TINJAUAN KRIMINOLOGI MEMASUKI ATAU MENYUSUP KEDALAM SUATU JARINGAN KOMPUTER SECARA TIDAK SAH MENURUT UU NO.11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

Kurniawan Sihaloho, Josua Sitohang, Bella Fazrina

Fakultas Hukum Universitas Prima Indonesia
Jalan Sekip Simpang Sikambing, Medan, Sumatera Utara

Kurniawansihaloho00@gmail.com, bellafazrina97@gmail.com

ABSTRACT

This research has an information technology background that plays an important role in human life both in the present and in the future. The internet can penetrate the boundaries between countries and accelerate the spread and exchange of knowledge both among scientists or scholars throughout the world. Behind the ease of use of the internet, there is a dark side that worries the users, namely in terms of security. Public and global internet networks are very vulnerable to various forms of crime. The actions taken by the government to overcome in terms of reducing crime activities enter or infiltrate into a computer network illegally is the issuance of Law NO.11 of 2008 concerning Information and Information Transactions can be interpreted as a crime committed by a person or group of people with the intention of taking the advantage of others through a computer network. This study uses legal normative juridical research. The purpose of this study was to find out how the modus operandi and how prevention efforts enter or infiltrate into a computer network illegally. The mode is carried out with the intention of sabotage or theft of important and confidential information. Criminology review aims to investigate the widest possible crime symptoms. crime as needed prevention efforts are preventive (prevention) before the crime occurs and (eradication) after the crime has occurred is (refresive).

Keyboard: *Criminolgy, Enter or Infiltrate, Computer Network, Invailed*

Intisari

Penelitian ini berlatarbelakang teknologi informasi yang memegang peranan penting dalam kehidupan manusia baik di masa kini maupun masa yang akan datang. Internet dapat menembus batas-batas antar negara dan mempercepat penyebaran dan pertukaran ilmu baik di kalangan ilmuwan atau cendekiawan di seluruh dunia. Dibalik kemudahan penggunaan internet, terdapat sisi gelap yang merisaukan penggunanya, yaitu dari segi keamanannya. Jaringan internet yang bersifat publik dan global sangat rentan dari berbagai bentuk kejahatan. Adapun tindakan yang dilakukan pemerintah untuk mengatasi dalam hal mengurangi kegiatan kejahatan memasuki atau menyusup kedalam suatu jaringan komputer secara tidak sah ialah dengan diterbitkannya UU NO.11 TAHUN 2008 tentang Informasi dan Transaksi Informatika dapat diartikan sebagai suatu kejahatan yang dilakukan seseorang atau sekelompok orang dengan niat mengambil keuntungan dari orang lain melalui suatu jaringan komputer. Penelitian ini menggunakan penelitian hukum secara yuridis normatif. Tujuan penelitian ini dilakukan untuk mengetahui bagaimana modus operani dan bagaimana upaya penanggulangan memasuki atau menyusup kedalam suatu jaringan komputer secara tidak sah. Modus dilakukan dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Tinjauan kriminologi bertujuan untuk menyelidiki gejala kejahatan seluas-luasnya. kejahatan sebagaimana diperlukan upaya penanggulangan bersifat prefentif (pencegahan) sebelum kejahatan terjadi dan (pemberantasan) setelah kejahatan terjadi bersifat (refresif).

Kata kunci : Kriminologi, Memasuk atau Menyusup, Jaringan Komputer, Tidak Sah

A. Latar Belakang

Pada era globalisasi seperti sekarang ini, masyarakat semakin cepat berkembang. Hal ini disebabkan oleh kemajuan ilmu pengetahuan dan pola pikir masyarakat serta teknologi yang semakin canggih. Perkembangan teknologi yang semakin canggih memasuki era revolusi industry 4.0. Perubahan gaya hidup dipengaruhi oleh perkembangan tersebut melalui program dan layanan yang menyediakan atau menggunakan teknologi dalam aktifitas masyarakat. Pada saat ini penggunaan jaringan komputer digunakan dalam kehidupan sehari-hari.

Jaringan komputer merupakan sebuah system yang terdiri dari berbagai komputer beserta *resource* nya yang di desain untuk menggunakan sumber daya yang ada dapat mengakses informasi yang diperlukan.[1] Tidak jarang ditemukan kejahatan yang dilakukan dalam suatu system jaringan komputer secara tidak sah, tanpa izin atau tanpa pengetahuan dari pemilik system jaringan komputer yang dimasukinya. Hal ini dapat dilihat dari kasus yang terjadi pada tahun 1999 di Timur Timor beberapa

[1]Afrianto Irawan, Setiawan Eko Budi, *Kajian Virtual Privat Network (VPN) Sebagai System Pengamanan Data Pada Jaringan Komputer*, Majalah Ilmiah UNIKOM volume 12 No1 Hal 44.

website milik pemerintah Republik Indonesia dirusak.[2]

Pada tahun 2000 sebuah perusahaan Amerika dibidang ecomers yang memiliki kerahasiaan berhasil di hacker dengan cara memasuki data base perusahaan tersebut. Pada tahun 2004 situs Komisi Pemilihan Umum di bobol hacker.[3]

Adapun jaringan (port) yang paling banyak diincar peretas adalah portsmbd sebanyak 2,1 juta serangan. Kemudian, port Sipsession 1,3 juta dan SipCall sebanyak 1,2 juta serangan. Port adalah mekanisme yang mengizinkan sebuah computer untuk mendukung beberapa sesi koneksi dengan computer lain. Sementara itu tipe malware yang paling banyak menyerang cyber Indonesia adalah Win32/Conficker.worm.167765 sebanyak 429.208 serangan. Sebanyak 21 sensor Honeynet yang mendeteksi serangan siber ini baru tersedia di enam provinsi di Indonesia. Sensor ini aktif mengumpulkan raw data, file malware, dan menganalisa malware tersebut menggunakan metode analisis statis dan analisis dinamis. Sensor ini dipasang sejak 2014. Ke depan, Honeynet berencana memasang sensor di 170 titik di 34 provinsi di Indonesia.[4]

Dari kasus tersebut diperlukan upaya penanggulangan kejahatan Memasuki atau Menyusup kedalam Suatu Jaringan Komputer Secara Tidak Sah. Perbuatan tersebut diatur dalam pasal 30 ayat 2 dan 3 , hal tersebutlah yang melatar belakangi penelitian ini dengan judul "MEMASUKAN ATAU MENYUSUP KEDALAM SUATU JARINGAN KOMPUTER SECARA TIDAK SAH MENURUT UNDANG-UNDANG NO.11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK".

B. Rumusan Masalah

Berdasarkan pada latar belakang maka rumusan maslaah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana Modus Operandi Kejahatan Memasuki atau Menyusup Kedalam Suatu Jaringan Komputer Secara Tidak Sah?

[2] Surat Kabar Kompas, 11 Agustus Tahun 1999.
[3] *Ibid.*
[4] Desy Setyowati, Serangan Cyber Ke Indonesia Capai 12,9 juta Paling Banyak diRussia, Katadata, 2019

2. Bagaimana Upaya Penanggulangan Kejahatan Memasuki atau Menyusup Kedalam Suatu Jaringan Komputer Secara Tidak Sah dalam Tujuan Kriminologi?

C. Metode Penelitian

Jenis penelitian yang digunakan penelitian Yuridif Normatif menggunakan bahan hukum primer Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Bahan hukum sekunder berupa doktrin, teori hokum, pendapat hokum yang diperoleh dari literature, hasl penelitian, artikel maupun website terkai dengan penelitian. Teknik pengumpulan data dilakukan dengan penelitian kepustakaan (Library Research) yaitu menghimpun data dengan melakukan penelaahan bahan kepustakaan atau data sekunder yang meliputi bahan hokum primer adalah hukum yang mengikat dari suatu norma dasar, peraturan dasar dan peraturan perundangan-undangan.

4. Analisis Data

Metode yang digunakan penulis adalah dengan metode pendekatan kualitatif yaitu dengan mengumpulkan bahan hukum primer, sekunder dan tersier yang berkaitan dengan penelitian. Analisis data dengan menggunakan metode deduktif dan induktif.

D. Hasil Penelitian

1. Modus Operandi Kejahatan Memasuki atau Menyusup ke Dalam Suatu Jaringan Komputer Secara Tidak Sah

Modus operandi kejahatan memasuki atau menyusup kedalam suatu jaringan komputer secara tidak sah adalah Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi ini dikelompokkan dalam beberapa bentuk sesuai. Salah satu dari dari modus operandi yaitu:

Unauthorized Access to Computer System and Service

Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (*hacker*) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang

melakukannya hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi Internet/intranet.[5] Kita tentu belum lupa ketika masalah Timor Timur sedang hangat-hangatnya dibicarakan di tingkat internasional, beberapa *website* milik pemerintah RI dirusak oleh *hacker* (Kompas, 11/08/1999). Beberapa waktu lalu, *hacker* juga telah berhasil menembus masuk ke dalam *data base* berisi data para pengguna jasa America Online (AOL), sebuah perusahaan Amerika Serikat yang bergerak dibidang *ecommerce* yang memiliki tingkat kerahasiaan tinggi (Indonesian Observer, 26/06/2000). Situs Federal Bureau of Investigation (FBI) juga tidak luput dari serangan para *hacker*, yang mengakibatkan tidak berfungsinya situs ini beberapa waktu lamanya.[6]

Kejahatan yang berhubungan dengan komputer mencakup 2 kategori, yaitu kejahatan yang mejadikan komputer sebagai target atau objek kejahatan (komputer sebagai sasaran), dan kejahatan yang menggunakan komputer sebagai alat melakukan kejahatan (komputer sebagai sarana).[7]

Adapun langkah-langkah yang dilakukan oleh para hacker pada umumnya adalah sama, yang membedakan ialah dampak yang ditimbulkan dari kegiatan yang dilakukan oleh para hacker tersebut. Suatu kegiatan memasuki atau menyusup ke dalam suatu jaringan komputer dapat terjadi apabila ditujukan untuk mengambil data, mengganti isi di dalam jaringan komputer, sehingga tindakan tersebut menyebabkan kerusakan pada sistem jaringan komputer yang dituju sehingga sistem tersebut tidak berfungsi dengan baik dan harus dilakukan perbaikan secara menyeluruh terhadap suatu sistem computer yang telah dirusak.

Ada beberapa tahapan yang dilakukan para hacker sebelum melakukan penyusupan terhadap suatu jaringan komputer, antara lain :[8]

1. Footing Printing/Pencarian Data

   Tahap ini merupakan tahap awal yang dilakukan para pelaku untuk mengintai dan mencari suatu sistem

[5] Maskun, *Kejahatan Siber Cyber Crime Suatu Pengantar*, Kencana, Jakarta: 2013, hal 51.

[6] http://www.fbi.org

[7] Widodo, *Perspektif Hukum Pidana dan Kebijakan Pemidanaan*, Aswaja Pressindo,Yogyakarta: 2017, hal 94.

[8] Nur Khalimatus Sa'diyah, *Modus Operandi Tindak Pidana Cracker Menurut Undang-Undang Informasi dan Transaksi Elektronik*, Jurnal Fakultas Hukum Universitas Wijaya Kusuma, Surabaya: Vol. XVII, No. 2 Tahun 2012 Edisi Mei, hal 83.

yang dapat disusupi atau dimasukin. Kegiatan ini dilakukan dengan mencari data dan informasi sebanyak mungkin. Semua kegiatan ini dilakukan dengan sebuah alat dan informasi yang dicari merupakan informasi yang umum dan tersedia bebas di Internet.

2. Scanning/Pemilihan Sasaran

   Setelah menemukan data yang cukup dan dianggap mampu untuk disusupi, maka para pelaku mulai mencari lebih dalam apakah di dalam suatu sistem tersebut terdapat kelemahan sehingga dengan adanya kelemahan tersebut, memungkinkan para pelaku untuk melancarkan aksinya. Pada tahap ini sesungguhnya telah memberikan sinyal bahwa jaringan yang hendak disusup dan mudah dikenali oleh sasaran, kecuali dengan menggunakan stealth scanning. Untuk melindungan diri dari kegiatan scanning ialah dengan cara memasang Firewall misalnya Zone Alarm.

3. Enumerasi

   Pada tahap ini para pelaku dapat mencari account name yang valid, password, serta share resources yang ada dan tersedia dijariangan yang dituju. Dengan diperolehnya data yang valid tersebut maka para pelaku dapat dengan mudah melakukan penyusupan kedalam jaringan tersebut.

4. Gaining Access/Akses Ilegal

   Pada tahap ini, pelaku mencoba untuk memasuki suatu sistem sebagai user biasa. Tahap ini merupakan tahap kelanjutan dari Enumerasi yang mana para pelaku mulai mencoba mencari password dari jaringan yang hendak disusupi. Bila share resourcesnya diproteksi dengan suatu password, maka password tersebut dapat diperoleh melalui dictionary attack yang mana dilakukan untuk mencoba menebak password melalui kombinasi kata-kata.

5. Escalating Privilege

   Tahap ini dianggap bahwa para pelaku sudah mendapatkan akses untuk masuk ke sebuah jaringan sebagai user biasa. Setelah berhasil masuk, biasanya para pelaku mencoba untuk menjadi admin sehingga mampu menguasai jaringan tersebut. Teknik yang dilakukan para pelaku pun sudah berbeda yaitu dengan mencuri password file yang

tersimpan di dalam sistem dengan memanfaatkan kelemahan sistem.

6. Pilfering

   Pada tahap ini pelaku siap untuk melakukan suatu proses pencurian atau pun perusakan sistem jaringan dengan melakukan pengumpulan informasi untuk mengidentifikasi mekanisme yang dapat dilakukan agar mendapatkan akses ke trusted system.

7. Covering Tracks/Menutup jejak

   Setelah pelaku berhasil mendapatkan akses tersebut dan telah mampu menguasainya, maka pelaku berusaha untuk menutupi jejak agar tidak mudah untuk diketahui yaitu dengan cara membersihkan network log dan menggunakan hide tool seperti rootkit dan file streaming.

8. Creating Backdoors/Membuat Jalan Pintas

   Tahap ini para pelaku membuat sebuah alternatif lain yang ditujukan untuk mengantisipasi dan memudahkan kembali masuk ke jaringan tersebut. Pada tahap ini sudah dapat dipastikan ketika pelaku hendak masuk kembali kedalam jaringan, maka para pelaku tidak perlu bersusah payah untuk melalui tahap-tahap yang dilakukan sebelumnya untuk dapat masuk ke dalam jaringan itu kembali.

9. Denial of Service/Melumpuhkan Sistem

   Pada tahap ini pelaku sudah bisa melakukan suatu pengerusakan, pengubahan data-data yang diinginkan sehingga mampu menyebabkan jaringan sistem tersebut menjadi crash ataupun kacau. Penyerangan ini sangat sulit untuk dicegah, hal ini dikarenakan memakan habis bandwidth yang digunakan untuk suatu jaringan. Pencegahan harus melibatkan ISP yang bersangkutan.

Pada umumnya, modus dari kejahatan memasuki atau menyusup ke suatu jaringan komputer ialah dengan melakukan pencurian data-data account penting dari jaringan tersebut. Para pelaku biasanya menjebak orang lain untuk memberikan data-data account milik si korban. Modus yang digunakan pun beragam, salah satunya ialah dengan mengirimkan sebuah e-mail, SMS, dll untuk memperoleh data yang diinginkan.

Pada awalnya, aturan hukum mengenai tindak pidana memasuki atau

menyusup ke dalam suatu jaringan komputer masih bersifat umum yaitu menggunakan Kitab Undang-Undang Hukum Pidana (KUHP) Undang-Undang Telekomunikasi . Walaupun dalam Hukum Pidana dikenal suatu asas legalitas yang memuat bahwa setiap tindak pidana harus diatur dalam sebuah Undang-Undang. Namun, dalam hal ini suatu perbuatan yang tidak diatur dalam Undang-Undang tentu tidak bisa dikesampingkan begitu saja hal ini dapat dilakukan dengan penemuan hukum baru.

Seiring perkembangan zaman, maka saat ini pemerintah telah menerbitkan sebuah Undang-Undang yang mengatur secara khusus tentang tindak pidana ini yaitu Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Di dalam UU ITE ini, tindak pidana memasuki atau menyusup ke dalam suatu Jaringan Komputer diatur secara khusus di dalam Pasal 30.

Dalam Pasal 30 ayat 2, menjelaskan bahwa " setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik."[9] Berdasarkan penjelasan pasal tersebut kejahatan yang dilakukan para pelaku yaitu dengan modus operandi sebagai berikut : "Seseorang yang dengan sengaja dan dengan suatu cara yang tidak sah atau melawan hukum memasuki jaringan komputer milik orang lain tanpa seizin pemilik yang bersangkutan guna memperoleh, merusak, atau mencuri data milik orang lain. Perbuatan para pelaku dilakukan dengan modus operandi yaitu dengan cara menerobos atau membobol sistem pengamanan jaringan komputer yang ada untuk mendapatkan data-data yang diinginkan guna melancarkan aksi kejahatannya.

Dalam Pasal 30 ayat 3 menyatakan bahwa "setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan".[10] seseorang yang dengan sengaja mengakses komputer atau sistem elektronik dengan cara melanggar, menerobos, melampaui, atau menjebol sistem pengamanan yang dimiliki oleh si pemilik/user. Hal ini dilakukan para pelaku

[9] Pasal 30 ayat (2) Undang-Undang No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

[10] *Ibid*, Pasal 30 ayat (3)

untuk memperoleh keuntungan sendiri baik secara financial atau bahkan untuk memenuhi kepuasan tersendiri dengan cara merusak jaringan komputer dan sejenisnya dengan cara menguasai secara keseluruhan sistem jaringan tersebut. Sistem pengamanan yang dimaksud dalam pasal ini ialah sistem yang membatasi akses komputer untuk masuk kedalam suatu jaringan komputer melalui tahap-tahapan yang telah dibuat sebelumnya pada jaringan komputer tersebut.

2. Upaya Penanggulangan Memasuki atau Menyusup kedalam Suatu Jaringan Komputer Secara Tidak Sah dalam Tinjauan Kriminologi

Kriminologi adalah ilmu yang mempelajari tentang kejahatan. Menurut para ahli hukum memberikan definisi kriminologi di antaranya:

a. Bonger memberikan definisi kriminologi sebagai ilmu pengetahuan yang bertujuan menyelidiki gejala kejahatan seluas-luasnya.[11]

b. Sutherland merumuskan kriminologi sebagai keseluruhan ilmu pengetahuan yang bertalian dengan perbuatan jahat sebagai segala sosial.[12]

c. Mulyono memberikan definisi kriminologi sebagai ilmu pengetahuan yang memperlajari kejahatan sebagai masalah manusia.[13]

Tindak pidana terhadap kejahatan memasuki atau menyusup kedalam suatu jaringan komputer yang secara tidak sah telah menimbulkan korban yang tidak sedikit jumlahnya. Maka tindakan atau perbuatan tersebut merupakan perbuatan yang melanggar hukum, karena memiliki unsur-unsur dimana adanya korban-korban yang dirugikan. Sehingga mereka memiliki keinginan bisa mengetahui lebih luas untuk tidak menjadi korban kembali. Hal yang sekarang perlu dibuat adalah melaksanakan upaya penanggulangan terhadap adanya kemungkinan-kemungkinan terjadi kembali yang merugikan kita sebagai pelaku

[11] Santoso Topo dan Eva Achjani Zulfa, *Kriminologi,* Rajawali Pers, Jakarta: 2009, hal 9
[12] *Ibid,* hal *10*
[13] *Ibid,* hal 12

kejahatan yang memasuki atau menyusup kedalam suatu jaringan komputer secara tidak sah.

Upaya penanggulangan kejahatan adalah suatu usaha untuk menanggulangi kejahatan melalui penegakan hukum pidana yang rasional yaitu memenuhi rasa keadilan dan daya guna. Tindak pidana memasuki atau menyusup kedalam suatu jaringan komputer secara tidak sah perlu dilakukan upaya penanggulangan seperti:

a. Upaya Preventif

Penanggulangan kejahatan secara preventif dilakukan untuk mencegah terjadinya atau timbulnya kejahatan yang pertama kali. Jadi didalam upaya preventif itu adalah bagaimana kita menciptakan suatu kondisi seperti faktor ekonomi, lingkungan, juga kebiasaan masyarakat yang menjadi suatu daya dinamika dalam pembentukan dan bukan sebaliknya seperti menimbulkan keributan-keributan sosial yang mendong timbulnya perilaku menyimpang serta bagaimana untuk menumbuhkan kesadaran dan partisipasi masyarakat bahwa kedamaian dan disiplin merupakan tanggung jawab bersama.

Kebijakan kriminalisasi merupakan bagian dari kebijakan kriminal (criminal policy) dengan menggunakan sarana hukum pidana (penal), dan oleh karena itu termasuk bagian dari "kebijakan hukum pidana" (penal policy).[14] Metode untuk mengurangi frekuensi dari kejahatan yaitu:

1. Metode untuk mengurangi pengulangan dari kejahatan Yakni suatu cara yang ditujukan kepada pengurangan jumlah residivis (pengulangan kejahatan) dengan suatu pembinaan yang dilakukan secara konseptual.
2. Metode untuk mencegah kejahatan pertama kali (the first crime) Yakni satu cara yang ditujukan untk mencegah terjadinya kejahatan yang pertama kali (the first crime) yang akan dilakukan oleh seseorang dan metode ini juga dikenal sebagai metode preventif (prevention).[15]

[14] Suhariyanto Budi, *Tindak Pidana Teknologi Informasi (Cybercrime)*, PT Rajagrafindo Persada, Depok: 2012, hal31.
[15] https://core.ac.uk/download/pdf/25491441.pdf

Upaya penanggulangan kejahatan "Non Penal" bersifat preventif (Pencegahan) sebelum kejahatan terjadi.[16] Adapun upaya penanggulangan secara non penal yaitu:

a. Melakukan Konfigurasi yang Aman

   Sudah pasti hal ini mutlak Anda lakukan.Demi menjaga keamanan, paling tidak Anda harus mengaplikasikan tiga program, yaitu antivirus, antispyware, dan firewall.

b. Melindungi Identitas

   Jangan pernah memberitahukan identitas kepada siapapun seperti nomor rekening, nomor kartu penduduk, dan lain-lain karena dapat disalah gunakan.

c. Melindungi Account

   Setiap kata sandi sebaiknya gunakan kombinasi antara huruf,angka serta simbol. Hal ini agar tidak mudah diketahui dan mencegah dibajak.

b. Upaya Represif

   Upaya represif merupakan suatu cara upaya penanggulangan kejahatan menurut rancangan yang ditempuh setelah terjadinya kejahatan. Penanggulangan dengan upaya represif dilakukan untuk menyadarkan para pelaku untuk memperbaiki kembali perbuatan kejahatan serta menindak perbuatan yang melanggar hukum dan merugikan masyarkat. Upaya penanggulangan kejahatan "Penal" bersifat represif (pemberantasan) setelah kejahatan terjadi.[17] Upaya represif dilakukan dengan metode perlakuan (treatment) dan penghukuman (punishment) sebagai berikut:

1. Perlakuan

   Yaitu upaya pencegahan dan pemberantasan terhadap pelaku kejahatan agar tidak melakukan yang lebih buruk kedepannya.

2. Penghukuman

   Bagi pelanggar hukum yang tidak dapat untuk diberikan perlakuan (treatment), maka perlu diberikan penghukuman sesuai undang-undang hukum pidana yang berlaku karena terlalu beratnya kesalahan yang pernah dilakukan.

[16] Arief, Barda Nawawi, *Kebijikan Hukum Pidana*, Kencana Prenada Media Group, Jakarta: 2011, hal 46.

[17] *Ibid*

Adapun solusi untuk mencegah kejahatan dengan menggunakan teknologi informasi adalah sebagai berikut :[18]

1. Tidak akan ada tempat perlindungan yang aman bagi mereka yang menyalahkan teknologi informasi.
2. Sistem hukum harus melindungi kerahasiaan, integritas, dan keberadaan data dan sistem dari perbuatan yang tidak sah dan menjamin bahwa penyalahgunaan yang serius harus dipidana.
3. Sistem hukum harus mengizinkan perlindungan dan akses cepat terhadap data elektronik, yang sering kali kritis bagi sukses nya penyidikan kejahatan
4. Untuk kepentingan praktis, sistem informasi dan telekomunikasi harus di desain untuk membantu mencengah dan mendeteksi penyalahgunaan jaringan, dan harus memfasilitasi pencarian penjahat dan pengumpulan bukti.

A. KESIMPULAN

1. Modus operandi kejahatan memasuki atau menyusup kedalam suatu jaringan komputer secara tidak sah adalah tentang yang bisa merugikan masyarakat dan pemilik sistem jaringan komputer yang di akses tersebut, yaitu ***Unauthorized acces to computer system and service***, kejahatan ini semakin marak dengan berkembangnya teknologi internet. Adapun modus yang dilakukan ialah dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu,ada juga yang melakukan hanya karena merasa tertantangan untuk mencoba kehaliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Tindakan ini pada umumnya di lakukan secara tidak sah dan atau tanpa sepengatahuan dari pemilik sistem jaringan komputer yang di akses.

2. Upaya penanggulangan kejahatan memasuki atau menyusup kedalam suatu jaringan komputer secara tidak sah adalah upaya preventif yaitu, penanggulangan kejahatan secara preventif dilakukan untuk mencegah terjadinya atau timbulnya kejahatan yang pertama kali. Jadi didalam upaya preventif itu adalah bagaimana kita menciptakan suatu kondisi seperti faktor ekonomi, lingkungan, juga kebiasaan masyarakat yang menjadi suatu daya dinamika dalam pembentukan dan bukan sebaliknya seperti menimbulkan keributan-

[18] Maskun, *Ibid,* Hal : 59

keributan sosial yang mendong timbulnya perilaku menyimpang serta bagaimana untuk menumbuhkan kesadaran dan partisipasi masyarakat bahwa kedamaian dan disiplin merupakan tanggung jawab bersama. upaya represif yaitu, suatu cara upaya penanggulangan kejahatan menurut rancangan yang ditempuh setelah terjadinya kejahatan. Penanggulangan dengan upaya represif dilakukan untuk menyadarkan para pelaku untuk memperbaiki kembali perbuatan kejahatan serta menindak perbuatan yang melanggar hukum dan merugikan masyarakat.

B. Saran

1. Tindakan kejahatan yang memasuki atau menyusup kedalam suatu jaringan komputer secara tidak sah sangat merugikan banyak pihak, sehingga pemerintah serta peran masyarakat perlu lebih serius dalam menangani kasus ini sehingga dengan mempelajari banyak modus-modus yang telah dilakukan oleh banyak pelaku kejahatan ini mampu diatas dengan baik.

   Perlu adanya sosialisasi yang dilakukan secara berkesinambungan dalam rangka untuk memberikan wawasan dan pengetahuan kepada masyarakat tentang tindakan-tindakan antisipasi yang memungkinkan untuk mengurangi kejahatan cyber crime di dunia teknologi sehingga dengan adanya kemampuan tersebut maka masyarakat mampu menjadi berperan aktif dalam partisipasinya untuk memberantas tindakan kejahatan memasuki atau menyusup kedalam suatu jaringan komputer secara tidak sah.

DAFTAR PUSTAKA

A. BUKU

Afrianto Irawan, Setiawan Eko Budi, *Kajian Virtual Privat Network (VPN) Sebagai System Pengamanan Data Pada Jaringan Komputer,* Majalah Ilmiah UNIKOM

Maskun, *Kejahata Siber Cyber Crime Suatu Pengantar* , Kencana, jakarta, 2013, Hal 51

Widodo, *Perspektif Hukum Pidana dan Kebijakan Pemidanaan,* Aswaja Pressindo, Yogyakarta: 2013, hal 94

Topo Santosom Eva Achjani, *Kriminologi,* Rajawali Pers, Jakarta: 2009, Hal 9

Suhariyanto, Budi, *Tindak Pidana Teknologi Informasi (Cyber Crime),* PT RajaGrafindo Persada, Jakarta: 2012, Hal 31

Arief, Barda Nawawi, Kebijakan Hukum Pidana, Kencana Prenada Media Group, Jakarta:2011, Hal 46

B. Peraturan Perundang-Undangan

Undang-undang No.11 Tahun 2008 Tentang Memasuki Atau Menyusup Kedalam Suatu Jaringan Komputer Secara Tidak Sah

C. Jurnal/Artikel

Surat Kabar Compas, 11 Agustus Tahun 1999

Desy Setyowati, Serangan Cyber ke Indonesia Capai 12,9 juta Paling Banyak di Rusia, Katadana, 2019

Nur Khalimatus Sa'diyah, *Modus Operandi Tindak Pidana Craker Menurut Undang-Undang Informasi Dan Transaksi Elektronik,* Jurnal Fakultas Hukum Universitas Wijaya Kusuma, Surabaya: Vol.XVII, No.2 Tahun 2012 Edisi Mei, Hal 83

D. Situs Web

http://www.fbi.org

https://core.ac.uk/download/pdf/2549 1441.pdf