PENEGAKAN HUKUM TERHADAP CYBER CRIME DI BIDANG PERBANKAN SEBAGAI KEJAHATAN TRANSNASIONAL

Oleh:

Tri Kuncoro

Mahasiswa Magister Ilmu Hukum Unud

ABSTRACT

Internet has been used in various fields of life, one of which is banking. Banking activities are performed through Internet-banking. Through the internet-banking service, customers can conduct financial transactions without having to come to the bank. In this study addressed two issues namely the forms of cyber crime in the banking and jurisdiction in the law enforcement against cyber crime in banking. This research is a normative legal research. Legal materials collected through library research. In this research, legal materials were analyzed by using the description, interpretation, argumentation, evaluation and systematization.

The forms of cyber crime in banking are typo site, keylogger / keystroke recorder, sniffing, brute-force attacking, deface web, email spamming, denial of service and virus, worm, trojan. Jurisdiction in the law enforcement against cyber crime in banking jurisdiction includes legislative, executive and enforcement jurisdiction. Jurisdiction specifically stipulated in Article 2 of Act of Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions. Banks should have an electronic security system to protect the system. The Law enforcement against cyber crime in banking requires cooperation between countries.

Key words: law enforcement, jurisdiction, cyber crime, banking.

I. PENDAHULUAN

1. Latar Belakang

Internet banking merupakan salah satu bentuk transaksi elektronik/ *electronic transaction,* seperti halnya ATM (*Automatic Teller Machine)* dan *credit card*, yang ditawarkan kepada nasabah secara elektronik melalui *website*. Nasabah dapat melakukan transaksi *non cash* kapan saja dan dimana saja dengan mengakses jaringan internet melalui melalui perangkat yang kompatibel seperti komputer, laptop, tablet, note maupun telepon genggam. Inovasi

pelayanan perbankan melalui *internet banking*, diharapkan dapat memberikan kemudahan, disamping dapat menekan biaya transaksi dan antrian panjang. *Internet banking* dapat digunakan untuk melakukan bermacam-macam transaksi *online,* yakni untuk mengecek saldo rekening dan *history* transaksi bank, membayar macam-macam tagihan, transfer antar *account*. Pelayanan *internet banking* yang ditawarkan tersebut diharapkan akan semakin berkembang sesuai dengan kebutuhan, sehingga pangsa pasar yang dilayani akan semakin luas.

Kondisi globalisasi teknologi tersebut sangat penting dan menguntungkan bagi dunia perbankan. Namun, tidak dapat dipungkiri bahwa kemajuan tersebut telah membawa dampak pada perkembangan bentuk kejahatannya. Salah satu sasaran yang memiliki potensi kerugian akibat dari perkembangan bentuk kejahatan yang memanfaatkan teknologi informasi, yang dikenal dengan istilah *cyber crime* atau kejahatan dunia maya adalah sektor perbankan, karena komputer dan sistem informasi telah menjadi bagian dari strategi bisnisnya. Siapapun pengguna komputer yang terhubung ke suatu jaringan internet berpeluang menjadi korban *cyber crime.* Berbeda dengan kejahatan konvensional yang dampaknya lebih mudah dilokalisasi dan maksimum nilai kerugian biasanya sebesar nilai yang melekat pada sasaran kejahatan, sedangkan *cyber crime* lebih sulit untuk dilokalisasi dan nilai kerugian yang ditimbulkannya tidak terbatas pada nilai material yang melekat pada sasaran, artinya nilai kerugian dapat lebih besar nilainya.

Kasus *cyber crime* yang mengejutkan dunia perbankan Indonesia adalah tindakan yang telah dilakukan Steven Haryanto seorang jurnalis majalah Master Web, yang memanfaatkan perkembangan teknologi melalui

media Internet (*e-banking*) untuk pembuatan *website* yang hampir serupa dengan situs asli. **Cara ini diterapkan dengan menggunakan domain www.klik-bca.com, kilkbca.com, clikbca.com, klickca.com, dan klikbac.com sebagai domain yang mirip dengan situs resmi *internet banking* BCA yaitu www.klikbca.com. Nasabah yang salah mengetik alamat *website* resmi NCA tersebut akan terjebak pada salah satu web palsu miliki Haryanto.Jika sudah masuk ke situs yang salah maka nasabah akan memasukkan *user ID* dan identitas pribadi lainnya.**[1]

Cyber crime dalam bidang perbankan perlu segera ditanggulangi karena kejahatan ini merugikan nasabah dan mampu merusak sistem perekonomian dunia. **Penanggulangan terhadap *cyber crime* di bidang perbankan dapat dilakukan melalui penegakan hukum. Penegakan hukum merupakan sarana langkah penting dalam mencapai tujuan hukum yakni menciptakan kondisi masyarakat yang tertib hukum. Namun pada kenyataannya seringkali menghadapi kendala yang berkaitan dengan dinamika masyarakat dan dinamika hukum. Secara faktual, seringkali masyarakat dihadapkan dengan fenomena ketertinggalan hukum yang belum mampu mengikuti perkembangan masyarakat. Terlebih lagi pada aktivitas manusia yang dilakukan di dunia maya. Oleh sebab itu sangat menarik untuk membahas permasalahan mengenai "Penegakan Hukum Terhadap Cyber Crime di**

[1] Menurut Steven pada situs para webmaster di Indonesia, tujuan membuat situs plesetan adalah agar masyarakat berhati-hati dan tidak ceroboh saat melakukan pengetikan alamat situs (*typo site*), bukan untuk mengeruk keuntungan.

Lihat Golose, Petrus Reinhard. *Perkembangan Cyber Crime dan Upaya Penanggulangannya di Indonesia Oleh Polri,* Jakarta: Buletin Hukum Perbankan dan Kebanksentralan, Vol 4 No 2, Agustus, 2006, hal. 32.

Bidang Perbankan Sebagai Kejahatan Transnasional."

2. Rumusan Masalah

Adapun rumusan masalah dalam penelitian ini adalah:

a. Bagaimanakah bentuk-bentuk *cyber crime* di bidang perbankan?
b. Bagaimanakah yurisdiksi dalam penegakan hukum terhadap *cyber crime* di bidang perbankan?

3. Tujuan Penulisan

1.3.1 Tujuan Umum

Tujuan umum penelitian ini adalah untuk memahami dan mendalami penegakan hukum *cyber crime* di sektor perbankan dalam perspektif hukum positif.

1.3.2 Tujuan Khusus

Tujuan khusus dalam penelitian yang dilakukan ini adalah untuk mengetahui dan memahami :

a. Bentuk-bentuk *cyber crime* di bidang perbankan.
b. Yurisdiksi dalam penegakan hukum terhadap *cyber crime* di bidang perbankan.

II METODE PENELITIAN

Penelitian ini termasuk penelitian hukum normatif atau lingkup ilmu hukum teoritis atau dogmatik yang mengkaji hukum yang dikonsepkan sebagai norma atau kaidah yang berlaku dalam masyarakat dan menjadi acuan perilaku setiap orang. Penelitian ini menggunakan pendekatan perundang-undangan (*The Statute Approach*) yaitu melihat peraturan perundang-undangan yang berkaitan dengan penegakan hukum *cyber crime* yang mengacu pada bahan hukum primer. Pendekatan perundang-undangan (*The statute approach*) dilakukan dengan menelaah undang-undang dan regulasi yang terkait dengan isu hukum yang sedang ditangani.[2] Penelitian ini juga menggunakan pendekatan analisis dan konsep hukum (*analitical and conseptual approach*), yakni dengan

[2] Peter Mahmud Marzuki, *op.cit.,* hal. 93

menganalisis bahan hukum menyangkut hukum positif yang terkait dengan penegakan hukum *cyber crime.* Selain itu, digunakan pendekatan konseptual. **Pendekatan konseptual mendasarkan pada pendapat para ahli hukum yang tertuang dalam teori-teori hukum.**

Sumber bahan hukum penelitian ini menggunakan penelitian kepustakaan (*library research*), berupa bahan hukum primer, sekunder dan tertier. Bahan hukum primer adalah bahan yang isinya mengikat karena dikeluarkan oleh pemerintah, contohnya berbagai peraturan perundang-undangan maupun kesepakatan Internasional yang terkait dengan *cyber crime,* seperti *Vienna Conventian* tahun 2000 dan *Manila Declaration* tahun 1997. Sumber bahan sekunder adalah bahan-bahan yang membahas materi bahan hukum primer, seperti buku maupun artikel, sedangkan **bahan hukum tertier menurut Burhan Ashshofa berupa kamus dan buku pegangan yang sifatnya menunjang bahan hukum primer dan sekunder.**[3] Adapun bahan hukum primer yang digunakan dalam penelitian ini, antara lain Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Bahan hukum sekunder yang diambil dari pendapat para ahli dalam bidang *cyber crime* akan digunakan sebagai bahan dalam membuat konsep hukum yang berkaitan dengan penelitian, sedangkan bahan hukum tertier yang digunakan sebagai rujukan untuk mengetahui konsep hukum yang ada, yaitu melalui Kamus Hukum, Kamus Bahasa Indonesia dan Inggris.

Bahan hukum yang terkumpul akan diperiksa untuk mengetahui apakah bahan hukum tersebut sudah lengkap, relevan dan jelas. Kemudian dilakukan pendataan pada bahan

[3] Burhan Ashshofa, 1996, *Metode Penelitian Hukum,* PT. Rineka Cipta, Jakarta, hal. 103

hukum yang diperoleh dengan memberi penomoran atau tanda tertentu yang menunjukkan klasifikasi bahan hukum menurut jenis dan sumber, dengan tujuan untuk memudahkan analisis bahan hukum. Bahan hukum sekunder berupa literatur biasanya diberi tanda sumber bahan hukum, tahun penerbitan dan halaman tempat bahan hukum ditemukan. Bahan hukum sekunder berupa perundang-undangan biasanya diberi tanda nomor undang-undang, tahun penerbitan, judul undang-undang, pasal undang-undang, nomor lembaran negara dan tahun penerbitan lembaran negara. Selanjutnya dilakukan penyusunan atau sistematisasi bahan hukum dengan mengelompokkan secara sistematis bahan hukum yang sudah diedit dan diberi tanda menurut klasifikasi bahan hukum dan urutan masalah, serta membuat catatan mengenai hal yang dianggap penting bagi penelitian.

Teknik analisis bahan hukum menggunakan teknik *content analysis*, yaitu pengumpulan bahan hukum dengan interpretasi, untuk ketentuan hukum dipakai interpretasi berdasarkan pada tujuan norma. Selain itu, digunakan pendekatan Undang-undang terkait, berupa Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Analisis bahan hukum dilakukan dengan menguraikan bahan hukum dalam bentuk kalimat yang baik dan benar, agar mudah dibaca dan diinterpretasikan. Hasil analisis bahan hukum digunakan untuk memudahkan pengambilan kesimpulan. Dalam penelitian ini bahan hukum dianalisis dengan menggunakan teknik deskripsi, interpretasi, argumentasi, evaluasi dan sistematisasi.

III HASIL DAN PEMBAHASAN

1. Bentuk-bentuk Cyber Crime di Bidang Perbankan

Globalisasi merupakan fenomena yang ditandai dengan ciri-ciri dimana dunia semakin terasa dekat. Jarak bukan lagi menjadi masalah bagi setiap orang untuk berinteraksi dengan orang lain. Dengan pemanfaatan teknologi informasi, pergerakan modal, barang, jasa dan informasi dapat berputar lintas negara dengan cepat dan *real time*. Pengaruh globalisasi juga dirasakan pada sektor perbankan. Pelayanan yang diberikan oleh bank tidak selalu memerlukan kehadiran fisik dari nasabah. Nasabah dapat bertransaksi hanya dengan bermodalkan telepon genggam, tablet, laptop atau alat komunikasi lainnya yang terkoneksi dengan jaringan internet. Kondisi ini tentu sangat memudahkan sistem pelayanan perbankan, menjamin akurasi data, menghemat waktu dan biaya.

Salah satu strategi bank dalam meningkatkan kualitas operasionalisasi pelayanan kepada nasabahnya maupun menghadapi persaingan antar bank adalah dengan mengubah produk pelayanan transaksi manual menjadi pelayanan transaksi yang memanfaatkan teknologi. Sehingga penggunaan teknologi informasi telah mengubah sistem konvensional menjadi digital yang memungkinkan dunia perbankan melakukan transaksi dengan menggunakan media elektronik yang lebih menawarkan kemudahan, kecepatan, dan efisiensi. Saat ini hampir seluruh proses penyelenggaraan sistem pembayaran di bidang perbankan telah dilakukan dengan memanfaatkan perkembangan teknologi. Dalam *Annual Report on High Technology Crime in California* dilaporkan bahwa oada 1996 saja, 154 bank Eropa sudah memiliki website sedangkan tahun 1997 lebih dari 1.100 bank melakukan hubungan dengan

www (*world wide web*).[4] Bagi dunia perbankan, media internet telah memberikan peluang dan tantangan dalam proses inovasi produk dan jasa dengan menempatkan teknologi sebagai unsur utama.

Fenomena *cyber crime* dibidang perbankan memiliki karakteristik tersendiri dibandingkan dengan kejahatan konvensional lainnya. Siapa pun bisa menjadi korban dari kejahatan ini. Pelaku tidak menetapkan target korban, sehingga kejahatan ini perlu diwaspadai oleh setiap pengguna jasa layanan internet. Hal ini disebabkan sifat internet global yang memungkinkan *Cyber crime* dapat dilakukan tanpa mengenal batas teritorial dan tidak memerlukan interaksi langsung antara pelaku dengan korban kejahatan. Sementara sistem informasi perbankan mutlak memerlukan layanan internet. Kepolisian Inggris menyatakan bahwa *Cyber Crime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital[5]. Beberapa bentuk potensi *cyber crime* dalam kegiatan perbankan antara lain ;

a. ***Typo site*, yaitu membuat nama domain dan alamat situs yang mirip dengan situs resmi. Pelaku memanfaatkan kekeliruan dari pengguna internet dalam pengetikan alamat situs yang dicari.**

b. *Keylogger/ keystroke recorder*. Kegiatan ini dilakukan dengan menggunakan *software* atau program *keylogger*. Cara kerja dari *keylogger* adalah dengan mencatat segala aktivitas yang dilakukan oleh pengguna

[4] Barda Nawawi Arief, 2006, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia,* RajaGrafindo Persada, Jakarta, hal. 53.

[5] Abdul Wahid dan Mohammad Labib, 2005. *Kejahatan Mayantara*, PT Refika Aditama, Bandung, hal. 40

internet melalui huruf-huruf yang diketikkan pada *keyboard.* Dalam berselancar di dunia maya, pengguna internet mungkin saja memasukkan nomor identitas dan *password* yang dapat dimanfaatkan oleh pelaku. Cara kejahatan ini biasanya terjadi pada tempat umum yang digunakan untuk mengakses internet seperti warnet atau restoran, bandara dan tempat umum lainnya yang menyediakan komputer didukung dengan fasilitas internet.

c. *Sniffing*. *Sniffing* cara yang digunakan oleh pelaku dengan mengamati paket data internet yang digunakan oleh pengguna untuk mendapatkan nomor identitas dan *password* yang bersangkutan.

d. *Brute Force Attacking*, yaitu upaya pencurian nomor identitas dan *password* melalui mencoba kemungkinan atas kombinasi yang dibuat.

e. *Web Deface*: *System Exploitation*, yaitu eksploitasi sistem dengan megganti tampilan awal dari sebuah situs resmi.

f. *Email Spamming*, yakni dengan mengirimkan *email* kepada pemilik akun dengan menawarkan produk-produk atau menyatakan bahwa pemilik akun telah memenangkan suatu undian.

g. *Denial of Service*, yaitu pelumpuhan sistem elektronik dengan membanjiri akun atau sistem elektronik dengan data dalam jumlah yang besar.

h. *Virus, worm, trojan*: Penyebaran virus komputer dilakukan untuk menyerang sistem komputer, memperoleh data, memanipulasi data

atau tindakan lain yang dilakukan secara melawan hukum.

Potensi *cyber crime* dalam kegiatan perbankan menghantui transaksi perdagangan elektronik melalui sistem perbankan. Pada dasarnya kegiatan perdagangan melalui transaksi elektronik *(electronic commerce),* bukan hanya menjadi bagian dari perdagangan nasional, tetapi juga telah meluas pada **perdagangan lintas batas negara. Kondisi ini perlu didukung dengan inovasi-inovasi teknologi dan perangkat elektronik yang mampu mencegah terjadinya kejahatan di dunia virtual.**

Lalu lintas pembayaran melalui sistem perbankan elektonik yang berpotensi terserang kejahatan di dunia maya yaitu melalui aktivitas pembayaran dengan menggunakan kartu kredit pada *online shopping* atau penggunaan fasilitas *online booking* yang disediakan oleh penyedia layanan yang menggunakan fasilitas internet. Kedua aktivitas internet tersebut akan meminta pengguna memasukkan nomor identitas, PIN atau password yang dapat dimanfaatkan oleh pelaku.

2. Yurisdiksi Dalam Penegakan Hukum Terhadap *Cyber Crime* Di Bidang Perbankan

Dalam konteks penegakan hukum *cyber crime* di Indonesia, baik yang menyangkut *cyber crime* di sektor Perbankan maupun sektor lainnya cukup kompleks. Hal ini tidak lepas dari aspek transnasional dari *cyber crime* di bidang perbankan. Transaksi dilakukan secara lintas batas negara, yang artinya harus berhadapan dengan masalah yurisdiksi. Masalah penentuan yurisdiksi menjadi inti dalam penegakan hukum. Huala Adolf mengemukakan bahwa ”Yurisdiksi adalah kekuatan atau kewenangan hukum negara terhadap orang,

benda atau peristiwa (hukum)."[6] Yurisdiksi akan menentukan hukum negara mana yang akan digunakan dan negara mana yang berwenang untuk melakukan penegakan hukum. Untuk itu diperlukan pengetahuan mengenai tempat dimana kejahatan dilakukan sementara *cyber crime* terjadi secara lintas batas negara.

Berbicara mengenai yurisdiksi adalah berbicara mengenai kewenangan dari suatu negara yang berdaulat untuk menentukan pengaturan terhadap setiap tindakan dari orang, peristiwa hukum dan pengaturan tentang kebendaan yang terkait dengan kepentingan dari negara bersangkutan. Kewenangan tersebut tidak hanya terbatas pada warga negara atau batas wilayah negaranya saja namun juga menyangkut kepentingan negara bersangkutan meskipun terhadap peristiwa hukum yang terjadi di luar batas negaranya atau dilakukan oleh warga negara asing. Pada prinsipnya ada 3 jenis jurisdiksi:

1) Yurisdiksi untuk menetapkan ketentuan hukum pidana (*jurisdiction to precribe* atau *legislative jurisdiction atau prespective jurisdiction*).
2) Yurisdiksi untuk menerapkan atau melaksanakan ketentuan yang telah ditetapkan oleh badan legislatif (*executif jurisdictrion*).
3) Yurisdiksi untuk memaksakan ketentuan hukum yang telah dilaksanakan oleh badan eksekutif atau yang telah diputuskan oleh badan peradilan (*enforcement jurisdiction* atau *jurisdiction to ajudicate*).[7]

Dari ketiga jenis yurisdiksi tersebut, Barda Nawawi Arief menyatakan[8] bahwa problem yurisdiksi yang lebih menonjol

[6] Huala Adolf, 2002, *Aspek-aspek Negara Dalam Hukum Internasional* edisi revisi, PT RajaGrafindo Persada, Jakarta, hal. 183 (selanjutnya disebut Huala Adolf I).

[7] Huala Adolf, 1996, *Aspek-aspek Hukum Pidana Internasional*, RajaGrafindo Persada, Jakarta, hal. 34 (selanjutnya disebut Huala Adolf II).

[8] Barda Nawawi Arief, *op.cit.,*hal. 29

dalam *cyber crime* adalah pada yurisdiksi yudikatif dan eksekutif, **karena harus berhadapan dengan penghormatan terhadap asas kedaulatan negara lain. Dalam konteks penerapan hukum, maka suatu negara tentu akan berhadapan dengan ketentuan hukum negara lain dan penegak hukum negara lain yang tentunya mungkin sekali terdapat perbedaan sistem hukum dengan negara yang berkepentingan. Untuk mengatasi problematika tersebut, maka diperlukan harmonisasi ketentuan hukum yang didukung dengan berbagai kerjasama internasional yang dituangkan dalam perjanjian internasional antara negara-negara pihak.**

Pada umumnya suatu negara mempunyai prinsip-prinsip yurisdiksi yang menyangkut perkara pidana, sebagai berikut[9]:

1) Prinsip teritorial, yaitu prinsip yurisdiksi yang diterapkan suatu negara terhadap orang, badan hukum dan semua benda yang berada diwilayahnya, baik suatu tindak pidana yang dimulai di suatu negara (teritorial subyektif) maupun berakhir di negara lain (teritorial obyektif).
2) Prinsip nasionalitas, yaitu prinsip yurisdiksi yang diterapkan suatu negara pada warganegaranya yang menjadi pelaku tindak pidana (nasional aktif), baik di dalam negara dan di negara lain, maupun warganegaranya yang menjadi korban tindak pidana (nasional pasif), baik di dalam negara dan di negara lain.
3) Prinsip perlindungan, yaitu prinsip yurisdiksi yang diterapkan suatu negara terhadap pelaku tindak pidana, meskipun dilakukan diluar wilayah negara tersebut.
4) Prinsip universal, yaitu prinsip

[9] Starke. JG, 2006, *Introduction To International Law*. Edisi kesepuluh. Terjemahan Djajaatmaja, Bambang Iriana., Sinar Grafika, Jakarta, hal. 202-240

yurisdiksi yang diterapkan apabila tindak pidana yang dilakukan membahayakan nilai-nilai universal dan kepentingan umat manusia.

Penentuan pemberlakuan hukum dapat ditelaah dari beberapa asas hukum yang ada dan telah diterima secara universal, yaitu:

1) Asas *Subjective Territorial* yaitu berlakunya hukum berdasarkan tempat perbuatan dan penyelesaian tindak pidana dilakukan di Negara lain,
2) Asas *Objective Territorial* yaitu hukum yang berlaku adalah akibat utama perbuatan itu terjadi dan memberikan dampak kerugian bagi Negara yang bersangkutan,
3) Asas *Nationality* adalah hukum berlaku berdasarkan kewarganegaraan pelaku,
4) Asas *Passive Nationality* adalah Hukum berlaku berdasarkan kewarganegaraan korban,
5) Asas *Protective Principle* adalah berlakunya berdasarkan atas keinginan Negara untuk melindungi kepentingan Negara dari kejahatan yang dilakukan diluar wilayahnya,
6) Asas *Universality* adalah yang berlaku untuk lintas Negara terhadap kejahatan yang dianggap sangat serius seperti terorisme (*crimes against humanity*).

Berdasarkan atas bentuk dan karakteristik dunia *cyber*, dapat dikemukakan beberapa teori yang relevan untuk membahas kejahatan ini, yaitu :

1) *The uploader and the downloader theory*. Teori ini menekankan pada pembatasan terhadap kegiatan *uploading* dan

downloading **yang bertentangan dengan ketentuan dan kepentingan negara bersangkutan.**

2) ***The law of the server theory.*** **Teori ini menunjukkan bahwa pemberlakuan *cyber law* terhadap *web pages* dari para *server* beroperasi.**

3) ***Theory of international spaces*****. Teori ini menganggap bahwa *cyber space* adalah *the fourth spaces* yang bersifat international dengan analogi bahwa ruang maya ini adalah tanpa kedaulatan.[10]**

Dengan kemajuan dan perkembangan telekomunikasi multimedia, ruang lingkup dan kecepatan komunikasi lintas batas meningkat, ini berarti masalah hukum yang berkaitan dengan yurisdiksi dan penegakan serta pemilihan hukum yang berlaku terhadap suatu sengketa multi-yurisdiksi akan bertambah penting dan konfleks.[11] **Yurisdiksi dalam penegakan terhadap *cyber crime* di bidang perbankan dapat dilihat dalam Pasal 2 Undang-undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Dalam ketentuan tersebut dapat diketahui bahwa ketentuan Undang-undang ini berlaku bagi setiap orang tanpa terbatas kewarganegaraannya sepanjang melakukan perbuatan yang diatur dalam undang-undang tersebut.**

[10] Teori ini menganalogikan bahwa *cyber space* tidak terletak pada kesamaan fisik, melainkan pada sifat international, yakni *sovereignless equality*. Lebih lanjut baca Ahmad Ramli, 2004. *Cyber Law dan HKI dalam System Hukum Indonesia*, Rafika Aditama, Bandung, hal. 22.

[11] Tien S. Saifullah, *Yurisdiksi sebagai Upaya Penagakan Hukum dalam Kegiatan Cyberspace", Cyber Law: Suatu Pengantar*, Pusat Studi *Cyber Law*, UNPAD, Bandung, hal. 96

Undang-undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menekankan pada akibat hukum yang ditimbulkan bagi Indonesia berdasarkan kepentingan Indonesia, sehingga Undang-undang ini tetap berlaku meskipun dilakukan di luar wilayah Indonesia. Berdasarkan ketentuan tersebut Indonesia memiliki kewenangan untuk menerapkan hukumnya terhadap *cyber crime* di bidang perbankan.

IV. SIMPULAN DAN SARAN

1. Simpulan

a. Bentuk-bentuk *cyber crime* di bidang perbankan adalah *typo site, keylogger / keystroke recorder, sniffing, brute force attacking, web deface, email spamming, denial of service dan virus, worm, trojan.* **Kegiatan transaksi perbankan yang berpotensi menjadi target *cyber crime* adalah sistem layanan pembayaran pada online shopping dengan pembayaran melalui kartu kredit** dan kedua, adalah fasilitas layanan *online banking*. Hal tersebut dapat terjadi karena maksud jahat seseorang yang memiliki kemampuan dalam bidang teknologi informasi, atau seseorang yang memanfaatkan kelengahan pihak bank, pihak merchant maupun pihak nasabah.

b. Yurisdiksi dalam penegakan hukum terhadap *cyber crime* di bidang perbankan meliputi yurisdiksi untuk menetapkan ketentuan hukum, yurisdiksi untuk menerapkan atau melaksanakan ketentuan yang telah ditetapkan oleh badan legislatif dan yurisdiksi untuk memaksakan ketentuan hukum yang telah dilaksanakan oleh badan eksekutif atau yang telah diputuskan oleh badan peradilan. Yurisdiksi diatur secara khusus dalam Pasal 2 Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi

Elektronik yang menentukan bahwa 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.

2. Saran

a. Perbankan hendaknya memiliki suatu sistem pengamanan elektronik untuk melindungi sistemnya. Upaya ini juga perlu didukung oleh nasabah dengan menyimpan data pribadinya dan tidak memberikan kepada pihak lain yang tidak berkepentingan.

b. Penegakan hukum terhadap *cyber crime* di bidang perbankan memerlukan kerjasama antar negara. Oleh sebab itu diperlukan komitmen bersama untuk menanggulangi kejahatan ini.

DAFTAR PUSTAKA

Abdul Wahid dan Mohammad Labib, 2005. *Kejahatan Mayantara*, PT Refika Aditama, Bandung.

Ahmad Ramli, 2004. *Cyber Law dan HKI dalam System Hukum Indonesia*, Rafika Aditama, Bandung.

Barda Nawawi Arief, 2006, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia,* RajaGrafindo Persada, Jakarta.

Burhan Ashshofa, 1996, *Metode Penelitian Hukum,* PT. Rineka Cipta, Jakarta.

Golose, Petrus Reinhard. *Perkembangan Cyber Crime dan Upaya Penanggulangannya di Indonesia Oleh Polri,* Jakarta: Buletin Hukum Perbankan dan Kebanksentralan, Vol 4 No 2, Agustus, 2006, hal. 32

Huala Adolf, 2002, *Aspek-aspek Negara Dalam Hukum Internasional* edisi revisi, PT RajaGrafindo Persada, Jakarta.

_____, 1996, *Aspek-aspek Hukum Pidana Internasional*, RajaGrafindo Persada, Jakarta.

Peter Mahmud Marzuki, 2008, *Penelitian Hukum,* Kencana Prenada Media Group, Jakarta.

Starke. JG, 2006, *Introduction To International Law*. Edisi

kesepuluh. Terjemahan Djajaatmaja, Bambang Iriana., Sinar Grafika, Jakarta.

Tien S. Saifullah, *Yurisdiksi sebagai Upaya Penagakan Hukum dalam Kegiatan Cyberspace", Cyber Law: Suatu Pengantar*, Pusat Studi *Cyber Law*, UNPAD, Bandung.

Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

BIODATA PENULIS

Nama lengkap dengan gelar:
Tri Kuncoro, S.E.

Alamat rumah:
Asrama Polisi Kreneng B/3
Denpasar

Tempat bekerja:
Polda Bali

HP
081999407962

Alamat e-mail.
tribli@yahoo.com