UNIVERSITAS INDONESIA

MANAJEMEN PENYIDIKAN TINDAK PIDANA *HACKING*

(Studi Kasus : Penyidikan Tindak Pidana Hacking Website Partai Golkar Oleh Unit V IT & Cybercrime Bareskrim Polri)

RINGKASAN DISERTASI

Untuk dipertahankan dalam Ujian Promosi di hadapan Senat Guru Besar Universitas Indonesia
guna meraih gelar Doktor dalam bidang Kajian Ilmu Kepolisian
pada hari Sabtu, tanggal 7 Juni 2008
di Gedung Balai Sidang Universitas Indonesia Kampus UI Depok

PETRUS REINHARD GOLOSE
NPM : 9103070058

PROGRAM STUDI KAJIAN ILMU KEPOLISIAN
PROGRAM PASCASARJANA
2008

UNIVERSITAS INDONESIA

MANAJEMEN PENYIDIKAN TINDAK PIDANA *HACKING*

(*Studi Kasus: Penyidikan Tindak Pidana Hacking Website Partai Golkar Oleh Unit V IT & Cybercrime Bareskrim Polri*)

RINGKASAN DISERTASI

Untuk dipertahankan dalam Ujian Promosi di hadapan Senat Guru Besar Universitas Indonesia
guna meraih gelar Doktor dalam bidang Kajian Ilmu Kepolisian
pada hari Sabtu, tanggal 7 Juni 2008
di Gedung Balai Sidang Universitas Indonesia Kampus UI Depok

PETRUS REINHARD GOLOSE
NPM: 9103070058

PROGRAM STUDI KAJIAN ILMU KEPOLISIAN
PROGRAM PASCASARJANA
2008

DAFTAR ISI

KATA PENGANTAR

Cybercrime merupakan suatu kasus transnasional yang dihadapi oleh dunia pada saat ini. Salah satu bentuk kejahatan *cyber* adalah *hacking*. Sudah terdapat dua kasus *hacking* yang telah disidangkan di Indonesia. Kasus yang pertama adalah kasus *hacking website* KPU yang ditangani oleh Polda Metro Jaya. Sedangkan kasus yang kedua adalah kasus *hacking website* Partai Golkar yang ditangani oleh Unit V *IT & Cybercrime* Direktorat II Eksus Bareskrim Polri.

Dengan menggunakan metode penelitian kualitatif, disertasi ini berupaya mengungkapkan Manajemen Penyidikan Tindak Pidana *Hacking* dengan studi kasus: Penyidikan *hacking website* Partai Golkar oleh Unit V *IT & Cybercrime* Bareskrim Polri.

Judul ini saya pilih, mengingat ketertarikan saya terhadap *cybercrime* terutama kasus *hacking*, dimana kaedah normatif baik materil maupun formil saat itu belum diatur secara khusus. Selain itu, pengalaman penyidik, penuntut umum dan hakim dalam menangani kasus *hacking* masih langka. Sedangkan ke depan, diperkirakan *cybercrime* akan semakin marak terjadi di Indonesia dengan beragam cara dan berbagai bentuk seiring dengan perkembangan teknologi yang semakin canggih.

Tujuan yang ingin dicapai dalam penelitian ini adalah untuk mengkaji dan memberikan pemahaman yang komprehensif mengenai *hacking* sebagai bagian dari *cybercrime*, karakteristik tindak pidana *hacking* yang berbeda dengan tindak pidana konvensional dan manajemen penyidikan *hacking* serta faktor-faktor yang mempengaruhi meliputi faktor kepemimpinan, budaya organisasi dan *stakeholders*.

Untuk mendeskripsikan *hacking* sebagai suatu kejahatan diperlukan pengetahuan mengenai konsep dan teori kejahatan tentang *hacking*. Oleh karenanya penelitian ini didasarkan pada pengamatan di lapangan yaitu pengamatan terlibat selama penanganan kasus *hacking website* Partai Golkar, selanjutnya bagaimana pemaknaan atau penafsiran para penyidik Unit V *IT & Cybercrime* terhadap ketentuan yuridis normatif baik materil maupun formil yang berlaku saat itu dihubungkan dengan tindak pidana *hacking*.

Penafsiran terhadap ketentuan hukum dan karakteristik *hacking* yang khas berbeda dengan kejahatan konvensional merupakan permasalahan dan tantangan bagi para penyidik dalam melakukan penyidikan. Penyidik menerapkan prinsip-prinsip dan fungsi manajemen dalam proses penyidikan yang dipengaruhi oleh faktor-faktor kepemimpinan, budaya organisasi dan *stakeholders*.

Puji dan syukur saya ucapkan kepada Tuhan yang telah memberkati saya, sehingga saya dapat menyelesaikan tulisan ini. Selama penulisan disertasi ini, telah begitu banyak menyerap energi, pikiran dan waktu saya selama berbulan-bulan. Selama itu pula, orang tua, istri dan anak-anak tercinta, setia memberikan perhatian, menemani dan menyemangati agar saya dapat menyelesaikan tugas ini dengan baik dan tepat waktu. Untuk itu saya ucapkan terima kasih dan rasa cinta yang kian mendalam kepada mereka. Tanpa dorongan mereka, saya telah patah arang di tengah jalan.

Dalam penulisan disertasi ini, saya sadar bahwa tanpa bimbingan, arahan dan bantuan dari berbagai pihak tentunya sulit untuk mewujudkan disertasi ini. Saya ingin mengucapkan penghargaan yang tulus dan terimakasih yang mendalam kepada Prof. Parsudi Suparlan, Phd. (Alm) pada awalnya sebagai Promotor yang selalu bersedia memberikan waktu dan menyumbangkan pemikiran dalam penulisan disertasi ini. Semoga amal ibadahnya diterima oleh Tuhan Yang Maha Kuasa. Terima kasih yang sedalam-dalamnya juga saya sampaikan kepada Prof. Dr. Victor Purba, SH., LLM (Alm), yang pada awalnya melakukan pengujian untuk usulan penelitian saya, semoga Tuhan Yang Maha Kuasa menerima segala amal ibadahnya.

Selanjutnya saya juga ingin mengucapkan penghargaan dan terimakasih yang sebesar-besarnya kepada Prof. Dr. Sarlito W. Sarwono, Psi selaku Promotor, dan Prof. Mardjono Reksodiputro, S.H., M.A serta Prof. Dr. Tb. Ronny Nitibaskara selaku Ko Promotor. Prof. Dr. Awaloedin Djamin, MPA, Prof. Dr. Valerine Kriekhoff, S.H., M.A, Prof Dr. Barda Nawawi Arief, S.H., Prof. Drs. Koesparmono Irsan, S.H., M.M, MBA, Prof. Dr. Toemin Masoem, yang senantiasa memberikan sumbangan pemikiran dalam penulisan disertasi ini.

Ungkapan yang tulus kepada Kabareskrim Polri Komjen Pol Drs. Bambang Hendarso Danuri, MM, Kalakhar BNN Irjen Pol Drs. Gories Mere, Brigjen Pol Drs. Surya Dharma dan seluruh anggota satuan tugas anti teror/bom atas dukungan moril kepada saya, kemudian terima kasih juga kepada Brigjen Pol. Wenny Warouw mantan Direktur II Tindak Pidana Ekonomi & Khusus Bareskrim Polri. Kombes Pol Drs. Edmon Ilyas, MH selaku Direktur II Tindak Pidana Ekonomi & Khusus Bareskrim Polri. Saya juga mengucapkan terima kasih yang sebesar-besarnya kepada seluruh penyidik Unit V *IT & Cybercrime* Bareskirm Polri yang telah bersedia memberikan waktu untuk menerima permintaan wawancara, bahkan beberapa diantaranya bersedia diwawancara untuk kedua-kalinya demi pemahaman yang komprehensif atas gejala yang ada. Terima kasih juga saya ucapkan kepada rekan-rekan korespondensi di luar negeri yang telah bersedia memberikan jawaban atas rangkaian pertanyaan yang telah saya kirimkan.

Tidak lupa saya ucapkan terima kasih kepada Sdri. Sri Maulani Heuer, S.H., M.H. dan Sdr. Agung Nugroho W., S.H., S.Sos., M.M., serta rekan-rekan sekalian dari BM & Partners Law Office yang kerap memberikan pertimbangan, sumbang saran dan diskusi intensif, berikut pencarian berbagai bahan literatur sehingga disertasi ini dapat terselesaikan dengan baik. Selain itu, saya juga mengucapkan terima kasih kepada semua pihak yang telah membantu saya dalam menulis disertasi ini, yang tidak mungkin saya dapat sebutkan satu persatu.

Demikianlah, kata pengantar ini saya sampaikan, saya menyadari sekali walau saya telah berupaya sebaik mungkin, namun tentu saja tetap ada kelemahan dalam disertasi ini. Untuk itu saya sangat mengharapkan sumbangan saran serta kritik agar pada penulisan yang akan datang, saya dapat menghasilkan suatu karya yang lebih baik lagi. Untuk itu saya sangat menghargai setiap komentar dan saran pembaca sekalian. Pembaca dapat menghubungi saya di petrus@golose.net. Terima kasih untuk partisipasi dan investasi anda membaca disertasi saya.

Jakarta, 7 Juni 2008

Petrus Reinhard Golose

ABSTRAK

Disertasi ini merupakan hasil analisis dari penelitian kualitatif dan literatur secara mendalam yang terfokus pada manajemen penyidikan *hacking* oleh Unit V *IT & Cybercrime* yang diterapkan pada proses penyidikan kasus *hacking website* Partai Golkar. Dalam pelaksanaan penyidikan *hacking*, Unit V *IT & Cybercrime* menghadapi permasalahan berkaitan dengan belum adanya ketentuan hukum materil yang secara tegas mengatur mengenai tindak pidana *hacking* pada saat itu dan secara khusus mengenai penanganan bukti digital. Permasalahan tersebut berhasil dihadapi penyidik dengan melakukan interpretasi terhadap ketentuan hukum yang ada. Disertasi ini mengajukan suatu pengertian tindak pidana *hacking* sebagai setiap kegiatan yang menggunakan komputer atau sistem elektronik lainnya yang dilakukan dengan cara mengakses suatu sistem jaringan komputer baik yang terhubung dengan internet atau tidak, baik dengan tujuan maupun tidak, untuk memperoleh, mengubah dengan cara menambah atau mengurangi, menghilangkan atau merusak informasi dalam sistem komputer dan atau sistem elektronik lainnya dengan melawan hukum. *Hacking* berbeda dengan kejahatan konvensional. *Hacking* bersifat *borderless*, transnasional dan *paperless* karena semua jejak hanya tersimpan dalam komputer dan jaringan berupa *log files*. Penyidikan tindak pidana *hacking* juga berbeda dengan penyidikan kejahatan konvensional yaitu sebagian proses penyidikan dilakukan di *cyberspace*, adanya masalah yurisdiksi hukum, eksistensi bukti digital dan penanganan komputer sebagai tempat kejadian perkara, dimana diperlukan dukungan laboratorium forensik komputer untuk menganalisa bukti digital yang telah didapat. Penyidik menerapkan prinsip-prinsip dan fungsi manajemen dalam proses penyidikan. Secara khusus disertasi ini memotret proses manajemen penyidikan *hacking* sehingga menghasilkan proses manajemen yang terdiri dari penerimaan laporan (*accepting input*), penugasan (*assigning*), perencanaan (*planning*), pelaksanaan dan penyesuaian (*executing and adjusting*), pengendalian dan evaluasi (*controlling and evaluation*), penyerahan hasil (*result delivery*), bantuan di persidangan (*court support*) serta dokumentasi hukum (*legal documentation*). Dengan manajemen penyidikan tindak pidana *hacking* tersebut, proses manajemen penyidikan terus berlanjut sampai ke tahap persidangan. Disamping itu, putusan hakim akan didokumentasikan oleh penyidik sehingga dapat digunakan sebagai pertimbangan dalam perencanaan penyidikan pada kasus *hacking* di kemudian hari. Proses manajemen penyidikan tersebut tidak berjalan secara independen melainkan terdapat faktor-faktor yang mempengaruhi proses tersebut seperti: budaya organisasi, kepemimpinan dan peranan *stakeholders*. Sub budaya organisasi Unit V *IT & Cybercrime* saat ini adalah mendorong anggotanya untuk terus maju (*progresif*) hal ini didukung dengan penghargaan dari pemimpin dan *peer pressure* dari anggota unit lainnya sebagai motivasi ekstrinsik. Peranan Kepala Unit sebagai pemimpin menjadi motivator Unit V *IT & Cybercrime* tampak dominan terlihat dari ketergantungan Unit V *IT & Cybercrime* terhadap pemimpinnya dalam hubungannya dengan *stakeholders* dan dalam melakukan transformasi budaya.

Jakarta, 7 Juni 2008

Petrus Reinhard Golose

RINGKASAN DISERTASI

MANAJEMEN PENYIDIKAN TINDAK PIDANA *HACKING*
(*Studi Kasus: Penyidikan Tindak Pidana Hacking Website Partai Golkar Oleh Unit V IT & Cybercrime Bareskrim Polri*)

LATAR BELAKANG

Salah satu kejahatan yang berkaitan dengan penggunaan sistem jaringan komputer dan teknologi informasi adalah *hacking*. *Hacking* dilakukan dengan memanfaatkan teknologi internet yang menghubungkan komputer satu dengan yang lainnya sehingga membentuk jaringan komputer. Tidak semua orang dapat melakukan *hacking*. Pelaku *hacking* atau disebut *hacker*, biasanya mempunyai pengetahuan dan keahlian khusus di bidang komputer dan internet, seperti penguasaan atas ilmu komputer, *programming*, dan pemanfaatan media internet. Disamping itu, pelaku juga harus mempunyai akses internet.

Dengan menggunakan teknologi komputer dan komunikasi, dalam hal ini jaringan komputer melalui media internet, *hacking* dapat dilakukan dari berbagai tempat yang terpisah dengan korbannya. Bahkan, korban dan pelaku *hacking (hacker)* dapat berada di negara yang berbeda. Sehingga *hacking* seringkali bersifat *borderless* (tanpa batas wilayah) bahkan transnasional (lintas batas negara). Di samping itu, perbuatan *hacking* tidak meninggalkan jejak berupa catatan atau dokumen fisik dalam bentuk kertas (*paperless*), akan tetapi semua jejak hanya tersimpan dalam komputer dan jaringannya tersebut dalam bentuk data atau informasi digital (*log files)*. Karakteristik-karakteristik tersebutlah yang membedakan *hacking* dengan jenis kejahatan lainnya yang bersifat konvensional.

Hacking merupakan salah satu jenis kejahatan yang merupakan dampak dari kemajuan teknologi informasi. Di Indonesia, menurut data dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), pada tahun 2003 telah terdapat 2.267 kasus *network incident,* sedangkan tahun 2004 terdapat 1.103 kasus serupa. Akan tetapi, ternyata tidak banyak kasus *hacking* yang benar-benar telah ditindak oleh penegak hukum dan yang pelakunya telah dikenai hukuman. Sampai saat ini tercatat hanya dua kasus *hacking* di Indonesia yang berhasil diungkap dan diproses ke pengadilan, yaitu kasus *hacking website* Komisi Pemilihan Umum Nasional pada tahun 2004 dan kasus *hacking website* Partai Golkar pada tahun 2006. Kedua kasus *hacking* yang terjadi di Indonesia tersebut telah menarik perhatian publik karena secara entah kebetulan atau tidak keduanya dilakukan terhadap dua *website* yang bernuansa politik kental dan istilah *hacking* sendiri relatif baru di telinga publik karena terminologinya belum dikenali dan dipahami secara baik oleh masyarakat umum.

Keberhasilan pengungkapan kedua kasus tersebut, merupakan hasil kerja keras penyidik Polri yang bernaung dalam suatu unit yang khusus menangani kasus *cybercrime*. Yang pertama, kasus *hacking website* Komisi Pemilihan Umum dengan tersangka *hacker* bernama Dani Firmansyah berhasil diungkap dan disidik oleh Satuan *Cybercrime* Polda Metro Jaya. Yang kedua, kasus *hacking website* Partai Golkar yang ditangani oleh Unit V *IT & Cybercrime*.

Pengungkapan kasus *hacking* merupakan perwujudan pelaksanaan tugas dan fungsi Polri sebagai aparat penegak hukum, diantaranya dilaksanakan oleh Unit V *IT & Cybercrime* sebagai suatu unit khusus di bawah Direktorat II Ekonomi dan Khusus Bareskrim Polri yang didirikan dengan tugas khusus dalam rangka mengantisipasi adanya dampak dari kemajuan teknologi informasi.

Polri merupakan salah satu fungsi pemerintahan negara di bidang pemeliharaan keamanan dan ketertiban masyarakat, penegakan hukum, perlindungan, pengayoman, dan pelayanan kepada masyarakat (Pasal 2 Undang-undang No.2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia, LN No. 2, TLN No. 4168 "**UU Kepolisian**"). Berkaitan dengan penegakan hukum, maka seorang polisi harus mengetahui hukum sebelum dia dapat menegakkan hukum secara adil dan cerdik (Sullivan, 1992: 113). Saat ini, masalah yang dihadapi oleh polisi Indonesia khususnya Unit V *IT & Cybercrime* adalah kondisi kejahatan yang harus diberantas berkembang sangat pesat sejalan dengan perkembangan teknologi informasi yang semakin canggih, sementara ketentuan hukum normatif yang harus ditegakkan belum tersedia pada saat itu. Sehingga dalam pelaksanaan tugas dan fungsinya, polisi dihadapkan pada berbagai permasalahan yang harus dicarikan solusinya agar tujuan organisasinya tetap dapat tercapai.

Upaya pemecahan masalah tersebut, dalam disertasi ini dipandang sebagai proses yang dilakukan dalam suatu sistem manajemen penyidikan yang dilaksanakan oleh Unit V *IT & Cybercrime* sejalan dengan upaya pencapaian tujuan organisasinya. Dalam pelaksanaan tugasnya, Unit V *IT & Cybercrime* ini dipimpin oleh seorang Komisaris Besar Polisi (Kombes Pol.) dengan didukung oleh 25 personil yang terdiri dari para penyidik maupun staf pendukung. Di samping ketersediaan sumber daya manusia tersebut, sumber daya lain yang tersedia adalah sumber daya *logistic/material* berupa infrastruktur teknologi dan laboratorium forensik komputer serta kerjasama dengan pihak luar.

Berkaitan dengan pelaksanaan tugas dan fungsi penyidikan yang diembannya selaku penegak hukum di bidang teknologi informasi, Unit V *IT & Cybercrime* melaksanakan fungsi penyidikan. Dalam melaksanakan penyidikan *hacking*, para penyidik dalam Unit V *IT & Cybercrime* dihadapkan pada hambatan-hambatan yang berkaitan dengan karakteristik dari perbuatan *hacking* yang telah diuraikan sebelumnya di atas seperti dalam proses penerapan hukum terhadap kejahatan *hacking* dan dalam proses penyidikannya.

Menghadapi hambatan-hambatan tersebut, Unit V *IT & Cybercrime* dituntut untuk mampu mendayagunakan seluruh kemampuan sumber daya yang dimilikinya dengan menggerakkan sistem manajemen penyidikannya, agar tujuan organisasi yang telah ditetapkan dapat tercapai. Selain itu, tipe dari organisasi juga akan berpengaruh terhadap manajemen penyidikan terutama dalam hal pembagian tugas dan distribusi kewenangan dan pertanggungjawaban penyidik dalam melaksanakan tugasnya (Ward, 2005: 68,70).

Berkaitan dengan hal tersebut di atas, dalam disertasi ini, menarik untuk dibahas mengenai penerapan prinsip dan pendayagunaan fungsi manajemen dalam proses penyidikan oleh Unit V *IT & Cybercrime*. Hal ini berkaitan dengan tuntutan terciptanya teknik penyidikan *hacking* sebagai suatu *cybercrime* yang mempunyai sifat dan karakteristik yang khas, sehingga penanganan dalam penyidikannya pun melahirkan karakteristik yang khas, khususnya karena melibatkan penyidik yang harus mempunyai kemampuan/keahlian teknologi informasi yang baik; memerlukan

Laporan lengkap tersedia
di Perpustakaan BNN