**Kasus Cybercrime di Indonesia**

**#1 Kasus tentang Asusila dalam media elektronik**

Aktor Taura Denang Sudiro alias Tora Sudiro dan Darius Sinathrya, mendatangi Sentra Pelayanan Kepolisian Polda Metro Jaya untuk membuat laporan penyebaran dan pendistribusian gambar atau foto hasil rekayasa yang melanggar kesusilaan di media elektronik.

"Saya membuat laporan, sesuai apa yang saya lihat di media twitter. Sebenarnya, saya sudah melihat gambar itu bertahun-tahun lalu. Awalnya biasa saja, namun sekarang anak saya sudah gede, nenek saya juga marahmarah. Padahal sudah dijelaskan kalau itu adalah editan," ujar Tora, di depan Gedung Direktorat Reserse Kriminal Khusus, Polda Metro Jaya, Rabu (15/5).

Ia melanjutkan, pihaknya memutuskan untuk membuat laporan dengan nomor TBL/1608//V/2013/PMJ/Dit Krimsus, tertanggal 15 Mei 2013, karena penyebaran foto asusila itu kian ramai dan mengganggu privasinya. "Saya merasa dirugikan. Sekarang juga kembali ramai (penyebarannya), Darius juga terganggu. Akhirnya kami memutuskan untuk membuat laporan. Pelakunya belum tahu siapa, namun kami sudah meminta polisi untuk menelusurinya," ungkapnya.

Dalam kesempatan yang sama, Darius, menyampaikan dirinya juga sudah mengetahui beredarnya foto rekayasa adegan syur sesama jenis itu, sejak beberapa tahun lalu.

"Sudah tahu gambar itu, beberapa tahun lalu. Awalnya saya cuek, mungkin kerjaan orang iseng saja. Namun, sekarang banyak teman-teman di daerah menerima gambar itu via broadcast BBM. Bahkan, anak kecil saja bisa melihat. Ini yang sangat mengganggu saya," jelasnya.

Darius yang merupakan saksi dan korban dalam laporan itu menambahkan, banyak teman-teman daerah memintanya untuk mengklarifikasi apakah benar atau tidak foto itu. "Ya, jelas foto ini palsu. Makanya kami laporkan," katanya.

Sementara itu, Kasubdit Cyber Crime Ditreskrimsus Polda Metro Jaya, AKBP Audie Latuheru, menuturkan berdasarkan penyeledikan sementara, disimpulkan jika foto itu merupakan rekayasa atau editan.

"Kami baru melakukan penyelidikan awal dan menyimpulkan ini foto editan, bukan foto asli. Hanya kepala mereka (Tora, Darius dan Mike) dipasang ke dalam gambar asli, kemudian ditambahkan pemasangan poster Film Naga Bonar untuk menguatkan karakter itu benar-benar Tora. Selain itu tak ada yang diganti. Editor tidak terlalu bekerja keras (mengubah), karena hampir mirip gambar asli," paparnya.

Langkah selanjutnya, kata Audie, pihaknya bakal segera melakukan penelusuran terkait siapa yang memposting gambar itu pertama kali.

"Kami akan mencoba menelusuri siapa yang mengedit dan memposting gambar itu pertama kali. Ini diedit kira-kira 3 tahun lalu, tahun 2010. Kesulitan melacak memang ada, karena terkendala waktu yang sudah cukup lama. Jika pelaku tertangkap, ia bakal dijerat Pasal 27 Ayat (1) Jo Pasal 45 Ayat (1) UU RI 2008, tentang Informasi dan Transaksi Elektronik," tegasnya.

Diketahui, sebuah foto rekayasa adegan syur sesama jenis yang menampilkan wajah Tora Sudiro, Darius Sinathrya dan Mike (mantan VJ MTV), beredar di dunia maya. Nampak adegan oral seks di dalam foto itu.

**#2 Kasus tentang Cybersquatting**

Cybersquatting adalah mendaftar, menjual atau menggunakan nama domain dengan maksud mengambil keuntungan dari merek dagang atau nama orang lain. Umumnya mengacu pada praktek membeli nama domain yang menggunakan nama-nama bisnis yang sudah ada atau nama orang orang terkenal dengan maksud untuk menjual nama untuk keuntungan bagi bisnis mereka . Contoh kasus cybersquatting, Carlos Slim, orang terkaya di dunia itu pun kurang sigap dalam mengelola brandingnya di internet, sampai domainnya diserobot orang lain. Beruntung kasusnya bisa digolongkan cybersquat sehingga domain carlosslim.com bisa diambil alih. Modusnya memperdagangkan popularitas perusahaan dan keyword Carlos Slim dengan cara menjual iklan Google kepada para pesaingnya. Penyelesaian kasus ini adalah dengan menggunakan prosedur Anticybersquatting Consumer Protection Act (ACPA), memberi hak untuk pemilik merek dagang untuk menuntut sebuah cybersquatter di pengadilan federal dan mentransfer nama domain kembali ke pemilik merek dagang. Dalam beberapa kasus, cybersquatter harus membayar ganti rugi uang.

Untuk kasus-kasus cybersquatting dengan menggunakan pasal-pasal dalam Kitab Undang-undang Pidana Umum, seperti misalnya pasal 382 bis KUHP tentang Persaingan Curang, pasal 493 KUHP tentang Pelanggaran Keamanan Umum Bagi Orang atau Barang dan Kesehatan Umum, pasal 362 KUHP tentang Pencurian, dan pasal 378 KUHP tentang Penipuan; dan

Pasal 22 dan 60 Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi untuk tindakan domain hijacking.

**#3 Kasus tentang Carding**

Carding, salah satu jenis cyber crime yang terjadi di Bandung sekitar Tahun 2003. Carding merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet. Para pelaku yang kebanyakan remaja tanggung dan mahasiswa ini, digerebek aparat kepolisian setelah beberapa kali berhasil melakukan transaksi di internet menggunakan kartu kredit orang lain. Para pelaku, rata-rata beroperasi dari warnet-warnet yang tersebar di kota Bandung. Mereka biasa bertransaksi dengan menggunakan nomor kartu kredit yang mereka peroleh dari beberapa situs. Namun lagi-lagi, para petugas kepolisian ini menolak menyebutkan situs yang dipergunakan dengan alasan masih dalam penyelidikan lebih lanjut.

Modus kejahatan ini adalah pencurian, karena pelaku memakai kartu kredit orang lain untuk mencari barang yang mereka inginkan di situs lelang barang. Karena kejahatan yang mereka lakukan, mereka akan dibidik dengan pelanggaran Pasal 378 KUHP tentang penipuan, Pasal 363 tentang Pencurian dan Pasal 263 tentang Pemalsuan Identitas.

Bunyi dari pasal 378 KUHP yang memuat tentang tindakan penipuan adalah sebagai berikut : Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, memakai nama/ keadaan palsu dengan tipu muslihat agar memberikan barang membuat utang atau menghapus utang diancam karena penipuan dengan pidana penjara maksimum 4 tahun.

Pasal 263 KUHP tentang pemalsuan surat yang berbunyi bahwa: barang siapa membuat secara palsu atau memalsukan sesuatu yang dapat menimbulkan suatu hak, perikatan atau suatu pembebasan utang atau yang diperuntukkan sebagai bukti suatu bagi suatu tindakan, dengan maksud untuk menggunakan atau menyuruh orang lain menggunakannnya seolaholah asli dan tidak palsu, jika karena penggunaan itu dapat menimbulkan suatu kerugian, diancam karena pemalsuan surat dengan pidana penjara maksimum enam tahun; diancam dengan pidana yang sama barang siapa dengan sengaja dengan sengaja menggunakan surat yang isinya secara palsu dibuat atau yang dipalsukan tersebut, seolah-olah asli dan tidak palsu jika karena itu menimbulkan kerugian.

**#4 Kasus tentang 1763 kejahatan Cyber yang sudah di tangani oleh polisi**

Cyber crime atau kejahatan siber dalam istilah hukumnya adalah mengacu pada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran, atau tempat terjadinya kejahatan. Kejahatan yang dimaksud di antaranya penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit atau carding, confidence fraud (penipuan kepercayaan), penipuan identitas, dan pornografi anak.

Kejahatan siber pun kini semakin 'bertumbuh subur'. Berdasarkan data yang diperoleh **Okezone**dari Direktorat Tindak Pidana Kejahatan Siber (Dit Tipidsiber) Bareskrim Polri sepanjang 2017, yakni Januari-Oktober, jajaran Polri di Indonesia menangani 1.763 kasus kejahatan siber.

Dari angka tersebut, polri setidaknya sudah menyelesaikan perkara (crime clearance) cyber crime sebanyak 835 kasus. Penyelesaian kasus itu dikategorikan dari berkas perkara dinyatakan lengkap (P21) atau surat permohonan penghentian proses penyidikan (SP3). Dalam data tersebut, kejahatan siber yang paling tinggi adalah penipuan.

Dalam pemaparan data itu, sepanjang 2017 Polda Aceh menangani tiga kasus kejahatan siber, satu kasus dengan konten pornografi dan dua perkara di kasus penghinaan dan pencemaran nama baik.

Polda Sumatera Utara (Sumut) menangani 95 kejahatan cyber crime, dengan rincian satu konten pornografi, satu perjudian online, 53 kasus penghinaan dan pencemaran nama baik sebanyak, 30 kasus penipuan, dua menyebar rasa permusuhan, enam kasus pengancaman, tiga kasus illegal access. Dari keseluruhan, sebanyak 45 kasus telah diselesaikan.

Polda Sumatera Barat (Sumbar) menangani perkara enam konten pornografi, satu perjudian online, 30 kasus penghinaan dan pencemaran nama baik kasus, 65 kasus penipuan, dua kasus penyebaran rasa permusuhan, tiga kasus pengancaman, illegal accesempat kasus, sehingga pada tahun 2017 total kasus yang ditangani 125 dengan penyelesaian 15 kasus.

Polda Sumatera Selatan (Sumsel) menangani dua kasus konten pornografi, tujuh kasus pencemaran dan penghinaan nama baik, 11 kasus penipuan, satu kasus defacing atau meng-hack website badan atau perorangan. Jika ditotal Polda Sumsel menangani 21 kasus kejahatan siber dan telah menyelesaikan 2 kasus.

Lalu, Polda Kepulauan Riau (Kepri) sepanjang 2017 menangani sebanyak 40 kasus, rinciannya empat konten pornografi, 16 kasus penghinaan dan pencemaran nama baik, 17 kasus penipuan, dan tiga kasus pencurian identitas.

Selanjutnya, Polda Lampung menangani dua konten pornografi, 11 kasus pencemaran dan penghinaan nama baik, empat kasus penipuan, satu kasus menyebarkan rasa permusuhan, enam kasus pengancaman, dua kasus distributed denial of service (DDOS) atau penolakan layanan secara terdistribusi dan satu pencurian identitas. Total, Polda Lampung menangani 28 kasus dengan tiga perkara di antaranya telah diselesaikan.

**#5 Kasus 92 WNA melakukan kejahatan Cyber dan meraup uang Rp.5,9 T**

Kepala Tim Tindak Surabaya Satgas Khusus Bareskrim Polri AKBP Susatyo Purnomo mengungkapkan, tersangka kasus cyber crime yang mereka tangani menerima keuntungan triliunan rupiah.

Para tersangka sebanyak 92 orang asal Negara Taiwan dan China. Mereka sudah ditangkap polisi dan kini dibawa dari tempatnya beroperasi di Surabaya menuju Polda Metro Jaya di Jakarta. "Berdasarkan koordinasi kami dengan polisi China, bahwa satu tahun kerugian dari modus ini mencapai Rp 600 miliar di Surabaya untuk satu TKP (tempat kejadian oerkara) saja. Hasil sementara beberapa bulan mereka menipu mencapai Rp 5,9 triliun," kata Susatyo kepada Kompas.com, Minggu (30/7/2017) siang.

Susatyo menjelaskan, komplotan penipu ini sudah beroperasi sejak Januari 2017 silam. Korbannya adalah warga negara asing (WNA) yang berada di Indonesia, kebanyakan warga Negara China. Modus penipuan yang dilakukan adalah meyakinkan para korban bahwa mereka tersandung kasus kriminal. Bagian dari komplotan penipu ini ada yang berpura-pura sebagai polisi, jaksa, hingga hakim untuk menguatkan cerita bahwa korbannya benar terkena kasus. Kemudian, ada beberapa orang dalam komplotan itu yang kemudian berperan sebagai calo penyelesaian perkara, dengan meminta sejumlah uang dari korban.

Ketika ditanya lebih lanjut mengenai jumlah korban, Susatyo menyebut pihaknya masih mendalaminya karena komplotan penipu ini tergabung dalam sindikat cyber crime internasional. Mereka dibawa dari Surabaya menuju Jakarta melalui Bandara Soekarno-Hatta dengan pesawat carteran pada Minggu siang. Rencananya, mereka akan diantar ke Polda Metro Jaya untuk dikumpulkan bersama warga negara asing lain yang juga diamankan terkait kasus cyber crime dari Jakarta dan Bali.

KASUS CYBERCRIME DI LUAR NEGERI

**#1 KASUS SATU MILIAR AKUN YAHOO BOCOR**

Yahoo mengakui bahwa lebih dari satu miliar akun bisa jadi telah menjadi korban pembobolan. Apakah Anda harus panik sekarang? Apa yang harus dilakukan untuk melindungi akun pada masa depan? Langkah pertama, kata pakar keamanan internet Graham Cluley, adalah mengganti kata sandi atau password yang dipakai untuk mengakses layanan Yahoo. Disarankan pula untuk mengganti kata sandi e-mail-e-mail lain dan pastikan kata sandi itu berbeda-beda. Ini perlu ditekankan karena demi alasan praktis, banyak orang yang memakai kata sandi yang sama untuk beberapa e-mail yang berbeda. "Jawaban atas pertanyaan keamanan (security question) juga sebaiknya diganti," kata Cluley. Para pakar memahami bahwa pengguna punya banyak akun, dan manajemen kata sandi tak lagi gampang.

Itu sebabnya disarankan untuk memakai aplikasi khusus untuk mengatur kata sandi, seperti Password Chef, LastPass, dan 1password. Semakin banyak penyedia layanan yang sekarang menawarkan verifikasi dua tahap, misalnya dengan mengirim kode masuk ke ponsel melalui SMS. Jika layanan semacam ini tersedia, sebaiknya dimanfaatkan. Dengan demikian, orang lain tak bisa dengan mudah memasuki akun yang Anda punya, meski ia punya kata sandinya.

Berbicara soal keamanan, Alan Woodward, guru besar di Universitas Surrey, Inggris, mengatakan bahwa pengguna harus ekstra hati-hati dan tak begitu saja menulis informasi penting, seperti tanggal lahir dan alamat, kecuali memang sangat perlu. "Saya misalnya, punya dua versi tanggal lahir, yang sebenarnya dan yang selalu saya pakai untuk mengisi formulir online," kata Woodward. Ini penting karena biasanya tanggal lahir sering dipakai sebagai alat untuk melakukan verifikasi. "Apakah saya menulis alamat asli? Tentu saja tidak, kecuali untuk hal-hal yang terkait dengan urusan uang, misalnya untuk tagihan listrik, gas, dan air," katanya. Pada akhirnya, banyak penyedia layanan yang memungkinkan pengguna mengecek aktivitas, dengan memberikan informasi peranti dan lokasi tempat akun diakses. Jika fasilitas seperti ini ada, para pengguna sebaiknya menggunakannya.

**#2 SERANGAN MASIF DDOS LUMPUHKAN TWITTER**

umat pagi, pukul 07.10, waktu timur Amerika Serikat atau sekitar pukul 8 malam WIB, sejumlah layanan online terkenal mendadak terasa lambat saat diakses atau tumbang sama sekali. Sebuah serangan brutal bernama Distributed Denial of Service ( DDoS) rupanya tengah menimpa server Dyn. Dyn merupakan perusahaan jasa penyedia Domain Name Services ( DNS) yang banyak dipakai oleh nama-nama besar, seperti Spotify, dan Twitter.

DDoS merupakan serangan paket data dalam jumlah besar ke sebuah server. Masifnya jumlah paket data yang diterima dalam waktu bersamaan bisa mengakibatkan server melambat, bahkan tumbang. Pantauan KompasTekno, Sabtu (22/10/2016) dini hari, dua situs tersebut tidak bisa diakses saat dibuka via beberapa operator seluler dan ISP.

Sejumlah pengguna di Indonesia juga mengeluhkan masalah sama lewat media sosial. Jasa DNS menerjemahkan alamat URL (misalnya Kompas.com) menjadi alamat IP numerik yang diperlukan untuk mengantar pengakses ke situs atau layanan online tujuan. Apabila penyedia jasa DNS ini tumbang, maka situs-situs atau layanan online yang terkait dengannya akan ikut terimbas dan tidak bisa diakses. Sebagaimana dirangkum dari ArsTechnica, serangan terjadi dua kali. Serbuan DDoS berikutnya mulai muncul siang hari, beberapa jam setelah kali pertama.

“Pada Jumat 21 Oktober 2016 pukul 11.10 UTC, kami mulai memonitor dan menangani serangan DDoS terhadap infrastruktur Dyn. Beberapa pelanggan bisa mengalami peningkatan latency (jeda waktu akses) dan penundaan perpindahan zona,” sebut Dyn dalam sebuah pernyataan resmi. Disebutkan bahwa serangan tersebut utamanya berdampak pada para pengguna internet di kawasan timur Amerika Serikat dan sebagian wilayah Eropa.

Selain Twitter dan Spotify, situs dan layanan online lain yang ikut bermasalah karena serangan tersebut termasuk PayPal, Reddit, Yammer, GitHub, AirBnb, serta sejumlah situs berita seperti New York Times, Mashable, dan The Guardian. Sebagian besar situs dan layanan online yang terdampak kini sudah bisa diakses kembali. Pengguna yang masih bermasalah mengakses disarankan mengganti DNS ke alamat Open DNS (208.67.222.222 atau 208.67.220.220) atau DNS Google (8.8.8.8 atau 8.8.4.4). Belum diketahui siapa hacker atau kelompok peretas yang bertanggungjawab melancarkan serangan ini. DDoS  diketahui banyak dilakukan dengan memanfaatkan “pasukan” perangkat IoT -misalnya IP camera, router, atau perabot pintar dengan koneksi ke internet- yang dibajak dengan program jahat.

**#3 KASUS HACKER CURI PASSWORD AKUN MEDIA SOSIAL MILIK MARK ZUCKERBERG**

Akun media sosial CEO Facebook Mark Zuckerberg ternyata sempat dibajak sekelompok orang yang menyebut dirinya sebagai OurMine Team. Namun, pembajakan tersebut bukan terjadi pada akun Facebook miliknya, melainkan media sosial lain. Tepatnya, peretas berhasil masuk ke dalam akun Twitter dan Pinterest milik Zuckerberg.

Mereka juga meninggalkan jejak berupa satu kicauan dan sebuah screenshot. “Hey, @Finkd Anda ada dalam database LinkedIn dengan password ‘dadada’ ! DM untuk buktinya,” begitu bunyi kicauan tersebut, seperti dilansir KompasTekno dari Venture Beat, Senin (6/6/2016).

Sedangkan screenshot yang dimaksud berisi sebuah akun Pinterest @zuck, menampilkan foto profil Zuckberberg dan nama yang telah diubah. menjadi Hacked By OurMine Team. Satu lagi, kelompok peretas itu juga mengaku berhasil mendapatkan password akun Instagram Zuckerberg, meski kemudian diketahui bahwa mereka sama sekali tak mengakses akun tersebut. Hingga sekarang belum ditemukan kepastian soal cara OurMine Team melakukan tindak peretasan kedua akun milik bos Facebook itu.

Tapi peretas mengklaim bahwa mereka menemukan password akun media sosial Zukerberg dalam basis data LinkedIn. Tepatnya pada medio Mei lalu, memang sempat terjadi kebocoran basis data jejaring sosial LinkedIn. Lebih kurang ada 6,5 juta password pengguna yang bocor. Perusahaan pun langsung menyetel ulang password yang bocor itu dan memberi tahu penggunanya. Update: KompasTekno mendapat klarifikasi langsung dari pihak LinkedIn.

Menurut pihak tersebut, tidak ada kebocoran data yang terjadi pada Mei 2016 lalu. Kejadian sebenarnya adalah perilisan nama dan password oleh pihak yang tidak bertanggung jawab, yang didapatkan dari insiden di tahun 2012. Tapi kebocoran data tersebut tak selesai dengan reset password semata. Pasalnya ada banyak orang yang memakai satu password untuk berbagai media sosial lain miliknya, katakanlah itu LinkedIn, Twitter, dan sejenisnya. Bisa saja Zuckerberg merupakan salah satu orang tersebut.

Sementara itu, Twitter bertindak cepat. Akun @finkd milik Zuckerberg langsung di-suspend. Setelah akun tersebut bisa diakses lagi, kicauan yang menjadi bukti peretasan itu sudah dihapus. Pinterest sedikit terlambat. Mereka butuh waktu lebih lama, namun sekarang akun @zuck milik bos Facebook itu sudah berhasil dipulihkan. Dari kejadian yang menimpa Zuckberberg ini, setidaknya kita bisa mengambil pelajaran. Jangan memakai satu password yang sama untuk seluruh akun media sosial.

**#4 ALASAN APPLE MELINDUNGI IPHONE TERORIS DARI PERETASAN FBI**

Biro Penyelidikan Federal AS ( FBI) pusing tujuh keliling ketika berusaha membuka data iPhone yang diduga merupakan milik teroris pelaku penembakan di San Bernardino, Syed Rizwan Farook. Pasalnya, para penyelidik terganjal sistem pengamanan iPhone yang mampu menghapus data ponsel apabila percobaan menjebol perangkat itu gagal hingga 10 kali.

FBI pun menempuh upaya hukum untuk menekan Apple agar mau membuka kunci iPhone yang bersangkutan. Tetapi, permintaan yang disuarakan lewat pengadilan federal ini kemudian ditolak mentah-mentah. Mengapa Apple tak mau membantu penyelidikan pihak berwajib? Tim Cook selaku CEO pabrikan gadget itu menerangkan alasannya dalam sebuah surat terbuka di situs Apple.

“Pemerintah AS meminta kami melakukan sesuatu yang di luar kemampuan dan terlalu berbahaya untuk dibuat. Mereka meminta kami membuat backdoor (untuk mengakses data) ke iPhone,” tulis Cook. Dia melanjutkan, backdoor yang dimaksud berupa software sistem operasi iPhone versi khusus yang menghilangkan sejumlah fitur keamanan untuk kemudian dipasang di ponsel iPhone milik sang teroris. Dengan begini, software tersebut--yang saat ini belum ada--bisa digunakan untuk mengakses data yang tersimpan di dalam iPhone. “FBI mungkin menyebutnya dengan istilah berbeda. Harap jangan salah: versi iOS yang menyabot keamanan dengan cara begini sama saja dengan membikin backdoor,” katanya. “Master key” Backdoor yang diminta FBI memungkinkan passcode untuk dimasukkan secara elektronik sehingga iPhone lebih mudah dijebol dengan teknik “brute force”, yakni menebak angka kunci dengan memasukkan jutaan kombinasi per detik dengan bantuan komputer. Apple khawatir aplikasi semacam itu nantinya bisa digunakan untuk membuka iPhone lain di luar kepunyaan sang teroris, tak peduli siapa pemiliknya ataupun berapa banyaknya. Memang, pihak pemerintah AS dalam hal ini hanya ingin memakai backdoor yang bersangkutan sebanyak sekali. Namun, tak ada jaminan bahwa sang program berbahaya tak bakal jatuh ke lain pihak atau digunakan oleh pihak berwajib untuk keperluan lain.

“Ini ibaratnya membuat satu kunci utama (master key) yang bisa dipakai membuka ratusan juta kunci--dari pintu restoran, bank, toko-toko, hingga rumah-rumah,” terang Cook. Lebih jauh, Cook menerangkan bahwa FBI kini berupaya menggunakan ayat “All Writs Act” dari tahun 1789 di undang-undang federal untuk melebarkan otoritasnya sehingga mampu memaksa Apple memenuhi perintah pengadilan. Apabila berhasil, maka kasus ini nantinya akan berimplikasi luas pada masa yang akan datang. Pemerintah AS bakal memiliki kuasa untuk memata-matai ponsel siapa pun untuk mengambil data dan bisa memerintahkan Apple untuk menyadap informasi pengguna.

Menurut Cook, Apple telah bersikap kooperatif terhadap FBI, tetapi permintaan kali ini dianggap sudah kelewatan. “Kami percaya FBI berniat baik, tetapi pemerintah melakukan kesalahan dengan memaksa Apple membikin backdoor ke produknya sendiri,” ujar Cook. “Menentang perintah ini adalah sesuatu yang kami anggap serius. Kami harus angkat bicara mengenai hal yang kami pandang sebagai tindakan melampaui batas dari pemerintah.”

**#5 SERANGAN CYBER ANCAM AMERIKA SERIKAT**

Mantan direktur badan intelijen Amerika, CIA, Barry Royden mengungkapkan bahwa dirinya percaya terorisme cyber adalah ancaman besar yang mengintai negara adidaya tersebut.

Hal tersebut diungkapkannya karena melihat perkembangan teknologi yang kian maju, serta dunia yang semakin bisa terhubung hanya melalui internet.

"Kenyataan yang ada saat ini adalah semua terhubung, dan selama Anda terhubung Anda rentan. Meski ada firewall, tetapi perangkat tersebut berpotensi defeatable," jelas Barry Royden, seperti dikutip dari Business Insider, Rabu (20/5/2015).

Menurutnya, serangan terhadap sistem komputer suatu negara bisa menurunkan pergolakan ekonomi, jaringan listrik, rumah sakit, atau sistem perbankan. Semua sistem yang terhubung adalah rentan dimasuki penjahat cyber.

Barry Royden sendiri adalah intelijen CIA yang bekerja selama 40 tahun, berada pada posisi operasi 35 tahun dan menjadi kepala kontra intelijen selama 5 tahun. Namun, selama lebih dari satu dekade dirinya mengamati perkembangan teknologi dan ancaman tersebut.