang yurisdiksi yang ada di peraturan perundang-undangan di Indonesia selalu menggunakan prinsip *objective territoriality* (teritorial objektif). Hal ini bisa kita lihat apabila kita bandingkan dua

undang-undang yang mengatur tentang *cybercrime*, yaitu Pasal 44 Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi dan Pasal 2 Undang-Undang No 11 Tahun 2008 tentang Information dan Transaksi Elektronik. Dari kedua Pasal diatas dapat ditarik kesimpulan bahwa yang dilihat dalam memberlakukan hukum Indonesia adalah akibat yang ditimbulkan dari perbuatan bukan tempat dilakukannnya perbuatan atau status kewarganegaraan si pelaku.

5.2. Saran

1. Pemerintah harus meratifikasi *Convention on Cybercrime* agar bisa menjalin kerja sama dengan peserta apabila terjadi kasus *cybercrime* yang merugikan Indonesia sekaligus menjalin kerjasama di bidang teknologi informasi agar Indonesia tidak ketinggalan dalam penanganan kasus *cybercrime*.

2. UU Informasi dan Transaksi Elektronik harus di amandemen agar sesuai dengan *Convention on Cybercrime* baik secara substantif maupun prosedural. Selain itu UU Keterbukaan Iinformasi Publik juga harus ditambahkan pengaturan mengenai yurisdiksi agar apabila terjadi penyalahgunaan informasi publik melalui *cyberspace* hukum Indonesia dapat di berlakukan.

3. Untuk mencegah data-data penting dan rahasia negara tidak dengan mudahnya diambil oleh pihak yang tidak bertanggungjawab dengan segala cara (di *hack* maupun di *spy*) maka pemerintah melalui Kementrian Komunikasi dan Informasi hendaknya mulai membangun sistem atau sebuah jaringan komputer yang memiliki sistem pengamanan yang tidak mudah di akses. Caranya adalah dengan menggunakan *firewall* yang berlapis serta *password* yang sulit untuk di pecahkan.

Daftar Pustaka

I. Buku, Artikel, Makalah dan Jurnal.

Arief Mansur, Dikdik M. dan Elisatris Gultom. *Cyber Law-Aspek Hukum Teknologi Informasi*, Cet.1. Bandung. PT Refika Aditama, 2005.

Barry, Colin. *the Future of Cyberterrorism*, Crime and Justice International, March 1997.

Burk, Dan L. *Jurisdiction in a World Without Border*. <www.cyberjurisdiction.net> , diakses tanggal 5 Mei 2009.

Connoly, Chris. *An Introduction to Internet Content Regulation in Asia and the Pacific*. Galexia intelligence reports, articles, papers, conferences and seminars. <www.galexia.com>, diakses pada tanggal 25 Juni 2009.

Dressler, Joshua. *ed. The Encyclopedia of Crime and Justice, edition* 2. New York. Macmillian Reference, 2001.

Granville, Johanna. *The Transnational Dimension of Cybercrime and Terrorism*. British Journal of Criminology volume .43, 2003.

Graycar, Adam. *Cybercrime: Old Wine in New Bottles?*. Makalah disampaikan dalam seminar dengan tema *Cybercrime* di Centre for Crimnology, The University of Hongkong, tanggal 24 Februari 2000.

Gregory Lastwoka, F and Dan Hutter. *Virtual Crime*. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=564801>, pada tanggal 5 Maret 2009.

Goodman, Mark D. and Susan W. Brenner. *The Emerging Consensus On Criminal Conduct in Cyberspace*. <http://www.lawtechjournal.com/articles/2002/03_020625_goodmanberner.php>. Diakses pada tanggal 1 April 2009.

Hariyanti Chandra, Francisca. *Internet:Information Superhighway*, Makalah pada Penataran Kualitas Dosen di Bidang Pengolahan Data dan Penyusunan Presentasi Melalui Media Komputer bagi Dosen PTS Kopertis Wilayah V1 di Semarang, 4-8 September 1995.

Hamano, Masaki. *Comparative Study I The Approach to Jurisdiction in Cyberspace*. <www.cyberjurisdiction.net>, diakses tanggal 13 Mei 2009.

Hamzah, Andi. *Aspek-aspek Pidana di Bidang Komputer*. Jakarta. Sinar Grafika, 1990.

Istijar, Muhammad. *Korupsi Kejahatan Luar Biasa*.<www.hokionline>, diakses pada 30 Juni 2009.

Johnson, David R. and David G. Post. *And How Should The Internet Be Governed?*. <www.itworld.com>, diakses tanggal 13 Mei 2009.

Keyser, Mike. *The Council of Europe Convention on Cybercrime*. Journal of Transnational Law and Policy, volume 12, 2003.

Lloyd, Ian J. *Information and Technology Law*. third edition. London. Butterworths. 2000.

Kanter, E.Y dan S.R Sianturi. *Asas-asas Hukum Pidana Di Indonesia Dan Penerapannya*, Cet.2. Jakarta. Storia Grafika, 2002.

Karnasudirja. Eddy Djunaidi. *Yurisprudensi Kejahatan Komputer*. Jakarta. CV. Tanjung Agung, 1993.

Nawawi Arief, Barda. *Kebijakan Kriminalisasi dan Masalah Yurisdiksi Tidak Pidana Maya Antara*. Makalah pada seminar nasional dalam rangka penyusunan RUU teknologi informasi.

Makarim, Edmon. *Kompilasi Hukum Telematika*, cet kedua. Jakarta. Rajagrafindo, 2003.

Menthe, Darrel. *Jurisdiction in Cyberspace : A Theory of International Spaces*. <www.mttlr.org/volfour/menthe_art.html> , diakses pada tanggal 20 April 2009.

Murphy, John F. *Civil Liability for the Commision of International Crimes as an Alternative to Criminal Prosecution*. Harvard Human Rights Journal 9 th edition 2007

Oberding, Juliet M. and Treje Norderhaug. *A Separate Jurisdiction for Cyberspace*. <www.cyberjurisdiction.net> , diakses pada 16 Mei 2009.

Pattiradjawane. Rene L. *Cyberlaw: Apakah bisa Melindungi Pribadi Pengguna Internet?*. <www.kompas.com>, diakses tanggal 23 Mei 2009.

Post, David G. *Anarchy, State and The Internet: An Essay on Law Making in Cyberspace*. Journal of Online Law, 1995.

Purbo, Onno W. Sejarah Internet, <www.ilmukomputer.com> , diakses pada tanggal 15 Maret 2009.

Rasch, Mark D. *Criminal Law and The Internet*. <www.cybercrime.net>, diakses tanggal 20 April.

Rahardjo, Agus. *Cybercrime :Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*. Bandung. Citra Aditya, 2002.

Ramli, Ahmad M. *Cyberlaw dan HaKI Dalam Sistem Hukum Indonesia*, cet-1. Bandung. PT Refika Aditama, 2004.

Reinhard Golose, Peter. *Perkembangan Cybercrime dan Penanganannya di Indonesia oleh POLRI*. Makalah disampaikan pada seminar nasional mengenai "Penanganan *Cybercrime* di Indonesia ke Arah Pengembangan Kebijakan Menyeluruh dan Terpadu", tanggal 10 Agustus 2006.

Roden, Adrian. *Computer Crime and The Law*. Criminal Law Journal, 1991.

Sanford, Kadish and May T Morrison. *ed.Encyclopedia of Crime and Justice*",Law University of California, Berkeley, Volume I.

Sarwoko, Djoko. *Computer Crime sebagai Dimensi Baru Tindak Pidana Ekonomi*. Varia Peradilan Nomor 21 Tahun II, Juni 1987.

Starke, J.G. *Introduction to International Law*. 9th ed. London. Butterworths, 2000

Sudirman, Ivan dan Romi Satria. *Sejarah Komputer*. Makalah disampaikan pada Training Ilmu Komputer,bahan didownload dari <www.ilmukomputer.com>,

Sood, Vivek. *Cyber Law Simplified*. New Delhi. Tata McGraw-Hill Publishing Co.Ltd, 2001.

Sutadi, Heru. *"Cybercrime, apa yang bisa diperbuat?"*, <http://www.sinarharapanbaru.co.id/berita/0304/05/op01.html>, diakses tanggal 15 April 2009.

UNESCO. *The International Demension of Cyberspace Law*. England. Ashgate Publishing Ltd., 2000.

Wilske, Stephen and Teresa Schiller. *International Jurisdiction in Cyberspace: Which States May Regulate The Internet*. <www.cyberjurisdiction.net> , diakses tanggal 23 Mei 2009.

Wisnubroto, A.L. *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer*. Yogjakarta. Penerbitan Universitas Atmajaya, 2001.

II. Konvensi Internasional dan Peraturan Perundang-undangan.

Council of Europe, *Convention on Cybercrime*.

Indonesia, Undang-Undang Tentang Telekomunikasi No. 36 Tahun 1999, Lembaran Negara No. 154 Tahun 1999, tambahan lembaran negara No. 3881

Indonesia, Undang-Undang Tentang Informasi dan Transaksi Elektronik No 11 Tahun 2009, Lembaran Negara No.

Indonesia, Undang-Undang Tentang Keterbukaan Informasi Publik No. 14 Tahun 2008, Lembaran Negara No. 61 Tahun 2008, Tambahan Lembaran Negara No. 4846

III. Sumber Lainnya

Gobal Internet Policy Initiative. *Trust and Security in Cyberspace :The Legal and Policy Framework for Adressing Cybercrime*, 2005.

Information Warfare Monitor.*Tracking GhostNet : Investigating a Cyber Espionage Network*, 29 March 2009.

Major Cyberspy Network Uncovered, <http://news.bbc.co.uk/2/hi/americas/7970471.stm> , diakses tanggal 25 Juni 2009.

Chinese Cyberspy Networks Hacks into 103 Nations, <www.independent.co.uk/.../**chinese-cyber-spy**-network-hacks-into-103-nations-1657045.html> ,diakses tanggal 10 Juni 2009.

Prita Mulyasari Hari Ini Didakwa , www.hukumonline.com, diakses pada tanggal 29 Juni 2009.

RS OMNI dapatkan pasien dari hasil lab fiktif, <http://suarapembaca.detik.com/read/2008/08/30/111736/997265/283/rs-omni-dapatkan-pasien-dari-hasil-lab-fiktif >, diakses tanggal 25 Juni 2009.

Anggara, UU ITE merupakan ancaman bagi bloger indonesia, <http://anggara.org/2008/03/26/uu-informasi-dan-transaksi-elektronik-adalah-ancaman-serius-bagi-bolger-indonesia/>, diakses tanggal 1 Juli 2009.

Daftar Lampiran

1. Pasal 22 *Convention on Cybercrime*.
2. Pasal 34, 40 dan 44 Undang-Undang No. 36 Tahun 1999 Tentang Telekomunikasi.
3. Pasal 2, 27-31 Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.
4. Pasal 54 dan 55 Undang-Undang No. 14 Tahun 2008 Tentang Keterbukaan Informasi Publik.
5. Laporan *Interntional Warfare Monitor* yang berjudul *Tracking GhostNet* : *Investigating a Cyber Espionage Network*.
6. Surat Pembaca yang ditulis oleh Prita Mulyasari.

Lampiran 1

Pasal 22 Convention on Cybercrime

Article 22 – Jurisdiction

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a in its territory; or

b on board a ship flying the flag of that Party; or

c on board an aircraft registered under the laws of that Party; or

d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Lampiran 2

Pasal 38, 40, 44 dan Penjelasannya UU No. 36 Tahun 1999 tentang Telekomunikasi

Pasal 38

Setiap orang dilarang melakukan perbuatan yang dapat menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi

Pasal 40

Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melaiui jaringan telekomunikasi dalam bentuk apapun.

Pasal 44

(1) Selain Penyidik Pejabat Polisi Negara Republik Indonesia, juga Pejabat Pegawai Negeri Sipil tertentu di Iingkungan Departemen yang Iingkup tugas dan tanggung jawabnya di bidang telekomunikasi, diberi wewenang khusus sebagai penyidik sebagaimana dimaksud dalam Undang-undang Hukum Acara Pidana untuk melakukan penyidikan tindak pidana di bidang telekomunikasi.

(2) Penyidik Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) berwenang :

a. melakukan pemeriksaan atas kebenaran Iaporan atau keterangan berkenaan dengan tindak pidana di bidang telekomunikasi;
b. melakukan pemeriksaan terhadap orang dan atau badan hukum yang diduga melakukan tindak pidana di bidang telekomunikasi;
c. menghentikan penggunaan alat dan atau perangkat telekomunikasi yang menyimpang dari ketentuan yang berlaku;
d. memanggil orang untuk didengar dan diperiksa sebagai saksi atau tersangka;
e. melakukan pemeriksaan alat dan atau perangkat telekomunikasi yang diduga digunakan atau diduga berkaitan dengan tindak pidana di bidang telekomunikasi;
f. menggeledah tempat yang diduga digunakan untuk melakukan tindak pidana di bidang telekomunikasi;

Pejelasan

Pasal 38

Perbuatan yang dapat menimbulkan gangguan terhadap penyelenggaraan telekomunikasi dapat berupa :

a. tindakan fisik yang menimbulkan kerusakan suatu jaringan telekomunikasi sehingga jaringan tersebut tidak dapat berfungsi sebagaimana mestinya;
b. tindakan fisik yang mengakibatkan hubungan telekomunikasi tidak berjalan sebagaimana mestinya;
c. penggunaaan alat telekomunikasi yang tidak sesuai dengan persyaratan teknis yang berlaku;
d. penggunaan alat telekomunikasi yang bekerja dengan gelombang radio yang tidak sebagaimana mestinya sehingga menimbulkan gangguan terhadap penyelenggaraan telekomunikasi Iainnya; atau

e. penggunaan alat bukan telekomunikasi yang tidak sebagaimana mestinya sehingga menimbulkan pengaruh teknis yang tidak dikehendaki suatu penyelenggaraan telekomunikasi.

Pasal 40

Yang dimaksud dengan penyadapan dalam pasal ini adalah kegiatan memasang alat atau perangkat tambahan pada jaringan telekomunikasi untuk tujuan mendapatkan informasi dengan cara tidak sah. Pada dasarnya informasi yang dimiliki oleh seseorang adalah hak pribadi yang harus dilindungi sehingga penyadapan harus dilarang.

Pasal 44

Ayat (1)

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Lampiran 3

Pasal 2, 27-32 Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Pasal 2

Undang Undang ini berlaku untuk setiap Orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.

Pasal 27

(1)Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.

(2)Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.

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

(4)Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

Pasal 28

(1)Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.

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

Pasal 29

Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut nakuti yang ditujukan secara pribadi.

Pasal 30

(1)Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.

(2)Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

(3)Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Pasal 31

(1)Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.

(2)Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang

menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.

(3)Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hokum lainnya yang ditetapkan berdasarkan undang undang.

(4)Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 32

(1)Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

Lampiran 5

Surat Pembaca yang ditulis oleh Prita Mulyasari

(http://suarapembaca.detik.com/read/2008/08/30/111736/997265/283/rs-omni-dapatkan-pasien-dari-hasil-lab-fiktif)

RS OMNI Dapatkan Pasien Dari Hasil Lab Fiktif.

Jangan sampai kejadian saya ini akan menimpa ke nyawa manusia lainnya. Terutama anak-anak, lansia, dan bayi. Bila anda berobat berhati-hatilah dengan kemewahan rumah sakit (RS) dan title international karena semakin mewah RS dan semakin pintar dokter maka semakin sering uji coba pasien, penjualan obat, dan suntikan.

Saya tidak mengatakan semua RS international seperti ini tapi saya mengalami kejadian ini di RS Omni International. Tepatnya tanggal 7 Agustus 2008 jam 20.30 WIB. Saya dengan kondisi panas tinggi dan pusing kepala datang ke RS OMNI Internasional dengan percaya bahwa RS tersebut berstandard International, yang tentunya pasti mempunyai ahli kedokteran dan manajemen yang bagus.

Saya diminta ke UGD dan mulai diperiksa suhu badan saya dan hasilnya 39 derajat. Setelah itu dilakukan pemeriksaan darah dan hasilnya adalah thrombosit saya 27.000 dengan kondisi normalnya adalah 200.000. Saya diinformasikan dan ditangani oleh dr Indah (umum) dan dinyatakan saya wajib rawat inap. dr I melakukan pemeriksaan lab ulang dengan sample darah saya yang sama dan hasilnya dinyatakan masih sama yaitu thrombosit 27.000.

dr I menanyakan dokter specialist mana yang akan saya gunakan. Tapi, saya meminta referensi darinya karena saya sama sekali buta dengan RS ini. Lalu referensi dr I adalah dr H. dr H memeriksa kondisi saya dan saya menanyakan saya sakit apa dan dijelaskan bahwa ini sudah positif demam berdarah.

Mulai malam itu saya diinfus dan diberi suntikan tanpa penjelasan atau izin pasien atau keluarga pasien suntikan tersebut untuk apa. Keesokan pagi, dr H visit saya dan menginformasikan bahwa ada revisi hasil lab semalam. Bukan 27.000 tapi 181.000 (hasil lab bisa dilakukan revisi?). Saya kaget tapi dr H terus memberikan instruksi ke suster

perawat supaya diberikan berbagai macam suntikan yang saya tidak tahu dan tanpa izin pasien atau keluarga pasien.

Saya tanya kembali jadi saya sakit apa sebenarnya dan tetap masih sama dengan jawaban semalam bahwa saya kena demam berdarah. Saya sangat khawatir karena di rumah saya memiliki 2 anak yang masih batita. Jadi saya lebih memilih berpikir positif tentang RS dan dokter ini supaya saya cepat sembuh dan saya percaya saya ditangani oleh dokter profesional standard Internatonal.

Mulai Jumat terebut saya diberikan berbagai macam suntikan yang setiap suntik tidak ada keterangan apa pun dari suster perawat, dan setiap saya meminta keterangan tidak mendapatkan jawaban yang memuaskan. Lebih terkesan suster hanya menjalankan perintah dokter dan pasien harus menerimanya. Satu boks lemari pasien penuh dengan infus dan suntikan disertai banyak ampul.

Tangan kiri saya mulai membengkak. Saya minta dihentikan infus dan suntikan dan minta ketemu dengan dr H. Namun, dokter tidak datang sampai saya dipindahkan ke ruangan. Lama kelamaan suhu badan saya makin naik kembali ke 39 derajat dan datang dokter pengganti yang saya juga tidak tahu dokter apa. Setelah dicek dokter tersebut hanya mengatakan akan menunggu dr H saja.

Esoknya dr H datang sore hari dengan hanya menjelaskan ke suster untuk memberikan obat berupa suntikan lagi. Saya tanyakan ke dokter tersebut saya sakit apa sebenarnya dan dijelaskan saya kena virus udara. Saya tanyakan berarti bukan kena demam berdarah. Tapi, dr H tetap menjelaskan bahwa demam berdarah tetap virus udara. Saya dipasangkan kembali infus sebelah kanan dan kembali diberikan suntikan yang sakit sekali.

Malamnya saya diberikan suntikan 2 ampul sekaligus dan saya terserang sesak napas selama 15 menit dan diberikan oxygen. Dokter jaga datang namun hanya berkata menunggu dr H saja.

Jadi malam itu saya masih dalam kondisi infus. Padahal tangan kanan saya pun mengalami pembengkakan seperti tangan kiri saya. Saya minta dengan paksa untuk diberhentikan infusnya dan menolak dilakukan suntikan dan obat-obatan.

Esoknya saya dan keluarga menuntut dr H untuk ketemu dengan kami. Namun, janji selalu diulur-ulur dan baru datang malam hari. Suami dan kakak-kakak saya menuntut penjelasan dr H mengenai sakit saya, suntikan, hasil lab awal yang 27.000 menjadi revisi

181.000 dan serangan sesak napas yang dalam riwayat hidup saya belum pernah terjadi. Kondisi saya makin parah dengan membengkaknya leher kiri dan mata kiri.

dr H tidak memberikan penjelasan dengan memuaskan. Dokter tersebut malah mulai memberikan instruksi ke suster untuk diberikan obat-obatan kembali dan menyuruh tidak digunakan infus kembali. Kami berdebat mengenai kondisi saya dan meminta dr H bertanggung jawab mengenai ini dari hasil lab yang pertama yang seharusnya saya bisa rawat jalan saja. dr H menyalahkan bagian lab dan tidak bisa memberikan keterangan yang memuaskan.

Keesokannya kondisi saya makin parah dengan leher kanan saya juga mulai membengkak dan panas kembali menjadi 39 derajat. Namun, saya tetap tidak mau dirawat di RS ini lagi dan mau pindah ke RS lain. Tapi, saya membutuhkan data medis yang lengkap dan lagi-lagi saya dipermainkan dengan diberikan data medis yang fiktif.

Dalam catatan medis diberikan keterangan bahwa bab (buang air besar) saya lancar padahal itu kesulitan saya semenjak dirawat di RS ini tapi tidak ada follow up-nya sama sekali. Lalu hasil lab yang diberikan adalah hasil thrombosit saya yang 181.000 bukan 27.000.

Saya ngotot untuk diberikan data medis hasil lab 27.000 namun sangat dikagetkan bahwa hasil lab 27.000 tersebut tidak dicetak dan yang tercetak adalah 181.000. Kepala lab saat itu adalah dr M dan setelah saya komplain dan marah-marah dokter tersebut mengatakan bahwa catatan hasil lab 27.000 tersebut ada di Manajemen Omni. Maka saya desak untuk bertemu langsung dengan Manajemen yang memegang hasil lab tersebut.

Saya mengajukan komplain tertulis ke Manajemen Omni dan diterima oleh Og(Customer Service Coordinator) dan saya minta tanda terima. Dalam tanda terima tersebut hanya ditulis saran bukan komplain. Saya benar-benar dipermainkan oleh Manajemen Omni dengan staff Og yang tidak ada service-nya sama sekali ke customer melainkan seperti mencemooh tindakan saya meminta tanda terima pengajuan komplain tertulis.

Dalam kondisi sakit saya dan suami saya ketemu dengan Manajemen. Atas nama Og (Customer Service Coordinator) dan dr G (Customer Service Manager) dan diminta memberikan keterangan kembali mengenai kejadian yang terjadi dengan saya.

Saya benar-benar habis kesabaran dan saya hanya meminta surat pernyataan dari lab RS ini mengenai hasil lab awal saya adalah 27.000 bukan 181.000. Makanya saya diwajibkan masuk ke RS ini padahal dengan kondisi thrombosit 181.000 saya masih bisa rawat jalan.
Tanggapan dr G yang katanya adalah penanggung jawab masalah komplain saya ini tidak profesional sama sekali. Tidak menanggapi komplain dengan baik. Dia mengelak bahwa lab telah memberikan hasil lab 27.000 sesuai dr M informasikan ke saya. Saya minta duduk bareng antara lab, Manajemen, dan dr H. Namun, tidak bisa dilakukan dengan alasan akan dirundingkan ke atas (Manajemen) dan berjanji akan memberikan surat tersebut jam 4 sore.
Setelah itu saya ke RS lain dan masuk ke perawatan dalam kondisi saya dimasukkan dalam ruangan isolasi karena virus saya ini menular. Menurut analisa ini adalah sakitnya anak-anak yaitu sakit gondongan namun sudah parah karena sudah membengkak. Kalau kena orang dewasa laki-laki bisa terjadi impoten dan perempuan ke pankreas dan kista.
Saya lemas mendengarnya dan benar-benar marah dengan RS Omni yang telah membohongi saya dengan analisa sakit demam berdarah dan sudah diberikan suntikan macam-macam dengan dosis tinggi sehingga mengalami sesak napas. Saya tanyakan mengenai suntikan tersebut ke RS yang baru ini dan memang saya tidak kuat dengan suntikan dosis tinggi sehingga terjadi sesak napas.
Suami saya datang kembali ke RS Omni menagih surat hasil lab 27.000 tersebut namun malah dihadapkan ke perundingan yang tidak jelas dan meminta diberikan waktu besok pagi datang langsung ke rumah saya. Keesokan paginya saya tunggu kabar orang rumah sampai jam 12 siang belum ada orang yang datang dari Omni memberikan surat tersebut.
Saya telepon dr G sebagai penanggung jawab kompain dan diberikan keterangan bahwa kurirnya baru mau jalan ke rumah saya. Namun, sampai jam 4 sore saya tunggu dan ternyata belum ada juga yang datang ke rumah saya. Kembali saya telepon dr G dan dia mengatakan bahwa sudah dikirim dan ada tanda terima atas nama Rukiah.
Ini benar-benar kebohongan RS yang keterlaluan sekali. Di rumah saya tidak ada nama Rukiah. Saya minta disebutkan alamat jelas saya dan mencari datanya sulit sekali dan membutuhkan waktu yang lama. LOgkanya dalam tanda terima tentunya ada alamat jelas surat tertujunya ke mana kan? Makanya saya sebut Manajemen Omni pembohon besar semua. Hati-hati dengan permainan mereka yang mempermainkan nyawa orang.

Terutama dr G dan Og, tidak ada sopan santun dan etika mengenai pelayanan customer, tidak sesuai dengan standard international yang RS ini cantum.

Saya bilang ke dr G, akan datang ke Omni untuk mengambil surat tersebut dan ketika suami saya datang ke Omni hanya dititipkan ke resepsionis saja dan pas dibaca isi suratnya sungguh membuat sakit hati kami.

Pihak manajemen hanya menyebutkan mohon maaf atas ketidaknyamanan kami dan tidak disebutkan mengenai kesalahan lab awal yang menyebutkan 27.000 dan dilakukan revisi 181.000 dan diberikan suntikan yang mengakibatkan kondisi kesehatan makin memburuk dari sebelum masuk ke RS Omni.

Kenapa saya dan suami saya ngotot dengan surat tersebut? Karena saya ingin tahu bahwa sebenarnya hasil lab 27.000 itu benar ada atau fiktif saja supaya RS Omni mendapatkan pasien rawat inap.

Dan setelah beberapa kali kami ditipu dengan janji maka sebenarnya adalah hasil lab saya 27.000 adalah fiktif dan yang sebenarnya saya tidak perlu rawat inap dan tidak perlu ada suntikan dan sesak napas dan kesehatan saya tidak makin parah karena bisa langsung tertangani dengan baik.

Saya dirugikan secara kesehatan. Mungkin dikarenakan biaya RS ini dengan asuransi makanya RS ini seenaknya mengambil limit asuransi saya semaksimal mungkin. Tapi, RS ini tidak memperdulikan efek dari keserakahan ini.

Sdr Og menyarankan saya bertemu dengan direktur operasional RS Omni (dr B). Namun, saya dan suami saya sudah terlalu lelah mengikuti permainan kebohongan mereka dengan kondisi saya masih sakit dan dirawat di RS lain.

Syukur Alhamdulilah saya mulai membaik namun ada kondisi mata saya yang selaput atasnya robek dan terkena virus sehingga penglihatan saya tidak jelas dan apabila terkena sinar saya tidak tahan dan ini membutuhkan waktu yang cukup untuk menyembuhkan.

Setiap kehidupan manusia pasti ada jalan hidup dan nasibnya masing-masing. Benar. Tapi, apabila nyawa manusia dipermainkan oleh sebuah RS yang dipercaya untuk menyembuhkan malah mempermainkan sungguh mengecewakan.

Semoga Allah memberikan hati nurani ke Manajemen dan dokter RS Omni supaya diingatkan kembali bahwa mereka juga punya keluarga, anak, orang tua yang tentunya

suatu saat juga sakit dan membutuhkan medis. Mudah-mudahan tidak terjadi seperti yang saya alami di RS Omni ini.

Saya sangat mengharapkan mudah-mudahan salah satu pembaca adalah karyawan atau dokter atau Manajemen RS Omni. Tolong sampaikan ke dr G, dr H, dr M, dan Og bahwa jangan sampai pekerjaan mulia kalian sia-sia hanya demi perusahaan Anda. Saya informasikan juga dr H praktek di RSCM juga. Saya tidak mengatakan RSCM buruk tapi lebih hati-hati dengan perawatan medis dari dokter ini.

Salam,

Prita Mulyasari
Alam Sutera
prita.mulyasari@yahoo.com
081513100600

JR02-2009

Tracking *GhostNet*:

Investigating a *Cyber Espionage* Network

Information Warfare Monitor

March 29, 2009

TheSecDevGroup

University of Toronto
Munk Centre
For International Studies
At Trinity College

http://www.infowar-monitor.net/ghostnet
http://www.tracking-ghost.net

March 29, 2009

Foreword

Cyber espionage is an issue whose time has come. In this second report from the Information Warfare Monitor, we lay out the findings of a 10-month investigation of alleged Chinese cyber spying against Tibetan institutions.

The investigation, consisting of fieldwork, technical scouting, and laboratory analysis, discovered a lot more.

The investigation ultimately uncovered a network of over 1,295 infected hosts in 103 countries. Up to 30% of the infected hosts are considered high-value targets and include computers located at ministries of foreign affairs, embassies, international organizations, news media, and NGOs. The Tibetan computer systems we manually investigated, and from which our investigations began, were conclusively compromised by multiple infections that gave attackers unprecedented access to potentially sensitive information.

But the study clearly raises more questions than it answers.

From the evidence at hand, it is not clear whether the attacker(s) really knew what they had penetrated, or if the information was ever exploited for commercial or intelligence value.

Some may conclude that what we lay out here points definitively to China as the culprit. Certainly Chinese cyber-espionage is a major global concern. Chinese authorities have made it clear that they consider cyberspace a strategic domain, one which helps redress the military imbalance between China and the rest of the world (particularly the United States). They have correctly identified cyberspace as the strategic fulcrum upon which U.S. military and economic dominance depends.

But attributing all Chinese malware to deliberate or targeted intelligence gathering operations by the Chinese state is wrong and misleading. Numbers can tell a different story. China is presently the world's largest Internet population. The sheer number of young digital natives online can more than account for the increase in Chinese malware. With more creative people using computers, it's expected that China (and Chinese individuals) will account for a larger proportion of cybercrime.

Likewise, the threshold for engaging in cyber espionage is falling. Cybercrime kits are now available online, and their use is clearly on the rise, in some cases by organized crime and other private actors. Socially engineered malware is the most common and potent; it introduces Trojans onto a system, and then exploits social contacts and files to propagate infections further.

Furthermore, the Internet was never built with security in mind. As institutions ranging from governments through to businesses and individuals depend on 24-hour Internet connectivity, the opportunities for exploiting these systems increases.

This report serves as a wake-up call. At the very least, a large percentage of high-value targets compromised by this network demonstrate the relative ease with which a technically unsophisticated approach can quickly be harnessed to create a very effective spynet…These are major disruptive capabilities that the professional information security community, as well as policymakers, need to come to terms with rapidly.

These are major disruptive capabilities that the professional information security community, as well as policymakers, need to come to terms with rapidly.

Ron Deibert, Director, the Citizen Lab,
Munk Centre for International Studies,
University of Toronto.

Rafal Rohozinski, Principal and CEO,
The SecDev Group,
Ottawa, Canada.

Acknowledgements

This investigation was prepared by a dedicated team of professionals.

Greg Walton conducted and coordinated the primary field-based research in India, Tibetan Missions abroad, and Europe. Greg is a SecDev Group associate and editor of the Information Warfare Monitor website. He is currently a SecDev Fellow at the Citizen Lab. The Indian portion of the field work benefited from the expertise of Dr. Shishir Nagaraja, Security Laboratory, Cambridge University. Dr. Nagaraga visited Dharamsala for a period of five days in September to assist on aspects of the technical data collection.[1]

The technical scouting and computer network interrogation was carried out by Nart Villenueve. Nart is the CTO of Psiphon Inc, and the Psiphon Fellow at the Citizen Lab. His investigations included the discovery and exploration of the *GhostNet* control servers. He led the data analysis research, which included log files gathered in the field, as well as data obtained through technical scouting of the *GhostNet* control servers.

This report represents a collective effort. The drafting team consisted of the following individuals (listed in alphabetical order). Ronald Deibert (Citizen Lab), Arnav Manchanda (SecDev Group), Rafal Rohozinski (SecDev Group and Psiphon Inc.), Nart Villeneuve (Psiphon Fellow, Citizen Lab) and Greg Walton (SecDev Fellow, Citizen Lab). Layout and design was led by Jane Gowan (Psiphon Inc. and Citizen Lab). Belinda Bruce (Blurb Media) and James Tay (Citizen Lab), provided additional support to the team.

Countless others also contributed to the research effort. This includes individuals in India and Tibet, who for security reasons we cannot name. We are also grateful to the Private Office of his Holiness the Dalai Lama, the Tibetan Government-in-Exile, the missions of Tibet in London, Brussels, and New York, and Drewla (a Tibetan NGO).

1 Aspects of the research carried out by Dr. Nagaraga focusing on socially engineered malware are published in a separate study. See, *The snooping dragon: social-malware surveillance of the Tibetan movement*, Shishir Nagaraja, Ross Anderson, Cambridge University Computer Laboratory Technical Report, Mar 29 2009

Summary

Trojan horse programmes and other associated malware are often cited as vectors for conducting sophisticated computer-based espionage. Allegations of cyber espionage (computer network exploitation) are increasingly common, but there are few case studies in the unclassified realm that expose the inner workings of such networks.

This study reveals the existence and operational reach of a malware-based cyber espionage network that we call *GhostNet*.

Between June 2008 and March 2009 the Information Warfare Monitor conducted an extensive and exhaustive two-phase investigation focused on allegations of Chinese cyber espionage against the Tibetan community.

We conducted field-based investigations in India, Europe and North America. In India we worked directly with affected Tibetan organizations, including the Private Office of the Dalai Lama, the Tibetan Government-in-Exile, and several Tibetan NGOs. In Europe and North America we worked with Tibetan missions in London, Brussels, and New York. The fieldwork generated extensive data that allowed us to examine Tibetan information security practices, as well as capture *real-time* evidence of malware that had penetrated Tibetan computer systems.

During the second phase of our investigation, the data was analyzed, and led to the discovery of insecure, web-based interfaces to four control servers. These interfaces allow attacker(s) to send instructions to, and receive data from, compromised computers. Our research team successfully scouted these servers, revealing a wide-ranging network of compromised computers. This extensive network consists of at least 1,295 infected computers in 103 countries.

Significantly, close to 30% of the infected computers can be considered high-value and include the ministries of foreign affairs of Iran, Bangladesh, Latvia, Indonesia, Philippines, Brunei, Barbados and Bhutan; embassies of India, South Korea, Indonesia, Romania, Cyprus, Malta, Thailand, Taiwan, Portugal, Germany and Pakistan; the ASEAN (Association of Southeast Asian Nations) Secretariat, SAARC (South Asian Association for Regional Cooperation), and the Asian Development Bank; news organizations; and an unclassified computer located at NATO headquarters.

The *GhostNet* system directs infected computers to download a Trojan known as *gh0st RAT* that allows attackers to gain complete, *real-time* control. These instances of *gh0st RAT* are consistently controlled from commercial Internet access accounts located on the island of Hainan, People's Republic of China.

Our investigation reveals that *GhostNet* is capable of taking full control of infected computers, including searching and downloading specific files, and covertly operating attached devices, including microphones and web cameras.

The vector for spreading the *GhostNet* infection leverages social means. Contextually relevant emails are sent to specific targets with attached documents that are packed with *exploit code* and Trojan

horse programmes designed to take advantage of vulnerabilities in software installed on the target's computer.

Once compromised, files located on infected computers may be mined for contact information, and used to spread malware through e-mail and document attachments that appear to come from legitimate sources, and contain legitimate documents and messages. It is therefore possible that the large percentage of high value targets identified in our analysis of the *GhostNet* are coincidental, spread by contact between individuals who previously communicated through e-mail.

Nonetheless the existence of the *GhostNet* network is a significant fact in and of itself. At the very least, it demonstrates the ease by which computer-based malware can be used to build a robust, low-cost intelligence capability and infect a network of potentially high-value targets.

Key findings:

- **Documented evidence of a cyber espionage network—*GhostNet*—infecting at least 1,295 computers in 103 countries, of which close to 30% can be considered as high-value diplomatic, political, economic, and military targets.**

- **Documented evidence of *GhostNet* penetration of computer systems containing sensitive and secret information at the private offices of the Dalai Lama and other Tibetan targets.**

- **Documentation and reverse engineering of the *modus operandi* of the *GhostNet* system—including vectors, targeting, delivery mechanisms, data retrieval and control systems—reveals a covert, difficult-to-detect and elaborate cyber-espionage system capable of taking full control of affected systems.**

Introduction

Computer network exploitation represents the leading edge of signals intelligence in the information age. The proliferation of computer systems throughout governments, businesses, and civic organizations represents a boon for would-be cyber spies.

Awareness of cyber vulnerabilities, and even basic information security practices, is in its infancy, and largely absent in most organizations outside of the classified realm. Commercial computer systems, which represent most of the world's installed base, are insecure. This lack of security consciousness is reflective of the infancy of the information age. The Internet was never designed for security and, for the most part, there has been little incentive for software manufacturers to make security a first priority in the design and development of products, many of which are destined for consumer and/or small business use.

These challenges are present in advanced industrial societies, but are amplified many times over in developing countries. Ownership of computers is a relative rarity among many government departments. Where they exist, they often use grey market or pirated software. Resources are lacking to employ properly trained computer professionals, and many staff are barely computer literate. In this context, information security is often a distant priority.

And yet, computers in the hands of individuals or at government offices, ministries, embassies, and civic and non-governmental organizations contain information that can be valuable. Files and e-mails with contact information, lists of meetings and attendees, draft position papers, internal PowerPoint presentations, organizational budgets, and lists of visitors can represent items of strategic value to rivals and enemies. Organizations, like individuals, can be subject to identity theft, leading to potentially serious breaches of security.

Rise of the cyber spies

Little is known of the sophistication of state-based cyber espionage capabilities, such as those of the United States, Israel, and the United Kingdom, all considered leaders in this field. They are assumed to be considerable as the security doctrines of these countries treat cyberspace as a strategic domain equivalent to that of land, air, sea, and space.[2]

Other powers including China have made cyberspace a key pillar of their national security strategies. China is actively developing an operational capacity in cyberspace, correctly identifying it as the domain in which it can achieve strategic parity, if not superiority, over the military establishments of the United States and its allies. Chinese cyber warfare doctrine is well developed, and significant resources have been invested by the People's Liberation Army and security services in developing defensive and offensive capabilities.[3]

---

2 http://www.dod.mil/pubs/foi/ojcs/07-F-2105doc1.pdf ; http://www.afa.org/media/reports/victorycyberspace.pdf

3 http://findarticles.com/p/articles/mi_m0PBZ/is_6_88/ai_n31140190 ; http://www.infowar-monitor.net/modules.php?op=modload&name=Archive&file=index&req=viewarticle&artid=2&page=1

But the most significant actors in cyberspace are not states. The online engagements that accompanied the recent Russia-Georgia conflict in August 2008[4] and Israel's January 2009 offensive in Gaza[5] were carried out by independent attackers. The May 2007 denial of service attacks against Estonia[6] resulted in a single conviction of a Russian living in Estonia. Likewise, previous high-profile investigations of hacking against strategic U.S. targets were never positively attributed to foreign intelligence services[7], and in many cases were the work of individuals.[8]

The contest in the shadows currently underway in cyberspace appears to rely largely on third parties. In numerous instances, including case studies conducted by the Information Warfare Monitor's sister project, the OpenNet Initiative, third party attackers were responsible for triggering national-level cyber events. In Kyrgyzstan (2005)[9], Belarus (2006)[10], during the Russia Georgia war (2008), and Kyrgyzstan (2009), individuals and/or loose coalitions were responsible for publishing target lists and attack tools on semi-private websites. The ensuing "cyclones in cyberspace" were sufficient to precipitate events outside of cyberspace.[11]

International cooperation has for the most part focused on establishing capabilities for counteracting the criminal use of cyberspace, and with good reason. In 2009, the FBI estimated that cybercrime is responsible for over $10 billion worth of losses each year.[12] Cybercrime is a relatively low cost, low threshold activity. Techniques such as phishing and targeted malware are easy to construct, and the chances of prosecution are minimal given a general lack of international coordination.

This is slowly changing as national and international authorities become more aware of the threat. The attacks on Estonia, for example, led to the establishment of NATO's Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia.[13] The International Telecommunication Union has also established its own specialized agency, IMPACT, designed to aid intelligence sharing and tracking of

---

4 http://blog.wired.com/defense/2008/10/government-and.html ; http://www.slate.com/id/2197514

5 http://www.csmonitor.com/2009/0123/p04s03-wome.html

6 http://www.webpronews.com/topnews/2008/01/24/man-convicted-in-estonia-cyber-attack

7 For example, a US government investigation of systematic hacking of Department of Defense networks and defence laboratories dubbed 'Titan Rain' never provided conclusive evidence to substantiate allegations that the hacking was conducted at the behest of the Chinese government. http://www.time.com/time/magazine/article/0,9171,1098961,00.html

8 A good example is the 1998 'Solar Sunrise' investigation. The evidence gathered by US authorities eventually led to the conviction of an Israeli citizen, Ehud Tenebaum, although the involvement of Israeli security services was never proven. http://www.sans.org/resources/idfaq/solar_sunrise.php

9 http://opennet.net/special/kg/

10 http://opennet.net/sites/opennet.net/files/ONI_Belarus_Country_Study.pdf

11 http://www.infowar-monitor.net/modules.php?op=modload&name=News&file=article&sid=2146

12 http://kn.theiet.org/magazine/issues/0903/hacking-goes-pro-0903.cfm

13 http://www.nato.int/docu/update/2008/05-may/e0514a.html

malicious criminal activity in cyberspace.[14] Countries such as the United States, Russia and China have also entered into bilateral agreements with allied countries and partners.

A focus on China

Recent allegations of Chinese cyber espionage largely rely on anecdotal evidence. The most common proof provided by victims of these attacks consists of log files or malware that shows connections being made by infected computers to IP addresses assigned to the People's Republic of China.

This kind of evidence is circumstantial at best. Internet usage statistics suggest that focusing on Chinese instances of information warfare is misleading.[15] With 41% of the world's Internet users located in Asia, China alone accounts for the largest national population of Internet users—some 300 million, nearly one-fifth of the global number of users. Coupled with the rapid growth in Chinese use of the Internet—a 1,200% increase in the period 2000-2008—this would more than account for the rise in instances of Chinese-oriented malware.[16]

At the same time, however, allegations of Chinese hacking and exploitation of private and government computer systems are persistent enough to warrant an evidence-based investigation.

This report provides such an investigation.

Outline of report

This report is divided into **three parts**:

Part one provides a brief introduction to the context and background to this report. We examine past allegations of cyber espionage by China-based actors and the challenge of evidence-based research in this field. Part one concludes with a brief description of the methods used in our two-phase investigation.

Part two provides a detailed account of the conduct of our investigation. The findings of each phase are presented sequentially.

Part three analyses the overall findings of the investigation, suggests alternative explanations and assesses the implications.

---

14 http://www.itu.int/osg/csd/cybersecurity/gca/impact/index.html

15 For global Internet usage statistics please see http://www.internetworldstats.com

16 http://blog.stopbadware.org/2009/03/03/wheres-the-badware

PART ONE:
Context and background

Context and background: Alleged Chinese operations in cyberspace

China has been developing its cyberspace doctrine and capabilities since the late 1990s as part of its military modernization programme. The Chinese doctrine of 'active defence,' which is the belief that China must be ready to respond to aggression immediately, places an emphasis on the development of cyber warfare capabilities.

The Chinese focus on cyber capabilities as part of its strategy of national asymmetric warfare involves deliberately developing capabilities that circumvent U.S. superiority in command-and-control warfare. The strategy recognizes the critical importance of the cyber domain to American military and economic power and the importance of offensive cyber operations to victory in a modern conflict with the United States. Chinese doctrine also emphasizes the contiguity between military and non-military realms.[17]

In recent years, there has been an increase in allegations that China-based hackers are responsible for high-level penetrations of computer systems in Europe, North America and Asia. Attackers originating in China have been accused of infiltrating government computers in the United States, Britain, France, Germany, South Korea, and Taiwan. China-based hackers have been accused of data theft from foreign government computers and commercial and financial institutions. The U.S. Department of Defense reports it is continuously targeted by Chinese attackers, most notably in the series of attacks since 2003 known as 'Titan Rain,' which targeted the Department of Defense and numerous defence companies.[18]

There are also allegations of attacks originating from China directed against non-governmental organizations active in regions where China has a national interest. This includes organizations advocating on the conflict in the Darfur region of Sudan,[19] Tibetan groups active in India, and the Falun Gong. The majority of attacks involve website defacements, denial of service attacks, or virus writing campaigns. Nationalistic and patriotic cyber-activity by Chinese nationals intensifies during crises, such as during Sino-American or Sino-Taiwanese tensions (see below). To date none of these attacks have been traced back to Chinese state authorities or specific individuals, although many have benefited official Chinese policy and interests.

---

17 http://findarticles.com/p/articles/mi_m0PBZ/is_6_88/ai_n31140190 ; http://www.infowar-monitor.net/modules.php?op=modload&name=Archive&file=index&req=viewarticle&artid=2&page=1 ; http://www.heritage.org/Research/asiaandthepacific/upload/bg_2106.pdf

18 http://www.time.com/time/magazine/article/0,9171,1098961,00.html ; http://findarticles.com/p/articles/mi_m0PBZ/is_6_88/ai_n31140190 ; http://www.afa.org/media/reports/victorycyberspace.pdf

19 http://www.insidetech.com/news/articles/1630-mysterious-forces-hack-pro-tibet-save-darfur-sites ; http://www.washingtonpost.com/wp-dyn/content/article/2008/03/20/AR2008032003193.html

Applying the evidence-based approach to cyber attacks: the challenge of attribution

Determining those responsible for cyber attacks, commonly known as the *attribution problem*, is a major challenge. The Internet was never built with security as a priority. The current version of the Internet's address assignment system, IP V4, provides a wealth of loopholes and methods by which a perpetrator can mask his or her real identity and location. Online identities and servers can be cleverly hidden. Packet flows and connections can be masked and redirected through multiple servers. A clever attacker can often hijack a machine belonging to an otherwise innocent organization and use it as a base for launching attacks.

Hand-in-hand with the problem of attribution is the difficulty of identifying motivating factors behind a cyber attack. Many perpetrators of Internet-based attacks and exploits are individuals whose motivation can vary from a simple profit motive through to fear of prosecution or strong emotional feelings, including religious belief and nationalism. Many cyber attacks and exploits which *seem* to benefit states may be the work of third-party actors operating under a variety of motivations. This makes it difficult to separate the motivation of the individual from the potential motives of the party on whose behalf the attacks have occurred, or a prospective client to which the perpetrator is trying to market his or her wares. In either case, the challenge of identifying perpetrators and understanding their motives gives state actors convenient *plausible deniability* and the ability to officially distance themselves from attacks.

Cyber campaigns can also take on a life of their own. Even though a state might 'seed' a particular campaign through tacit encouragement or the absence of sanctions or prosecutions, these campaigns are inherently chaotic and unpredictable in scope and outcome.[20] Phenomena such as spontaneous 'cyber rioting' can surpass the initial purposes of the cyber campaign. Low barriers to entry to this sort of activity enable anyone with a computer and Internet connection to take part in a cyber-attack.[21] For the most part, governments appear to passively benefit from online manifestations of nationalistic and patriotic fervour, although outcomes are inherently unpredictable.[22]

In China, the authorities most likely perceive individual attackers and their online activities as convenient instruments of national power.[23] A favourite target of Chinese hackers is Taiwanese computer systems, especially during times of Sino-Taiwanese tensions, such as elections and

---

20 http://www.yorku.ca/robarts/projects/canada-watch/obama/pdfs/Deibert.pdf

21 http://worldanalysis.net/modules/news/article.php?storyid=343

22 For instance, during the Russia-Georgia conflict in August 2008, tools were made available online for those who wished to participate in the ongoing 'cyber-war' against Georgian websites. http://blog.wired.com/defense/2008/10/government-and.html ; http://www.slate.com/id/2197514

23 http://findarticles.com/p/articles/mi_m0PBZ/is_6_88/ai_n31140190 ; http://fmso.leavenworth.army.mil/documents/Beijings-rising-hackers.pdf

referendums.[24] In April 2001, following the death of a Chinese fighter pilot after a collision with an American spy plane near the Chinese island of Hainan, Chinese hackers began a sustained campaign to target American computer networks. No link was made with elements of the Chinese government.[25]

However, governments cannot always preserve direct control over such activities; groups can maintain their freelance and autonomous status and undertake their own cyber initiatives that may not always attain official sanction or serve state interests.[26]

Targeting Tibet

Accusations of Chinese *cyber war* being waged against the Tibetan community have been commonplace for the past several years. The Chinese government has been accused of orchestrating and encouraging such activity as part of a wider strategy to crack down on dissident groups and subversive activity.[27] Earlier research has traced these attacks against Tibetan groups to IP addresses registered in the People's Republic of China. The attacks used malware hidden in legitimate-looking email messages, infecting unsuspecting users' computers and exploiting the data on it by sending it to control servers.[28]

The identity of the attackers has never been attributed in a conclusive manner to any specific group or individual.[29] The motivation of those behind the attacks, despite conjecture, is also unproven.

In earlier studies, researchers focused on attacks specifically targeting the Tibetan community. But a wide variety of other victims of computer penetrations have reported infections similar to those used against Tibetan organizations, following a similar *modus operandi* and also reporting to control servers usually located in China. These additional targets include the Falun Gong[30], the U.S. Government, and multinational corporations.[31] While reports of these targeted attacks have circulated, the extent to which attackers successfully exploited the affected computers is unknown.

---

24 http://fmso.leavenworth.army.mil/documents/Beijings-rising-hackers.pdf

25 http://news.bbc.co.uk/2/hi/americas/1305755.stm

26 http://fmso.leavenworth.army.mil/documents/Beijings-rising-hackers.pdf

27 http://www.washingtonpost.com/wp-dyn/content/article/2008/03/21/AR2008032102605.html

28 See, http://isc.sans.org/diary.html?storyid=4177 ; http://isc.sans.org/diary.html?storyid=4176 and http://archive.cert.uni-stuttgart.de/isn/2002/09/msg00086.html for background information on these attacks.

29 Attribution for previous penetrations of Tibetan groups has never been publicly attributed and is not available from open sources. Classified studies may reveal a finer grained detail, as many of the attacks are relatively unsophisticated, and given proper assets, could be traced back to specific locations and presumably individuals.

30 Research by Maarten Van Horenbeeck shows that similar attacks have targeted the Falun Gong. http://www.daemon.be/maarten/Crouching_Powerpoint_Hidden_Trojan_24C3.pdf and http://isc.sans.org/presentations/SANSFIRE2008-Is_Troy_Burning_Vanhorenbeeck.pdf

31 See http://www.businessweek.com/print/magazine/content/08_16/b4080032218430.htm

Conduct of the investigation

From June 2008 to March 2009 the Information Warfare Monitor conducted an in-depth investigation of alleged cyber espionage against the Tibetan community. We chose this case study because of the unprecedented access that we were granted to Tibetan institutions through one of our researchers, and persistent allegations that confidential information on secure computers was somehow being compromised. Our lead field investigator had a long history of working with the Tibetan community, and was able to work with the private office of the Dalai Lama, the Tibetan Government-in-Exile, and a number of Tibetan non-governmental organizations.

The investigation consisted of two distinct phases.

Phase 1: Field-based investigations in India, Europe, and North America (June-November 2008)

Field research was carried out in Dharamsala, India, the location of the Tibetan Government-in-Exile. Follow-up research was conducted at Tibetan missions abroad in London, Brussels and New York. During this phase we had unprecedented access to the Tibetan government and other Tibetan organizations. This allowed us to establish a baseline understanding of information security practices at these locations and to design an evidence-based approach to the investigation.

We also conducted extensive on-site interviews with officials in the Tibetan Government-in-Exile, the private office of the Dalai Lama, and Tibetan non-governmental organizations. The interviews focused on the allegations of cyber espionage. We also sought alternative explanations for leakage of confidential documents and information and examined basic information security practices at these locations.

Network monitoring software was installed on various computers so as to collect forensic technical data from affected computer systems, and initial results were analysed *in situ*.[32] This initial analysis confirmed the existence of malware and the transfer of information between infected computers and a number of control servers.[33]

Phase 2: Computer-based scouting, target selection, and data analysis (December 2008-March 2009)

During the second phase of the investigation, researchers based at the Citizen Lab analysed the data collected by the field team.

The data collected in Dharamsala and at Tibetan missions abroad led to the discovery of four control servers and six command servers. These control servers were identified and geo-located from the captured

---

32 A portion of the fieldwork was carried out in conjunction with Dr. Shishir Nagaraja who spent five days in Dharamsala at the request of IWM researchers and assisted in conducting technical tests.

33 A packet capturing program, Wireshark, was installed at each test location. All traffic from each of the affected systems was captured in real-time, and recorded for further analysis. Compromised systems try to connect to control servers in order check-in and report an infection. Once a connection is made, infected computers may receive instructions or additional locations from where they are to download instructions. The Wireshark data is sufficient to analyse these connections, determine the behaviour of the attack vector, and identify the location of control servers.

traffic using a simple IP lookup.[34] The control servers were then probed and web-based control interfaces were identified on four control servers, which allowed us to view and control the network. The system was actively monitored for two weeks, which allowed us to derive an extensive list of infected systems, and to also monitor the systems operator(s) as the operator(s) specifically instructed target computers.

The data collected during both phases was integrated in Palantir, a data visualization and analysis tool. The Palantir platform provides a data fusion and visualization environment that enhances analytical capabilities.

34 We looked up the associated Internet Protocol (IP) address in all five Regional Internet Registries in order to identify the country and network to which the IP address is assigned. We then performed a reverse Domain Name System (DNS) look-up on each IP address. DNS is the system that translates domain names into IP addresses; reverse DNS is a system that translates an IP address into a domain name. This can potentially provide additional information about the entity that has been assigned a particular IP address. If we discovered a domain name, we then looked up its registration in WHOIS, which is a public database of all domain name registrations and provides information about who registered the domain name.

PART TWO:
Tracking *GhostNet*

Phase 1: Field investigation

We conducted our investigation in Dharamsala between July and September 2008. The initial purpose was to gather targeted malware samples from Tibetan NGOs based in the area and to brief the Tibetan Government-in-Exile (TGIE) on the basics of information security. This included raising end-user awareness about social engineering and its policy implications for the secure use of information systems.

The investigator met with the Dalai Lama's representative in Geneva, Tseten Samdup. During the meeting, Samdup inquired about the potential threat to computer security at the Office of His Holiness the Dalai Lama (OHHDL) in light of the targeted malware threat. Samdup requested that the investigator perform a preliminary security review of OHHDL systems, including Dalailama.com and the office computer network. A five day mission was scheduled in early September. Malware was discovered on computers located in the OHHDL.

Following the discovery of malware in the OHHDL, our investigator shifted focus to the campus network of the Tibetan Government-in-Exile. We approached Thubten Samphel, a senior civil servant in the Department for Information and International Relations, and sought permission to run Wireshark on several key computer systems, and to access the firewall logs at the Tibetan Computing Resource Centre. This access was readily granted.

Additional testing was carried out at a Tibetan NGO. This was done at the suggestion of Phuntsok Dorjee, the director of a local NGO, TibTec. Dorjee suggested that we conduct testing and monitoring at the offices of Drewla.[35] As was the case at other sitesthe investigator conducted a series of interviews with the NGO staff.

Targeted malware — previous research

In September 2002, Tibetan groups reported that they were targeted with malware originating from servers in mainland China. They claimed that this was a coordinated attempt to disrupt their operations and *spy* on their computer networks. Similar attacks have occurred since then against a range of Tibetan non-state actors, including exile groups, human rights organizations, trade unions and labour organizers, writers, scholars and intellectuals.

In 2005, a member of our investigating team convened a working group that coordinated the collection and archiving of the malware, including the payloads and associated examples of social engineering employed. Since early 2008, we have analysed every sample available to us, and identified control servers for at least fifty incidents.

During an analysis of attacks which occurred during the 2008 Beijing Olympics we discovered the location of a control server that was later identified as part of the network which infected a computer in the private office of the Dalai Lama.

---

35 The Drewla Initiative Project is an outreach model that seeks new ways to communicate directly with citizens of the People's Republic of China. It relies heavily on the Internet.

We were able to gain access to the command *interface* of this control server and identify the infected computers which reported back to this server. While were are unable to prove exactly how the computer in the Dalai Lama's office became infected, this case demonstrates one of the attack vectors used by the attacker(s) behind the network of infected computers we later uncovered.[36]

The following steps illustrate the attack vector using the malicious document we collected, which was configured to connect to a control server to which we later acquired access. (**See Fig. 1** - p.19)

An email message arrives in the target's inbox carrying the malware in an attachment or web link. The attackers(s)' objective is to get the target to open the attachment or malicious link so that the malicious code can execute. In this case, the attacker(s) sent a carefully crafted email message which was configured to appear as if it was sent from campaigns@freetibet.org with an attached infected Word document named "Translation of Freedom Movement ID Book for Tibetans in Exile.doc" to entice the recipient to open the file.[37] (**See Fig. 2** - p. 20)

Over time, it has been observed that the carrier emails have become more sophisticated in their targeting and content in order to trick their recipients into believing that they are receiving legitimate messages. This is also known as "social engineering." It is common to see legitimate documents recycled for such attacks or the attacker injecting their message into an ongoing group conversation. There are also cases where it appears that content stolen from previously-infected machines was recycled to enhance the appearance of legitimacy.

The targeted user proceeds to opens the attachment or malicious link. Once opened, the infected file or link exploits a vulnerability on the user's machine and installs the malware on the user's computer, along with a seemingly benign file. From the user's perspective, the infected document will often open normally, leaving the user unaware of the infection that just took place.

Only 11 of the 34 anti-virus programs provided by Virus Total[38] recognized the malware embedded in the document. Attackers often use executable packers to obfuscate their malicious code in order to avoid detection by anti-virus software. (**See Fig. 3** - p. 21)

Researchers monitoring the use of socially engineered malware attacks against the Tibetan community have identified over eight different Trojan families in use.[39] Control over some targeted machines is maintained using the Chinese *gh0st RAT* (Remote Access Tool). These Trojans generally allow for near-unrestricted access to the infected systems.

---

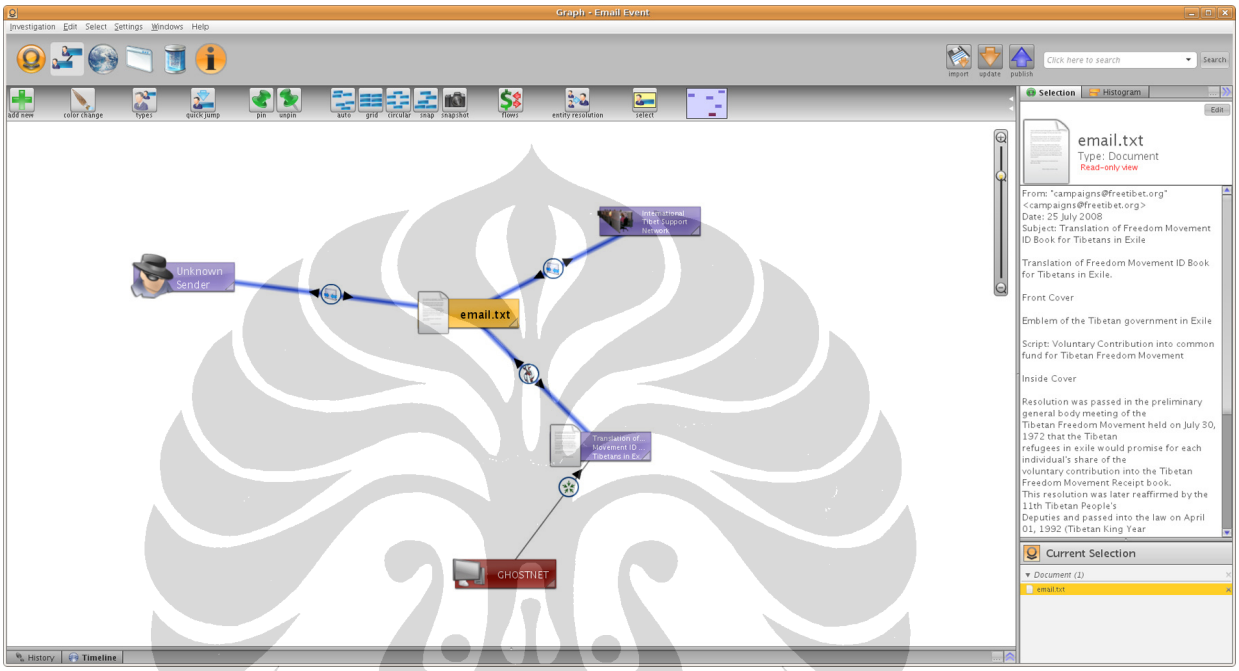
36 A detailed technical investigation of a similar case of a targeted attack which connected to the same control server is available here: [redacted] another investigation of targeted attacks connecting to the same control server is available here: [redacted]

37 For a detailed list of malicious files and control servers see [redacted]

38 VirusTotal.com is a free, web-based service that allows users to upload malicious files that are scanned with 34 leading anti-virus products.

39 http://isc.sans.org/diary.html?storyid=4177

Fig. 1
A "Social Engineering" attack connects to GhostNet.



This Palantir screen capture summarizes the relationships between an "unknown sender" pretending to be "campaigns@freetibet.org", the email sent to the International Tibet Support Network , and the attachment ("Translation of Freedom Movement ID Book for Tibetans in Exile.doc") that contained malware that connected to a *GhostNet* control server.

Fig. 2

A "Socially Engineered" email sent to the International Tibet Support Network.

From: "campaigns@freetibet.org" <campaigns@freetibet.org>
Date: 25 July 2008
Subject: Translation of Freedom Movement ID Book for Tibetans in Exile

Translation of Freedom Movement ID Book for Tibetans in Exile.

Front Cover

Emblem of the Tibetan government in Exile

Script: Voluntary Contribution into common fund for Tibetan Freedom Movement

Inside Cover

Resolution was passed in the preliminary general body meeting of the Tibetan Freedom Movement held on July 30, 1972 that the Tibetan refugees in exile would promise for each individual,Äôs share of the voluntary contribution into the Tibetan Freedom Movement Receipt book. This resolution was later reaffirmed by the 11th Tibetan People,Äôs Deputies and passed into the law on April 01, 1992 (Tibetan King Year 2119)

Until the last page of this book is used, the book stands valid until August 15, 2012

Date: August 16, 2008
Emblem of the Tibetan Government in Exile

Official Signature

Attachment: Translation of Freedom Movement ID Book for Tibetans in Exile.doc

This email was sent on July 25, 2008 by an unknown attacker pretending to be "campaigns@freetibet.org" to the International Tibet Support Network. Attached to the message was a Microsoft Word document named "Translation of Freedom Movement ID Book for Tibetans in Exile.doc" that exploits a vulnerability in Word to install malware on the target's computer system.

Fig. 3
A Virus Total screen capture of a malware infected email attachment.

Antivirus	Version	Last Update	Result
AntiVir	-	-	EXP/Word.Dropper.Gen
Authentium	-	-	CVE-2006-2492
Avast	-	-	MW97:CVE-2006-2492
eTrust-Vet	-	-	W97M/SmartTags!exploit
F-Prot	-	-	CVE-2006-2492
Fortinet	-	-	MSWord/ObjPointer.A!exploit.M20062492
GData	-	-	MW97:CVE-2006-2492
Ikarus	-	-	Virus.MW97.CVE.2006.2492
Microsoft	-	-	Exploit:Win32/Wordjmp.gen
Sophos	-	-	Troj/MalDoc-Fam
Webwasher-Gateway	-	-	Exploit.Word.Dropper.Gen

This is a screen capture from VirusTotal.com, a free, web-based service that allows users to upload malicious files that are scanned with anti-virus products. It shows that only 11 of 34 anti-virus products detected the malicious file ("Translation of Freedom Movement ID Book for Tibetans in Exile.doc").

After infecting the target, the Trojan packed in the Word document performed a DNS look-up to find its control server and then connected to that server. This Trojan attempted to connect to [redacted]. This is one of the control servers that we later scouted and was in the same Trojan family that infected computers in the Dalai Lama's private office.

About 70% of the control servers behind the attacks on Tibetan organizations are located on IP addresses assigned to China. However, servers have also been identified in the United States, Sweden, South Korea and Taiwan. The host names pointing to these servers are quite often configured on dynamic DNS services, such as 3322.org. While these services in and of themselves are not malicious, they are heavily used in these specific attacks.[40]

Information Warfare Monitor field research

In September and October 2008 the Information Warfare Monitor investigated information security practices and alleged cyber espionage activities on the computer systems in various offices related to the work of the Dalai Lama and other Tibetan groups. The offices that we investigated were: the Office of His Holiness the Dalai Lama (OHHDL), based in Dharamsala, India; the Tibetan Government-in-Exile (TGIE); various Offices of Tibet (OOT) in New York City, London, Paris, Brussels, and Geneva; and the Tibetan activist NGO, Drewla. (**See Fig. 4** - p. 23)

Office of His Holiness the Dalai Lama

The OHHDL is the personal office of the Dalai Lama. The OHHDL provides secretarial assistance and is responsible for all matters related to the Dalai Lama and acts on his behalf. It is worth noting that the OHHDL's primary responsibilities include organization of the Dalai Lama's international schedule, handling all diplomatic, governmental and personal correspondence, and acting as the liaison between the Dalai Lama and officials of the Tibetan Government-in-Exile (TGIE) and the Offices of Tibet (OOT) worldwide. Therefore the OHHDL's computer network is continuously transmitting and receiving extremely sensitive data.

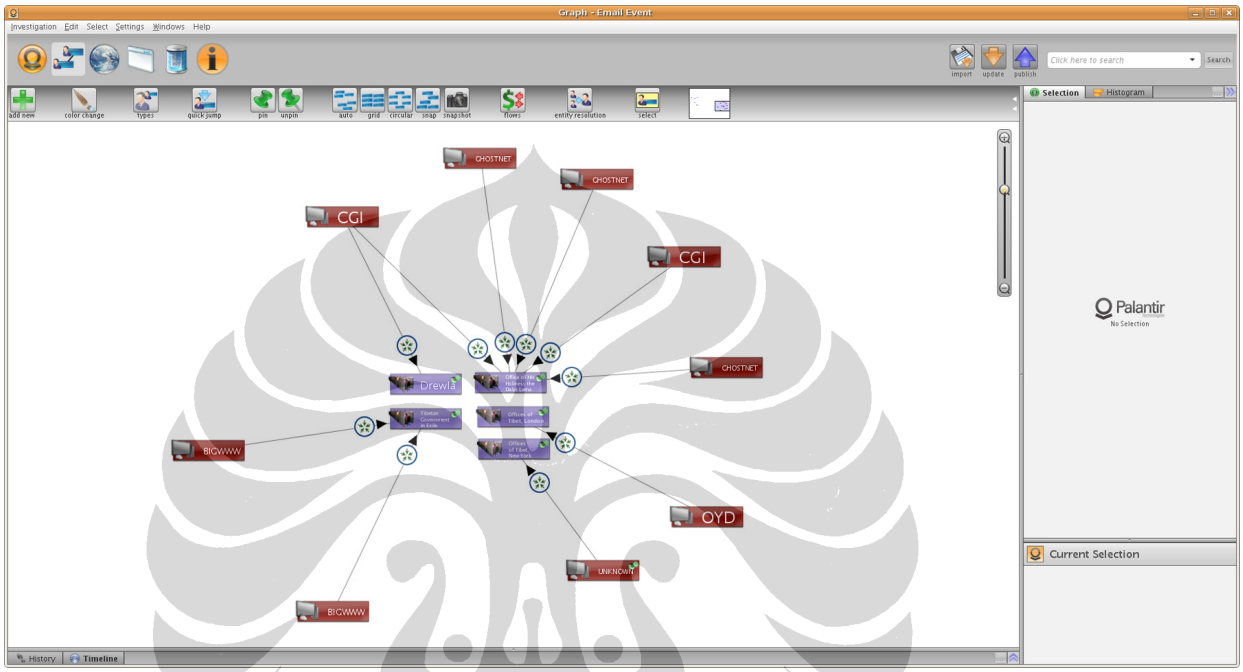
While the Office does not have any *secrets*, it is essentially the hub of the Tibetan movement and thus handles strategic, time-sensitive communications. Examples of these communications include scheduling meetings with world leaders, and, since 2002, coordinating the negotiations between the People's Republic of China and Dharamsala.

On September 10, 2008, we used Wireshark to capture packets from an OHHDL computer named [redacted] We chose [redacted] from among 23 computers on the OHHDL internal network due to time constraints and consultations with office staff to identify the computers most likely to be infected, such as those operated by relatively inexperienced users vulnerable to social engineering techniques, or those handling particularly sensitive data.

An analysis of the data collected reveals that this computer was compromised by malware that was in interactive communication with identified control servers. The infected computer connected to

40 http://www.businessweek.com/print/magazine/content/08_16/b4080032218430.htm

Fig. 4
Field researchers discovered malware at five Tibetan locations.



A Palantir screen capture showing the Tibetan organizations at which we conducted field research and the connections from infected computers at these locations and various control servers located in China. The locations at which we found evidence of infection are: the Office of His Holiness the Dalai Lama, the Tibetan Government-in-Exile, the Offices of Tibet in New York City and London and the Tibetan activist NGO, Drewla.

four different IP addresses, each with a somewhat different method. While there are four groupings of communications between the infected computer and the control servers, they are related such that there appear to be two distinct families of malware. In both cases, the malware uses the protocol for standard web traffic, HTTP, in order make the network activity appear as if it were normal Internet browsing.

The first family of malware used HTTP connections to connect to PHP files.[41] Despite connecting to different IP addresses and requesting different files, both used the same unique key when communicating, indicating that they are part of the same family of malware.

1) The malware made connections to a control server on IP address [redacted] using two host names, [redacted] and [redacted]. The IP address [redacted] is in a range assigned to Hainan-TELECOM [redacted] in China. The malware used HTTP to connect to various PHP files on the control server in order to update its status and receive instructions about where to download commands. The commands are embedded in what appear to be image files (e.g. JPEG).

2) The malware made connections to a control server on IP address [redacted], port 8000. This IP address reverse resolved to [redacted].broad.hk.hi.dynamic.163data.com.cn and is in an IP range assigned to Hainan-TELECOM (HAIFU node adsl dialup ports) in China. The malware used HTTP POST to upload content to the control server.[42]

The investigation carried out in Phase 2 identified the network of control servers used in this particular attack. The control servers we discovered include the control server used in the well-documented instances of social malware used frequently against Tibetan targets during the 2008 Olympics in Beijing.

The second family of malware used HTTP POST to connect to a CGI[43] script to communicate between the infected computer and the control server. While their functions appear to be different, with one malware focusing on reporting and commands and the other on document retrieval, they are likely part of the same family of malware. In addition, the domain names used, www.lookbytheway.net and www.macfeeresponse.org, are registered to the same person, "zhou zhaojun" (losttemp33@hotmail.com).

1) The malware made connections to a control server on IP address 221.5.250.98 using the host name www.lookbytheway.net. The IP address 221.5.250.98 is assigned to CNCGROUP-CQ (CNC Group CHINA169 Chongqing Province Network) in China. The malware on the infected computer used HTTP to connect to a file in an attempt to inform the control server of the infected computer's status and to download commands.

---

41 PHP is a popular scripting language often used in web applications.

42 HTTP POST is a method often used to upload content to a web server.

43 CGI scripts are often written in the Perl programming language.

In one case, the file the infected computer was requesting was not present and the infected computer received a 404 error. However, successful connections were made via HTTP to CGI scripts. The infected computer used HTTP POST to submit data to CGI scripts hosted on the control server.

2) The malware made connections to a control server on 218.241.153.61 using the host name www.macfeeresponse.org. The IP address 218.241.153.61 is assigned to BITNET (Beijing Bitone United Networks) in Beijing, China. The malware on the infected computer used HTTP to connect to a file to inform the control server of the infected computer's status and download commands. In addition, connections were made via HTTP to CGI scripts. The infected computer used HTTP POST to submit data to CGI scripts hosted on the control server. Connections to one CGI script appear to inform the control server of the presence of particular documents, while connections to a second CGI script appear to cause the infected computer to upload documents to the control server using HTTP POST.

Instances of malware that connect to control server locations www.lookbytheway.net and www.macfeeresponse.org have been analysed by security companies.[44] This network extends to a variety of domain names including:

- www.lookbytheway.com – 210.51.7.155
- www.macfeeresponse.com - 210.51.7.155
- www.msnppt.net - 221.5.250.98
- www.msnxy.net - 210.51.7.155
- www.msnyf.com - 221.5.250.98
- www.networkcia.com - 210.51.7.155
- www.indexnews.org - 61.188.87.58
- www.indexindian.com - 210.51.7.155

During the *in situ* investigation at the Dalai Lama's private office we observed several documents being exfiltrated from the computer network and uploaded to www.macfeeresponse.org, including a document containing thousands of email addresses and one detailing and discussing the Dalai Lama's envoy's negotiating position. (**see Fig. 5** - p. 26)

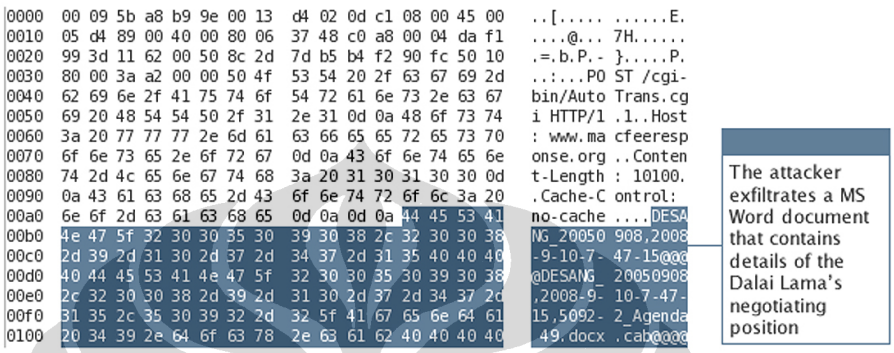
Our investigators did not have access to the stolen documents for reasons of confidentiality. However, we can assume their significance to Sino-Tibetan negotiations. One example is the fact that *GhostNet* penetrated computers of organizations involved in China-TGIE negotiations.[45]

---

44 See, http://www.threatexpert.com/report.aspx?md5=79f7f4695b8878cf1760e8626129ca88 and http://www.threatexpert.com/report.aspx?md5=ea03a7359505e19146994ad77b2a1e46

45 Lodi Gyari is the lead person designated by the Dalai Lama to coordinate negotiations with the Chinese government. Our invesigator interviewed him in December 2008 in Delhi. We briefed him on our ongoing investigation and offered advice on information security while engaged in negotiations in Beijing. Lodi Gyari is also the Executive Chairman of the Board of the International Campaign for Tibet (ICT), an independent Washington-based human rights advocacy group. (Note that our investigation uncovered that seven of ICT's computers were compromised by *GhostNet*).

Fig. 5
Malware retrieving a sensitive document.



This screen capture of the Wireshark network analysis tool shows an infected computer at the Office of His Holiness the Dalai Lama uploading a sensitive document to one of the CGI network's control servers.

Tibetan Government-in-Exile (TGIE)

On September 11, 2008, Wireshark was used to capture packets from a TGIE computer [redacted]. An analysis revealed that this computer was compromised by malware which sent communication to, and received communication from, control servers.

The malware made connections to a control server on 221.10.254.248 using the host name 927.bigwww.com. The IP address 221.10.254.248 is assigned to CNCGROUP-SC (CNC Group CHINA169 Sichuan Province Network) in China. The malware on the infected computer used HTTP to connect to a JPEG file, which was not an image file but instead contains an IP address and port number (124.135.97.21:8005). This IP address, 124.135.97.21, is assigned to CNCGROUP-SD (CNC Group CHINA169 Shandong Province Network) in China.

Offices of Tibet

London

On October 1, 2008 Wireshark was used to capture packets from a computer in the London OOT. An analysis revealed that this computer was compromised by malware which sent communication to, and received communication from, control servers.

The malware made connections to a control server on 58.141.132.66 using the hostname oyd.3322.org on port 4501. The IP address 58.141.132.66 is assigned to NamBu TV in Seoul, South Korea. 3322.org is a Chinese dynamic domain service.

New York

On March 3, 2008, Wireshark was used to capture packets from a computer in the New York OOT. An analysis revealed that this computer was compromised by malware which attempted to send communication to a control server.

The malware attempted to make a connection to what appears to be a control server at 125.108.172.81 but there was not an active server at that location. The IP address 125.108.172.81 is assigned to CHINANET-ZJ-WZ (CHINANET-ZJ Wenzhou node network) in China.

Drewla

Following the discovery of targeted malware on the OHHDL, TGIE and OOT networks, we performed similar analysis on Tibetan NGOs to see if we could identify more infected machines communicating with control servers in China. While we carried out such analysis on a number of NGOs, in this report we focus on Drewla's network.

The Drewla ('connection' in Tibetan) is an online outreach project was set up in 2005 that employs Tibetan youth with Chinese language skills to chat with people in mainland China and in the diaspora, raising awareness about the Tibetan situation, sharing the Dalai Lama's teachings, and supplying information on how to circumvent Chinese government censorship on the Internet.

On September 12, 2008 Wireshark was used to capture packets from a Drewla computer. An analysis revealed that this computer was compromised by malware which sent communication to, and

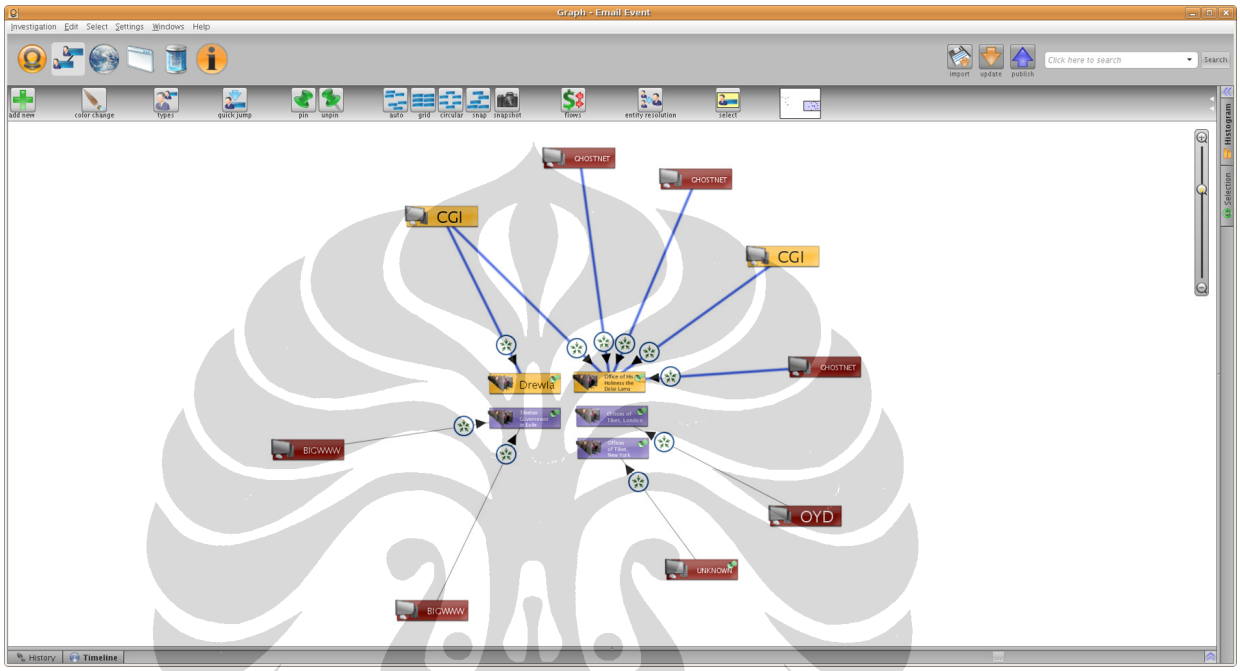
received communication from, control servers.

The malware made connections to a control server on 221.5.250.98 using the host name www.lookbytheway.net. The IP address 221.5.250.98 is assigned to CNCGROUP-CQ (CNC Group CHINA169 Chongqing Province Network) in China. The malware on the infected computer used HTTP to connect to a file in an attempt to inform the control server of the infected computer's status and download commands. The infected computer used HTTP POST to submit data to CGI scripts hosted on the control server. (**see Fig. 6** - p. 29)

Box 1.
Chinese Internet SIGINT in practice

During the course of our research, we were informed of the following incident. A member of Drewla, a young woman, decided to return to her family village in Tibet after working for two years for Drewla. She was arrested at the Nepalese-Tibetan border and taken to a detention facility, where she was held incommunicado for two months. She was interrogated by Chinese intelligence personnel about her employment in Dharamsala. She denied having been politically active and insisted that she had gone to Dharamsala for studies. In response to this, the intelligence officers pulled out a dossier on her activities and presented her with full transcripts of her Internet chats over the years. They indicated that they were fully aware of, and were monitoring, the Drewla outreach initiative and that her colleagues were not welcome to return to Tibet. They then released her and she returned to her village.

Fig. 6
The OHHDL and Drewla were infected by the same malware.



This Palantir screen capture shows the relationship between an infected computer at the Office of His Holiness the Dalai Lama (OHHDL) and the Tibetan NGO Drewla. Both attempted to connect to the same control server in the CGI network.

Phase 2: Identifying command and control servers

This phase of the investigation focused on the discovery of the command and control servers. We were able to identify and connect to the control servers used by the *GhostNet* by analysing the data from the OHHDL obtained during the field investigations carried out in Phase 1. During this process we were able to find and access web-based administration interfaces on the control server identified from the OHHDL data. These servers contain links to other control servers as well as command servers, and so therefore we were able to enumerate additional command and control servers.

After discovering several instances of malware on these servers, we set up a *honey pot* computer and were able to identify additional malicious servers by monitoring the traffic generated by our infected *honey pot*. Using the attacker(s)' web-based administration interface, we were able to command our *honey pot* computer to download *gh0st RAT*, one of the Trojans used by *GhostNet*. Eventually, our *honey pot* computer established a connection to the attacker(s)' *gh0st RAT* client. The attacker(s) proceeded to execute commands on our *honey pot*. We were able to discover several IP addresses within a DSL range in Hainan Island (PRC) that the attacker(s) used to communicate with computers infected with *gh0st RAT*.

Finally, we were able to map out the methods and capabilities of the *GhostNet* by a triangulated analysis of three sources: 1) data obtained from our collection of socially engineered emails with backdoor attachments, 2) the captured network traffic from Tibetan targets; and, 3) data obtained by gaining access to the command and control interface. (**see Fig. 7** - p. 31)

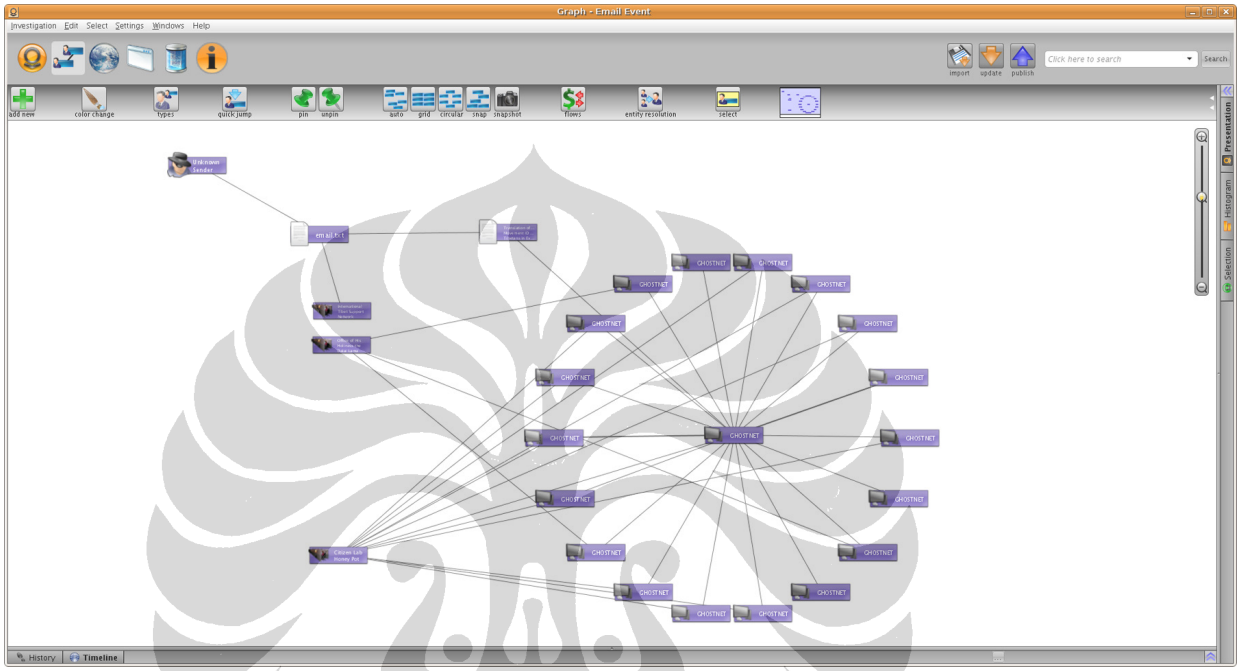
While analysing the data collected from the infected OHHDL computer [redacted], we discovered web-based administration *interfaces* to four control servers. Through some *strategic guessing* concerning file paths and file names, we were able to access web interfaces to multiple control servers. In total, we found 26 instances of the administration interface across the four servers. It remains unclear why the attacker(s) did not secure access to the control interface. Perhaps the attacker(s) concluded that the file paths and file names could not be easily guessed.

The control servers' web interface contains three main components: 1) a listing of all the infected computers that have reported to the control server; 2) an interface to issue commands to the infected computers; and 3) an interface to monitor pending commands to infected computers and their results when completed.

The commands issued to the infected computers direct the infected computer to download files from additional *command servers* under the attacker(s)' control. In some cases, these servers act as control servers themselves; however, some appear to be used exclusively to host malicious files that infected computers are meant to download. The attacker(s) set commands on the control servers that instruct infected computers to download additional remote administration Trojans, such as *gh0st RAT*, in order to take complete real-time control of the infected computers.

Three of the four control servers are located in three different locations in China: Hainan, Guangdong and Sichuan. One of the control servers is located at a web-hosting company in the United States. Five of the six command servers are located in mainland China (Hainan, Guangdong, Sichuan and Jiangsu) and one in Hong Kong.

Fig. 7
The *GhostNet* control servers.



This Palantir screen capture shows the *GhostNet* servers we uncovered and their relationship with the malicious email sent to, 1) the International Tibet Support Network, 2) the infected computer at the Office of His Holiness the Dalai Lama; and, 3) the *honey pot* network set up at the Citizen Lab.

The four control servers are:

- [redacted], Hainan-TELECOM, CN
- [redacted] US
- [redacted] CHINANET-GD, CN
- [redacted] CHINANET-SC, CN

The six control/command servers are:

- [redacted] CHINANET-HI, CN
- [redacted] CUHKNET, HK
- [redacted] CHINANET-GD, CN
- [redacted], CHINANET-SC, CN
- [redacted], CHINANET-JS, CN
- [redacted] CHINANET-SC, CN

The data obtained from WHOIS records concerning domain name registration reveals that most of the domains are traceable to the same individual. However, the attacker(s) could have simply stolen the domains from someone else, or compromised the servers hosting these domains.

Table 1: Domain name registration information

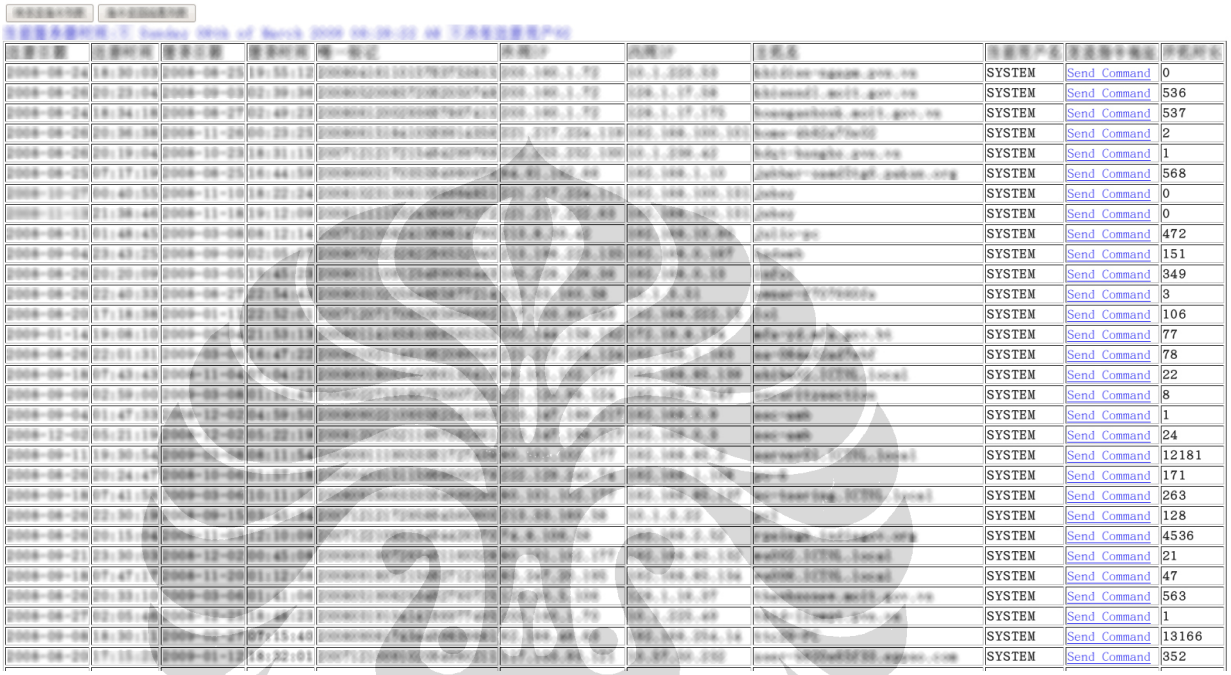
[redacted]	[redacted]	25/04/06
[redacted]	[redacted]	26/11/07
[redacted]	[redacted]	20/06/08
[redacted]	[redacted]	03/09/08

List of infected computers (**see Fig. 8** - p. 33)

The *Server List* interface provides information on each computer infected by the attacker(s)' malware, indicating the name given to the computer (by its owner/operator), its IP address, when it was first infected, when it last *called home* (i.e. the control server), and how many times it has *called home*. Each infected computer is assigned a unique identification number so that the infected computer can be tracked even when its IP address changes. The page also features a link to the *Send Command* interface, through which the attacker(s) sends instructions to the infected

Fig. 8

The *GhostNet* "Server List" interface.



This screen capture of the *GhostNet* interface shows all infected computers that have "checked in" with the control server. It has been obscured to protect the identity of the victims.

computers. There is also a button at the top of the page that links to a *Command Result* page that shows the status of the commands sent to the host and their results.

To corroborate our findings, there was an entry in the *Server List* page of the infected OHHDL computer that we analysed during our field investigations outlined in Part One. It contained the unique ID, the IP address, computer name, and a link to issue commands to the infected computer.

Sending commands

The *Send Command* link provided for each entry yields an interface that allows an attacker(s) to send specific commands to the selected infected computer. In addition to a custom command, the attacker(s) may choose from a menu of commands, which includes options to download binaries that provide additional functionality (such as keystroke logging or remote administration), acquire system information (list computer information, software and documents on the computer), or cause the malware to become dormant. (**See Fig. 9** - p. 35)

Using the *Send Command* interface, the attacker(s) issues instructions to the infected computers to download malicious files that are disguised as standard image files. As mentioned above, the files are most often hosted on additional command servers that appear to be dedicated to hosting these infected files.[46] These command servers contain a variety of files. While the exact function of each file is not known, the file names given to them by the attacker(s) provide some indication of their functionality. There are file names associated with the retrieval of files as well as keystroke logging.

One of the commands available to the attacker(s) instructs infected computers to download the *gh0st RAT* remote administration tool, which gives the attacker(s) full, real-time control of the infected computer. *Gh0st RAT* is an open source Trojan that is widely available online. It was developed by Chinese programmers but has now been translated into English. The program allows an attacker to create an executable file that can be repacked and disguised and used to infect and compromise a target computer. This file can be configured to directly connect to the *gh0st RAT* owner or to a third location, a control server, when it retrieves the current IP address of the *gh0st RAT* owner. (**See Fig. 10** - p. 36)

Once the infected computer connects to the *gh0st RAT* owner, an entry appears in the *Connection* window with some information about the infected computer. The *gh0st RAT* owner may then issue commands to the infected computer. These commands include file manager, screen capture, keylogger, remote shell, system, webcam view, audio capture, as well as the ability to force the infected host to download and execute additional malware, such as a *gh0st RAT* update.

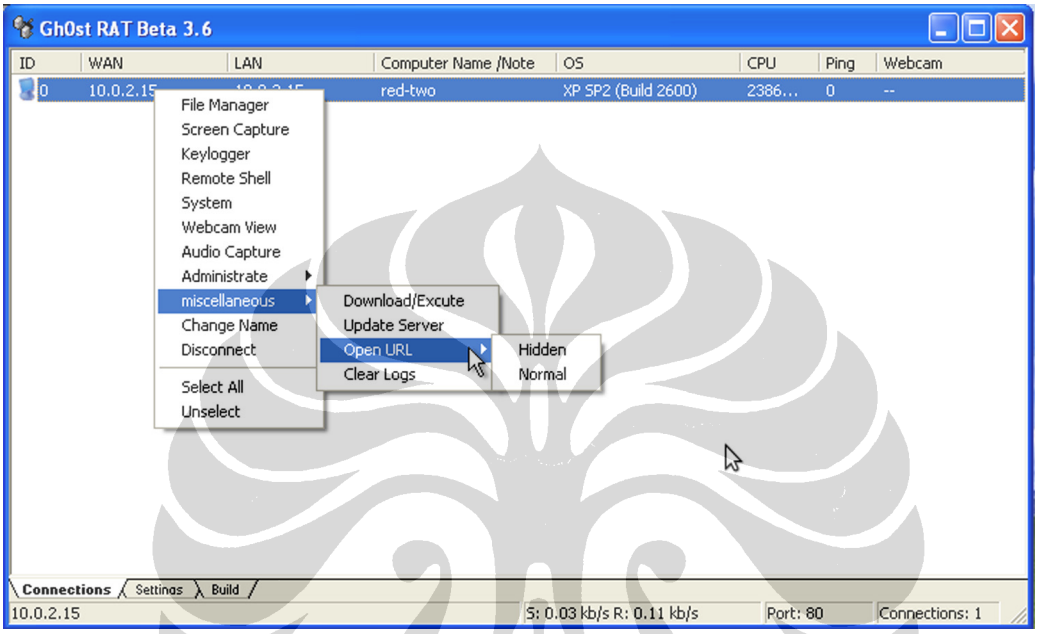
During the course of the investigation, we infected a *honey pot* computer with the attacker(s)' malware. We instructed our infected computer to download the attacker(s)' version of *gh0st RAT* using the malicious network's web-based administration interface. The *gh0st RAT* attempted to connect to several *.broad.hk.hi.dynamic.163data.com.cn IP addresses before finally successfully connecting to [redacted].broad.hk.hi.dynamic.163data.com.cn).

46 In some cases the malicious image files are hosted on the control servers themselves.

Fig. 9
The *GhostNet* "Send Command" interface.

This screen capture of the *GhostNet* interface shows how the attacker(s) can send specific commands to infected computers. It has been obscured to protect the identity of the victims.

Fig. 10
The *ghOst RAT* interface.



This screen capture of the English language version of the *ghOst RAT* software shows the commands that an attacker is able to execute on the compromised computer.

The gh0st RAT tool attempts to connect to IP addresses of a DSL provider in Hainan, China:

- [redacted].broad.hk.hi.dynamic.163data.com.cn
- [redacted].broad.hk.hi.dynamic.163data.com.cn
- [redacted].broad.hk.hi.dynamic.163data.com.cn
- [redacted].broad.hk.hi.dynamic.163data.com.cn
- [redacted].broad.hk.hi.dynamic.163data.com.cn
- [redacted]broad.hk.hi.dynamic.163data.com.cn

After a successful connection, the attacker(s) proceed to issue commands on our infected computer in real-time.

We found similar but unsuccessful connections to the same IP address range from some of the infected computers we analysed and discovered that a rudimentary version of the web-based administration interface contained only one infection from the same IP address range in Hainan. In addition, one of the servers used to host the attacker(s)' malicious files is a Government of Hainan web server located in Hainan, and one of the control server interfaces we gained access to is also located in Hainan. However, one should not rush to judgement concerning the identity of the attacker(s) based on this location. The *gh0st RAT* software can be configured with a proxy server; therefore it is possible that the attacker(s) were using a compromised system as a proxy to hide their true location.

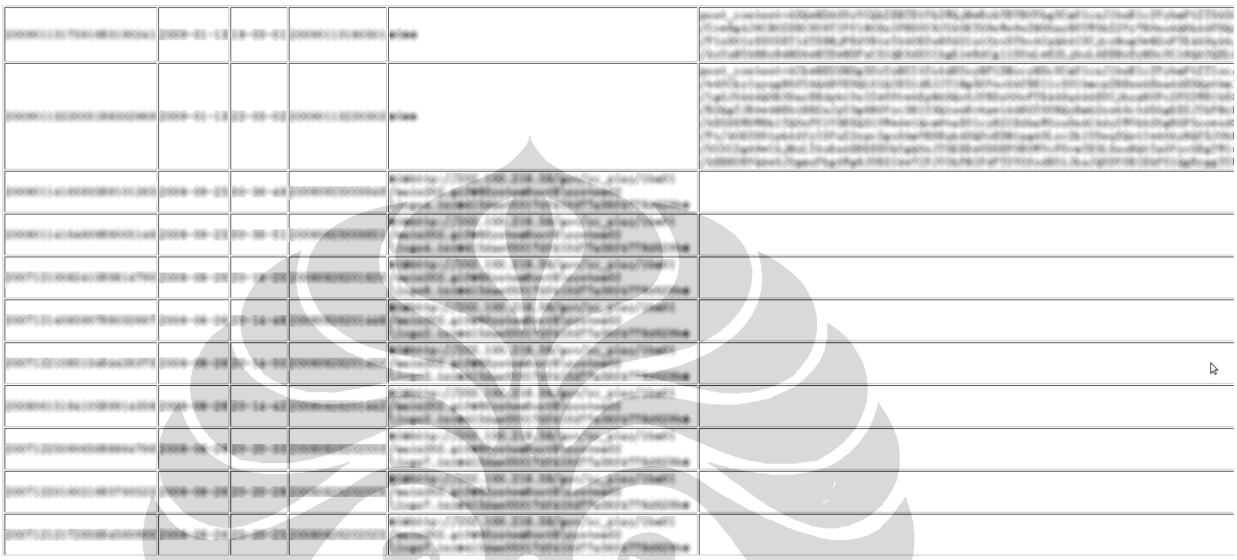
Command results

The *Command Result* page lists the commands issued through the *Send Command* page and the status of those commands. Each entry in this interface shows what command was sent to the infected computer, including the URL to the command server and the command file (the malicious file disguised as an image). Upon the successful completion of a command, the relevant date, time, and result are recorded. (**See Fig. 11** - p. 38)

The *Command Result* page contains a column that displays the content sent back to the control server from the infected computer. The command issued to retrieve this content in the *Send Command* interface is labelled "Acquire System Information." Even though we have been unable to properly decode the content,[47] the plain text values in the binary content indicate that these entries contain information about the infected computer (CPU, memory, operating system, programmes installed) as well as file names of documents on the computer, presumably for later retrieval. This information is likely used to determine which targets the attacker(s) will further exploit and control using remote administration tools such as *gh0st RAT*.

47 The content is base64 encoded and XORed with values we have yet to identify.

Fig. 11
The GhostNet "List Command" interface.



This screen capture of the *GhostNet* interface lists the commands issued to infected computers. It has been obscured to protect the identity of the victims.

Methods and capabilities

The attacker(s) are able to exploit several infection vectors. First, they create web pages that contain "drive by" exploit code that infects the computers of those who visit the page. Second, the attacker(s) have also shown that they engage in *spear phishing* in which contextually relevant emails are sent to targets with PDF and DOC attachments which, when executed, create *back doors* that cause the infected computer to connect to a control server and await further instructions.

With each successful infection the attacker(s) may use any contextually relevant data to further exploit the targeted community and may also impersonate the initial target in order to infect all the targets' contacts. Finally, the targets themselves may infect others by forwarding infected documents to their contacts. In this way, the network of infected computers grows organically.

The first stage of infection focuses on getting targets to execute malicious code. Once infected, the target's computer routinely checks in with a control server in order to receive further instructions. At this stage, the attacker(s) acquires some initial information regarding the identity of the infected computer.

Newer versions of the administration interface contain a direct link to a web service that looks up the relevant WHOIS information about the IP address of the infected computer along with a simple port scan. This version also does a geoIP lookup on the infected computer's IP address and lists the country in which the computer is located, indicating that the attacker(s) has an interest in the geographical location of the infected computers.

The attack may also issue an acquire *system information* command that causes the infected computer to upload its hardware statistics, list of programs installed, list of recent documents, and current network connections. The attacker(s) may use this information to target the infected computer for further exploitation.

The attacker(s) directs the infected computers to download and install a remote administration Trojan. The attacker(s) have demonstrated a preference for *gh0st RAT* but may choose from a variety of Trojans. The attacker(s) simply browses to the "send command" interface and pastes in a link to a version of *gh0st RAT* on a "command" server under his or her control. The next time the infected computer *checks in* to the control server, it will be instructed to download and execute *gh0st RAT*. Upon completion, the infected computer notifies the control server and the result appears in the attacker(s)' web interface.

Once *gh0st RAT* is installed on the target, the infected computer will periodically check a specific location and retrieve the IP address to which it is supposed to connect. When the attacker(s) is not available, he or she will often change this IP to 127.0.0.1 (localhost) so that the amount of potentially suspicious external traffic is limited. When the attacker(s) is ready to receive connections, the IP address is changed to a valid external IP address.

When the attacker(s) turns on *gh0st RAT*, he or she is able to see all the infected machines that have established connections to him or her. The attacker(s) may then execute a wide variety of commands, including file manager, screen capture, keylogger, remote shell, system, webcam view, audio capture, as well as the ability to force the infected host to download and execute additional malware, such as a *gh0st RAT* update. The attacker(s) may also secretly execute programs on the target computer.

Analysis of list of infected computers

A detailed analysis of the list of infected computers revealed an overwhelming number of unique infections in many countries. The same malware that infected computers at the Dalai Lama's office and other Tibetan organizations had a much more extensive set of targets. The list of entities and locations of those targeted was quite varied.

In total, we found 1,295 infected computers located in 103 countries. We found that we were able to confidently—on a scale of low, medium, high—identify 397 of the 1,295 infected computers (26.7%), and labelled each one as a high-value target. We did so because they were either significant to the relationship between China and Tibet, Taiwan or India, or were identified as computers at foreign embassies, diplomatic missions, government ministries, or international organizations.

Of the remaining infected computers, 536 appear to be computers on private broadband Internet providers. The remaining IP addresses do not reverse resolve and available information on these hosts does not allow us to make judgements regarding the identity or purpose of these computers.

Methodology

We compiled a unified and comprehensive list of infected computers from all the control servers, as there was considerable duplication across them. There were several duplicate entries in the list of infected computers—in some cases, the same infected computer was logged multiple times as it was connecting from a different IP address. In other instances, multiple infected computers were assigned different internal IP addresses and had different computer names but shared the same external IP address. This signifies that there were multiple infected computers sharing Internet access. Where possible, we filtered the results by unique computer name, and if no computer name was present, we filtered by unique external IP address.[48] (**See Fig. 12** - p. 41)

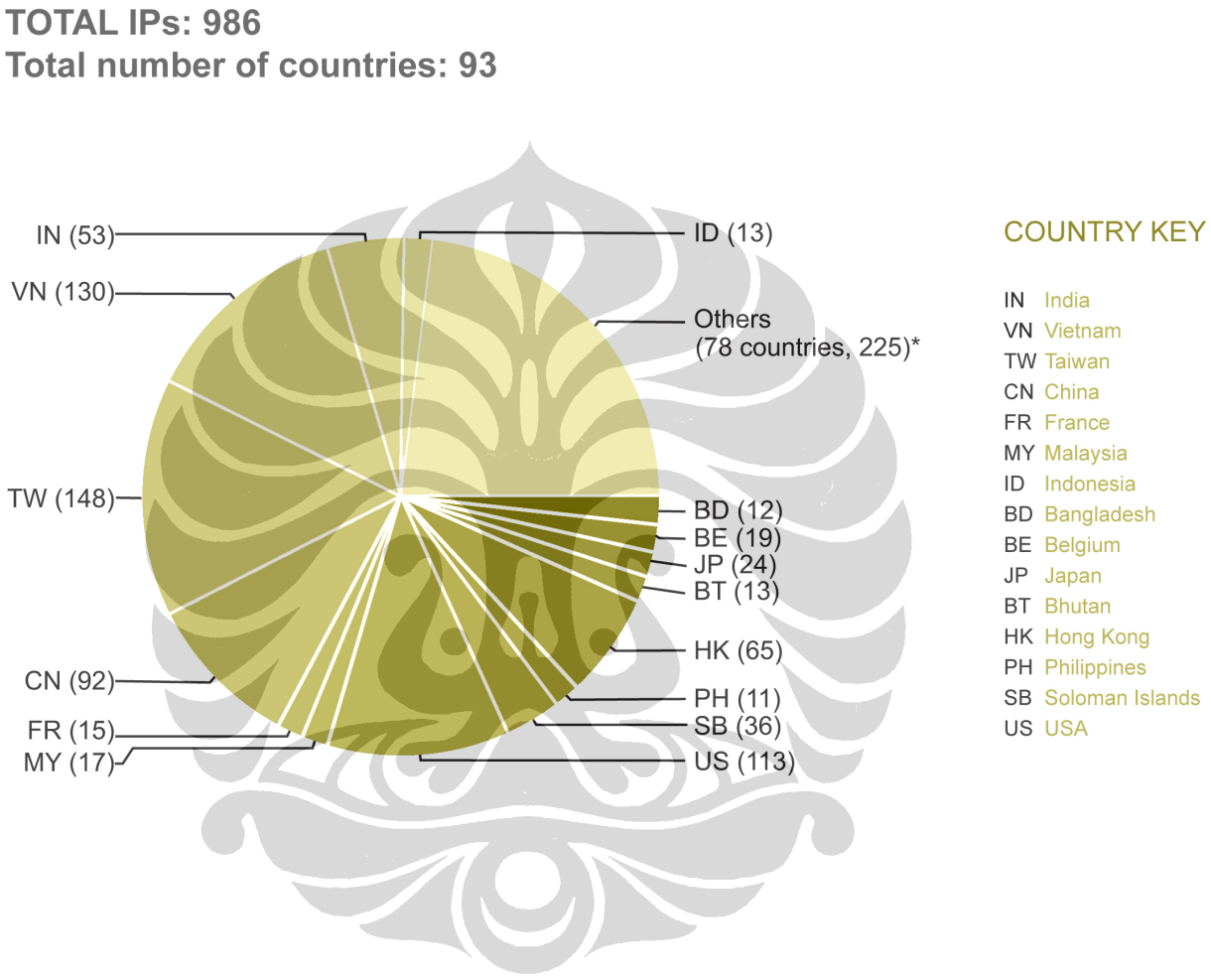
On the surface, the names of the infected computers in the sample are provocative. There are references to ministries of foreign affairs, foreign embassies, and other government entities. Some contains names of officials or their positions/titles. However, we recognize that a computer name can be anything its owner wishes, and may be completely unrelated to the location, function, or owner of that particular computer.

Therefore, in order to be more confident as to the true identity or purpose of the infected computer, we relied on reverse DNS look-ups and each IP address' record from the Regional Internet Registries. Using these two pieces of information we were able to confirm the validity of the identity of several infected computers with a **high (H)** degree of confidence.

In some cases the computer name associated with the infected computer is actually a domain name or an acronym for a recognizable institution or organization. In these cases we classified our identification of the target with either a **medium (M)** or **low (L)** level of confidence. **Medium** confidence refers to instances where we have otherwise identified a related high confidence target,

48 In one case we removed 117 unique IP addresses from Mexico that appeared to belong to the same computer connecting in to the control server from a DSL provider.

Fig. 12
The geographic location of infected hosts.



This graphic illustrates the global reach of the *GhostNet*. There were 1,295 infected computers that reported to the control server. The infections were spread across 103 countries. Taiwan reported the most infections followed by the United States, Vietnam and India.

but for which we rely on the computer name for identification. **Low** confidence refers to instances in which we rely solely on the computer name for identification.

Table 2: Selected infections

Organization	Confidence	Location	Infections
ASEAN	H	ID, MY	3
Asian Development Bank	H	PH, IN	3
Associated Press, UK	H	GB, HK	2
Bureau of International Trade Relations	L	PH	1
CanTV, Venezuela	H	VE	8
Ceger, Portugal	H	PT	1
Consulate General of Malaysia, Hong Kong	H	HK	1
Deloitte & Touche, New York	H	US	1
Department of Commerce, Solomon Islands	L	SB	1
Department of Foreign Affairs, Indonesia	H	ID	3
Department of Foreign Affairs, Philippines	H	PH	1
Department of Science and Technology, Philippines	H	PH	2
Embassy of China, US (see footnote 50)	H	US	1
Embassy of Cyprus, Germany	H	DE	1
Embassy of Germany, Australia	M	AU	1
Embassy of India, Belgium	L	BE	1
Embassy of India, Serbia	L	CS	1
Embassy of India, Germany	H	DE	1
Embassy of India, Italy	H	IT	1
Embassy Of India, Kuwait	H	KW	1
Embassy of India, USA	H	US	7
Embassy of India, Zimbabwe	H	ZA	1
Embassy of Indonesia, China	H	CN	1
Embassy of Malaysia, Cuba	H	CU	1
Embassy of Malaysia, Italy	H	IT	1
Embassy of Malta	L	MT	4
Embassy of Malta, Australia	L	AU	1
Embassy of Malta, Belgium	L	BE	11
Embassy of Malta, Libya	L	LY	1
Embassy of Pakistan, Bahrain	L	BH	1
Embassy of Papua New Guinea, China	L	CN	1
Embassy of Portugal, Finland	H	FI	1
Embassy of Portugal, Germany	H	DE	1
Embassy of The Republic Of China (Taiwan), Swaziland	H	TW	1
Embassy of Romania, Finland	H	FI	1
Embassy of Romania, France	H	FR	1

Table 2: Selected infections (cont'd)

Organization	Confidence	Location	Infections
Embassy of Romania, Norway	H	NO	1
Embassy of Romania, PRC	H	CN	1
Embassy of Thailand, Philippines	H	PH	2
Embassy of the Republic of Korea, China	H	CN	2
Government Integrated Telecommunication Network, Malaysia	L	MY	2
High Commission of India, Cyprus	H	CY	1
High Commission Of India, United Kingdom	H	GB	1
Institute for Information Industry, Taiwan	L	TW	1
International Campaign for Tibet	H	NL	7
International Chamber of Shipping, United Kingdom	L	GB	1
Lanka Education and Research Network, Sri Lanka	L	LK	1
Malta External Trade Corporation Ltd.	H	MT	1
Maritime Police, Solomon Islands	H	SB	1
Ministry of Communications, Brunei	H	BN	1
Ministry of Education, Solomon Islands	H	SB	1
Ministry of Foreign Affairs, Bangladesh	H	BD	4
Ministry of Foreign Affairs, Barbados	M	BB	5
Ministry of Foreign Affairs, Bhutan	L	BT	11
Ministry of Foreign Affairs, Brunei	L	BN	1
Ministry Of Foreign Affairs, Iran	H	IR	1
Ministry of Foreign Affairs, Latvia	H	LV	2
Ministry of Industry and Trade, Vietnam	L	VN	30
Ministry of Labour and Human Resources, Bhutan	H	BT	1
National Informatics Centre, India	L	IN	12
NATO, (SHAPE HQ)	H	NL	1
Net Trade, Taiwan	H	TW	1
New Tang Dynasty Television, United States	L	US	1
Office of the Dalai Lama, India	H	IN	2
Pakistan Mission to The United Nations	L	US, JP	4
Permanent Delegation of Cyprus to the European Union	L	BE	1
Permanent Mission of Cuba to the United Nations	L	US	1
PetroVietnam	L	VN	74
Prime Minister's Office, Laos	H	LA	5
Public Service Division, Solomon Islands	H	SB	1
Russian Federal University Network, Russian Federation	H	RU	1
Software Technology Parks of India, India	L	IN	2
South Asian Association for Regional Cooperation	L	BD, US	5
Students for a Free Tibet, United States	H	US	2
TAITRA, Taiwan	H	TW, NG	79

Table 2: Selected infections (cont'd)

Organization	Confidence	Location	Infections
Taiwan Government Service Network, Taiwan	H	TW	1
Tibetan Government in Exile, India	H	IN, US	4
Trade and Industry Department, Government of Hong Kong	H	HK	1

Infection timeline

The earliest infected computer *called home* to the control server on May 22, 2007. The most recent entry in our sample is March 12, 2009. On average, the amount of time that a host was actively infected was 145 days.[49] While 90 infected computers were only infected for one day, 145 were infected for over 400 days. The longest infection span was 660 days. In total, 422 hosts *checked in* March 1-12, 2009; 373 of these computers were infected in 2008. The data indicates that despite a reduction in new infections, the network continues to be operational. (**See Fig. 13** - p. 45)

There are significant spikes in infection rates in December 2007 and August 2008.

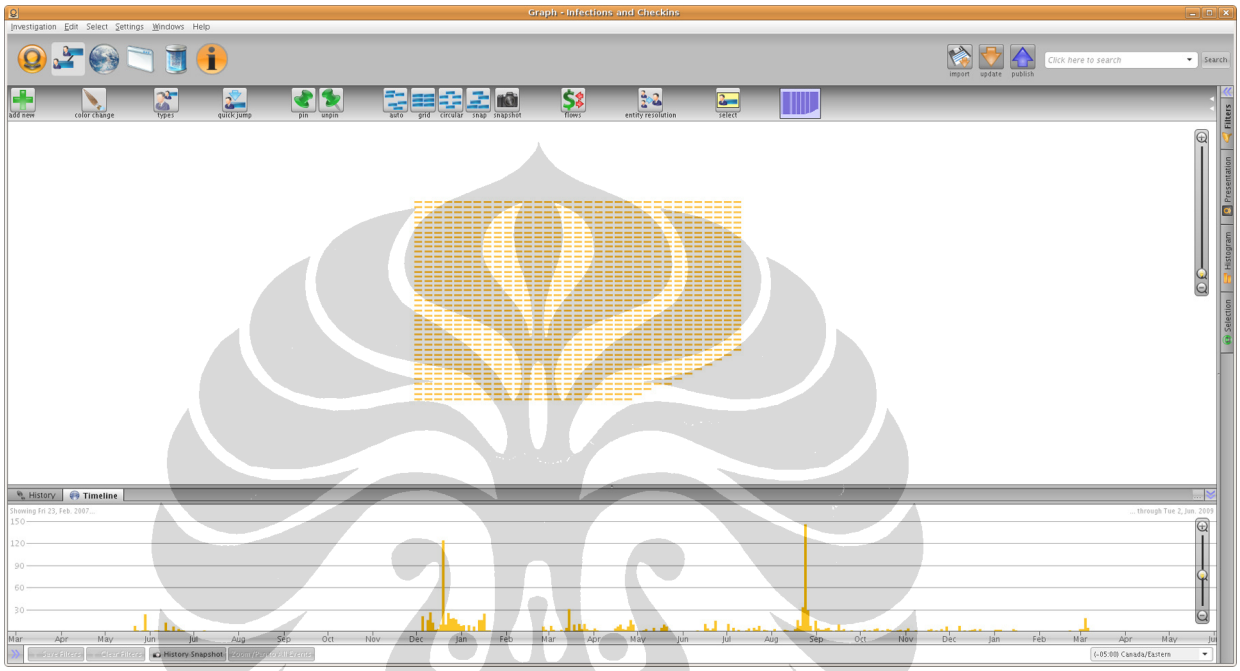
There were 320 infections in December 2007 spread across 56 countries. However, 113 were located within Taiwan and the majority of these infections occurred within a single organization: the Taiwan External Trade Development Council. During this same period, computers at the Embassies of India in Belgium and Zimbabwe were infected as were the Embassies of Indonesia and the Republic of Korea in the People's Republic of China. In addition, computers at the Ministry of Foreign Affairs in Iran were infected as were several computers at the Tibetan Government-in-Exile.

The spike in August 2008 totalled 258 infections spread across 46 countries. The OHHDL computer was infected during one of these spikes in August 2008 (It last checked in to the control server in September 2008). This spike included the Chinese Embassy in the United States,[50] 3 computers at the Embassy of India in the Unites States, and the High Commission of India in the United Kingdom and in Cyprus. It also included the Embassy of Cyprus in Germany, the Embassy of Malaysia in Cuba, the Embassy of Thailand in the Philippines and the Ministry of Industry in Vietnam. Several companies were also compromised, including Net Trade in Taiwan, the New York Office of Deloitte & Touche, and PetroVietnam, the government-owned oil and gas Company.

49 The average number of days from the initial infection to the last time an infected computer "checked in" with a control server.

50 It is unclear whether the affected embassy is the Republic of China (Taiwan) or People's Republic of China.

Fig. 13
GhostNet infection timeline.



This screen capture of a timeline generated with Palantir illustrates when and how many computers were infected by the *GhostNet*. It shows that there are significant spikes in infection rates in December 2007 and August 2008.

PART THREE:
Investigating *GhostNet*: Conclusions

The evidence presented in this report—through a combination of field investigations, interviews, technical scouting, data analysis, mining and visualization—paints a disturbing picture.

GhostNet represents a network of compromised computers resident in high-value political, economic, and media locations spread across numerous countries worldwide. At the time of writing, these organizations are almost certainly oblivious to the compromised situation in which they find themselves. The computers of diplomats, military attachés, private assistants, secretaries to Prime Ministers, journalists and others are under the concealed control of unknown assailant(s).

In Dharamsala and elsewhere, we have witnessed machines being profiled and sensitive documents being removed. At our Laboratory, we have analysed our own infected "honey pot" computer and discovered that the capabilities of *GhostNet* are potent and wide ranging. Almost certainly, documents are being removed without the targets' knowledge, keystrokes logged, web cameras are being silently triggered, and audio inputs surreptitiously activated.

This raises the question, how many sensitive activities have been preemptively anticipated by intelligence gathered through this network? How many illegal transactions have been facilitated by information harvested through *GhostNet*? Worst of all, how many people may have been put at risk?

While these questions are compelling, it would be imprudent to read these findings as an indictment, or to attribute to the owners of *GhostNet* motivations and intentions for which there is no evidence.

Alternative explanations

The list of computers controlled by the *GhostNet* is significant, and certainly atypical for a cybercrime network. The size of the network is small, and the concentration of high-value systems is significant.

At the same time, penetrations of this type are not uncommon. Recently, several large-scale spy nets have been discovered, including ones containing lists of affected computers of a magnitude higher than that harvested by *GhostNet*.

This trend is predictable, converging with accumulating incidents of cyber-attacks facilitated by lower entry-thresholds for computer exploitation methods and technologies. The tools we profile in our investigation, though apparently amassed in a complex way to achieve a definite purpose, are not restricted to an exclusive guild of experts with specialized and confidential knowledge.

Today, pirated cyber-crime kits circulate extensively on the Internet and can be downloaded by anyone about as easily as the latest pirated DVD.[51] Cyberspace has empowered individuals and small groups of non-state actors to do many things, including executing sophisticated computer network operations that were previously only the domain of state intelligence agencies. We have entered the era of *do-it-yourself* (DIY) signals intelligence.

---

51 http://ddanchev.blogspot.com/2008/11/zeus-crimeware-kit-gets-carding-layout.html

Attribution

Who is ultimately in control of the *GhostNet* system? While our analysis reveals that numerous politically sensitive and high-value computer systems were compromised, we do not know the motivation or the identity of the attacker(s) or how to accurately characterize this network of infections as a whole. We have not been able to ascertain the type of data that has been obtained by the attacker(s), apart from the basic system information and file listings of the documents located on the target computers. Without this data we are unable to deduce with any certainty what kind of data the attacker(s) were after. There are thus several possibilities for attribution.

The most obvious explanation, and certainly the one in which the circumstantial evidence tilts the strongest, would be that this set of high profile targets has been exploited by the Chinese state for military and strategic-intelligence purposes. Indeed, as described above, many of the high confidence, high-value targets that we identified are clearly linked to Chinese foreign and defence policy, particularly in South and South East Asia. Like radar sweeping around the southern border of China, there is an arc of infected nodes from India, Bhutan, Bangladesh and Vietnam, through Laos, Brunei, Philippines, Hong Kong, and Taiwan. Many of the high profile targets reflect some of China's most vexing foreign and security policy issues, including Tibet and Taiwan. Moreover, the attacker(s)' IP addresses examined here trace back in at least several instances to Hainan Island, home of the Lingshui signals intelligence facility and the Third Technical Department of the People's Liberation Army.[52]

However, we must be cautious to rush to judgement in spite of circumstantial and other evidence, as alternative explanations are certainly possible and charges against a government of this nature are gravely serious. On the other end of the spectrum is the explanation that this is a random set of infected computers that just happens to include high profile targets of strategic significance to China, collected by an individual or group with no political agenda *per se*. Similarly one can postulate that the targets gathered together happened less by concerted effort than by sheer coincidence. Given the groupings of various entities in the infected computer list (by country and organization), internal email communications and sloppy security practices could have led to cross-infection and subsequent listing on the control servers.

Another possible explanation is that there is a single individual or set of individuals (criminal networks, for example) who are targeting these high-value targets for profit. This can be in the form of stealing financial information or critical data that can be sold to clients, be they states or private entities. There are countless examples of large-scale fraud and data theft worldwide and numerous apparent instances of outsourcing to third parties of cyber-attacks and espionage, some of which the Information Warfare Monitor and its related research project, the OpenNet Initiative, have documented. *GhostNet* could very well be a for-profit, non-state venture. Even "patriotic hackers" could be acting on their own volition, or with the tacit approval of their government, as operators of the *GhostNet*.

Finally, it is not inconceivable that this network of infected computers could have been targeted by a state other than China, but operated physically within China (and at least one node in

52 http://www.globalsecurity.org/military/world/china/lingshui.htm

the United States) for strategic purposes. Compromised proxy computers on Hainan Island, for example, could have been deployed as staging posts, perhaps in an effort to deliberately mislead observers as to the true operator(s) and purpose of the *GhostNet* system.

The Significance of *GhostNet*

GhostNet is significant, as it does not appear to be a typical cybercrime network. The potential political fallout is enormous. But ultimately, the question of who is behind the *GhostNet* may matter less than the strategic significance of the collection of affected targets. What this study discovered is serious evidence that information security is an item requiring urgent attention at the highest levels. It demonstrates that the subterranean layers of cyberspace, about which most users are unaware, are domains of active reconnaissance, surveillance, and exploitation.

Regardless of who or what is ultimately in control of *GhostNet*, its capabilities of exploitation and the strategic intelligence that can be harvested from it matter most. Indeed, although the Achilles' heel of the *GhostNet* system allowed us to monitor and document its far-reaching network of infiltration, we can safely hypothesize that it is neither the first nor the only one of its kind.

PART FOUR:
About Information Warfare Monitor

About the Information Warfare Monitor

http://infowar-monitor.net/

The Information Warfare Monitor is an advanced research activity tracking the emergence of cyberspace as a strategic domain. We are an independent research effort. Our mission is to build and broaden the evidence base available to scholars, policymakers, and others. We aim to educate and inform.

The Information Warfare Monitor is a public-private venture between two Canadian institutions: The SecDev Group, an operational think tank based in Ottawa (Canada), and the Citizen Lab at the Munk Centre for International Studies, University of Toronto. The Principal Investigators and co-founders of the Information Warfare Monitor are Rafal Rohozinski (The SecDev Group) and Ronald Deibert (Citizen Lab).

The Information Warfare Monitor is supported by The SecDev Group which conducts field-based investigations and data gathering. Our advanced research and analysis facilities are located at the Citizen Lab. IWM is part of the Citizen Lab's network of advanced research projects, which include the OpenNet Initiative and ONI Asia.

The Information Warfare Monitor also benefits from donations from a variety of sponsors including Psiphon Inc, and Palantir Technologies.

The Information Warfare Monitor engages in **three primary activities:**

1. Case Studies. We design and carry out active case study research. These are self-generated activities consistent with our mission.

We employ a rigorous and multidisciplinary approach to all our case studies blending qualitative, technical, and quantitative methods. As a general rule, our investigations consist of at least two components:

> *Field-based investigations*. We engage in qualitative research among affected target audiences and employ techniques that include interviews, long-term *in situ* interaction with our partners, and extensive technical data collection involving system monitoring, network reconnaissance, and interrogation. Our field-based teams are supported by senior analysts and regional specialists, including social scientists, computer security professionals, policy experts, and linguists, who provide additional contextual support and substantive back-up.
>
> *Technical scouting and laboratory analysis.* Data collected in the field is rigorously analysed using a variety of advanced data fusion and visualization methods. Leads developed on the basis of infield activities are pursued through "technical scouting," including computer network investigations, and the resulting data and analysis is shared with our infield teams and partners for verification and for generating additional entry points for follow-on investigations.

2. Open Source Trend Analysis. We collect open-source information from the press and other sources tracking global trends in cyberspace. These are published on our public website.

3. Analytical Workshops and Outreach. We work closely with academia, human rights organizations, and the defense and intelligence community. We publish reports, and occasionally conduct joint workshops. Our work is independent, and not subject to government classification. Our goal is to encourage vigorous debate around critical policy issues. This includes engaging in ethical and legal considerations of information operations, computer network attacks, and computer network exploitation, including the targeted use of Trojans and malware, denial of service attacks, and content filtering.

About The SecDev Group

http://www.secdev.ca

The SecDev Group is a Canadian-based operational consultancy focused on countries and regions at risk from violence and insecurity. We deliver to our clients insights and access to a diverse range of cultures, audiences, challenging environments and *ungoverned spaces*. Our approach combines a field research capability with advanced techniques and methods for generating policy-relevant analysis and solutions. As a think tank, we identify and communicate realistic options to enhance effectiveness through evidence-based research on the causes, consequences and trajectories of insecurity and violence. We are operational because we design and conduct activities in complex and insecure environments.

About The Citizen Lab

http://www.citzenlab.org

The Citizen Lab is an interdisciplinary laboratory based at the Munk Centre for International Studies at the University of Toronto, Canada focusing on advanced research and development at the intersection of digital media and world politics. We are a *hothouse* that combines the disciplines of political science, sociology, computer science, engineering, and graphic design. Our mission is to undertake advanced research and engage in development that monitors, analyses, and impacts the exercise of political power in cyberspace. The Citizen Lab's ongoing research network includes the Information Warfare Monitor and the OpenNet Initiative, ONI Asia, and benefits from collaborative partnerships with academic institutions, NGOs, and other partners in all regions of the world.