

Fenomena Hactivism dan Permasalahannya

Prof. Richardus Eko Indrajit

Fenomena dan Profil Hacker di Tanah Air

Belakangan ini kehadiran dan aksi hacker mulai marak terjadi di dunia maya. Kontroversi mengenai definisi dan perilaku hacker telah pula menjadi sebuah wacana menarik bagi masyarakat moderen dalam era internet dewasa ini. Kehadiran buku-buku mengenai hacker dan berbagai kiat pekerjaannya telah pula mulai mewarnai ranah publik di Indonesia – terbukti dengan sangat lakunya publikasi tersebut dijual secara luas di pasar. Bahkan tidak tanggung-tanggung para praktisi teknologi informasi dan komunikasi dari negara tetangga seperti Malaysia, Brunei, dan Singapura tidak jarang berkunjung ke Indonesia untuk mendapatkan buku-buku tersebut. Hal ini disebabkan tidak semata-mata karena buku-buku tersebut dijual dengan harga relatif murah, namun juga karena telah begitu banyaknya koleksi referensi yang diperdagangkan secara bebas di toko-toko buku terkemuka dengan kualitas konten yang dianggap baik. Tidaklah heran jika dalam hitungan hari, jumlah hacker amatir maupun profesional di Indonesia bertambah secara cukup signifikan. Tidak saja dipandang dari segi kuantitas semata, namun ditinjau dari segi kualitas, mereka cukup baik menguasai berbagai ilmu “hacking” dan relatif aktif “berkarya” di dunia maya. Berikut adalah sekelumit seluk beluk kehidupan mereka.

Hacktivism sebagai Sebuah Gerakan Komunitas

Istilah “hacktivism” mengacu pada sebuah inisiatif dan kegiatan yang berfokus pada tindakan melakukan “hacking” karena atau untuk alasan tertentu. Alasan yang dimaksud dapat beraneka ragam.

1. Thrill Seekers
2. Organized Crime
3. Terrorist Groups
4. Nation-States



Gambar: Alasan Hacker Beraksi

Dalam sejumlah referensi yang ada, paling tidak ada 4 (empat) alasan mengapa para hacker melakukan aksi “hacktivism”-nya. Pertama, adalah untuk mencari “sensasi diri”. Perlu diperhatikan, generasi yang lahir setelah tahun 85-an telah terbiasa dengan keberadaan komputer di lingkungannya, berbeda dengan mereka yang lahir di masa-masa sebelumnya. Jika generasi lama merasakan sebuah “sensasi diri” yang menyenangkan dengan cara bermain catur, mengisi teka teki silang, bermain kartu “truft”, menyelesaikan misteri cerita detektif, dan lain sebagainya – maka generasi baru mendapatkan “sensasi diri” yang sama dengan cara “utak-atik” atau “ngoprek” komputer, bermain *game*, dan tentu saja melakukan kegiatan “hacking”. Jika pada jaman dahulu pemain catur merasa tertantang jika harus “membunuh” raja dengan dua kuda, maka saat ini hacker merasa tertantang jika dapat masuk ke sebuah sistem tertentu yang dianggap sulit untuk dipenetrasi. Senang atau tidak senang, suka atau tidak suka,

tindakan melakukan “hacking” tersebut telah berhasil menstimulus hormon-hormon dalam tubuh manusia masa kini yang memberikan sebuah sensasi tersendiri secara alami. Kedua, adalah untuk melakukan kejahatan. Bukan rahasia umum bahwa di negara-negara maju misalnya, telah banyak “berkeliaran” para hacker profesional yang tugasnya adalah melakukan kejahatan terorganisasi. Kejahatan yang dimaksud sifatnya beraneka ragam, mulai dari tindakan kriminal berlatar belakang ekonomi dan keuangan (seperti: perampokan bank, penipuan transaksi, pencucian uang, pencurian surat berharga, dan lain sebagainya), hingga yang bersifat kejahatan sosial (seperti: pencemaran nama baik, perusakan citra individu, pembunuhan karakter, pembohongan publik, dan lain sebagainya). Mereka ini biasanya dibayar mahal oleh pihak-pihak yang tidak bertanggung jawab untuk melakukan tindakan kejahatan tersebut. Ketiga, adalah untuk menjalankan aktivitas terorisme. Di jaman moderen ini para teroris melihat bahwa internet dan dunia maya merupakan lahan dan media yang cukup efektif untuk melakukan aktivitas teror dimana-mana. Sasaran “terrorist hacker” biasanya adalah *critical infrastructure* alias obyek-obyek vital sebuah negara seperti: perusahaan listrik, instalasi militer, pusat transportasi publik, sentra-sentra keamanan negara, jaringan keuangan perbankan, dan lain sebagainya. Karena kebanyakan organisasi-organisasi ini telah melibatkan teknologi informasi dan internet sebagai bagian tak terpisahkan dari aktivitas operasionalnya, maka penyerangan terhadap sistem jaringan dan komputer yang dimiliki akan mendatangkan dampak teror yang luar biasa. Dengan melakukan penyerangan terhadap obyek-obyek vital ini, maka pesan dibalik aksi terorisme yang dilakukan diharapkan dapat sampai ke pihak-pihak pemangku kepentingan yang menjadi sasaran. Keempat, adalah untuk alasan intelijen. Seperti diketahui bersama, setiap negara pasti memiliki jaringan intelijen di dalam dan di luar negeri untuk keperluan pertahanan dan keamanan nasional. Karena saat ini seluruh percakapan, interaksi, komunikasi, diskusi, kooperasi, transaksi, dan negosiasi dilakukan dengan memanfaatkan teknologi informasi dan internet, maka kegiatan intelijen-pun mulai masuk ke ranah ini. Dalam konteks inilah maka dibutuhkan sejumlah hacker profesional yang dapat membantu melakukan kegiatan intelijen demi keutuhan negara ini. Lihatlah bagaimana Amerika dengan lembaga NSA (National Security Agency) merekrut dan mendidik sedemikian banyak hacker dengan intelegensia dan keahlian tinggi untuk membantu mereka melaksanakan tugas kenegaraannya.

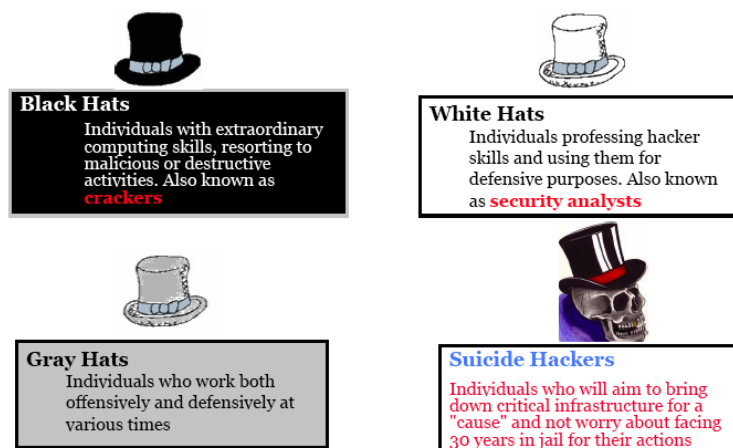
Beragam Tipe Hacker

Dengan berlatarbelakang penjelasan sebelumnya, dan dilihat dari sisi atau motivasi seorang hacker melakukan aktivitas yang menjadi bidang keahliannya, dunia internet kerap mengkategorikan hacker menjadi empat tipe, masing-masing adalah sebagai berikut:

1. Black Hats – merupakan kumpulan dari individu dengan keahlian tinggi di bidang keamanan komputeryang memiliki motivasi untuk melakukan tindakan-tindakan destruktif terhadap sistem komputer tertentu yang menjadi sasarannya demi mendapatkan sejumlah “imbalan” tertentu (dalam dunia kejahatan internet hacker ini dikenal sebagai *crackers*);
2. White Hats – merupakan kumpulan dari profesional yang memiliki keahlian di bidang internet yang bertugas untuk menjaga keamanan sebuah sistem komputer agar terhindar dari tindakan yang merugikan dari pihak-pihak yang

menyerangnya (dalam dunia internet hacker ini dikenal sebagai *security analysts*);

3. Gray Hats - merupakan kumpulan dari orang-orang yang terkadang melakukan kegiatan yang bersifat *offensive* namun di lain waktu melakukan kegiatan yang bersifat *deffensive* terkait dengan keamanan sebuah jaringan komputer; dan
4. Suicide Hackers - merupakan kumpulan dari mereka yang dengan sengaja memiliki visi utama menyerang obyek-obyek vital kenegaraan untuk tujuan tertentu dan tidak khawatir terhadap ancaman perdata maupun pidana yang mengincarnya.



Dengan berkaca pada berbagai seluk beluk hacker ini, dapat diambil kesimpulan bahwa sebenarnya istilah "hacker" di mata praktisi teknologi informasi dan internet tersebut sebenarnya bersifat netral. Namun kesalahpahaman definisi yang menjadi persepsi masyarakat menempatkan istilah "hacker" pada suatu pengertian yang bernuansa negatif, sehingga sering kali kegiatan "hacktivism" dianggap sebagai tindakan kriminal yang senantiasa melawan hukum. Melalui sosialisasi yang tepat dan strategi yang baik, keberadaan para individu hacker yang berkembang di masyarakat dapat dijadikan sebagai sebuah kesempatan untuk meningkatkan kinerja keamanan beraneka ragam sistem komputer yang dimiliki oleh masyarakat Indonesia agar tidak terhindar dari serangan dan penetrasi pihak luar yang dapat merugikan bangsa dan negara.



Richardus Eko Indrajit, guru besar ilmu komputer ABFI Institute Perbanas, dilahirkan di Jakarta pada tanggal 24 Januari 1969. Menyelesaikan studi program Sarjana Teknik Komputer dari Institut Teknologi Sepuluh Nopember (ITS) Surabaya dengan predikat Cum Laude, sebelum akhirnya menerima bea siswa dari Konsorsium Production Sharing Pertamina untuk melanjutkan studi di Amerika Serikat, dimana yang bersangkutan berhasil mendapatkan gelar Master of Science di bidang Applied Computer Science dari Harvard University (Massachusetts, USA) dengan fokus studi di bidang artificial intelligence. Adapun gelar Doctor of Business Administration diperolehnya dari University of the City of Manila (Intramuros, Phillipines) dengan disertasi di bidang Manajemen Sistem Informasi Rumah Sakit. Gelar akademis lain yang berhasil diraihinya adalah Master of Business Administration dari Leicester University (Leicester City, UK), Master of Arts dari the London School of Public Relations (Jakarta, Indonesia) dan Master of Philosophy dari Maastricht School of Management (Maastricht, the Netherlands). Selain itu, aktif pula berpartisipasi dalam berbagai program akademis maupun sertifikasi di sejumlah perguruan tinggi terkemuka dunia, seperti: Massachusetts Institute of Technology (MIT), Stanford University, Boston University, George Washington University, Carnegie-Mellon University, Curtin University of Technology, Monash University, Edith-Cowan University, dan Cambridge University. Saat ini menjabat sebagai Ketua Umum Asosiasi Perguruan Tinggi Informatika dan Komputer (APTIKOM) se-Indonesia dan Chairman dari International Association of Software Architect (IASA) untuk Indonesian Chapter. Selain di bidang akademik, karir profesionalnya sebagai konsultan sistem dan teknologi informasi diawali dari Price Waterhouse Indonesia, yang diikuti dengan berperan aktif sebagai konsultan senior maupun manajemen pada sejumlah perusahaan terkemuka di tanah air, antara lain: Renaissance Indonesia, Prosys Bangun Nusantara, Plasmedia, the Prime Consulting, the Jakarta Consulting Group, Soedarpo Informatika Group, dan IndoConsult Utama. Selama kurang lebih 15 tahun berkiprah di sektor swasta, terlibat langsung dalam berbagai proyek di beragam industri, seperti: bank dan keuangan, kesehatan, manufaktur, retail dan distribusi, transportasi, media, infrastruktur, pendidikan, telekomunikasi, pariwisata, dan jasa-jasa lainnya. Sementara itu, aktif pula membantu pemerintah dalam sejumlah penugasan. Dimulai dari penunjukan sebagai Widya Iswara Lembaga Ketahanan Nasional (Lemhannas), yang diikuti dengan beeperan sebagai Staf Khusus Bidang Teknologi Informasi Sekretaris Jendral Badan Pemeriksa Keuangan (BPK), Staf Khusus Balitbang Departemen Komunikasi dan Informatika, Staf Khusus Bidang Teknologi Informasi Badan Narkotika Nasional, dan Konsultan Ahli Direktorat Teknologi Informasi dan Unit Khusus Manajemen Informasi Bank Indonesia. Saat ini ditunjuk oleh pemerintah Republik Indonesia untuk menakhodai institusi pengawas internet Indonesia ID-SIRTII (Indonesia Security Incident Response Team on Internet Infrastructure). Seluruh pengalaman yang diperolehnya selama aktif mengajar sebagai akademisi, terlibat di dunia swasta, dan menjalani tugas pemerintahan dituliskan dalam sejumlah publikasi. Hingga menjelang akhir tahun 2008, telah lebih dari 25 buku hasil karyanya yang telah diterbitkan secara nasional dan menjadi referensi berbagai institusi pendidikan, sektor swasta, dan badan pemerintahan di Indonesia – diluar beragam artikel dan jurnal ilmiah yang telah ditulis untuk komunitas nasional, regional, dan internasional. Seluruh karyanya ini dapat dengan mudah diperoleh melalui situs pribadi <http://www.eko-indrajit.com> atau <http://www.eko-indrajit.info>. Seharian-hari dapat dihubungi melalui nomor telepon 0818-925-926 atau email indrajit@post.harvard.edu.