BAB III

PERUSAKAN SITUS RESMI INSTANSI PEMERINTAH YANG DILAKUKAN MELALUI MEDIA INTERNET

A. Modus Perusakan Situs Resmi Suatu Instansi Pemerintah

Kebutuhan akan teknologi jaringan komputer semakin meningkat. Selain sebagai media penyedia informasi, melalui Internet pula kegiatan komunitas komersial menjadi bagian terbesar, dan terpesat pertumbuhannya serta menembus berbagai batas negara. Bahkan melalui jaringan ini kegiatan pasar di dunia dapat diketahui selama 24 jam. Melalui dunia *internet* atau disebut juga *cyberspace*, apapun dapat dilakukan. Segi positif dari dunia maya ini merupakan ciri perkembangan teknologi dunia dengan segala bentuk kreatifitas manusia, namun dampak negatif pun tidak dapat dihindari.

Cyberspace sebagai wahana komunikasi yang berbasis komputer (*computer mediated communication*), banyak menawarkan realitas baru dalam berinteraksi di dunia maya. Adanya interaksi antar pengguna *cyberspace* telah banyak terseret ke arah terjadinya penyelewengan hubungan sosial berupa kejahatan yang khas yang memiliki karakteristik berbeda dengan tindak pidana konvensional yang selama ini telah dikenal. Namun ada juga yang berpandangan bahwa kejahatan melalui internet (*cybercrime*) memiliki kesamaan bentuk dengan kejahatan yang ada di dunia nyata.[1]

[1] Tubagus Ronny Rahman Nitibaskara, *Ketika Kejahatan Berdaulat, Sebuah Pendekatan Kriminologi, Hukum dan Sosiologi,* Peradaban, Jakarta, 2001, hlm. 53

Seiring dengan perkembangan teknologi *internet*, menyebabkan munculnya kejahatan yang disebut dengan *cybercrime* atau kejahatan melalui jaringan *internet*. Munculnya beberapa kasus *cybercrime* di Indonesia, seperti pencurian kartu kredit, *hacking* beberapa *situs*, menyadap transmisi data orang lain, misalnya *e-mail*, dan memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki kedalam *programmer* komputer, sehingga dalam kejahatan komputer dimungkinkan adanya delik formil dan delik materil. Delik formil adalah perbuatan seseorang yang memasuki komputer orang lain tanpa ijin, sedangkan delik materil adalah perbuatan yang menimbulkan akibat kerugian bagi orang lain. Adanya *Cybercrime* telah menjadi ancaman stabilitas, sehingga pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer, khususnya jaringan internet dan intranet.

Menurut Andi Hamzah kejahatan komputer adalah kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal. Berdasarkan pengertian di atas, secara ringkas dapat dikatakan bahwa *cybercrime* dapat didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi.

Selama ini dalam kejahatan konvensional, dikenal adanya dua jenis kejahatan sebagai berikut:

1. Kejahatan kerah biru (*blue collar crime*)

   Kejahatan ini merupakan jenis kejahatan atau tindak kriminal yang dilakukan secara konvensional seperti misalnya perampokkan, pencurian, pembunuhan dan lain-lain.

2. Kejahatan kerah putih (*white collar crime*)

   Kejahatan jenis ini terbagi dalam empat kelompok kejahatan, yakni kejahatan korporasi, kejahatan birokrat, malpraktek, dan kejahatan individu.

Cybercrime merupakan kejahatan yang muncul sebagai akibat adanya komunitas dunia maya di internet, memiliki karakteristik tersendiri yang berbeda dengan kedua model di atas. Karakteristik unik dari kejahatan di dunia maya tersebut antara lain menyangkut lima hal berikut:

1. Ruang lingkup kejahatan;
2. Sifat kejahatan;
3. Pelaku kejahatan;
4. Modus Kejahatan;
5. Jenis kerugian yang ditimbulkan.

Berdasarkan jenis aktifitas yang dilakukannya, *cybercrime* dapat digolongkan menjadi beberapa jenis, antara lain sebagai berikut:[2]

1. *Unauthorized Access*

   Merupakan kejahatan yang terjadi ketika seseorang memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. *Probing* dan *port* merupakan contoh kejahatan ini.

2. *Illegal Contents*

   Merupakan kejahatan yang dilakukan dengan memasukkan data atau informasi ke internet tentang suatu hal yang tidak

[2] *http://balianzahab.wordpress.com/cybercrime/modus-modus-kejahatan-dalam-teknologi-informasi/,* 27 Maret 2010, Pkl. 21:00:24

benar, tidak etis, dan dapat dianggap melanggar hukum atau menggangu ketertiban umum, contohnya adalah penyebaran pornografi.

3. Penyebaran virus secara sengaja

   Penyebaran virus pada umumnya dilakukan dengan menggunakan email. Sering kali orang yang sistem emailnya terkena virus tidak menyadari hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya.

4. *Data Forgery*

   Kejahatan jenis ini dilakukan dengan tujuan memalsukan data pada dokumen-dokumen penting yang ada di internet. Dokumen-dokumen ini biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis *web database*.

5. *Cyber Espionage, Sabotage, and Extortion*

   Cyber Espionage merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran. *Sabotage and Extortion* merupakan jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

6. *Cyberstalking*

   Kejahatan jenis ini dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer,

misalnya menggunakan *e-mail* dan dilakukan berulang-ulang. Kejahatan tersebut menyerupai teror yang ditujukan kepada seseorang dengan memanfaatkan media internet. Hal itu bisa terjadi karena kemudahan dalam membuat email dengan alamat tertentu tanpa harus menyertakan identitas diri yang sebenarnya.

7. *Carding*

   Carding merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet.

8. *Hacking* dan *Cracker*

   Istilah *hacker* biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Adapun mereka yang sering melakukan aksi-aksi perusakan di internet lazimnya disebut *cracker*. Boleh dibilang cracker ini sebenarnya adalah hacker yang yang memanfaatkan kemampuannya untuk hal-hal yang negatif. Aktivitas cracking di internet memiliki lingkup yang sangat luas, mulai dari pembajakan account milik orang lain, pembajakan situs web, probing, menyebarkan virus, hingga pelumpuhan target sasaran. Tindakan yang terakhir disebut sebagai DoS (Denial Of Service). Dos attack merupakan serangan yang bertujuan melumpuhkan target (hang, crash) sehingga tidak dapat memberikan layanan.

9. *Cybersquatting and Typosquatting*

Cybersquatting merupakan kejahatan yang dilakukan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. Adapun typosquatting adalah kejahatan dengan membuat domain plesetan yaitu domain yang mirip dengan nama domain orang lain. Nama tersebut merupakan nama domain saingan perusahaan.

10. *Hijacking*

    Hijacking merupakan kejahatan melakukan pembajakan hasil karya orang lain. Yang paling sering terjadi adalah Software Piracy (pembajakan perangkat lunak).

11. *Cyber Terorism*

    Suatu tindakan cybercrime termasuk cyber terorism jika mengancam pemerintah atau warganegara, termasuk cracking ke situs pemerintah atau militer. Beberapa contoh kasus Cyber Terorism sebagai berikut :

    a. Ramzi Yousef, dalang penyerangan pertama ke gedung WTC, diketahui menyimpan detail serangan dalam file yang di enkripsi di laptopnya.
    b. Osama Bin Laden diketahui menggunakan steganography untuk komunikasi jaringannya.
    c. Suatu website yang dinamai Club Hacker Muslim diketahui menuliskan daftar tip untuk melakukan hacking ke Pentagon.

d. Seorang hacker yang menyebut dirinya sebagai DoktorNuker diketahui telah kurang lebih lima tahun melakukan defacing atau mengubah isi halaman web dengan propaganda anti-American, anti-Israel dan pro-Bin Laden.

Berdasarkan motif kegiatan yang dilakukannya, cybercrime dapat digolongkan menjadi dua jenis sebagai berikut :

1. *Cybercrime* sebagai tindakan murni kriminal

   Kejahatan yang murni merupakan tindak kriminal merupakan kejahatan yang dilakukan karena motif kriminalitas. Kejahatan jenis ini biasanya menggunakan internet hanya sebagai sarana kejahatan. Contoh kejahatan semacam ini adalah *Carding*, yaitu pencurian nomor kartu kredit milik orang lain untuk digunakan dalam transaksi perdagangan di internet. Juga pemanfaatan media internet (*webserver*, *mailing list*) untuk menyebarkan material bajakan. Pengirim *e-mail* anonim yang berisi promosi (*spamming*) juga dapat dimasukkan dalam contoh kejahatan yang menggunakan internet sebagai sarana. Di beberapa negara maju, pelaku *spamming* dapat dituntut dengan tuduhan pelanggaran privasi.

2. *Cybercrime* sebagai kejahatan abu-abu

   Pada jenis kejahatan di internet yang masuk dalam wilayah abu-abu, cukup sulit menentukan apakah itu merupakan tindak kriminal atau bukan mengingat motif kegiatannya terkadang bukan untuk kejahatan. Salah satu contohnya adalah *probing*

atau *portscanning*. Ini adalah sebutan untuk semacam tindakan pengintaian terhadap sistem milik orang lain dengan mengumpulkan informasi sebanyak-banyaknya dari sistem yang diintai, termasuk sistem operasi yang digunakan, *port-port* yang ada, baik yang terbuka maupun tertutup, dan sebagainya.

Sementara itu, berdasarkan sasaran kejahatan, *cybercrime* dapat dikelompokkan menjadi beberapa kategori seperti berikut ini :[3]

1. *Cybercrime* yang menyerang individu (*Against Person*)

   Jenis kejahatan ini, sasaran serangannya ditujukan kepada perorangan atau individu yang memiliki sifat atau kriteria tertentu sesuai tujuan penyerangan tersebut. Beberapa contoh kejahatan ini antara lain :

   a. Pornografi

      Kegiatan yang dilakukan dengan membuat, memasang, mendistribusikan, dan menyebarkan material yang berbau pornografi, cabul, serta mengekspos hal-hal yang tidak pantas.

   b. *Cyberstalking*

      Kegiatan yang dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya dengan menggunakan e-mail yang dilakukan secara berulang-ulang seperti halnya teror di dunia cyber. Gangguan tersebut bisa saja berbau seksual, religius, dan lain sebagainya.

[3] *http://id.wikipedia.org/wiki/Situs_web.Loc Cit.*

c. *Cyber-Tresspass*

Kegiatan yang dilakukan melanggar area privasi orang lain seperti misalnya *Web Hacking*. *Breaking* ke *PC*, *Probing*, *Port Scanning* dan lain sebagainya.

2. *Cybercrime* menyerang hak milik (*Againts Property*)

Cybercrime yang dilakukan untuk menggangu atau menyerang hak milik orang lain. Beberapa contoh kejahatan jenis ini misalnya pengaksesan komputer secara tidak sah melalui dunia *cyber*, pemilikan informasi elektronik secara tidak sah/ pencurian informasi, *carding*, *cybersquating*, *hijacking*, *data forgery* dan segala kegiatan yang bersifat merugikan hak milik orang lain.

3. *Cybercrime* menyerang pemerintah (*Againts Government*)

Cybercrime Againts Government dilakukan dengan tujuan khusus penyerangan terhadap pemerintah. Kegiatan tersebut misalnya *cyber terorism* sebagai tindakan yang mengancam pemerintah termasuk juga *cracking* ke situs resmi pemerintah atau situs militer.

Revolusi komputer maupun perkembangan teknologi informasi dan telekomunikasi ternyata masih menjadi barang mahal di Indonesia. Menurut Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), baru sekitar 10 persen dari 220 juta rakyat Indonesia yang mengenal komputer. Indonesia menduduki peringkat kedua dalam kasus kejahatan digital di

dunia. Indonesia hanya dikalahkan oleh Ukraina, salah satu negara sosialis pecahan Uni Soviet.[4]

Secara garis besar, *cybercrime* terdiri atas dua jenis, yaitu kejahatan yang menggunakan teknologi informasi sebagai fasilitas dan kejahatan yang menjadikan sistem dan fasilitas teknologi informasi sebagai sasaran. Beberapa modus kejahatan digital yang menggunakan teknologi informasi sebagai fasilitas, antara lain, penipuan finansial dengan media komunikasi digital (*banking fraud*).

Pelaku sengaja membuat situs jebakan yang alamat maupun fiturnya mirip dengan aslinya untuk menjerat nasabah yang ceroboh untuk memasukkan nomor rekening dan *password*. Bila terjebak, dalam sekejap seluruh tabungan anda berpindah nomor rekening, bahkan bisa jadi nomor rekening di Swiss atau negeri manapun. Kasus ini pernah menimpa nasabah *mobile banking* sebuah bank nasional terbesar Bank Central Asia yang terjebak masuk ke situs palsu. Modus itu namanya *type site,* yakni kejahatan yang dilakukan pelakunya dengan membuat nama situs palsu yang sama persis dengan situs aslinya, sedangkan untuk mengganti halaman muka (*webpage*) dinamakan *web deface*.

Kejahatan digital jenis baru yang cukup meresahkan banyak orang adalah *phising* atau penipuan lewat *e-mail*. *Phising* merupakan teknik untuk mencari *personal information* (alamat *e-mail*, nomor rekening, dan data pribadi lainnya) dengan mengirimkan *e-mail* yang seolah-olah datang dari bank yang bersangkutan. Sementara, kejahatan digital yang bertujuan pada peralatan teknologi informasi antara lain *defacting* dan *hacking*.

[4] *http://www.gsn-soeki.com/wouw/a000610.php,* 9 Februari 2010, Pkl 01:23:18

Keduanya bertujuan mencuri data-data milik orang lain dalam jaringan komunikasi data, maupun sekadar memasuki jaringan sistem komputer untuk mengganggu privasi maupun bertujuan membuat sistem gagal berfungsi (*denial of service/ DoS*).

Pelaku yang berupaya masuk ke sistem jaringan sekadar untuk mengadu ilmu, pelakunya disebut *hacker*. Sementara itu, yang tujuannya merusak jaringan kerap disebut *cracker*. Contoh kasus lain adalah perusakan situs Komisi Pemilihan Umum (KPU) dan situs Partai Golkar, dimana pelakunya yang kemudian tertangkap mengaku hanya ingin berolok-olok sekaligus mengingatkan pengelola jaringan teknologi informasi KPU yang sebelumnya menyatakan di media bahwa jaringannya 100 persen kebal serangan *hacker*. Modus yang sering digunakan para perusak jaringan ini antara lain menyebarkan *virus*, *worm*, *backdoor*, maupun *trojan* pada perangkat komputer sebuah organisasi yang mengakibatkan terbukanya akses-akses bagi orang-orang yang tidak berhak.

Modus Kejahatan *Cybercrime* Indonesia yang terjadi di Indonesia antara lain sebagai berikut:[5]

1. Pencurian nomor kartu kredit (*carding*);
2. Memasuki, memodifikasi, atau merusak homepage (*hacking*);
3. Penyerangan *situs* atau *e-mail* melalui *virus* atau *spamming*.

Bentuk kejahatan digital yang paling banyak terjadi di Indonesia adalah mencuri nomor dan *password* kartu kredit untuk transaksi di situs belanja seperti *E-Bay* maupun *Amazon*. Pelakunya kerap disebut *carder*.

[5] *http://mohtar.staff.uns.ac.id/, Loc. Cit.*

E-commerce menggolongkan Indonesia sebagai pusat *carder*. Pusat *carder* utama di Indonesia secara berurutan adalah Semarang, Jogjakarta, Medan, Bandung, Jakarta, Denpasar, dan Surabaya, karena reputasi yang buruk, sampai saat ini sulit bagi orang yang menggunakan *internet protocol address* (*IP Address*) asal Indonesia untuk berbelanja secara legal di situs belanja. Ada beberapa kasus penolakan kartu kredit jaringan global yang diterbitkan di Indonesia yang dibawa pemiliknya bepergian ke luar negeri.

Polri sejauh ini berhasil mengungkap sejumlah pelaku *carder* di Jogjakarta, Semarang, dan Bandung. Akhir tahun lalu, APJII memperkirakan kerugian akibat pembobolan kartu kredit mencapai USD 6-7 juta. Modus tradisional *carder* adalah menadah data kartu kredit dari transaksi konvensional, misalnya pembayaran dengan kartu kredit di hotel, biro wisata, restoran, dan toko cinderamata.

Virus komputer sendiri merupakan program komputer yang dapat menggandakan atau menyalin dirinya sendiri dan menyebar dengan cara menyisipkan salinan dirinya ke dalam program atau dokumen lain. Virus komputer dapat dianalogikan dengan virus biologis yang menyebar dengan cara menyisipkan dirinya sendiri ke sel makhluk hidup. Virus komputer dapat merusak (misalnya dengan merusak data pada dokumen), membuat pengguna komputer merasa terganggu, maupun tidak menimbulkan efek sama sekali. Virus komputer umumnya dapat merusak perangkat lunak komputer dan tidak dapat secara langsung merusak perangkat keras komputer dengan cara memuat program yang memaksa *over process* ke perangkat tertentu misalnya *VGA*, *Memory* bahkan *Processor* (terutama pada sistem operasi , seperti sistem operasi berbasis keluarga *Windows*

(*Windows XP, Windows Vista* dsb). Sementara itu *Spam* atau *junk mail* adalah penyalahgunaan dalam pengiriman berita elektronik untuk menampilkan berita iklan dan keperluan lainnya yang mengakibatkan ketidaknyamanan bagi para pengguna *situs web*. Bentuk berita *spam* yang umum dikenal meliputi: *spam* surat elektronik, *spam* pesan instan, *spam Usenet newsgroup*, *spam* mesin pencari informasi *web* (*web search engine spam*), *spam* blog, *spam* berita pada telepon genggam, *spam* forum Internet, dan lain lain.

Spam ini biasanya datang bertubi-tubi tanpa diminta dan sering kali tidak dikehendaki oleh penerimanya. Beberapa contoh lain dari *spam* ini bisa berupa *e-mail* berisi iklan, surat masa singkat (SMS) pada telepon genggam, berita yang masuk dalam suatu forum kelompok warta berisi promosi barang yang tidak terkait dengan kegiatan kelompok warta tersebut, *spamdexing* yang menguasai suatu mesin pencari (*search engine*) untuk mencari popularitas bagi suatu URL tertentu, ataupun bisa berupa berita yang tak berguna dan masuk dalam suatu *blog*, buku tamu *situs web*, dan lain-lain.

Spam dikirimkan oleh pembuat iklan dengan biaya operasi yang sangat rendah, karena *spam* ini tidak memerlukan senarai (*mailing list*) untuk mencapai para pelanggan-pelanggan yang diinginkan. Sebagai akibatnya banyak pihak yang dirugikan. Selain pengguna Internet itu sendiri, *ISP* (Penyelenggara Jasa Internet atau *Internet Service Provider*), dan masyarakat umum juga merasa tidak nyaman, karena biasanya sangat mengganggu dan kadang-kadang membohongi, berita *spam* termasuk

dalam kegiatan melanggar hukum dan merupakan perbuatan pidana yang bisa ditindak melalui undang-undang Internet.

B. Kasus Mengenai Perusakan Situs Resmi Instansi Pemerintah Melalui Media Internet

Salah satu kegiatan yang sering dilakukan oleh *cracker* adalah mengubah halaman *web*, yang dikenal dengan istilah *deface*. Pembajakan dapat dilakukan dengan mengeksploitasi lubang keamanan. Sekitar 4 bulan yang lalu, statistik di Indonesia menunjukkan satu (1) *situs web* dibajak setiap harinya. Contoh kasusnya antara lain :

1. Pembajakan *web* KPU tahun 2004

   Pada hari Sabtu, 17 April 2004, Dani Firmansyah, konsultan Teknologi Informasi (TI) PT. Danareksa di Jakarta berhasil membobol situs milik Komisi Pemilihan Umum (KPU) di *http://tnp.kpu.go.id* dan berhasil melakukan perubahan pada seluruh nama partai disitus TNP KPU pada jam 11:24:16 sampai dengan 11:34:27. Perubahan ini menyebabkan nama partai yang tampil pada situs yang diakses oleh publik, seusai Pemilu Legislatif lalu, berubah menjadi nama-nama lucu seperti Partai Jambu, Partai Kelereng, Partai Cucak Rowo, Partai Si Yoyo, Partai Mbah Jambon, Partai Kolor Ijo, dan lain sebagainya. Dani menggunakan teknik *SQL Injection* (pada dasarnya teknik tersebut adalah dengan cara mengetikkan *string* atau perintah tertentu di *address bar browser*) untuk menjebol situs KPU. Selanjutnya Dani tertangkap pada hari

Kamis, 22 April 2004. Dan sidang kasus pembobolan situs TNP Komisi Pemilihan Umum (KPU) digelar Senin (16/8/2004).

2. Pembajakan *web* KPU tahun 2009

   Web resmi KPU *kpu.go.id* Sabtu 15 Maret pukul 20.15 diganggu orang tak bertanggungjawab. Bagian situs *kpu.go.id* yang diganggu *hacker* adalah halaman berita, dengan menambah berita dengan kalimat ”*I Love You Renny Yahna Octaviana*. *Renny How Are You There?*”. Bukan hanya itu, pengganggu juga mengacak-acak isi berita *kpu.go.id.* Pengurus *situs web kpu.go.id* untuk sementara menutup *kpu.go.id*/ sehingga tidak bisa diakses oleh publik yang ingin mengetahui berita-berita tentang KPU khususnya mengenai persiapan Pemilu 2009. Awal April 2008 tahapan awal pelaksanaan Pemilu 2009 yaitu pemutakhiran data pemilih dan pendaftaran Parpol peserta Pemilu mulai dilaksanakan.

3. Pembajakan Situs Depkominfo
4. Pembajakan situs Komisi Hukum Nasional Republik Indonesia
5. Pembajakan situs PDAM Kota Denpasar Bali

Selain itu ada beberapa situs yang di *deface* menjelang HUT RI tahun 2007 :

1. http://www.kajen.go.id/hut.htm
2. http://disnakerkarawang.go.id/
3. http://www.bazisdki.go.id/hut.htm
4. http://depnakertrans.net/
5. http://dikmas.com/hut.htm

6. http://indosatschool.com/indosat/caching/
7. http://amikom.ac.id/images/
8. http://www.telkomjogja.net/hut.htm
9. http://kopegtel.pekalongan.net
10. http://bisnisjakarta.com/
11. http://bursatransmigrasi.net/
12. http://alattulis.net/item.php?id=0,26
13. http://dosasex.com/ap/artikel.php?aid=247
14. http://harianterbit.com/
15. http://tvkatalog.com/hut.htm

Berdasarkan contoh-contoh kasus di atas dapat dilihat bahwa tindak pidana perusakan situs internet masih banyak terjadi, terutama situs resmi instansi pemerintah, dalam hal merusak program pemerintah dalam hubungannya dengan pelayanan kepada publik melalui media ini. Masalah perusakan situs resmi instansi pemerintah dapat dikenakan sanksi berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, akan tetapi dalam perusakan situs instansi pemerintah yang dilakukan melalui media internet masih sulit untuk diungkap oleh para penegak hukum karena berbagai kendala. Oleh karena itu penulis mencoba membahas hal ini agar di kemudian hari diharapkan dapat dijadikan masukan dalam perkembangan bidang ilmu hukum mengenai masalah kejahatan perusakan situs resmi instansi pemerintah yang dilakukan melalui media internet.