**MAKALAH**

**KEJAHATAN DUNIA MAYA ( CYBER CRIME ) :**

**TANTANGAN DAN SOLUSI PERSPEKTIF ISLAM**

**“**Untuk memenuhi tugas mata kuliah Al Islam dan Kemuhammadiyahan**”**

**Logo

Description automatically generated**

Dibuat oleh :

ARIF MUNANDAR

B02220148

Dosen Pengampu : ***Muchlis, S.Pd, M.Pd.I***

**UNIVERSITAS MUHAMMADIYAH BIMA**

**FAKULTAS ILMU KOMPUTER**

**PROGRAM STUDI ILMU KOMPUTER**

**TAHUN 2022**

**KATA PENGANTAR**

Tiada kalimat yang pantas penulis ucapkan kecuali rasa syukur kepada Tuhan Yang Maha Esa atas selesainya makalah yang berjudul "KEJAHATAN DUNIA MAYA (CYBER CRIME ): TANTANGAN DAN SOLUSI PERSPEKTIF ISLAM ". Tidak lupa pula dukungan baik secara materil dan non-materil yang diberikan kepada penulis dalam penyusunan makalah ini. Oleh karena itu, izinkan penulis mengucapkan rasa terima kasih kepada Bapak Muchlis, S.Pd, M.Pd.I, selaku dosen pengampu pada mata kuliah Al Islam dan Kemuhammadiyahan.

Penulis sadar bahwa makalah yang disusun ini masih belum sempurna. Oleh karena itu, dengan rendah hati penulis memohon kritik dan saran yang membangun dari pembaca untuk penyempurnaan makalah ini.

Bima, 11 November 2022

Penulis,

**PENDAHULUAN**

Cybercrime dewasa ini muncul ketika penyalahgunaan internet sudah di luar batas sehingga menjadi suatu kejahatan. Pengertian kejahatan komputer pada umumnya sebagai kejahatan melalui pengetahuan khusus tentang teknologi komputer. Hukum terlalu lambat untuk mengikuti perkembangan teknologi computer, kemudian bereaksi terhadap perubahan dan perkembangan teknologi yang demikian cepat. Bahkan undang-undang yang sekarang ini tidak mampu  
untuk menangani kejahatan dunia maya secara tuntas.Internet sebagai hasil rekayasa teknologi bukan hanya menggunakan kecanggihan teknologi komputer tapi juga melibatkan teknologi telekomunikasi di dalam pengoperasiannya.

Keunggulan komputer berupa kecepatan dan ketelitiannya dalam menyelesaikan suatu pekerjaan dapat menekan jumlah tenaga kerja, biaya, serta dapat memperkecil kemungkinan melakukan kesalahan. akibatnnya masyarakat

**PEMBAHASAN**

**Apa Itu Kejahatan Siber?**

Kejahatan tak hanya terjadi di dunia nyata, namun juga di dunia maya. Kejahatan yang terjadi di dunia maya inilah yang disebut dengan istilah **kejahatan siber** atau *cyber crime*. Sesuai dengan namanya, kejahatan yang terjadi di dunia maya ini menggunakan komputer dan akses internet sebagai sarana untuk merugikan pihak lain.

Seiring dengan semakin meningkatnya pengguna internet, jumlah kasus kejahatan di dunia maya ini pun juga makin bertambah. Bentuk kejahatan ini pun beragam, misalnya seperti pencurian data pribadi, penipuan mengatasnamakan orang lain di media sosial, hingga pembobolan rekening. Sulitnya melacak pelaku kejahatan, jadi salah satu tantangan menyelesaikan kejahatan ini.

Contoh Kasus *Cyber Crime*di Indonesia

* **Pencuriandan penggunaan account Internet milik orang lain.**Diantara kesulitan dari sebuah ISP (Internet Service Provider) adalah adanya account pelanggan mereka yang “dicuri” dan digunakan secara tidak sah. Berbeda dengan pencurian yang dilakukan secara fisik, “pencurian” account cukup menangkap “userid” dan “password” saja. Hanya informasi yang dicuri. Sementara orang yang kecurian tidak merasakan hilangnya “benda” yang dicuri. Pencurian baru terasa efeknya jika informasi ini digunakan oleh yang tidak berhak. Akibat dari pencurian ini, penggunaan dibebani biaya penggunaan account tersebut. Kasus ini banyak terjadi di ISP.
* **Membajak situs web.** 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.
* **Probing dan port scanning.** Salah satu langkah yang dilakukan cracker sebelum masuk ke server target yaitu melakukan pengintaian, dengan cara melakukan “port scanning” atau “probing” untuk melihat servisservis apa saja yang tersedia di server target. Misalnya, hasil scanning dapat menunjukkan bahwa server target menjalankan program web server Apache, mail server sendmail, dan seterusnya. Analogi hal ini dengan dunia nyata yaitu dengan melihat-lihat apakah pintu rumah target terkunci, merek kunci yang digunakan, jendela mana yang terbuka, apakah pagar terkunci (menggunakan *firewall* atau tidak) dan seterusnya. Yang bersangkutan memang belum melakukan kegiatan pencurian atau penyerangan, akan tetapi kegiatan yang dilakukan sudah mencurigakan.
* **Virus.** Seperti halnya di tempat lain, virus komputer pun menyebar di Indonesia. Penyebaran umumnya dilakukan dengan menggunakan email. Seringkali sistem email seseorang yang terkena virus tidak sadar akan hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya. Kasus virus ini sudah cukup banyak seperti virus Mellisa, I love you, dan SirCam. Untuk orang yang terkena virus, kemungkinan tidak banyak yang dapat dilakukan.
* **Denial of Service (DoS) dan Distributed DoS (DDos) attack.** DoS attack merupakan serangan yang bertujuan untuk melumpuhkan target (hang, crash) sehingga dia tidak dapat memberikan layanan. Aktifitas serangannya tidak melakukan pencurian, penyadapan, ataupun pemalsuan data. Akan tetapi dengan hilangnya layanan maka target tidak dapat  
  memberikan servis sehingga ada kerugian finansial. Bagaimana status dari DoS attack ini? Bayangkan bila seseorang dapat membuat ATM bank menjadi tidak berfungsi. Akibatnya nasabah bank tidak dapat melakukan transaksi dan bank termasuk nasabah dapat mengalami kerugian finansial. DoS attack dapat ditujukan kepada server (komputer) dan juga dapat ditargetkan kepada jaringan (menghabiskan bandwidth). Tools untuk melakukan hal ini banyak tersebar di Internet. DDoS attack meningkatkan serangan ini dengan melakukannya dari beberapa (puluhan, ratusan, dan bahkan ribuan) komputer secara serentak. Efek yang dihasilkan lebih dahsyat dari DoS attack saja.
* **Kejahatan yang berhubungan dengan nama domain** (domain name) digunakan untuk mengidentifikasi perusahaan dan merek dagang. Namun banyak orang mencoba menarik keuntungan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya dengan harga yang lebih mahal. Pekerjaan ini mirip dengan calo karcis.  
  Istilah yang sering digunakan adalah cybersquatting. Masalah lain adalah menggunakan nama domain saingan perusahaan untuk merugikan perusahaan lain. (Kasus: mustika-ratu.com) Kejahatan lain yang berhubungan dengan nama domain adalah membuat “domain plesetan”,  
  yaitu domain yang mirip dengan nama domain orang lain. (Seperti kasus klikbca.com) Istilah yang digunakan saat ini adalah typosquatting.
* **IDCERT (Indonesia Computer Emergency Response Team)**. Salah satu cara untuk mempermudah penanganan masalah keamanan dengan membuat sebuah unit untuk melaporkan kasus keamanan. Masalah keamanan ini di luar negeri mulai dikenali dengan munculnya “*sendmail worm*” (sekitar tahun 1988) yang menghentikan sistem email Internet kala itu. Kemudian dibentuk sebuah *Computer Emergency Response Team* (CERT). Semenjak itu di negara lain mulai juga dibentuk CERT untuk menjadi *point of contact* bagi orang untuk melaporkan masalah keamanan. IDCERT merupakan CERT Indonesia .
* **Sertifikasi perangkat security**. Perangkat yang digunakan untuk menanggulangi keamanan semestinya memiliki peringkat kualitas. Perangkat yang digunakan untuk keperluan pribadi tentunya berbeda dengan perangkat yang digunakan untuk keperluan militer. Namun sampai  
  saat ini belum ada institusi yang menangani masalah evaluasi perangkat keamanan di Indonesia.

Mengingat kejahatan *e-commerce* merupakan salah satu kejahatan baru dan canggih, maka wajar dalam penegakan hukumnya masih mengalami beberapa kendala yang harus segera ditangani agar peluang pelaku kejahatan bisnis canggih dapat diatasi dan tidak dapat mengembangkan bakatkejahatannya di dunia maya khususnya kejahatan *e-commerce*. Meskipun demikian, ada kendala yang harus dipecahkan atau dicarikan solusinya diantaranya:

1. Pembuktian (bukti elektrik)  
   Persoalan yang muncul, yaitu belum adanya kebulatan penafsiran terhadap kepastian dari alat bukti elektrik, dikarenakan alat bukti ini mudah sekali untuk di copy, digandakan atau bahkan dipalsukan, dihapus atau dipindahkan. Walaupun mengacu pada Pasal 5 Undang-Undang ITE telah jelas menyebutkan mengenai alat bukti ini, namun masih saja aparat penegak hukum mengalami kesulitan untuk mendapatkan alat bukti yang otentik.
2. Perbedaan Persepsi  
   Perbedaan persepsi yang dimaksud yaitu bahwa terjadinya perbedaan antara penegak hukum dalam menafsirkan kejahatan yang terjadi dengan penerapan pasal-pasal dalam hukum positif yang berlaku sehingga menimbulkan ketidakpastian hukum bagi pencari keadilan.
3. Lemahnya penguasaan komputer  
   Kurangnya kemampuan dan keterampilan aparat penegak hukum di bidang komputer yang mengakibatkan taktis, teknis penyelidikan, penuntutan dan pemeriksaan di pengadilan tidak dikuasai karena menyangkut sistem yang ada didalam komputer.
4. Sarana dan prasarana  
   Fasilitas komputer mungkin memang ada di setiap kantor-kantor para penegak hukum, namun hanya berfungsi sebatasuntuk administrati, seperti mengetik saja, sedangkan kejahatan *e-commerce* ini dilakukan dengan menggunakan komputer yang berjaringan dan berkapasitas teknologi yang lumayan maju sehingga pihak aparat sulit untuk mengimbangi kegiatan para pelaku kejahatan tersebut.
5. Kesulitan Menghadirkan korban  
   Terhadap kejahatan yang korbannya berasal dari luar negeri umumnya sangat sulit untuk melakukan pemeriksaan yang mana keterangan saksi korban sangat dibutuhkan untuk membuat sebuah berita acara pemeriksaan.

Cybercrime membutuhkan *global action* dalam penanggulangannya mengingat kejahatan tersebut seringkali bersifat transnasional. Adapun langkah penting yang harus dilakukan setiap negara dalam penanggulangan cybercrime adalah:

1. Melakukan modernisasi hukum pidana nasional beserta hukum acaranya, yang diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut
2. Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar Internasional
3. Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan cybercrime
4. Meningkatkan kesadaran warga negara mengenai masalah cybercrime serta pentingnya upaya pencegahan kejahatan agar tidak mudah terjadi.
5. Meningkatkan kerjasama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan cybercrime, antara lain melalui perjanjian ekstradisi dan mutual assistance treaties.

Terdapat tiga pendekatan untuk mempertahankan keamanan di *cyberspace*, pertama adalah pendekatan teknologi, kedua pendekatan sosial budaya-etika dan ketiga pendekatan hukum. Untuk mengatasi keamanan gangguan pendekatan teknologi sifatnya mutlak dilakukan, sebab tanpa suatu pengamanan jaringan akan sangat mudah disusupi, diintersepsi atau diakses secara ilegal dan tanpa hak.

**Cyber Crime Ditinajau dari Hukum Islam**Dipahami dari pengertian dan jenis–jenis cyber crime tersebut di atas, *cybercrime* merupakan bentuk kejahatan yang muncul di era modern sekarang ini. Dengan demikian, perbuatan kejahatan *cyber crime* menurut analisa hukum Islam (jinayat) dapat dihukum dengan ta’zir. Ta’zîr menurut pengertian bahasa berarti pencegahan (*al-man’u*). adapun menurut istilah ta’zîr merupakan hukuman edukatif (*ta’dîb*) dalam arti mengantisipasi dengan cara menakut-nakuti (*tankîf*). Adapun secara syar’î, ta’zîr dimaksudkan sebagai sanksi yang dijatuhkan atas dasar kemaksiatan, karena secara tegas tidak termasuk kejahatan yang termaktub dalam Al Quran da  
Hadis, sebagaimana had, Qisas, atau kafârat.

Hukuman *Ta’zîr*macamnya dapat berupa sangsi dalam bentuk:

1. Hukuman mati
2. Jilid atau cambuk tidak melebihi 10 kali
3. Pengasingan, pemboikotan, atau penjara
4. Salib
5. Ganti rugi (*ghuramah*) atau dengan cara penyitaan
6. Peringatan atau nasehat
7. Pencabutan Sebagian hak kekayaan (*hurmân*)
8. Pencelaan (*taubîkh*)
9. Pewartaan (*tasyhîr*)

Bentuk sanksi ta‘zîr hanya terbatas pada bentuk-bentuk tersebut. Khalifah atau yang mewakilinya yaitu *qâdhî* (hakim) diberikan hak oleh syariat untuk memilih di antara bentuk-bentuk sanksi tersebut dan menentukan kadarnya; ia tidak boleh menjatuhkan sanksi di luar itu.

Kasus ta‘zîr secara umum terbagi menjadi:

1. Pelanggaran terhadap kehormatan
2. Pelanggaran terhadap kemuliaan
3. Perbuatan yang merusak akal
4. Pelanggaran terhadap harta
5. Gangguan keamanan
6. Subversi
7. Pelanggaran yang berhubungan dengan agama.

**KESIMPULAN**

Cyber Crime merupakanaktivitas kejahatan dengan menggunakan fasilitas computer atau jaringan computer tanpa ijin dan melawan hokum, baik cara mengubahnya atau tanpa perubahan (kerusakan) pada fasilitas komputer yang dimasuki atau digunakan, atau kejahatan yang dengan menggunakan sarana media elektronik internet karena dikategorikan sebagai kejahatan dunia maya, atau kejahatan di bidang komputer dengan cara illegal, Dapat pula dikategorikan sebagai  
kejahatan komputer yang ditujukan kepada sistem atau jaringan komputer, yang mencakup segala bentuk baru kejahatan yang menggunakan bantuan sarana media elektronik internet.Sangsi bagi para pelaku cybercrime menurut syari’at Islam adalah Ta’zir melalui proses peradilan dengan vonis Hakim dengan ancaman hukuman berupa kurungan penjara, pengasingan, cambuk, sampai pada hukuman mati sesuai dengan tingkat mudharat yang telah dilakukannya.

**REFERENSI**

Al-Mundziri, Imam. *Ringkasang Shahih Muslim*.Jakarta: Pustaka Amani.

Tahir, Ach. *Cyber Crime :Akar Masalah, Solusi, dan Penanggulangannya.*Yogyakarta: Suka Press. 2013

Wahid, Abdul dan Muhammad Labib. *Kejahatan Dunia Mayantara*. Bandung: PT  
Rafika Aditama. 2005.

Widodi. *Memerangi Cyber Crime Karakteristik, Motivasi dan Strategi  
Penangannya dalam perspektif Kriminologi*. Yogyakarta: Aswaja Persindo.  
2013.