Manajemen penyelidikan tindak pidana hacking (Studi kasus: penyelidikan tindak pidana hacking website partai Golkar oleh unit V IT & Cybercrime Bareskrim Polri)

Golose, Petrus Reinhard, author

Abstrak

Disertasi ini merupakan hasil analisis dari penelilian 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. Kasus hacking website Partai Golkar merupakan kasus hacking pertama yang telah berkekuatan hukum tetap yang ditangani oleh Unit V IT & Cybercrime. Dalam pelaksanaan penyidikan hacking, Unit V IT & Cybercrime menghadapi permasalahan berkaitan dcngan belum adanya ketentuan hukum materil yang secara tegas mengatur mengenai tindak pidana hacking pada saat itu dan belum adanya ketentuan hukum formil yang mengatur secara khusus mengenai penanganan bukti digital. Permasalahan tersebut berhasil dihadapi penyidik dengan melakukan interpretasi terhedap ketentuan hukum yang ada.

Disertasi ini mengajukan suatu pengertian tindak pidana hacking sebagai setiap kegiatan yang menggunakan komputer atau sistem elektronik lainnya yang dilalcukan dengan cara mengakses suatu sistem jaringan komputer baik yang terhubung dengan internet atau tidak, baik dengan tujuan maupun tidak, untuk memperoleh, mengubah dengan cara menamhah atau mengurangi, menghilangkan atau merusak informasi dalam sistem komputer dan atau sistem elektronik lainnya dengan melawan hukum. Hacking berbeda dengan kejahatan konvensional.

Hacking dapat dilakukan dari berbagai tempat yang terpisah atau tidak mengenal batas wilayah (borderless) dan transnasional (lintas batas ncgara). Hacking tidak meninggalkan jejak berupa catatan atau dokumen fisik dalam bentuk kertas (paperless) akan tetapi semua jejak hanya tersimpan dalam komputer dan jaringan tersebut dalam bentuk data atau informasi digital 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 digtal (digital evidence) dun penanganan komputer sebagai tempat kejadian perkara (crime scene) dimana diperlukan dukungan laboratorium komputer forensik untuk menganalisa bukti digital yang telah didapat. Penyidik menerapkan prinsip-prinsip dan fungsi manajemen dalam proses penyidikan. Proses manajemen tersebut diterapkan sebagai suatu siklus yang terdiri dari perencanaan, pengorganisasian, implementasi, serta pengawasan dan evaluasi. Secara khusus disertasi ini memotret proses manajemen penyidikan hacking sehingga menghasilkan prooses 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 tidak berhenti

pada penyerahan berkas perkara ke penuntut umum saja, tetapi terus berlanjut ke tahap pemidangan, dimana penyidik berperan sebagai saksi verbalisan dan membantu penuntut turun dalam menghadirkan saksi dan ahli. Disamping itu terdapat pula dokumentasi hukum, dimana putusan hakim akan didokumentasikan oleh penyidik sehingga dapat digunakan sebagai penimbangan dalam perencanaan penyidikan pada kasus hacking yang terjadi 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. Berdasarkan hasil diskusi kelompok dan wawancara berpedoman diketahui bahwa Unit V IT & Cybercrime mempunyai budaya organisasi yang berbeda. Sub budaya organisasi yang ada saat ini di Unit V IT & Cybercrime 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.