ISSN : NO. 0854-2031
TERAKREDITASI BERDASARKAN SK.DIRJEN DIKTI NO.55a/DIKTI/KEP/2006

ANALISIS KRIMINOLOGIS TENTANG PENYEBAB PELAKU KEJAHATAN YANG BERHUBUNGAN DENGAN KOMPUTER (STUDI DI UNIT V INFOTEK/*CYBERCRIME*, DIREKTORAT II MARKAS BESAR KEPOLISIAN NEGARA REPUBLIK INDONESIA)

Oleh : **Widodo ***

ABSTRAK

Perkembangan ilmu pengetahuan dan teknologi mengakibatkan terbentuknya sistem dan jaringan komputer (internet). Di Indonesia, banyak kejahatan yang menjadikan sistem dan jaringan komputer sebagai sasaran kejahatan, dan kejahatan yang menggunakan komputer sebagai sarana. Kedua kategori kejahatan tersebut dikenal dengan istilah kejahatan yang berhubungan dengan komputer *(computer-related crime*). Berdasarkan teori asosiasi diferensial, penyebab pelaku kejahatan tersebut adalah adanya proses belajar teknik-teknik melakukan kejahatan melalui internet atau media massa lain dari kelompok intim, komunikasi antar anggota *underground* tersebut berjalan lama dan intensif. Sedangkan dari telaah teori netralisasi diketahui, pelaku melakukan kejahatan karena ingin balas dendam, merasa tidak berdaya menghadapi masyarakat dan hukum, bahaya yang ditimbulkan tidak serius bagi masyarakat, dan ingin memperoleh kebebasan bertingkah laku dengan cara menganggap Undang-Undang sebagai penghalang aktivitas di internet, serta korban juga merupakan kriminogen. Dengan demikian, penyebab pelaku kejahatan yang berhubungan dengan komputer di Indonesia selaras dengan ajaran *multiple-factors "theory"*, bahwa pelaku kejahatan tersebut disebabkan oleh sejumlah faktor yang kompleks.

Kata Kunci: Kriminologi, Kejahatan Komputer

PENDAHULUAN

Kejahatan di dunia *mayantara* (*cybercrime*) sudah marak terjadi di Indonesia, khusus dalam bidang perbankan sudah ada sejak tahun 1983.[1] Kejahatan kategori ini dapat disebut *cybercrime*[2], atau tindak pidana dalam bidang telematika[3], atau kejahatan yang berhubungan dengan komputer (*computer-related crime*)[4]. Pengertian *cybercrime* dengan *computer-related crime* tersebut sama[5]. Dalam penelitian ini, penulis menggunakan istilah kejahatan yang berhubungan dengan komputer (*computer-related crime*) karena selaras dengan hasil kongres PBB, yaitu mencakup 2 kategori kejahatan, yakni aktivitas yang menjadikan komputer sebagai target atau objek kejahatan, dan kejahatan yang menggunakan komputer sebagai alat melakukan kejahatan.[6]

Kerugian meterial dari kejahatan yang berhubungan dengan komputer di Indonesia sangat tinggi, antara lain selama tahun 2003 sebesar Rp 11.669.373.000.[7] dalam kasus *carding,* selama tahun 2003

* DR. Widodo, SH.MH Dosen Fakultas Hukum Universitas Wisnuwardhana Malang

1 Eddy Karnasudirdja, *Bahaya Kejahatan Komputer*, Tanjung Agung, Jakarta, 1999, hal. 35.

2 Tb. Ronny R. Nitibaskara, "*Problema Yuridis Cybercrime"*, Makalah pada Seminar *Cyber Law*, diselenggarakan oleh Yayasan Cipta Bangsa, Bandung, Juli 2000, p. 2.

3 Rancangan Undang-Undang tentang Kitab Hukum Pidana, ELSAM, Jakarta, 2006.

4 Dokumen Kongres PBB ke-10 di Wina, Http://www.uncjin.org/Documents/ Eigthcongress. Html. Diakses Tanggal 23 Maret 2006, Pukul 14.00 WIB.

5 Barda Nawawi Arief, *Perbandingan Hukum Pidana,* PT Raja Grafindo Persada, Jakarta, 2002, p. 259.

6 Dokumen Kongres PBB ke-10 di Wina, Http://www.uncjin.org/Documents/Eigthcongress.Html. Diakses Tanggal 23 Maret 2006, Pukul 14.00 WIB.

7 Susrini, *http:groups.or.id/pipermail/omepgt/2004-September/000002.html,* diakses tanggal 28 Januari 2006 pukul 09.00. WIB).

saja berkisar antara 50 sampai dengan 60 miliar rupiah.[8] Pembajakan *Video Compact Disc (VCD), cassette*, dan *ringtones* mengakibatkan kerugian negara 1,8 trilyun rupiah per tahun[9] Kerugian ini belum termasuk kerugian moral, yaitu menurunnya kepercayaan masyarakat pada hukum dan penegakannya. Karena itu, kejahatan tersebut perlu ditanggulangi melalui penerapan kebijakan hukum pidana maupun penerapan kebijakan non-hukum pidana. Agar penanggulangan tersebut efisien dan efektif diperlukan pertimbangan dari hasil analisis tentang penyebab orang melakukan kejahatan yan berhubungan dengan komputer.

Penelitian Aman Nursusila di Bagian Serse Ekonomi Polda Jawa Timur dan Polwil Malang, menyimpulkan bahwa faktor-faktor penyebab terjadinya kejahatan dalam bidang perbankan yang menggunakan fasilitas komputer (komputer sebagai sarana kejahatan) adalah karena mencoba kemampuan di bidang teknologi internet (66,6%), dan karena alasan ekonomi (33,3%).[10] Berkaitan dengan pelaku kejahatan, kongres PBB mengungkapkan, bahwa "*any person of any age with a modicum of skill, motivated by the technical challenge, by the potential for gain, notoriety or revenge, or by the promotion of ideological beliefs, is a potential computer criminal*."[11]

Berpijak pada ulasan di atas, maka penulis menganggap perlu mengadakan penelitian, dengan permasalahan utama apakah penyebab pelaku kejahatan yang berhubungan dengan komputer di Indonesia. Kejahatan tersebut termasuk *property crime*[12] sehingga penyebabnya sangat kompleks dan memerlukan pemahaman yang komprehensip. Penelitian ini dilakukan di Unit V Infotek/*Cybercrime*, Direktorat II Bidang Ekonomi Khusus (Eksus), Markas Besar Kepolisian Negara Republik Indonesia. Untuk menambah bahan analisis, penulis mengkaitkan hasil analisis kriminologis dengan kasus *defacing* situs Komisi Pemilihan Umum (2004) dan situs Partai Golongan Karya (Juli 2006). Hasil penelitian ini dapat digunakan oleh legislator dan pemerintah sebagai dasar perencanaan penanggulangan kejahatan (*criminal policy*) terhadap kejahatan yang tergolong dalam kejahatan berteknologi tinggi ini (*hight-tech crime*), karena analisis kriminologis berkaitan erat dengan penantuan *strafsourt*, *strafmodus*, dan kebijakan nopenal.

KERANGKA TEORETIK

Pengkajian secara kritis tentang penyebab seseorang melakukan kejahatan dapat dilakukan dengan menggunakan teori-teori kriminologi. Meskipun abstraks, teori ini diperlukan untuk mengkaji mengapa ada manusia yang mampu melaksanakan norma sosial dan norma hukum, tetapi ada juga manusia yang justru melanggar hukum. Teori kriminologi mencoba menjawab pertanyaan ini melalui pemahaman sosiologis, politis, dan variabel ekonomi yang dapat juga mempengaruhi hukum, keputusan administratif, implementasi hukum dalam sistem peradilan pidana. Hal ini dikemukakan oleh Ronald L. Akers and Christine S. Seller berikut.

8 http://students.ukdw.ac.id/~22971797/topik1.htm, diakses tanggal 23 Desember 2005, pukul 12.45. WIB.)

9 *Akibat Pembajakan Musik, Negara Rugi 1,8 Trilyun per Tahun*. LKBN Antara, http: www.antara.co.id/seenws/, diakses tanggal 28 Maret 2006, pukul 11.45 WIB.

10 Aman Nursusila, *Implementasi Penegakan Hukum terhadap Kejahatan di Bidang Komputer,* Tesis, Program Pascasarjana Universitas Brawijaya, Malang, 2003, hal 45.

11 *International Review of Criminal Policy-United Nations Manual on the Prevention And Control of Computer-Related Crime*. Http://www.uncjin.org/Documents/ Eigthcongress. Html. Diakses Tanggal 23 Maret 2005, Pukul 14.29 WIB.

12 Sue Titus Reid. *Crime and Criminology*, CBS College Publishing, New York, 1985, p. 316

Theories of making and enforcing criminal law (also here in referred to as theories of law and criminal justice) offer answers to questions of how or why certain behavior and people become defined and are dealt with as criminal in society. Why is a particular conduct considered illegal and what determines the kind of action to be taken when it occurs? How is it decided, and who makes the decision, that such conduct is criminal? And how are the resources of the public and state brought to bear against it? Theories try to answer these questions by proposing that social, political, and economic variables affect the legislation of law, administrative decisions and rules, and the implementation and operation of law in the criminal justice system. [13]

Penulis berpendapat, teori krimiologi yang dapat digunakan untuk mengkaji kejahatan yang berhubungan dengan komputer adalah teori asosiasi diferensial (*Differential Association Theory*), dan teori netralisasi (*Neutralization Theory*). Ini didasarkan pada pertimbangan bahwa secara teoretik ada kesesuaian antara proposisi-proposisi dalam teori tersebut dengan karakteristik pelaku kejahatan tersebut.

Frank William III, and Marilyn McShane berpendapat bahwa teori asosiasi diferensial dikemukakan oleh seorang sosiolog Amerika Serikat, Edwin H. Sutherland pada tahun 1939 yang kemudian disempurnakan tahun tahun 1947.[14] Teori ini dibangun berdasarkan 3 teori, yaitu Ecological and Cultural Transmission Theory dari Shaw dan McKay; Symbolic Interactionism dari George Mead; dan Culture Conflict Theory. Teori asosiasi diferensial mengkaji tentang elemen-elemen dalam masyarakat yang berpengaruh terhadap seseorang yang melakukan perbuatan kriminal. Teori ini dapat diterapkan pada kasus anak-anak maupun orang dewasa. Hal ini tampak dalam penjelasan berikut, " *strenght ... explains onset of criminality. Expalins the presence of crime in all elements of social structure. Explains why some people in hight crime areas refrain from criminality. Can apply to adults and juveniles".* [15]

Sutherland berpendapat, pengertian asosiasi diferensial adalah sebagai "*the contents of the patterns presented in association would differ from individual to individual*". Dalam pengertian tersebut terungkap bahwa isi dari pola keteladanan yang diperkenalkan dalam asosiasi akan berbeda antara individu ke individu. Meskipun demikian, bukan berarti bahwa hanya pergaulan dengan penjahat saja yang akan menyebabkan perilaku jahat, tetapi yang paling penting adalah isi dan proses komunikasi dengan orang lain tersebut.[16] Teori asosiasi diferensial mengutamakan proses belajar seseorang sehingga kejahatan, sebagaimana tingkah laku lain pada manusia, merupakan sesuatu yang dapat dipelajari. Dasar pemikiran yang melandasi teori tersebut adalah *"a criminal act accur when a situation appropriate for it, as defined by the person, is present*."[17] Hal ini dapat dipahami karena menurut Clements Bartollas paradigma yang melandasi teori asosiasi diferensial adalah *"...that delinquency, like any other form of behavior, is product of social interaction.... That individuals are constantly being changed as they take on the expectations and points of view of people with whom*

13 Ronald L. Akers and Chistine S. Seller, *Criminological Theories: Introduction, Evolution, and Application*. Fourt Edition, Roxbury Publishing Company, Los Angles California, 2004, hal. 20.

14 Frank William III, and Marilyn McShane, *Criminology Theory*, Princ Hall, Englewood, 1988, p. 49-50.

15 Larry J. Siegel, *Criminology,* West Publishing Company, St. Paul. 1989, hal. 336

16 Made Darma Weda. *Kriminologi*, Rajawali Press, Jakarta, 1996, hal. 26.

17 Paulus Hadisuprapto, *Juvenile Delinquence: Pemahaman dan Penanggulangannya*, PT Citra Aditya Bakti, Bandung, 1997, hal. 19.

they interact in intimate small groups.[18] Teori ini berdasarkan pemikiran bahwa, kenakalan sebagaimana bentuk perilaku lainnya, merupakan hasil interaksi sosial. Individu secara konstan akan berubah ketika menerima harapan dan pokok-pokok pandangan masyarakat, terutama dari mereka yang saling berhubungan dengan teman karib dalam kelompok kecil.

Larry J. Siegel mengungkapkan, "*Major premise youth learn ways of neutralizing moral restrain and periodically drift in and out of criminal behavior pattern. Explains way may delinquents do not adult criminals. Explains why youthful law violators can participate in conventional behavior*." [19] Pendapat utama teori netralisasi (*neutralization theory*), bahwa seseorang akan belajar untuk menetralkan moral yang mengendalikan tingkah laku manusia, kemudian melakukan perilaku menyimpang. Selain itu, teori ini menjelaskan bagaimana cara para pemuda melakukan penyimpangan, dan cara para pemuda tersebut terlibat dalam tingkah laku menyimpang. David Matza menegaskan, "*Theory neutralization stresses youth's learning of behavior rationalizations that enable them to overcome societal values and norms and engage in illegal bahaviour.*[20] Teori netralisasi menekankan tentang pembelajaran kaum muda untuk merasionalisasi perilaku menyimpang yang dilakukan sehingga diharapkan dapat memperdaya bekerjanya nilai-nilai kemasyarakatan dan norma-norma dalam masyarakat. John Hagan mengemukakan sebagai berikut.

At base, neutralization theory assumsed that peoples action are guided by their thought. Thus, the question asked by this theory is, what is it about the thought of otherwise good people that sometimes turn them bad? It can be noted that question posed assumsed that most people most of the time, are guided by "good" thought. In other words, neutralization theory, assumsed there is general agreement in our society about "the good think life" and the approriate ways of optaining them. [21]

Teori netralisasi mengasumsikan, bahwa tingkah laku manusia dikendalikan oleh pemikiran-pemikiran pelaku. Teori ini menanyakan, apakah yang ada di balik pemikiran orang-orang yang baik sehingga kadang-kadang membuat mereka berubah menjadi orang yang berperilaku jahat atau buruk atau menyimpang dari norma masyarakat? Berdasarkan pertanyaan tersebut, teori ini menganggap bahwa kebanyakan orang, dalam sebagian besar waktunya, pada saat melakukan sesuatu perbuatan dikendalikan oleh pemikiran-pemikiran yang baik, tetapi mengapa orang yang pada umumnya memiliki pemikiran yang baik tersebut sampai melakukan perbuatan yang menyimpang atau melakukan kejahatan. Untuk menjawab pertanyaan tersebut, Sykes dan Matza mengemukakan, bahwa "*The delinquent, is a apologenic failure, who drifs in to deviant lifestyle througt of justification "we call these justifications of devian behavior techniques of neutralization; and we believe these techniqies make up crucial component of Sutherland's definitions forable to the violation of law."*[22] Pelaku kejahatan adalah seorang yang *apologetic failure,* yaitu orang-orang yang gagal meminta maaf atas perbuatannya, kemudian terbawa ke dalam suatu gaya hidup yang menyimpang dari norma. Proses tersebut berlangsung secara halus, dan hal tersebut digunakan oleh pelaku sebagai pembenaran atas tingkah lakunya.

18 Clement Bartollas, *Juvenile Delinquency,* Second Edition, MacMillan Publishing Company, New York, 1990, hal 174 .

19 Laary. J. Siegel, *op.cit*., 1989, hal. 366.

20 Ibid, hal. 337.

21 John Hagan, *Modern Criminology, Crime, Criminal Behavior and its Control*. Mc Graw-Hill Inc, Singapore, 1985, hal. 156.

22 *Ibid*. hal. 159.

Pembenaran terhadap penyimpangan perilaku seseorang melibatkan banyak komponen yang rumit sebagaimana proses pelanggaran hukum sebagaimana didefiniskan oleh Shuterland. Selanjutnya, Sykes dan Matza menjabarkan 5 (lima) teknik netralisasi yang dapat dilakukan oleh pelaku kejahatan, yaitu sebagai berikut.

a. *Denial of Responsibility. Here delinquents picture themselves as the helpness agent of cocial forces (e.g. unloving parent, bad companions, or the slum neighborhood). Thus the lament of the delinquent to officer krupke in west side story, I am not a delinquent, I am missunderstood, I am psychologically disturbed.*
b. *Denial of Injury. Here delinquents argue that their behavior doesn't really cause any great harm. Thus vandalism is seen as "mischief", auto theft as "borrowing", and gang fighting as "private quarrel".*
c. *Denial of Victim. Here delinquents conceive of themselves as avangers, while victims are transformed in to wrongdoers. For example, the delinquents might describe themselves as "Robin Hood", stealing from the rich to give to the poor.*
d. *Condemnation of the Condemners. Here delinquents allage thet their captors a either hypocrites, deviants in disguise, or impelled by personal spite. The effecs of this approach is to "chenge the subject" of concern, placing the focus instead on the alleged misdeeds of others.*
e. *Appeal to Higher Loyalities. Here delinquents see themselves as caught between the demands of society, its laws, and the needs of smaller groups (siblings, the gang, or the frienship clique). The appeal is to "frend and familly first.* [23]

23 *Ibid*., p. 159-160.

Berdasarkan paparan tentang teori nertralisasi di atas, dapat dipahami bahwa teori netralisasi mengungkapkan bahwa tingkah laku menyimpang atau jahat dilakukan seseorang karena didasarkan pada pemikirannya sendiri dan didorong oleh beberapa kondisi di luar individu, sehingga pelaku selalu mencari alasan pembenar atas perbuatannya melalui proses rasionalisasi.

Berkaitan dengan banyaknya faktor penyebab dan bervariasinya faktor yang melatarbelakangi suatu bentuk kejahatan, Sutherland dan Cressey menjelaskan dalam uraian tentang *The Multiple Factors "Theory*" berikut.

> *"The multiple-factor approach, which is not theory, is use primarily in discussions of individual cases of crime, but one form of this approach is also used in analyses of variation in crime rate. Persons who study individual cases by means of this approach are convicted that one crime is caused by one combination of circumstances or "factor", another crime is caused by another combination of circumstances or "factor". This eclecticism is often considered more rigorously "empirical" than explanations states in terms of an integrated theory*." [24]

Selanjutnya Sutherland dan Cressey mengemukakan, bahwa *"This 'theory' should be recognized as an admission of defeat, for its means criminological studiest must always be 'exploratory'. The criminologist can carry his conclusions beyonds multiple factors and reduce the series of factors to simplicity by the method of logical abstraction*."[25] Berdasarkan uraian ini dapat dipahami bahwa "teori" multifaktor

24 Edwin H. Sutherland and Donald Cressey, *Principles of Criminology,* J. B. Lippincott Company, Chicago, Philadelphia, New York, 1960, hal. 59.
25 Ibid, hal. 71.

harus dipahami sebagai suatu pintu masuk untuk mengkaji kejahatan, karena perangkat studi kriminologi dapat menjelaskan kejahatan melalui suatu penyelidikan, kemudian kesimpulan tersebut dapat menyederhanakan metoda logika abstraksi dalam kriminologi.

METODE PENELITIAN

Penelitian ini dilakukan di Unit V Infotek/*Cybercrime*, Direktorat II bidang Ekonomi dan Khusus, Mabes Polri. Pengumpulan data dilakukan pada bulan Desember 2005 dan Januari 2006. Jenis data primer dan sekunder diperlukan dalam penelitian ini,[26] data primer dalam penelitian ini diperoleh dari responden di lokasi penelitian, sedangkan data sekunder diperoleh dari Daftar Kasus *Cybercrime* di Unit V Infotek/*Cybercrime* Mabes Polri dan mesia massa. Pengumpulan data primer dilakukan dengan teknik wawancara. Peneliti menggunakan panduan wawancara (*intervew guide*), dan responden diberi kesempatan memberikan jawaban atas pertanyaan penulis secara terbuka (*open ended*). Teknik wawancara seperti ini, disebut wawancara terbuka (*open ended responses)*.[27] Analisis data dilakukan secara kualitatif dengan cara menguraikan secara deskriptifanalitis dan preskriptif terhadap gejala kriminologis. Dalam melakukan analisis kualitatif yang bersifat deskriptif dan preskriptif ini, analisis bertitik tolak pada analisis sistematis yang dilengkapi dengan analisis empiris serta analisis komparatif.[28] Dalam anaslis data, penulis menggunakan teknik berpikir deduktif. Soerjono Soekanto berpendapat teknik berpikir deduktif dilakukan dengan bertitiktolak pada hal-hal yang abstraks untuk diterapkan pada proposisi-proposisi konkret.[29] Teknik ini dilakukan dengan cara menerapkan 2 teori kriminologi dalam kasus-kasus kejahatan yang berhubungan dengan komputer di Indonesia.

HASIL PENELITIAN

Berdasarkan data di Mabes Polri, ada 2 kategori kejahatan, yaitu (a) komputer sebagai sasaran kejahatan, dan (b) komputer sebagai sarana kekejahatan. Bentuk kejahatan yang berhubungan dengan komputer yang paling banyak terjadi di Indonesia adalah pemalsuan kartu kredit (*carding*). Selanjutnya secara berurutan, dari jumlah kasus yang terbesar ke yang terkecil adalah kasus *terorism*, *cracking*, *Banking Fraud, DoS/DDoS attack, Pornography, Illegal access,* pelanggaran hak cipta, penjiplakan situs (*typosquatting*), *Hacking,* penyebaran virus (*worm*), pencucian uang (*money laundering*), dan penggunaan jaringan internet milik pihak lain secara tidak sah (*phreaking*). Jumlah kejahatan terbesar terjadi pada tahun 2002, yaitu 126 kasus, sedangkan jumlah terkecil terjadi pada tahun 2001, yaitu hanya 11 kasus.[30] Danny Firmansyah ditangkap polisi karena melakukan *defacing* situs Komisi Pemilihan Umum (KPU). Pada tanggal awal bulan Agustus 2006, Unit V Infotek *Cybercrime* menangkap Iqra Syafaat, tersangka *defacing* situs Partai Golongan Karya.[31]

Berdasarkan hasil wawancara dengan Dicky Patrianegara, motivasi atau

26 Saoerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif, Suatu Tinjauan Singkat*, Rajawali Pres, Jakarta , 1995. hal. 12-13.

27 J. Vredenbregt, *Metode dan Teknik Penelitian Masyarakat*, PT Gramedia, Jakarta, 1978, ha. 87.

28 Sunaryati Hartono, *Penelitian Hukum di Indonesia pada Akhir Abad ke-20*, Alumni, Bandung, 1991, hal. 103.

29 Soerjono Soekanto, *Kesadaran Hukum dan Kepatuhan Hukum*, Rajawali, Jakarta, 1982. ha. 144

30 Daftar Perkara *Cybercrime* di Unit V Infotek/*Cybercrime* Mabes Polri, Januari 2006.

31 "Tersangka *Hacking* Situs Golkar Dibekuk", http://www.metrotvnews.com/ berita.asp?id=21857, diakses tanggal 2 Agustus 2006 pukul 08.00 WIB).

penyebab pelaku kejahatan yang berhubungan dengan komputer sangat bervariasi, tergantung pada bentuk kejahatan yang dilakukan dan karakteristik pribadi pelaku kejahatan. Selanjutnya diuraikan sebagai berikut.

a. Saat ini ada perubahan motivasi melakukan kejahatan. Jika dahulu para pelaku *cracking*, *Denial Service (DoS) Attack* atau *Distributed Denial Service (DDoS) Attack* atau kejahatan lain terhadap sistem atau jaringan komputer melakukan kejahatan karena merasa tertantang dengan teknologi, mencoba keandalan pengamanan sistem komputer pihak lain, dan bersenang-senang, saat ini banyak pihak termotivasi untuk memperoleh imbalan berupa uang (motivasi ekonomi). Saat ini seorang *cracker* dapat melakukan *cracking* karena diberi upah oleh orang pihak lain. Motivasi pihak yang menyuruh *cracker* (pemilik uang) antara lain balas dendam (karena situs miliknya pernah diserang), persaingan usaha, untuk mengetahui rahasia dagang pihak lain.
b. Dalam kasus *typosquating,* pelaku kejahatan dimotivasi oleh keinginan agar para pengguna *e-banking* dalam bertransaksi lebih berhati-hati dalam memasukkan PIN dan identitas pengguna (*user identity*), meskipun seringkali terjadi penipuan. Kasus ini terjadi pada *typosquatting* Bank Bank Central Asia (BCA).
c. Dalam kasus-kasus yang dapat mendatangkan keuntungan berupa uang, misalnya *carding,* penipuan melalui bank (transfer uang secara fiktif, transfer uang tanpa hak), tindak pidana korupsi, penyalahgunaan nama domein, pelanggaran hak cipta, dan *phishing*, sebagian besar pelaku didorong oleh motif untuk mendapatkan uang secara melawan hukum.
d. Motif politik dapat juga mendorong tindakan *cracking, defacing,* dan *DoS Attack*, misalnya pada saat antara Indonesia dengan Malaysia sedang membicarakan status Kepulauan Ambalat tahun 2005. Motif kekecewaan sekelompok orang atau sekelompok *cracker* dapat memacu kejahatan yang berhubungan dengan komputer. [32]
e. Selain itu, saat ini ada beberapa pelaku kasus pelanggaran lain yang dimotivasi oleh oleh rasa ingin menampilkan kelucuan (*funny*).[33] Banyak kasus yang terjadi di masyarakat tidak dapat diselesaikan dengan hukum pidana, karena perangkat hukumnya belum memadai. Penyebab pelaku kejahatan cukup beragam dan kompleks, bahkan antara kasus satu dengan lainnya tidak selalu sama.[34] Mayoritas kejahatan tersebut diawali dengan *illegal access*.[35]

PEMBAHASAN

Berdasarkan hasil identifikasi kasus kejahatan yang berhubungan dengan komputer Unit V Infotek/*Cybercrime* Mabes Polri dan hasil wawancara dengan penyidik tentang motivasi atau penyebab pelaku dalam kejahatan komputer di Indonesia, penulis mengkaitkan antara motivasi atau penyebab pelaku kejahatan yang berhubungan dengan komputer dengan bentuk kasus yang terjadi di Indonesia. Motivasi/penyebab dan bentuk kejahatan tersebut adalah sebagai berikut.

32 Hasil Wawancara dengan Komisaris Polisi Dicky Patrianegara (Penyidik *Cybercrime*) Mabes Polri pada tanggal 22 Desember 2005 di Ruang Penyidik *Cybercrime* Mabes Polri Jakarta.).

33 Hasil wawancara dengan Kepala Unit Anti-Teror *Trans-National Unit Crime Coordination Center* (TNCC) Mabes Polri, di Ruang TNCC Mabes Polri Jakarta tanggal 23 Desember 2005.

34 Hasil Wawancara dengan Komisaris Besar Polisi Deddy S.W. di Ruang Kepala Unit V, Mabes Polri, tanggal 22 Desember 2005.

35 Hasil Wawancara dengan Komisaris Polisi Dicky Patrianegara (Penyidik *Cybercrime*) Mabes Polri pada tanggal 22 Desember 2005 di Ruang Penyidik *Cybercrime* Mabes Polri Jakarta.).

a. Mencoba kemampuan dan keterampilan diri sendiri dalam mengoperasikan peralatan teknologi informasi. Hal ini terjadi pada pada sebagian besar bentuk kejahatan yang berhubungan dengan komputer.
b. Menguji kemampuan pihak lain yang mengelola dan mengamankan situs/*web site,* misalnya dalam kasus *hacking* situs Komisi Pemilihan Umum (KPU) oleh Danny Firmansyah (2004). Hal ini juga mempunyai motivasi yang sama sebagaima dilakukan oleh Iqra Syafaat, pelaku *defacing* situs Partai Golkar dari Batam pada tanggal 9 sampai 13 Juli 2006.
c. Bersenang-senang, misalnya pada kasus *defacing* di beberapa situs, termasuk *defacing* situs "AREMA *FOOT BALL CLUB*" Malang pada bulan Agustus 2006.
d. Ingin dianggap sebagai pahlawan *(hero)*, misalnya pada beberapa kasus *hacking* situs ke *website Connect Ireland* yang dianggap memperjuangkan kemerdekaan Timor Timur tahun (tahun 1998).
e. Memperkenalkan atau mempopulerkan kelompok *hacker,* misalnya dalam kasus *hacking* situs ke Bursa Efek Jakarta (BEJ), Bank Central Asia (BCA) dan Indosat-*net* yang dilakukan oleh *hacker* yang menyebut dirinya *fabianclone* dan *naisenodni* (tahun 2000).
f. Memperoleh uang dengan cara tidak sah, misalnya dalam kasus *Banking Fraud* di BCA Cabang Purwokerto (tahun 2001) dan *carding* di beberapa daerah. Motivasi ini sama dengan kasus memalsuan kartu kredit dengan menggunakan *Shimmer* sebagaimana dilakukan di beberapa pusat perbelanjaan di Jakarta dan Surabaya tahun 2006.
g. Balas dendam, misalnya *cracker* yang diduga berasal dari China, yang menyebut dirinya *discover,* mengacak-acak situs milik Badan Koordinasi Keluarga Berencana Nasional (BKKBN). Serangan ini merupakan reaksi atas pemberitaan media massa mengenai Kerusuhan Mei 1998 yang mengakibatkan etnis China di Indonesia menjadi korban pembantaian dan pemerkosaan. Serangan tersebut juga dibalas oleh *cracker* Indonesia.
h. Motif politik, misalnya kasus *craking* yang dilakukan *cracker* Indonesia ke *website Connect Ireland*, yaitu perusahaan yang dikenal sebagai penyedia *server* untuk situs yang beroperasi di bawah *East Timor Project* (*web* yang memeperjuangkan kemerdekaan Timor Timur) (tahun 1997), ancaman terhadap Perdana Menteri Australia.
i. Pelampiasan kekecewaan, misalnya dalam kasus serangan ke Situs Ajinomoto. Serangan ini merupakan reaksi atas dugaan pengguanaan *enzim porcine* yang sebagai katalis dalam proses pembuatan *monozodium glutamate* (bumbu penyedap rasa) yang mengandung lemak babi.
j. Persaingan usaha, misalnya dalam kasus penyalahgunaan nama domein Mustika-ratu.com (tahun 2002).

Berkaitan dengan motivasi, Avinanta Tarigan dan I Made Wiryana menjelaskan bahwa motivasi para *hacker* untuk menemukan *vunerability* adalah untuk membuktikan kemampuan pelaku dalam bidang teknologi informasi atau sebagai bagian dari sarana kontrol sosial terhadap sistem komputer pihak lain. Sedangkan motivasi para *cracker* sangat beragam, antara lain untuk propaganda (melalui *defacing* terhadap *website*), penyerangan destruktif (disebabkan oleh perasaan dendam atau ketidaksukaan terhadap suatu institusi) dan lain-lain.[36]

Penulis berpendapat, bahwa suatu bentuk kejahatan yang berhubungan

36 Avinanta Tarigan dan I Made Wiryana, "*Pertimbangan Sekuriti Pada Sistem Informasi Kelautan Nasional"*, RVS Arbeitsgruppe, Universität Bielefeld, http://www. antareja.rvs.uni-bielefeld.de/avinanta/Publication/Kelautan. Diakses tanggal 28 Januari 2006, pukul 13.00 WIB.

dengan komputer mungkin didorong oleh lebih dari satu jenis motivasi. Dalam kejahatan yang menggunakan komputer sebagai sasaran, misalnya korupsi, penipuan, *carding*, dan *banking fraud,* motif untuk memperoleh uang secara tidak sah lebih utama dibandingkan dengan motif-motif lainnya. Dalam kasus kejahatan yang menjadikan komputer sebagai sasaran, misalnya *defacing, cracking, DoS Attack, DDoS Attack,* motivasi utama pelaku adalah menguji kemampuan pihak lain, mencoba kemampuan diri sendiri, pelampiasan kekecewaan, balas dendam, ingin dianggap sebagai pahlawan, memperkenalkan popularitas kelompok *hacker*, dan bersenang-senang *(chalange)*. Pernyataan ini senada dengan pendapat Sue Titus Reid bahwa motivasi seseorang melakukan kejahatan yang berhubungan dengan komputer cukup bervariasi, yaitu bersenang-senang, meniru sebagaimana yang pernah ditampilkan di televisi atau film, dan melakukan sensasi baru.[37] Sedangkan menurut M. Arthur Gillis, motivasi pelaku kejahatan yang berhubungan dengan komputer bukan semata-mata karena uang, melainkan unsur *chalange,* yaitu bagaimana menyiasati *(ourtmartings)* suatu sistem komputer dan melakukan semua kegiatan tersebut untuk kesenangan.[38]

Berdasarkan hasil wawancara dengan Dicky Patrianegara, semua pelaku kejahatan yang berhubungan dengan komputer seakan-akan sudah menjadi anggota komunitas dunia maya (*underground)*.[39] Dony Budi Utoyo mengemukakan bahwa internet dapat digunakan sebagai media pembelajaran melakukan aktivitas "dunia nyata", termasuk teknik melakukan kejahatan, karena diantara anggota komunitas seringkali mengadakan pembicaraan santai/*ngrumpi (chatting)* sampai beberapa jam dalam sehari. Dalam proses *chatting* inilah sering diperoleh informasi tentang cara-cara melakukan kejahatan melalui jaringan komputer. Siapapun dapat melakukan *chatting* di internet, dan siapapun dapat secara mudah mendapat informasi, termasuk teknik penyusupan (*illegal access*) ke situs milik pihak lain. *Chatting* lebih digemari komunitas *underground* dari pada *e-mail*, karena proses penyampaian pesan lebih cepat, begitu pula tanggapan dari pihak lain. *Chatting* tidak memerlukan biaya, karena sudah termasuk dalam biaya akses internet, sedangkan *e-mail* kadangkala harus membayar, dan mendaftar terlebih dahulu pada saat akan menjadi *user*, misalnya pengiriman *e-mail* melalui *wasantara.net*. Sedangkan *e-mail* yang tidak perlu membayar (tetapi harus mendaftar) adalah mengirimkan *e-mail* melalui *telkom.net*. Selanjutnya Donny Budi Utoyo mengungkapkan, bahwa untuk kalangan *underground* yang sering melakukan *carding* dapat mamenfaatkan *chatroom*, yaitu sebuah media bagi para *carder* untuk bertukar data kartu kredit bajakan dan berjual-beli barang hasil *carding*.[40]

Untuk memberikan gambaran mengenai komunikasi antaranggota *underground*, berikut penulis mengutip isi komunikasi (*massage*) melalui internet. Pesan berikut disampikan kepada Jasakom (http:www.jasakom.com) yang meminta komentar kepada komunitas *underground* atas artikel yang ditulis tentang kelemahan beberapa sistem pengamanan sistem komputer di perusahaan-perusahaan di Indonesia. Artikel yang dimuat oleh Jasakom tersebut ternyata mendapat tanggapan negatif dari ahli-ahli teknologi informasi di Indonesia. Sedangkan para

37 Sue Titus Reid, op.cit., 1985, p. 316.

38 Muladi dan Arief, Kebijakan Hukum Pidana, Alumni, Bandung, 1998, p. 27

39 Hasil Wawancara dengan Komisaris Polisi Dicky Patrianegara (Penyidik *Cybercrime*) Mabes Polri pada tanggal 22 Desember 2005 di Ruang Penyidik *Cybercrime* Mabes Polri Jakarta.

40 Dony Budi Utoyo, "*Sebab Akibat dan Kepastian Hukum"*. Majalah Warta Ekonomi, Edisi No.15, Tahun XVI, tanggal 28 Juli 2004.

anggota *underground* lain justru menulis komentar, antara lain sebagai berikut.

Nama : sun gu kong
Comment : GUE PUNYA SEKITAR 150 NOMOR KARTU KREDIT YANG VALID + EXPIRED NUMBER + DATA-DATA PEMILIKNY NYA YANG LENGKAP (KEBANYAKAN PUNYA ORANG LUAR NEGERI). GUE BAKALAN BAGI2 KE LOE SEMUA.. DENGAN SYARAT KITA BARTER !! GUE NGA TERIMA YANG MAU GRATISAN !! CIAO. AL TALAVISTA.
ID : 3021

Nama : .::: blu3St4r :::.
Comment : pokoke JASAKOM harus seperti biasanya ! (maksa nihh!! =)..) jgn TAKUT! PANTANG MUNDUR!! kita SUPPORT abizz deh!! kalo nggak gini kapan lagi dunia cyber kita grow-up! buat om-om gedongan yg pada komplain ke JASAKOM pecat aja ADMINnya udah bego masih dipel lihara ngabisin duit aja! viva the UNDERGROUND WORLD INDONESIA!
ID : 379.[41]

Berdasarkan isi komunikasi tersebut, dapat diketahui bahwa komunikasi dapat mengarahkan setiap anggota *underground* untuk menindaklanjuti materi pesan tersebut, bahkan melakukan kejahatan. Selain itu, dalam internet seringkali ditemukan materi-materi yang menggambarkan terjadinya komunikasi antara anggota *underground* satu dengan yang lainnya untuk saling belajar melakukan kejahatan melalui internet.

Komunikasi bukan hanya dilakukan di lingkungan Indonesia, tetapi dapat juga dengan komunitas *underground* di luar negeri.

Komunikasi antaranggota *underground* lewat "dunia *real*" dapat juga dilakukan. Suheimi menulis, bahwa salah seorang *hacker* pernah menyebarluaskan *print out* hasil *hacking* yang diberikan secara langsung kepada sesama *hacker* dalam suatu pertemuan rahasia yang dihadiri para anggota *underground*. Data yang disebarluaskan adalah data bank yang memuat tentang nama-nama nasabah, termasuk jumlah uang yang dimiliki, tempat tanggal lahir, hutang-hutang, besarnya pendapatan, kartu kredit yang dimiliki beserta tanggal pembuatan dan daluwarsa, dan besarnya jumlah maksimal dalam suatu penarikan.[42]

Indikasi lain yang menunjukkan bahwa proses belajar melakukan kejahatan dapat diperoleh melalui internet dengan proses komunikasi, yaitu sebagaimana diuraikan Dani Firmansyah dalam penyidikan. Berdasarkan hasil penyidikan, tersangka pernah melakukan *test system security* www.kpu.go.id melalui XSS (*Cross Site Scripting*) dengan menggunakan *IP Public* PT Danareksa 202.158.10.117, tetapi tidak berhasil. Setelah itu, tersangka melakukan *chatting* sesama komunitas *underground* (yaitu *Indolinux, IndofreeBSD dan IndoOpenBSD*) dengan melakukan BNC ke IP 202.162.36.42 Warna Warnet di Jalan Kaliurang Kilometer 8 Yogyakarta dengan nama samaran Xnuxer, kemudian langsung ke server IRC Dalnet (Mesra) yang ada di Malaysia. Setelah gagal melakukan *cracking* situs KPU, pada hari berikutnya tersangka mencoba lagi menyerang *server* tnp.kpu.go.id. dengan cara SQL Injection yaitu menyerang dengan cara memberi perintah melalui program SQL, dan berhasil menembus IP tnp.kpu.go.id

41 http:www.jasakom.com/Artikel.asp, diakses, tanggal 28 Januari 2006, pukul 11.25. WIB.

42 Suheimi, *Kejahatan Komputer*, Andi Offset, Yogyakarta, 1990, hal. 146-147.

203.130.201.134 serta berhasil meng-*update* Tabel Nama Partai Politik Peserta Pemilihan Umum.[43] Berdasarkan hasil penyidikan tersebut dapat diketahui bahwa dalam melakukan kejahatan, tersangka melakukan komunikasi dan belajar melakukan kejahatan dengan sesama *underground.* Setelah berkomunikasi dan berkonsultasi, tersangka mampu melakukan *defacing*.

Selain belajar melakukan teknik penyusupan ke sistem komputer melalui internet, di Indonesia saat ini sudah beredar buku tentang *hacker* yang ditulis oleh *hacker* profesional yang memungkinkan setiap orang mempelajari teknik melakukan akses ilegal. Buku tersebut dapat digunakan oleh siapa saja untuk mempelajari teknik *hacking* dan *cracking.* Salah stu buku tersebut adalah Buku "Seni Teknik *Hacking* 1: *Uncensored* (SIH)" berisi 216 halaman yang ditulis oleh Sto, dan diterbitkan oleh Jasakom *Publishing*. Nama penulis buku ini sangat terkenal di dunia *underground*, bahkan dianggap sebagai pakar *hacking* karena sering berkomunikasi dan memberi komentar melalui internet. Buku tersebut berisi kumpulan teknik *hacking* yang sering digunakan para *hacker* yang sudah berhasil gemilang. Buku jilid pertama ini mengupas secara detail tentang dasar-dasar *hacking.* Teknik-teknik tentang aplikasi *hacking* lainnya akan dibahas pada jilid-jilid selanjutnya. Dalam waktu singkat, buku ini sudah dicetak ulang empat kali karena besarnya jumlah permintaan. Dalam cetakan ke-4 tersebut sebagai edisi yang disempurnakan tersebut mencantumkan bab khusus tentang *hacking* ke KPU dan *Frequently Asked Question (FAQ)*. Buku yang sangat laris di pasaran tersebut terutama dibeli oleh para pelajar dan mahasiswa. [44]

Sebagai perbandingan, sejak tahun 1971 sampai dengan 1973 di Amerika Serikat sudah ada media massa cetak yang khusus menerbitkan sarana komunikasi antar-*hacker*, misalnya Majalah Technological Assistance Program (TAP), antara lain memuat tentang cara pembuatan bom logika *(logic bomb),* pemalsuan kartu kredit, skema elektronik pembuatan *blue box*, kode-kode jaringan. Selain itu, pada tahun berikutnya sudah terbit beberapa Jurnal dan Majalah, antara lain *Journal 2600, Majalah Phrack, Processed World, Computel, Underground Informer Magazine,* dan *Bootlegger.* Media massa tersebut digunakan sebagai sarana tukar-menukar informasi antaranggota *underground.* [45]

Komunikasi dan pembelajaran melakukan kejahatan dari kelompok intim melalui internet, buletin khsusus, dan buku sebagaimana terjadi di Indonesia di atas selaras dengan uraian dalam *International Review of Criminal Policy-United Nations Manual on the Prevention and Control of Computer-Related Crime* sebagai berikut.

... Corresponding with this increasing cooperation in criminal activity, the escalating underground use of electronic bulletin boards for clandestine criminal communication has been detected around the world. Rapidly improving telecommunication technology has added to the threat from external sources. Computer-based voice mailbox systems, for example, are being used by the computer criminal community to exchange stolen access numbers, passwords and software. [46]

Hasil wawancara, fakta di internet, dan hasil penelitian penulis, serta isi dokumen PBB tersebut dapat mendukung kebenaran teori asosiasi diferensial bahwa

43 http:www. investorindonesia.com/news.html, diakses tanggal 30 Januari 2006, pukul 09.23 WIB).

44 http://herusutadi.com/media/20041216.shtml, diakses tanggal 30 Januari 2006 pukul 09.35.

45 Suheimi, *op.cit*., 1990, p. 89-92.

46http://conventions.coe.int/treaty/EN/Treaties/Html/185.htm, diakses tanggal 20 Desember 2006, pukul 10. 30 WIB.

kejahatan dipelajari melalui proses komunikasi dengan kelompok intim. Dalam konteks kejahatan yang berhubungan dengan komputer, teknik-teknik melakukan kejahatan tersebut dipelajari melalui komunikasi melalui internet (*chatting)*, buku-buku referensi, dan teman pergaulan *(peer group)*. Interaksi antarpelaku dalam komunitas maya dapat dilakukan melalui komunikasi kapan pun dengan media komputer maupun *hand phone* atau media lainnya dalam durasi waktu yang lama dan jangkauan yang luas. Komunikasi dan interaksi bukan hanya dilakukan di dunia virtual, tetapi juga bertemu secara langsung di suatu tempat tertentu, bahkan saat ini di Jakarta sudah ada sejenis "pasar gelap" yang digunakan sebagai media jual-beli hasil kejahatan (terutama hasil *carding*) yang berhubungan dengan komputer sekaligus media pertemuan para *underground.* Bahkan, menurut data di Mabes Polri, pelaku tersebut banyak yang berstatus mahasiswa dan relatif muda. Hal ini selaras dengan pernyataan Kongres PBB bahwa, *Such younger people may not yet be assimilated in to the ethics, and the organization of their professions, and they have often been trained in college and university campuses where "attacking campus computer system is not only condoned but often encouraged as an educational activity*".[47]

Dengan demikian, beberapa proposisi teori asosiasi diferensial, dapat digunakan untuk mengetahui tentang latar belakang terjadinya kejahatan yang berhubungan dengan komputer di Indonesia, dari sisi pelaku tindak pidana. Proposisi Sutherland yang relevan bahwa kejahatan dipelajari dapat seseorang, termasuk dalam teknik-teknik melakukan kejahatan, melalui proses komunikasi pada kelompok intim dalam jangka waktu relatif lama.

Berdasarkan perspektif teori netralisasi, kejahatan yang berhubungan dengan komputer di Indonesia ada yang dimotivasi oleh keinginan balas dendam, misalnya dalam kasus *craking* situs yang dilakukan oleh *cracker* Indonesia ke situs di Irlandia, karena dianggap sebagai basis gerakan prokemerdekaan Timor Timur. Selain itu, situs Polri juga pernah di-*hack* oleh Kesatuan Aksi *Cracker* Muslimin Indonesia (KAHMI). Serangan ini merupakan reaksi atas ditangkapnya pimpinan dari Pasukan Komando *Jihad*. Alasan kejahatan tersebut, dalam teori netralisasi disebut *Denial of Victim,* yaitu pelaku memahami diri mereka sendiri sebagai "sang penuntut balas", sedangkan para korban dari perbuatannya dianggap sebagai orang yang bersalah.

Dalam beberapa kasus yang pelaku kejahatan hanya berkeinginan mencoba kemampuan diri sendiri dalam bidang teknologi informasi dan keandalan pengamanan atau *pasword* korban (kasus *defacing* situs Partai Golkar) , dan bahkan pelaku hanya ingin bersenang-senang karena akibatnya dianggap tidak serius (kasus *blogger*), dan korban dianggap kriminogen karena pernah *sesumbar* di media Massa (Kasus defacing situs KPU). Dalam teori netralisasi, motivasi perbuatan tersebut ini disebut *denial of Injury,* yaitu pelaku berpandangan bahwa perbuatan yang dilakukan tidak menyebabkan kerugian yang besar pada masyarakat.

Dalam teori netralisasi dikenal

47Commission on Crime Prevention and Criminal Justice, Follow-up to the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders: Draft Plans of Action for the Implementation During the Period 2001-2005 of the Vienna Declaration on Crime and Justice, Meeting the Challenges of the Twenty-first Century, E/CN.15/2001/5, Tenth session, Vienna, 8-17 May 2001.

istilah *appeal to higher loyalities,* yaitu pelaku merasa bahwa dirinya terperangkapantara kemauan masyarakat dan ketentuan hukum yang ada di mayarakat dengan kebutuhan kelompok yang lebih kecil, yaitu kelompok tempat mereka berada atau bergabung. Ini misalnya terjadi pada kasus Dody, seorang mahasiswa Fakultas Matematika dan Ilmu Pengatahuan Alam (MIPA) Universitas Brawijaya Malang membobol bank, dan hasilnya digunakan untuk memenuhi kebutuhan sebagai mahasiswa dan menyumbang korban kerusuhan di Sampit Kalimantan Tengah. [48]

Motivasi ini juga terjadi pada sebagian besar pelaku kejahatan yang berhubungan dengan komputer, terutama dalam kasus *defacing, cracking* yang dilakukan oleh kelompok *cracker* untuk meraih popularitas. Pembenaran beberapa komunitas *underground* terhadap "Manifesto *Hacker*" (dari John Perry) yang tidak menghendaki adanya ketentuan hukum yang mengatur tentang aktivitas di *cyberspace* dapat disamakan dengan teknik netralisasi sebagaimana dikemukakan oleh Sykes dan David Matza, yaitu *condemnation of the condemners,* yakni pelaku beranggapan bahwa orang yang mengutuk perbuatan yang telah dilakukan sebagai orang-orang munafik, hipokrit, sebagai pelaku kejahatan terselubung, karena dengki, dan sebagainya.

Berdasarkan analisis beberapa kasus di atas, juga diketahui bahwa motivasi utama orang melakukan penipuan melalui komputer adalah memperoleh keuntungan ekonomi, meskipun masih ada penyebab lainnya, misalnya keinginan untuk mencoba kemampuan sistem teknologi informasi pihak lain, dan ingin dikenal oleh sesama komunitas *underground* sebagai orang yang piawai dalam mengoperasionalisasikan komputer. Dalam kasus *defacing, cracking, DoS Attack, DDoS Attack* berbeda-beda motivasinya, ada yang hanya ingin menguji kemampuan bidang teknologi informasi pihak lain, mencoba kemampuan diri sendiri dalam mengoperasikan komputer, pelampiasan kekecewaan, balas dendam, ingin dianggap sebagai pahlawan, memperkenalkan atau meraih popularitas kelompok *hacker*, dan bersenang-senang *(chalange),* tetapi ada juga yang dimotivasi oleh kepentingan ekonomi, misalnya dalam kasus "*cracker* bayaran" sebagaimana dikemukakan oleh penyidik *Cybercrime.* Hal ini juga selaras dengan ungkapan Kepala Unit V Infotek/*Cybercrime*.

Berpijak pada penjelasan tentang, "teori" atau pendekatan multifaktor terhadap penyebab kejahatan sebagaimana dikemukakan Sutherland dan Cressey,[49] dapat diketahui bahwa pendekatan tersebut dapat digunakan untuk menjelaskan tentang penyebab pelaku kejahatan yang berhubungan dengan komputer di Indonesia. Dengan demikian, hasil penelitian penulis yang menyimpulkan bahwa pelaku kejahatan yang berhubungan dengan komputer di Indonesia disebabkan oleh berbagai faktor dan motivasi yang sangat bervariasi, dan adanya perbedaan variasi tentang faktor-faktor penyebab antara bentuk kejahatan satu dengan lainnya, selaras dengan "*multiple-factors 'theory'*".

KESIMPULAN

Bahwa penyebab utama orang melakukan penipuan melalui komputer adalah memperoleh keuntungan ekonomi, keinginan untuk mencoba kemampuan sistem teknologi informasi pihak lain, dan

48"Haus Teknologi Dody Jadi Hacker," http://www. Forum cyber News. Com., diakses tanggal 31 Maret 2006, pukul 12.00. WIB.

49 Edwin H. Sutherland dan Donald Cressey, *op.cit*., 1960, p. 59..

ingin dikenal oleh sesama komunitas *underground* sebagai orang yang piawai dalam mengoperasionalisasikan komputer. Dalam kasus *defacing, cracking, DoS Attack, DDoS Attack* berbeda-beda penyebabnya, ada yang hanya ingin menguji kemampuan bidang teknologi informasi pihak lain, mencoba kemampuan diri sendiri dalam mengoperasikan komputer, pelampiasan kekecewaan, balas dendam, ingin dianggap sebagai pahlawan, memperkenalkan atau meraih popularitas kelompok *hacker*, dan bersenang-senang *(chalange)*

SARAN

Berdasarkan kesimpulan dan manfaat penelitian sebagaimana tersirat pada pendahuluan, penulis menyarankan agar penentu kebijakan kriminal mempertimbangkan hasil analisis penyebab pelaku kejahatan yang berhubungan dengan komputer sebagai landasan merancang penalisasi, khususnya tentang jenis pidana (*strafsourt)* karena keselarasan antara jenis pidana dengan penyebab pelaku melakukan tindak pidana akan mengefektifkan pencapaian tujuan pemidanaan. Selain itu, pelaksanaan pidana yang sudah dijatuhkan (*strafmodus*) juga akan lebih efektif jika selaras dengan hasil kajian kriminologis yang mengungkap tentang karekteristik terpidana dan faktor-faktor penyebab kejahatan. Upaya kebijakan nonpenal untuk menanggulangi kejahatan yang berhubungan dengan komputer di Indonesia juga memerlukan pertimbangan dari aspek kriminologis.

DAFTAR PUSTAKA

Akkers, Ronald L. and Chistine S. Seller.*Criminolgical Theories: Introduction, Evolution, and Application,* Fourt Edition, Roxbury Publishing Company. Los Angles California, 2004.

Arief, Barda Nawawi, *Sari Kuliah*: *Perbandingan Hukum Pidana*, PT Raja Grafindo Persada, Jakarta, 2002.

Bartollas, Clement. *Juvinile Delinquency,* Second Edition, MacMillan Publishing Company, New York, 1990.

Hadisuprapto, Paulus, *Juvenile Delinquence: Pemahaman dan Penanggulangannya*, PT Citra Aditya Bakti, Bandung, 1997.

Hagan, John, *Modern Criminology, Crime, Criminal Behavior and its Control*. Mc Graw-Hill Inc, Singapore, 1985

Karnasudirja, Edy Junaidi. *Bahaya Kejahatan Komputer*, Tanjung Agung, Jakarta, 1999.

Nursusila, Aman. *Implementasi penegakan hukum terhadap Kejahatan di Bidang Komputer*. Tesis. Program Pascasarjana Univ. Brawijaya, Malang, 2003

Muladi dan Barda Nawawi Arief. *Kapita Selekta kebijakan Hukum Pidana*, Alumni, Bandung, 1998.

Reid, Sue Titus. *Crime and Criminology*, CBS College Publishing, New York, 1985.

Sunaryati Hartono, *Penelitian Hukum di Indonesia pada Akhir Abad ke-20*, Alumni, Bandung, 1991.

Soekanto, Soerjono. *Kesadaran Hukum dan Kepatuhan Hukum*, Rajawali, Jakarta, 1982.

Saoerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif*, *Suatu Tinjauan Singkat*, Rajawali Pres, Jakarta , 1995.

Suheimi. *Kejahatan Komputer*, Andi Offset, Yogyakarta, 1990.

Sutherland, Edwin H. and Donald R. Cressey. *Principles of Crimonology*, J.B. Lippincott Company, Chicago, Philadelphia, New York, 1960.

Vredenbregt, J. *Metode dan Teknik Penelitian Masyarakat*, PT Gramedia, Jakarta, 1978.

William III, Frank, and Marilyn McShane. *Criminology Theory*, Princ Hall, Englewood, 1988.

Weda, Made Darma. *Kriminologi*, Rajawali Press, Jakarta, 1996.

Rancangan Undang-Undang (RUU)

Rancangan Undang-Undang tentang Kitab Undang-Undang Hukum Pidana (RUU-KUHP) Tahun 2005, ELSAM, Jakarta, 2006.

Makalah

Nitibaskara, Tb. Ronny R., "*Problema Yuridis Cybercrime"*, Makalah pada Seminar Cyber Law, diselenggarakan oleh Yayasan Cipta Bangsa, Bandung, Juli 2000.

Majalah

Utoyo, Dony Budi, *Sebab Akibat dan Kepastian Hukum.* Majalah Warta Ekonomi, Edisi No.15, Tahun XVI, tanggal 28 Juli 2004.

Internet

Akibat Pembajakan Musik, Negara Rugi 1,8 Trilyun per Tahun. LKBN Antara, http: www.antara.co.id/seenws/, diakses tanggal 28 Maret 2006, pukul 11.45 WIB.

Commission on Crime Prevention and Criminal Justice, Follow-up to the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders: Draft Plans of Action for the Implementation During the Period 2001-2005 of the Vienna Declaration on Crime and Justice, Meeting the Challenges of the Twenty-first Century, E/CN.15/2001/5, Tenth session, Vienna, 8-17 May 2001

Dokumen Kongres PBB ke-10 di Wina, tanggal 19 Juli 2000. Http://www.uncjin.org/Documents/Eigthcongress. Html. Diakses Tanggal 23 Maret 2006, Pukul 14.00 WIB

"Haus Teknologi Dody Jadi Hacker", http://www. Forum cyber News. Com., diakses tanggal 31 Maret 2004, pukul 12.00. WIB.

International Review of Criminal Policy-United Nations Manual on the Prevention And Control of Computer-Related Crime. Http://www.uncjin.org/Documents/Eigthcongress. Html. Diakses Tanggal 23 Maret 2005, Pukul 14.29 WIB.

h*ttp://herusutadi.com/media/20041216.shtml*, diakses tanggal 30 Januari 2006 pukul 09.35 WIB.*http:www.investorindonesia.com/news.html*, diakses tanggal 30 Januari 2006, pukul 09.23 WIB.

http:www.jasakom.com/Artikel.asp, diakses, tanggal 28 Januari 2006, pukul 11.25. WIB.

http://students.ukdw.ac.id/~22971797/topik1.htm, diakses tanggal 23 Desember 2005, pukul 12.45. WIB.

http://conventions.coe.int/treaty/EN/Treaties/Html/185.htm, diakses tanggal 20 Desember 2006, pukul 10. 30 WIB.

"Motivasi Hacker Hanya Peringatkan Tim TI KPU", Investorindonesia.com, http:www.investorindonesia.com/news.html, diakses tanggal 30Januari 2006, pukul 09.23 WIB.

Susrini, Ni Ketut, "*Kejahatan Cyber 2003 Timbulkan Kerugian Rp 11,7 Miliar",* http:groups.or.id/pipermail/omepgt/2004-September/000002.html, diakses tanggal 28 Januari 2006 pukul 09.00. WIB.

Tarigan, Avinanta dan I Made Wiryana, "*Pertimbangan Sekuriti Pada Sistem Informasi Kelautan Nasional"*, RVS Arbeitsgruppe, Universität Bielefeld, *http://www. antareja.rvs.uni-bielefeld. de/avinanta/Publication/Kelautan.* Diakses tanggal 28 Januari 2006, pukul 13.00 WIB.

"*Tersangka Hacking Situs Golkar Dibekuk*", http://www.metrotvnews.com/berita.asp?id=21857, diakses tanggal 2 Agustus 2006 pukul 08.00 WIB