TINJAUAN YURIDIS PENANGANAN KEJAHATAN SIBER (CYBERCRIME) DI SEKTOR PERBANKAN INDONESIA DAN AMERIKA

Rina Shahriyani Shahrullah
Delfind Kiwekhang

Abstract

Considering that the effect of Information Technology is worldwide and borderless, the jurisdiction concept is not only applicable in the territory of Indonesia but also in the territory of United States of America both country that is largely affected with the impact of cybercrime. Cybercrime deeply effected the interest of both country, government, population and their economic. There were so many kinds of cyberspace offenses, principally offense that should be applied is a formal offense, considering the criminal act of cyberspace element of loss is often even harder to prove because it is cross-territorial and unawareness of the victim, even if the offender and evidence have already been caught.

This research is a sociological law by using the method of comparative law. Sources of data used in the form of primary and secondary data sources. Data mining is done with field research and literature study (library research). After all the data collected, the data is then processed and analyzed, the qualitative analysis is used with the intention to classify aspects of data studied. Furthermore, it is concluded that the research associated with this, then described descriptively.

Based on the results of this study showed that there are some similarities and differences in the conception of cybercrime offences in Indonesia and United States of America. However, in terms of legal liability, the provisions of the United state of America to regulate is better than Indonesia, seen in terms and strategy to overcome the offences and to prevent the occurrence of cyberspace offence.

***Keywords**: Cybercrime, Bank Institution, Indonesia, United States of America*

A. Latar Belakang

Perkembangan teknologi informasi itu memberikan peluang kepada pelaku usaha mengubah dalam menjalankan bisnisnya dengan menempatkan teknologi sebagai unsur utama dalam proses inovasi produk dan jasa. Pelayanan *Electronic Transaction* (*e-banking*) melalui *Automatic Transaction Machine* (*ATM*), *phone banking* dan *internet banking* misalnya, merupakan bentuk-bentuk baru dan *delivery channel* pelayanan bank yang mengubah pelayanan transaksi manual menjadi pelayanan transaksi oleh teknologi.

Bagi perekonomian, kemajuan teknologi memberikan manfaat yang sangat besar, karena transaksi bisnis dapat dilakukan secara seketika (*real time*), yang berarti

perputaran ekonomi menjadi semakin cepat dan dapat dilakukan tanpa hambatan ruang dan waktu, begitu juga dari sisi keamanan, penggunaan teknologi memberikan perlindungan terhadap keamanan data dan transaksi.

Disamping berbagai manfaat positif yang diperoleh, teknologi informasi juga telah melahirkan bentuk-bentuk kejahatan yang baru yang perlu diantisipasi. Seperti penyalahgunaan teknologi informasi yang melanggar ruang-ruang publik maupun ruang privasi. Seperti halnya dunia nyata, dunia maya ternyata terdapat pula berbagai bentuk kejahatan. Internet dapat digunakan oleh pihak-pihak yang tidak bertanggungjawab untuk melakukan suatu tindakan kejahatan baik untuk mencari keuntungan atau pun hanya sekedar melampiaskan keisengan.

Hal ini memunculkan fenomena khas yang sering disebut sebagai *Cyber Crime* (kejahatan siber). *Cyber Crime* yang merupakan akibat dari penyalahgunaan teknologi ini bisa berupa perusakan, pemalsuan data, pencurian barang, hingga penyebarluasan informasi asusila (*cyber porn*).

Dalam dunia perbankan perkembangan *Cyber Crime* cukup mengejutkan terutama dikarenakan terjadinya beberapa kasus yang merugikan pihak perbankan seperti; kasus pembobolan melalui *e-banking* yang terjadi pada beberapa bank besar di Indonesia seperti bank Bank Central Asia (BCA) dan Bank Mandiri[91]. Sementara itu sejumlah nasabah pemegang *credit card* juga mengeluh, karena nomor kartu kreditnya telah dipakai pihak lain untuk melakukan transaksi *e-commerce* sehingga menimbulkan kerugian yang cukup besar.

Hal ini perlu mendapat perhatian mengingat karakteristik *Cyber Crime* sangat berbeda dengan tindak pidana konvensioal dan karakteristiknya yang bersifat *borderless* membuat pendekatan hukum di bidang ini tidak dapat lagi dilakukan secara konvensional[92]. Mengingat *Cyber Crime* menggunakan teknologi yang tinggi sebagai media, maka kebijakan kriminalisasi di bidang teknologi informasi juga harus memperhatikan perkembangan upaya penanggulangan *Cyber Crime* baik regional maupun internasional dalam rangka harmonisasi dalam pengaturan tentang *Cyber Crime* di Indonesia.

Ketentuan hukum yang dapat digunakan untuk menyeret pelaku *Cyber Crime* ini baru terbatas pada Peraturan perundang-undangan Kitab Undang-undang Hukum Pidana (KUHP) dan Undang-undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Ketentuan lainnya, jikapun ada, tersebar pada berbagai peraturan perundang-undangan dan tidaklah bersifat spesifik.

Sedangkan Amerika sudah memiliki beberapa Peraturan Perundang-undangan yang secara jelas mengatur mengenai *Cyber Crime* seperti *Title 18 U.S. Code § 1030* yang

[91] Soetarto dan M. Nasir, Teknologi *E-Bangking* dikalangan *Smart Customer*, http://repository.akprind.ac.id/sites/files/conference-paper/2008/nasir_2127.pdf diakses pada tanggal 5 Februari 2015

[92] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara* (*Cyber Crime*) (Jakarta: PT. Refika Aditama, 2005), hlm. 10

mengatur mengenai *Fraud and related activity in connection with computers*, *Title 18 U.S. Code § 1344* yang mengatur mengenai *Bank Fraud* dan *Title 18 U.S. Code § 2252B* yang mengatur mengenai *Misleading domain names on the internet*. selain itu Amerika juga merupakan anggota dari *Convention on Cyber Crime* (*Budapest Convention 2001*) yang merupakan organisasi yang bertujuan untuk melindungi masyarakat dari kejahatan di dunia Internasional. Organisasi ini dapat memantau semua pelanggaran yang ada di seluruh dunia. Indonesia yang bukan merupakan anggota dari konvesi tersebut sangatlah dirugikan karena konvensi tersebut menghasilkan suatu peraturan perundang-undangan yang sangat efesien dalam bentuk pelindungan terhadap tindakan *Cyber Crime*.

Sehingga dalam hal penanganan mengenai *Cyber Crime* apabila dibandingkan dengan Amerika, Indonesia masih kurang efektif. Hal ini dipengaruhi beberapa faktor antara lain dikarenakan peraturan perundang-undangan yang tidak mengatur secara rinci terhadap pelaku yang telah melanggar peraturan tersebut dan belum optimalnya pelaksanaan penanganan yang dilakukan oleh para penegak hukum. Dapat dilihat pada tabel penelitian yang membandingkan besarnya jumlah kasus *Cyber Crime* pada sektor perbankan selama setahun yang telah mendapat penanganan dan yang masih mengalami kendala baik di Indonesia maupun di Amerika, dibawah ini :

Table 1.1 : Perbandingan Jumlah Kasus Cyber Crime yang terjadi di Indonesia dan Amerika setiap tahunnya

No.	Tolak Ukur	Indonesia	Amerika
1	Jumlah Kasus *Cyber Crime* yang terjadi dalam jangka waktu satu tahun	±110	±220
2	Kasus yang telah selesai ditanganin	±50	±160
3	Kasus yang sedang ditanganin	±60	±60

Sumber: Data diolah Peneliti

Dari tabel diatas dapat kita dilihat bahwa penanganan kasus *Cyber Crime* di Indonesia yang telah sepenuhnya selesai ditangani lebih sedikit jumlahnya apabila dibandingkan dengan kasus yang masih dalam proses penanganan. Bertolak belakang dengan Amerika, walaupun memiliki jumlah kasus *Cyber Crime* yang lebih banyak daripada Indonesia, namun kasus yang telah selesai ditangani jumlahnya lebih besar dibandingkan dengan jumlah yang sedang dalam penanganan. Berdasarkan perbandingan diatas, maka dapat dipahami bahwa penanganan yang dilakukan oleh Amerika lebih tepat sasaran dan lebih efektif sehingga kasus-kasus *Cyber Crime* yang

dapat ditangani lebih banyak. Sedangkan Indonesia, dalam proses penanganan masih banyak mengalami kendala maupun hambatan.

Berdasarkan hal-hal yang telah diuraikan, terdapat beberapa rumusan masalah yang dibahas dalam penelitian ini yaitu ***pertama,*** bagaimana Strategi Penanganan terhadap *Cyber Crime* dalam sektor perbankan di Indonesia dan Amerika?, ***kedua,*** apakah kendala-kendala yang dihadapi oleh pemerintahan Indonesia dan Amerika dalam menangani masalah *Cyber Crime* pada sektor perbankan?.

B. Metode Penelitian

Metode Pendekatan yang digunakan dalam penelitian ini adalah metode yuridis empiris. Jenis data yang dipergunakan adalah data primer yang dihasilkan dari penelitian lapangan yang diperoleh dari hasil observasi lapangan yang terkait dengan penanganan *Cyber Crime* pada sektor perbankan yang terdiri dari bahan hukum primer yang berupa peraturan perundang-undangan yang berlaku, bahan hukum sekunder yang memberikan penjelasan mengenai bahan hukum primer dan bahan hukum tersier yaitu memberikan petunjuk atau penjelasan terhadap bahan hukum primer dan sekunder

Metode Pengumpulan data yang digunakan terdiri dari 2 yaitu penelitian kepustakaan dan penelitian lapangan. Setelah semua data yang terkumpul maka dilakukan pemeriksaan terhadap data yang ada. Data tersebut diolah dan disusun secara sistematis.

C. Hasil Penelitian dan Pembahasan

1. Hasil Penelitian

a. Hasil Wawancara

Polda Kepri khususnya pada Subdit Ditreskrimsus unit pelanggaran cybercrime yang telah didirikan pada bulan Maret tahun 2014 lalu yang berwenang melakukan penanganan terhadap pelanggaran cybercrime menyatakan bahwa pelanggaran cybercrime merupakan jenis pelanggaran yang tidak mudah untuk ditangani, hal ini dikarenakan proses pencaharian pelaku dan barang bukti pelanggaran tidaklah mudah.

Berdasarkan informasi yang diperoleh dari hasil wawancara kepada pihak kepolisian pada unit cybercrime ini jumlah pelanggaran cybercrime secara umum di seluruh Indonesia yang meliputi perbuatan penghinaan, penipuan, pelecehan yang dilakukan melalui media sosial, perjudian online berjumlah sekitar 400 kasus setiap tahunnya dan khususnya yang merugikan sektor perbankan di seluruh Indonesia berjumlah antara 103 sampai dengan 120 kasus per tahun dalam jangka waktu 5 tahun terkahir ini. Dari jumlah pelanggaran tersebut diatas, kasus yang telah selesai ditangani oleh pihak kepolisian adalah sebanyak 45 sampai dengan 60 kasus yang telah diserahkan ke Kejaksaan untuk ditindaklanjuti, sedangkan sisanya masih berada dalam proses penanganan oleh pihak kepolisian.

Menurut pihak kepolisian, kasus-kasus yang belum selesai tersebut sulit untuk ditangani dikarenakan mengalami kendala-kendala antara lain dalam mengumpulkan alat bukti pelanggaran yang karena sifat pelanggaran yang digital mengharuskan para penyidik juga memiliki alat dengan teknologi yang maju agar dapat menemukan alat bukti tersebut, tim penyidik yang masih kurang, proses penangkapan terhadap pelaku

pelanggaran cybercrime yang berada diluar yurisdiksi negara Indonesia yang dikarenakan tidak adanya kerjasama negara Indonesia dengan negara-negara lainnya.

Namun, berdasarkan informasi yang penulis peroleh, guna menangkap pelaku pelanggaran cybercrime, walau masih mengalami banyak kendala dan kesulitan. Hal tersebut tidak membuat pihak kepolisian kehilangan akal dan cara, pihak kepolisian masih memiliki cara-cara lain yang dipergunakan untuk mencari alat bukti maupun pelaku yang berada diluar negeri. Bentuk tindakan yang telah dilakukan oleh pihak kepolisian antara lain menjalin hubungan dan bekerjasama dengan pihak kepolisian negara lain sehingga dapat membantu proses penangkapan pelaku cybercrime didaerah persembunyiannya.

Sama halnya dengan Amerika, sebagai sebuah negara maju yang memiliki jumlah pelanggaran cybercrime lebih banyak apabila dibandingkan dengan Indonesia, setiap tahunnya Amerika mengalami pelanggaran cybercrime sebanyak 600 kasus setiap tahunnya. Khususnya dalam bidang perbankan, jumlah pelanggaran cybercrime mencapai angka 190 hingga 230 setiap tahunnya. Kasus-kasus yang telah ditangani sebanyak 150 hingga 170. Dalam pelaksanaan pelanggaran cybercrime di Amerika hampir dapat ditangani dan jumlah kasus yang telah diselesaikan lebih tinggi, hal ini dikarenakan Amerika merupakan bagian dari Convention of Cybercrime sehingga mendapat kemudahan dalam menangkap pelaku yang berada diluar yurisdiksi Amerika dan memiliki teknologi yang lebih maju. Namun, tetap mengalami kendala-kendala yang antara lain berupa kurangnya sumber daya manusia yang menjadi anggota untuk membantu proses penyelidikan dan penyidikan serta kurangnya sosialisasi terhadap masyarakat agar dapat mengurangi terjadi kasus cybercrime tersebut.

b. Tindakan yang termasuk *Cyber Crime* di sektor perbankan di Indonesia dan Amerika.

Mengingat pemamfaatan teknologi informasi bersifat lintas teritorial, maka konsep yurisdiksi tidak lagi dapat diberlakukan di suatu negara sebab terdapat kemungkinan terjadinya pelanggaran *Cyber Crime* oleh seorang pelaku yang menyebabkan kerugian, kepentingan pemerintah atau masyarakat suatu negara menjadi dilanggar haknya.

Terdapat begitu banyak modus tindak kejahatan *Cyber Crime*, pada prinsipnya delik yang harus diterapkan adalah delik formil, mengingat dalam tindakan kejahatan *Cyber Crime* unsur kerugian seringkali malah sulit untuk dibuktikan karena sifatnya yang lintas teritorial dan ketidaksadaran dari korban, padahal pelaku dan bukti-bukti kejahatan sudah dapat tertangkap tangan. Beberapa tindak kejahatan *Cyber Crime* yang terjadi di sektor perbankan di negara Indonesia dan Amerika antara lain sebagai berikut[93] :

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

[93] Kuncoro Tri, Penegankan Hukum terhadap *Cyber Crime* di bidang perbankan sebagai kejahatan Transnasional, di akses pada tanggal 18 Januari 2015.

2. *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
3. *Sniffing*. *Sniffing* cara yang digunakan oleh pelaku dengan mengamati paket data internet yang digunakan oleh pengguna untuk mendapatkan nomor identitas dan *password* yang bersangkutan.
4. *Web Deface*: *System Exploitation,* yaitu eksploitasi sistem dengan megganti tampilan awal dari sebuah situs resmi.
5. *Email Spamming,* yakni dengan mengirimkan *email* kepada pemilik akun dengan menawarkan produk-produk atau menyatakan bahwa pemilik akun telah memenangkan suatu undian.

Kelima pelanggaran tersebut merupakan perbuatan yang marak terjadi pada lembaga perbankan baik di Indonesia maupun di Amerika, walaupun pada dasarnya perekonomian di negara Indonesia dengan Amerika tidak sama, namun pelanggaran cybercrime pada sektor perbankan di Indonesia pada dasarnya menyerupai pelanggaran yang terjadi di Amerika, perbedaannya terletak pada tingginya jumlah pelanggaran cybercrime yang telah ditanganin di masing-masing negara.

Ulah para pelaku *Cyber Crime* untuk menerobos sistem komputer lembaga perbankan menimbulkan kerugian yang sangat meresahkan pada lembaga-lembaga perbankan. Selain data mereka dapat di akses secara ilegal oleh pelaku *Cyber Crime*, mereka juga dapat menyebarkan virus-virus yang berbahaya bahkan perbuatan mereka sampai kepada ancaman kerusakan data komputer kenbaga perbankan yang telah diterobos. Selain dapat menimbulkan kerugian materi dan keuangan yang besar pada perekonomian suatu negara bahkan perekonomian dunia dapat terancam, kejahatan komputer menimbulkan permasalahan yang serius bagi peradilan pidana di sebagian negara-negara didunia, oleh karena itu penaggulangannya permasalahan pelanggaran *Cyber Crime* harus dilakukan secara komprehensif. Dimana dalam penanganan pelanggaran *Cyber Crime* harus dilakukan secara meluas, berdimensi nasional maupun internasional

Dalam beberapa kasus *Cyber Crime,* pelaku menggunakan PIN, *password* milik nasabah untuk mengakses akun dan di jadikan sebagai rekening palsu para pelaku, sedangkan dalam kasus lain mereka mungkin ingin mencuri semua uang dan memindahkan dana ke rekening palsu. Kadang-kadang, niat kriminal di dunia maya secara umum hanya ingin merusak citra atau nama baik bank dan oleh karena itu, mereka memblokir sistem *server* bank tersebut sehingga klien tidak dapat mengakses akun miliknya.

Menurut negara Amerika, maraknya pelanggaran *Cyber Crime* di Amerika terutama pada sektor perbankan harus mencari cara untuk menangani terjadinya pelanggaran yang setidaknya dapat mencegah atau mengurangi perkembangan

pelanggaran *Cyber Crime.* Namun penanganan tersebut tidaklah mudah untuk direalisasikan[94].

Cyber Crime pada lembaga perbankan menjadi lebih sering, lebih canggih, dan semakin meluas. Meningkatnya pelangaran *Cyber Crime* dan serangan siber dapat dikaitkan dengan sejumlah factor, yakni[95]:

1. Kurangnya kerjasama negara-negara menghambat sistem untuk mencari intelijensi dalam teknologi, memecahkan permasalahan *Cyber Crime* dan kekayaan intelektual di dunia perbankan. Hacktivists bertujuan untuk membuat '*political statement*' dengan cara mengganggu sistem lembaga perbankan. Dengan melakukan pelanggaran ke dalam sistem perbankan suatu Negara yang bertujuan untuk mendapat keuntungan moneter, dengan mencuri dana melalui pengambilalihan akun, perampokan ATM, dan mekanisme lainnya.
2. Menurunnya perekonomian suatu negara, meningkatkan kesempatan bagi para penjahat dari semua kalangan untuk mencari cara-cara baru untuk melakukan penipuan siber atau kejahatan di dunia maya karena tipe kejahatan ini dapat dilakukan dengan mudah dan sedikit modal. Sebuah pasar gelap mengembangkan data-data pelanggaran berfungsi untuk mendorong pelaku kejahatan lebih lanjut.

1. Permasalahan yang timbul dari Tindak Pidana *Cyber Crime* di sektor Perbankan Indonesia dan Amerika

Beberapa permasalahan yang dapat ditimbulkan oleh tindak pidana *Cyber Crime* di sektor perbankan adalah[96]:

a. *Tabel 4.1:Permasalahan yang timbul dalam Penanganan Cyber Crime Indonesia dan Amerika*

	Tolak Ukur	**Persamaan**		**Perbedaan**	
		Indonesia	**Amerika**	**Indonesia**	**Amerika**
1	**Regulasi**	UU ITE No. 11 Tahun 2008 dan KUHP Di Indonesia Regulasi yang digunakan untuk	Title 18 U.S. Code § 1030 yang mengatur mengenai *Fraud and related activity in connection with*	Regulasi yang digunakan oleh Indonesia dalam mengatur kejahatan *Cyber Crime*	Amerika dalam menghadapi permasalahan kejahatan *Cyber Crime* telah membentuk Regulasi yang

[94] Anderson, R., et al., *Measuring the cost of cybercrime*. (Amerika: Harcourt, Brace&World.Inc. 2012). hlm, 28.
[95] *Ibid.* hlm. 29.
[96] *Symantec Cyber Crime Report, Cybercrime Report. http://now-static.norton.com /now/ en /pu/images /Promotions /2012/ cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912. Pdf* diakses pada tanggal 5 Februari 2015.

		mengatur mengenai *Cyber Crime* adalah UU ITE dan KUHP	*computers*, Title 18 U.S. Code § 1030 yang mengatur mengenai *Bank Fraud* dan Title 18 U.S. Code § 2252B yang mengatur mengenai *Misleading domain names on the internet*. Terdapat banyak perangkat hukum atau regulasi yang digunakan untuk mengatur berbagai jenis kejahatan *Cyber Crime* di Amerika dan tata cara penanggulangannya	masih sangat umum (general) kadang-kadang belum tepat pada sasaran	secara tepat guna dan khusus untuk mengatur tindakan kejahatan yang diakibatkan oleh *Cyber Crime*
2	**Lembaga**	IDCERT Merupakan lembaga yang dibentuk dengan tujuan untuk menghadapi maraknya kejahatan dunia maya di Indonesia *Cyber Crime*	Amerika juga membentuk banyak lembaga khusus seperti *Eletronic Crime Task Forces* (ECTFs) dan *Regional Computer Forensic Labs* (RCFLs) , untuk menangani permasalahan kejahatan *Cyber Crime* sesuai	Lembaga IDCERT yang dibentuk untuk menangani permasalahan *Cyber Crime* masih belum berfungsi secara penuh, tugas IDCERT masih terbatas dan kurang professional. Hal ini disebabkan	Lembaga-lembaga Amerika yang dibentuk untuk memeriksa dan menganalisis permasalahan *Cyber Crime* bekerja secara independen dan dapat mengambil sebuah keputusan yang dianggap baik

			dengan kebutuhan negaranya	kurangnya intelijensi pada maraknya kemajuan teknologi	sendirinya berdasarkan keahliannya.
3	**Kerjasama Antar Negara**	Indonesia menganut sistem kerjasama antar negara dalam menangani permasalahan *Cyber Crime*	Dikarenakan kerjasama antar negara sangat menunjang penanganan kasus kejahatan *Cyber Crime* maka, sama halnya dengan Indonesia Amerika juga melakukan kerjasama dengan negara-negara lainnya untuk menanggulangi permasalahan *Cyber Crime*	Kerjasama antar negara yang dilakukan negara Indonesia adalah secara bilateral yaitu dengan melakukan ekstradisi dengan beberapa negara . Namun hanya terbatas antar negara itu saja	Kerjasama antar negara yang dilakukan oleh Amerika adalah berdasarkan konvensi "Convention of *Cyber Crime*" yang mencakup negara-negara yang lebih luas dan banyak.
4	**Kerjasama dengan pihak swasta**	-	-	Belum terdapat kerjasama berbentuk swasta dengan pemerintahan di Indonesia dalam kaitannya dengan tindakan kejahatan *Cyber Crime*	Amerika telah melakukan perencanaan untuk bekerjasama dengan pihak swasta di negaranya salah satunya adalah bentuk kerjasama dengan universitas-universitas untuk meningkatkan ilmu dalam hal teknologi

					sehingga dapat membantu aparat penegak hukum menangani kejahatan *Cyber Crime*

Sumber : Data diolah Peneliti

Dari table diatas bisa diliat bahwa strategi yang digunakan oleh Negara Indonesia dalam penanganan permasalahan *Cyber Crime* masih tidak kompeten karena akibat dari ketidakpastian hukum atau regulasi yang mengatur secara jelas dan tegas. Sedangkan Amerika yang sudah mempunyai beberapa strategi atau tindakan yang jelas dalam penanganan permasalahan *Cyber Crime.*

2. Tabel Kasus yang telah ditangani

1. Strategi Penyelesaian di Indonesia

Tabel 4.2:Strategi penyelesaian kasus cybercrime di Indonesia

No.	Contoh Kasus	Strategi Penyelesaian
1	Kasus cybercrime yang dilakukan pelaku sebagai seorang kasir di Starbuck, pelaku mencatat nomor kartu kredit atau debet milik konsumen yang melakukan pembayaran di starbuck kemudian oleh pelaku tersebut untuk nomor kartu kredit yang berhasil dicatatnya dipergunakan untuk berbelanja secara online seperti membeli Ipad atau Iphone pada situs resmi perusahaan apple yang menyebabkan kerugian sebesar Rp. 30.000.000,- (tiga puluh juta Rupiah) pada lembaga perbankan	Tindakan yang dilakukan oleh pihak kepolisian yaitu pertama dengan menyelidiki pengunaan terakhir pada nomor kartu kredit yang telah dicuri oleh pelaku dengan melakukan kerja sama dengan pihak perbankan yang memberikan informasi berupa transaksi penggunaan dari kartu kredit tersebut yang kemudian di lacak lebih lanjut *ip address* yang digunakan oleh pelaku untuk berbelanja, maka akan menemukan pelaku dari pencurian nomor kartu kredit milik nasabah perbankan.
2	Kasus cybercrime dengan jenis *Token* pada bank BCA dan Mandiri dimana nasabah diminta untuk melakukan konfirmasi *token* pada saat nasabah menggunakan *internet banking.* Akan tetapi, pihak bank tidak pernah	Strategi penanganan terhadap kasus tersebut adalah dengan menyelidiki jenis virus yang menyebabkan hangnya komputer nasabah. Dan dari virus tersebut, akan lebih mudah untuk mencari

	meminta nasabah untuk melakukan konfirmasi *token* tersebut. Hal ini membahayakan dan dapat menyebabkan kerugian kepada nasabah bank sebab sinkronisasi token ini menyebabkan komputer nasabah dimasuki oleh virus yang menyebabkan komputer hang dan berdasarkan informasi yang diperoleh, setelah *restart* dan kembali *login* ke *Internet Banking* BCA, nasabah tersebut telah mendapati uangnya berkurang sebesar Rp. 13 juta. Lembaga perbankan telah melakukan sosialisasi terhadap masyarakat dan nasabah bank BCA itu sendiri	keberadaan pelaku. Namun, dari pihak kepolisian belum bisa secara sepenuhnya menangani kasus tersebut dikarenakan kurangnya informasi yang diperoleh, selain itu teknologi yang digunakan oleh kepolisian masih terbatas sehingga tidak dapat mengetahui jenis virus yang menyerang komputer nasabah tersebut.

Sumber : Data diolah Peneliti

2. Strategi Penyelesaian di Amerika

Tabel 4.3:Strategi penyelesaian kasus cybercrime di Amerika

No.	Contoh Kasus	Strategi Penyelesaian
1	Kasus pembobolan pada beberapa lembaga perbankan di Amerika yang dilakukan oleh 5 warga negara Rusia, Kelima pelaku tersebut bekerja sama memasuki sistem keamanan lembaga keamanan dengan cara menonaktifkan peranngkat lunak *anti-virus* lembaga perbankan dan pengumpulan data hasil pencurian pada beberapa *platform* milik mereka, kemudian mendistribusikan dan menjualnya. Data hasil pencurian tersebut berupa nomor dari kartu kredit dan kartu debet milik lembaga perbankan. Penanganan terhadap kasus tersebut mengalami kesulitan terutama dikarenakan para pelaku hacking tersebut berwarganegara Rusia karena Rusia tidak pernah ingin mengekstradisikan	Pihak kepolisian sudah mendapatkan bukti yang kuat untuk menangkap para pelaku cybercrime tersebut. Tetapi para pelaku yang telah melarikan diri ke negara lain mengharuskan adanya perjanjian antar kedua negara, untuk mempermudah penangkapan atau pengembalian pelaku tindak pidana yang telah menyebabkan kerugian tersebut. Dan pada kasus 5 warga negara Rusia tersebut, Amerika telah memiliki perjanjian kerjasama dengan Pemerintahan Belanda. Sehingga pada saat salah satu pelaku melarikan diri ke negara belanda, pelaku tersebut ditangkap dan dikembalikan ke

	warnanegaranya. Kelima pelaku tersebut dengan pencurian 160 juta nomor kartu kredit, menyebabkan kerugian ratusan juta dolar amerika. Salah satu pelaku merupakan spesialis dalam menembus keamanan jaringan dan mendapatkan akses ke sistem komputerisasi perusahaan korban, biasanya melalui eksploitasi *standardized query language* (SQL) *injection*. Para pelaku *Cyber Crime* sering mengambil keuntungan dari perbatasan internasional dan perbedaan sistem hukum, dengan harapan dapat menghindari ekstradisi untuk diadili, dari kasus ini menunjukkan bahwa melalui kerjasama internasional, dan melalui kerja sama tim besar antara Departemen Kehakiman dan Departemen Keamanan Dalam Negeri, mampu membawa pelaku *cyber cime* agar diadili di mana pun mereka melakukan kejahatan mereka.	Amerika untuk diadili sehingga dengan adanya kasus tersebut menunjukkan kerja keras para Jaksa umum dengan mitranya yaitu *US Secret Service* untuk mengungkap pelanggaran kasus pelaku *cyber crime* yang dilakukan pelaku cybercrime tersebut pada lembaga perbankan.
2	Kasus Kedua adalah jenis cybercrime dengan pencurian dana yang dilakukan oleh tiga pelaku yang berasal Ukraina dan New York dengan memasuki tanpa izin 14 buah rekening nasabah Amerika Serikat yang merupakan lembaga keuangan dan Departemen layanan *Payroll*. Jaksa federal mengumumkan dakwaan dari tiga orang yang mereka tuduh sebagai pelaku cybercrime internasional yang mencoba mencuri uang sejumlah 15 juta dollar Amerika pada ke 14 lembaga keuangan tersebut. Ketiga pelaku tersebut memasuki sistem jaringan dari lembaga keuangan	Berdasarkan sosialisasi yang telah dilakukan pihak kepolisian di Amerika kepada seluruh lembaga keuangan dan pembayaran termasuk lembaga perbankan. Meningkatkan kerjasama antara lembaga keuangan kepada pihak kepolisian apabila terjadi kasus cybercrime yang merugikan lembaga keuangan tersebut. Hal ini memudahkan pihak kepolisian melakukan pencaharian terhadap pelaku cybercrime karena adanya bantuan berupa informasi dan dukungan dari lembaga keuangan swasta.

	dan lembaga pembayaran tersebut dengan berpura-pura menjadi petugas perpajakan negara sehingga pelaku dapat masuk dan memperoleh data-data nasabah dari lembaga keuangan. Para pelaku tersebut dituntut melanggaran pasal mengakses secara tidak sah ke jaringan milik orang lain, mengalihkan dana nasabah ke rekening bank dan kartu debit prabayar, menggunakan "*cashers*" untuk melakukan penarikan ATM dan pembelanjaan di Georgia, Illinois, Massachusetts, New York dan di tempat lain.	

Sumber : Data diolah Peneliti

Dari tabel strategi penyelesaian dapat kita lihat bahwa Amerika memiliki strategi penyelesaian kasus *cybercrime* yang lebih baik dibandingkan dengan Indonesia, yang disebabkan Amerika sudah mempunyai persiapan matang serta melakukan pelatihan khusus terhadap kepolisian yang menangani kasus cybercrime dan juga memiliki teknologi yang lebih canggih, sedangkan pihak kepolisian Indonesia yang mendapatkan pelatihan khusus pada cybecrime masih sedikit, dikarenakan kekurangan biaya pelatihan dan alat yang digunakan masih kurang mampu secara sepenuhnya membantu pihak kepolisian untuk menyelesaikan permasalahan cybercrime.

c. Persamaan dan Perbedaaan kendala dalam penanganan Cyber Crime Indonesia dan Amerika

Tabel 4.5:Persamaan dan Perbedaan Kendala dalam Penanganan Cyber Crime Indonesia dan Amerika

	Tolak Ukur	**Persamaan**		**Perbedaan**	
		Indonesia	**Amerika**	**Indonesia**	**Amerika**
1	**Menemukan Pelaku pelanggaran *Cyber Crime***	Negara Indonesia dengan Amerika dalam menemukan pelaku pelanggaran *Cyber Crime* mengalami kendala yang hampir sama yaitu kesulitan dalam melacak pelaku pelanggaran *Cyber Crime* karena kejahatan *Cyber Crime* yang hanya menggunakan internet membuat		Dalam menemukan pelaku pelanggaran *Cyber Crime*, Indonesia masih merasa sulit dan lama	Teknologi internet yang sangat canggih mempersulit Amerika untuk menemukan pelaku pelanggaran

		pelaku dapat melakukan tindak kejahatan dimana saja mereka berada dan dapat mengakses keluar negeri tanpa batas.	karena kurangnya sumber daya serta kurangnya kerjasama dengan Negara lain	karena dunia maya yang tanpa batas (borderless)
2	**Penerapan Regulasi**	-	Karena Indonesia belum memiliki Peraturan khusus untuk menanggulangi permasalahan *Cyber Crime* maka terhadap kasus *Cyber Crime* sulit untuk menemukan hukuman yang sesuai dengan perbuatan pelaku	Berbeda dengan Amerika, yang telah mempunyai regulasi khusus untuk menangani kasus *Cyber Crime* dan tepat untuk diaplikasikan kepada pelaku pelanggaran *Cyber Crime*
3	**Pemeriksaan kasus**	Dalam pemeriksaan kasus kejahatan *Cyber Crime*, dikarenakan tidak ada saksi mata yang secara langsung melihat maupun mendengar menjadi kendala yang dihadapi oleh Indonesia maupun Amerika dalam memeriksa kasus kejahatan *Cyber Crime*	Peemriksaan kasus yang dilakukan di Negara Indonesia masih bersifat tradisional sehingga banyak mengalami kendala, penyebabnya adalah aparat yang kurang	Tindakan kejahatan yang banyak terjadi di Amerika merupakan kejahatan worldwide yang mencakup pelanggaran yang tidak hanya terjadi di Negara Amerika sendiri tetapi juga sampai

			berpengalaman dalam bidang *Cyber Crime* terutama pada sector perbankan	keluar negeri menyebabkan kendala bagi amerika dalam memeriksa kasus.
4	**Kerjasama dengan pihak swasta**	Untuk menyelesaikan permasalahan pelanggaran *Cyber Crime* memerlukan kerjasama bukan hanya kerjasama antar Negara akan tetapi kerjasama Negara dengan swasta pada Negara masing-masing juga sangat dibutuhkan namun baik di Indonesia maupun di Amerika belum menerapkan kerjasama antara pemerintah dengan swasta	Negara Indonesia belum mengadakan kerjasama antar pemerintahan dengan swasta kaitannya dengan pelanggaran *Cyber Crime*	Negara Amerika sedang merancang sebuah kerjasama antara pemerintah dengan swasta karena merasa diperlukannya bentuk kerjasama seperti ini untuk menanggulangi pelanggaran *Cyber Crime*
5	**Perekrutan personil**	Selain membentuk lembaga khusus untuk menangani kasus *Cyber Crime*, Indonesia dan Amerika juga membutuhkan anggota untuk bekerja pada lembaga tersebut, anggota mana harus memahami dan professional dalam bidang internet dan teknologi informasi serta memahami system pemeriksaan kasus kejahatan/tindak pidana agar memudahkan penyelesaian kasus *Cyber Crime*	Kendala yang dihadapi Indonesia dalam merekrut personil untuk menangani kasus *Cyber Crime* adalah kurangnya sumber daya yang ahli dalam bidang teknologi	Pemerintah amerika memerlukan dana yang cukup banyak untuk memperoleh personil dengan keahlian teknologi dan juga memahami system pemeriksaan kepolisian. Hal ini menjadi kendala Amerika

Sumber : Data diolah Peneliti

D. Kesimpulan

1. Strategi penanganan *Cyber Crime* di negara Indonesia dan Amerika pada sektor perbankan

Dalam menangani berbagai jenis pelanggaran *cybercrime* yang terjadi di sektor perbankan baik di Indonesia maupun di Amerika masing-masing mempersiapkan strateginya untuk dapat menjerat pelaku *cybercrime* dengan hukum yang berlaku. Berdasarkan penelitian yang telah dilakukan diketahui bahwa strategi penanganan pelanggaran *cybercrime* di Indonesia apabila dibandingkan dengan di Amerika masih sangat kurang dan kalah efektif. Penanganan pelanggaran yang dilakukan Indonesia memerlukan waktu yang lama, dikarenakan teknologi yang kurang canggih dan lembaga yang belum mandiri dalam penaganan.

Kerjasama dengan pihak swasta maupun dengan negara lain dalam hal penanganan pelanggaran *cybercrime* juga merupakan salah satu strategi penting dalam penanganan pelanggaran *cybercrime*, kerjasama dengan swasta dan kerjasama dengan Negara lain bertujuan untuk menjalin hubungan yang baik antara pemerintahan dengan swasta agar pihak swasta dapat membuka diri serta berpartisipasi aktif kepada pemerintahan terutama ketika menangani kasus pelanggaran *cybercrime*. Demikian juga kerjasama antar pemerintahan dengan negara-negara lain yang diharapkan agar terjalin hubungan kerjasama yang baik antar negara agar masing-masing negara dapat membantu kepentingan negara lainnya dalam hal melakukan ekstradisi pelaku *cybercrime* apabila kebetulan berada di dalam negaranya. Indonesia sampai saat ini masih kurang menerapkan kedua bentuk kerjasama ini, baik dengan pihak swasta maupun dengan negara lain, kerjasama antar negara hanya dilakukan terbatas kepada negara-negara tertentu saja, hal ini membuat keterbatasan pergerakan negara Indonesia apabila pelaku pelanggaran *cybercrime* yang menyebabkan kerugian di Indonesia ternyata tidak berada pada teritorial yurisdiksi negaranya akan tetapi berada di negara lain yang tidak memiliki hubungan ekstradisi atau hubungan kerjasama berbentuk apapun. Berbeda dengan negara Amerika yang saat ini sudah mulai membentuk dan menjalani kerjasama dengan pihak swasta seperti universitas dalam negeri dalam hal perekrutan SDM berpotensial serta meningkatkan kerjasama dengan Negara-negara lainnya untuk mempertinggi ekstradisi terhadap pelaku *cybercrime* yang melarikan dirinya ke Negara lain.

Indonesia juga belum memiliki rencana penanggulangan atau pencegahan terhadap pelanggaran *cybercrime*. Sedangkan berdasarkan informasi yang diperoleh, Amerika telah memiliki regulasi serta lembaga khusus untuk menangani permasalahan berkaitan dengan *cybercrime* itu sendiri dengan anggotanya yang mahir dalam bidang internet dan teknologi informasi. Amerika juga terus melakukan pembaharuan mengikuti cepatnya perkembangan internet sekarang ini. Membentuk dan merencanakan hal-hal yang dapat mencegah cepatnya perkembangan kejahatan melalui dunia maya. Sehingga diharapkan agar Indonesia dapat segera dengan serius menanggapi pelanggaran yang diakibatkan oleh *cybercrime* itu sendiri karena apabila tidak dari dini pencegahan dan penanggulangan dilakukan *cybercrime* dapat berkembang dan menjadi sulit untuk

dihapuskan sedangkan, *cybercrime* di sisi lain sangat membahayakan pereknonomian Negara Indonesia itu sendiri.

2. Kendala dalam penanganan *cybercrime* pada sektor perbankan di Negara Indonesia dan Amerika

   Di Indonesia dan Amerika bersama-sama mengalami kendala dalam hal penanganan kasus pelanggaran *cybercrime,* salah satu kendala yang dialami adalah susahnya menemukan pelaku pelanggaran *cybercrime* apabila pelaku tidak berada pada yurisdiksi territorial negaranya, baik Indonesia maupun Amerika mengalami kesulitan dalam menemukan pelaku sebab pelaku kejahatan *cybercrime* pada umumnya memanfaatkan keunggulan *cybercrime* yang tanpa batas untuk melakukan sebuah tindak pidana, sehingga tidak mudah ditemukan atau bahkan dapat terbebas dari hukuman, kendala kedua yang dialami oleh Negara Indonesia dan Amerika dalam menangani pelanggaran *cybercrime* adalah kurangnya personil khusus yang dapat melakukan penanganan terhadap pelanggaran *cybercrime,* kendala yang dialami Indonesia dalam kaitannya dengan personil dikarenakan masih sedikitnya edukasi dan sosialisasi mengenai *cybercrime* sehingga kurang minat dan sifat keingintahuan masyarakat mengenai pelanggaran *cybercrime*. Sedangkan Amerika sudah banyak melakukan penyebaran informasi perekrutan personil untuk menangani permasalahan *cybercrime*, namun keterbatasan SDM serta mahalnya biaya menyebabkan Amerika juga sulit menemukan personil yang dinginkan.

Daftar Pustaka

a. Buku & Jurnal

Abdul Wahid dan Mohammad Labib, 2005, *Kejahatan Mayantara* (*Cyber Crime*), PT. Refika Aditama, Jakarta.

Anderson, R., et al., 2012, *Measuring the cost of cybercrime*, Harcourt, Brace&World.Inc, Amerika.

b. Internet

Kuncoro Tri, Penegankan Hukum terhadap Cyber Crime di bidang perbankan sebagai kejahatan Transnasional, http:// repository.akprind.ac.id/sites/files/penegakan-hukum-terhadap-Cyber-crime, di akses pada tanggal 18 Januari 2015.

Soetarto dan M. Nasir, Teknologi *E-Bangking* dikalangan *Smart Customer*, http://repository.akprind.ac.id/sites/files/conference-paper/2008/nasir_2127.pdf diakses pada tanggal 5 Februari 2015

Symantec Cyber Crime Report, Cybercrime Report, http://now-static.norton.com /now/ en /pu/images /Promotions /2012/ cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912. Pdf diakses pada tanggal 5 Februari 2015.

c. Peraturan Perundang-undangan

Peraturan perundang-undangan Kitab Undang-undang Hukum Pidana (KUHP)

Undang-undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Title 18 U.S. Code § 1030 yang mengatur mengenai *Fraud and related activity in connection with computers*,

Title 18 U.S. Code § 1344 yang mengatur mengenai *Bank Fraud*

Title 18 U.S. Code § 2252B yang mengatur mengenai *Misleading domain names on the internet*