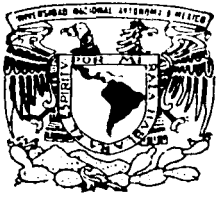
00721
197



UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE DERECHO

SEMINARIO DE DERECHO PENAL

INTRUSION CIBERNETICA (HACKING), CONDUCTA QUE DEBE SER TIPIFICADA EN NUESTRO CODIGO PENAL FEDERAL COMO DELITO TRANSNACIONAL.

T E S I S

QUE PARA OBTENER EL TITULO DE:

LICENCIADO EN DERECHO

P R E S E N T A :

CORTES RAMIREZ GELACIO

ASESOR: LICENCIADO ROBERTO REYES VELASQUEZ

MEXICO, D. F. 2003

9

PAGINACION DISCONTINUA

FACULTAD DE DERECHO
SEMINARIO DE DERECHO PENAL

OFICIO INTERNO FDER/140/SP/10/02
ASUNTO: APROBACION DE TESIS

DIRECTOR GENERAL DE LA ADMINISTRACION
ESCOLAR DE LA U.N.A.M.
P R E S E N T E.

El alumno CORTES RAMIREZ GELACIO, ha elaborado en este Seminario a mi cargo y bajo la dirección del LIC. ROBERTO REYES VELAZQUEZ, la tesis profesional intitulada "INTRUSION CIBERNETICA (HACKING), CONDUCTA QUE DEBE SER TIPIFICADA EN NUESTRO CODIGO PENAL FEDERAL COMO DELITO TRANSNACIONAL", que presentará como trabajo recepcional para obtener el título de Licenciado en Derecho.

El profesor LIC. ROBERTO REYES VELAZQUEZ, en su calidad de asesor, nos comunica que el trabajo ha sido concluido satisfactoriamente, que reúne los requisitos reglamentarios y académicos, y que lo aprueba para su presentación en examen profesional.

Por lo anterior, comunico a usted que la tesis "INTRUSION CIBERNETICA (HACKING), CONDUCTA QUE DEBE SER TIPIFICADA EN NUESTRO CODIGO PENAL FEDERAL COMO DELITO TRANSNACIONAL" puede imprimirse, para ser sometida a la consideración del H. Jurado que ha de examinar al alumno CORTES RAMIREZ GELACIO.

En la sesión del día 3 de febrero de 1998, el Consejo de Directores de Seminario acordó incluir en el oficio de aprobación la siguiente leyenda:

"El interesado deberá iniciar el trámite para su titulación dentro de los seis meses siguientes (contados de día a día) a aquél en que le sea entregado el presente oficio, en el entendido de que transcurrido dicho lapso sin haberlo hecho, caducará la autorización que ahora se le concede para someter su tesis a examen profesional, misma autorización que no podrá otorgarse nuevamente sino en el caso de que el trabajo recepcional conserve su actualidad y siempre que la oportuna iniciación del trámite para la celebración del examen haya sido impedida por circunstancia grave, todo lo cual calificará la Secretaría General de la Facultad"

A T E N T A M E N T E.
"POR MI RAZA HABLARA EL ESPIRITU"
Cd. Universitaria, D. F., 14 de octubre 2002

DR. LUIS FERNANDEZ DOBLADO.
DIRECTOR DEL SEMINARIO DE DERECHO PENAL

LFD/ipg.

6

A MIS PADRES:

SR. Gelacio Cortés Burgos y
Sra. Alvina Ramírez Bolaños.
Pilares de mi existencia, como un tributo a su
Esfuerzo y enseñanza.

A MI HERMANA:

Mónica Cortés Ramírez,
Por su gran apoyo.

A MIS ABUELOS Y TIOS:

Por sus consejos, apoyo y
noble ejemplo.

AL SEÑOR SANTIAGO VELÁZQUEZ Y A LA SEÑORA VIRGINIA RAMÍREZ:

Por su valioso apoyo para la realización
de la presente tesis.

INDICE.

INTRODUCCIÓN.

CAPÍTULO 1. MARCO CONCEPTUAL.

CAPÍTULO 2. PROBLEMA.

2.1.- LAS FORMAS DE ACTUACIÓN DEL INTRUSO CIBERNÉTICO, NO SOLOCAUSAN DAÑO A LOS BIENES MATERIALES, SINO QUE ORIGINAN UN PELIGRO INMINENTE Y GRAVE QUE PRODUCE INQUIETUD U

CAPITILO III. SOLUCIÓN AL PROBREMA.

CAPITULO IV. DEMOSTRACIÓN DE LA SOLUCIÓN.

INTRODUCCIÓN.

El principal objetivo de esta tesis, es el de mostrar la existencia de un tipo penal novedoso, así como el mostrar que no existe regulación en nuestro derecho positivo, aunque cabe mencionar que existen esfuerzos aunque no son suficientes, esto es porque el tema es novedoso y no existe mucha investigación, así como la información necesaria.

También se dará una posible solución a este tipo de delito, esto con la finalidad de poder combatirlo, ya sea complementando la ley con esta investigación o tomándola en cuenta para hacer más eficaz nuestro ordenamiento jurídico y así no estar en desventaja ante esta agresión.

En esta tesis no se profundizará en la manera de cómo operan, pero si se proveerán algunas cuestiones para entender la manera de operar de estos delincuentes.

Al ser este tema novedoso, tiene como consecuencia algunas dificultades para realizarlo, tales como que no existe bibliografía en español y que ninguno de estos libros es de autores mexicanos, motivo por el cual necesite realizar una traducción del idioma ingles al español, ya que norte América es un país adelantado en este tema y también porque el idioma ingles es tomado como el idioma universal.

Otra dificultad es que la mayoría de las consultas son en páginas de internet, siendo como todos sabemos volátiles, es decir, que después de un cierto tiempo ya no estan disponibles. También en algunas páginas se dificulta su acceso, principalmente a las referentes al de la agencia federal de investigación de Estados Unidos de Norte América (F.B.I.), ya que su acceso es restringido y aparte codificado y rastreado por ser sospechoso de terrorismo.

Otra dificultad, es que al ingresar a las mismas páginas de los intrusos cibernéticos, estas engañan y pueden leer toda la información que se tenga en el disco duro o poner páginas que en su mayoría contienen sexo, esto ultimo es con la finalidad de distraer para lograr leer todo lo que contenga la computadora, también a la hora de estar en una página hacker, en muchas ocasiones usan ganchos para que el usuario cometa robos, y lo peor es que muchas veces ni cuenta se dan, también se corre el peligro de ser infectado con un virus.

La tesis cuenta con cuatro capítulos, dándose en el capítulo primero las definiciones de intrusión cibernética, intruso cibernético (hacker), delito, dolo, tratado internacional, etcétera; proporcionándose en ésta tesis los diferentes nombres que recibe el intruso cibernético de acuerdo a sus diferentes conductas, así como los diferentes programas de cómputo que utiliza para engañar.

En el capítulo segundo se describe la intrusión cibernética que es la conducta del sujeto activo (hacker) así como la manera de operar del intruso cibernético, demostrándose así la necesidad que se tiene para regular esta conducta dentro de nuestro derecho positivo, a su ves parecería que con este delito se estuviera desalentando a las personas para que no utilicen el internet, pero no es así, es solo para prevenir el posible delito y para dar a los usuarios de internet una protección jurídica por si son victimas de este delito.

En el capítulo tercero se proporciona un proyecto de ley, la cual esta basada en las diferentes maneras y formas de actuar del intruso cibernético dados en el capítulo segundo.

En el mismo capítulo tercero se dan unas adiciones que se necesitan realizar al reglamento de la ley orgánica de la Procuraduría General de la República, ya que este delito al ser federal es a esta institución a quien compete la persecución de este delito.

En el capítulo cuarto se trata el de derecho comparado, siendo necesario para poder de mostrar la necesidad de regular esta conducta delictiva. Dentro de este parte se dan las legislaciones de los países que van como punteros en esta materia, siendo estos en América latina; Estados Unidos de Norte América, quien con el cyberterrorismo y el terrorismo sufrido el once de septiembre del dos mil uno, se ha intensificado y por lo tanto se ha hecho más estricto el uso de internet: Argentina, quien después de Estados Unidos, es el país más avanzado en este tema.

Con este capítulo cuarto de reafirma la necesidad de regular la conducta del intruso cibernético dentro de nuestro derecho, así como celebrar tratados internacionales con la finalidad de que todos o la mayoría de los Estados cooperen para facilitar la detección, persecución y aseguramiento del intruso cibernético, ya que al cometerse este delito a través del internet, puede cometerse desde y para cualquier parte del mundo.

Esta tesis cuenta con conclusiones y con un soporte de la investigación de este tema.

Finalmente cuenta con un anexo, el cual tiene la función de mostrar las diversas noticias de estos delincuentes y los diferentes proyectos de leyes que se están dando para combatir esta conducta.

Por último solo espero que la información que contiene esta tesis sea de utilidad para hacer, como lo mencioné al inicio, eficaz la ley para poder combatir esta conducta delictiva que en un determinado momento puede ser igual o más peligrosa que cualquier otro delito.

CAPITULO 1. MARCO CONCEPTUAL

1.1.- DEFINICIÓN DE HACKER.

"Junto a los avances de la informática y las comunicaciones en los últimos años, ha surgido una hueste de apasionados de estas tecnologías, que armados con sus ordenadores y conexiones a redes como Internet, ha logrado humillar a instituciones tan potencialmente seguras como el Pentágono y la NASA. La notoriedad de sus hazañas, su juventud y la capacidad de dejar en evidencia a instituciones muy poderosas, les hace aparecer ante la opinión pública rodeados de un halo de romanticismo. Pero, ¿quiénes son?, ¿son peligrosos para la sociedad?, ¿deben ser perseguidos?

Podemos encontrarnos con diferentes términos para definir a estos personajes:

- Cracker.- Es un término acuñado por los hackers hacia 1985; los cracker forman pequeños grupos secretos y privados que se adentran dentro del terreno de lo ilegal, que tienen que ver muy poco con la cultura abierta que se describe en el mundo de los intrusos cibernéticos.

  Todos los intrusos cibernéticos tienen habilidades de sobra para convertirse en crackers que han resistido la tentación y se mantienen dentro de la legalidad, pero cuando un intruso cibernético responde al llamado de su lado oscuro se convierte en un cracker o en un dark side hacker.

Los crackers son muy reconocidos por derribar cualquier sistema de seguridad, lo cual los eleva a ser expertos en cualquier sistema de seguridad.

- Samurai.- Es un intruso cibernético que crackea amparado por la ley y/o la razón, normalmente es alguien contratado para investigar fallos de seguridad, que investiga casos de derechos de privacidad y que esta

amparado por la primera enmienda estadounidense o cualquier otra razón de peso que legitima semejantes acciones.

- Warez doodz.- Una parte de los ángeles caídos se refieren a sí mismos de esta manera por que se dedican a obtener, desproteger y distribuir copias ilegales de sofweare's como si fueran originales (ware) .
- Phreakers.-Son aquellos que rompen y hacen un uso ilegal de las redes telefónicas. Durante un tiempo fue una actividad considerada respetable entre los hackers, pero este carácter aprobatorio se ha ido perdiendo.
- Formas de llamarles a los intrusos cibernéticos de acuerdo a su actividad:
  - ✓ Intruso cibernético experto en virus. El cual es el encargado de crear, enviar a citios web, correos u otros lugares de la red, estos virus, también se clasifican desde los inofensivos hasta los muy dañosos.
  - ✓ Intruso cibernético terrorista (cyber-terrorism), es el encargado de crear pánico en la red o el de propiciar en determinados casos malos entendidos entre Estados, como ocurrio recientemente en Estados Unidos de Norte América, esta actividad es tan poderosa que incluso se puede llegar a tomar el control de un avión, y pilotearlos como si fueran en el mismo avión.
  - ✓ Intruso cibernético experto en fraudes con tarjetas de crédito (cyber fraud the credit card), estos hackers expertos en obenet y usar los números confidenciales de tarjetas de crédito para usarlo en compras, traspasos, cancelación, de cuentas bancarias, las cuales el titular de las tarjetas no las ha realizado. A estos hackers se les facilita el ilicito porque en internet la mayoria de los negocios o compras son realizados con tarjetos de crédito.

Pirata informático.- Es el intruso cibernético dedicado a la copia y distribución de softweare iligal, tanto comercial como crackeado, registrado, etc.; también elimina las protecciones del softweare.

La definición otorgada al intruso cibernético (hacker) es aquel que entra ilegalmente a los sistemas, roba información y provoca caos en el sistema.

¿Por qué?, Hay varias respuestas, por diversión, por venganza, por pertenecer o por sentir la adrenalina correr por sus venas. La forma más común en la que se encuentran en la red es presentando softweare y documentos para atacar. Estos ataques pueden ser entradas ilegales, adquisición de pastword de sistemas y adquisición de softweare, siendo los juegos los blancos preferidos. También es común que entren a nuestra computadora para ver que hacemos, que tenemos, etc., este truco es muy usado por sitios que venden direcciones de e-mail y, por medio de galletas que reciben la información del usuario, su sistema operativo, etc. Las galletas son pequeños programas que envía un servidor para saber quien esta en su sistema.

El intruso cibernético por lo general, lo que hace es molestar a otros usuarios de la red, o incluso divertirse con los diferentes usuarios.

¿Cómo lo hace?, existen diversos ataques para realizar la intrusión cibernética en la computadora de la victima; por lo general se aprovechan de la ignorancia de los usuarios en la red, siendo una presa fácil para éstas personas. Los intrusos se consideran así mismos como una elite por sus méritos que se basan en la habilidad, aunque suelen recibir amablemente a nuevos miembros"[1].

El término intruso cibernético (*hacker*), por ejemplo, se utiliza normalmente para identificar a los que únicamente acceden a un sistema protegido como si se tratara de un reto personal, sin intentar causar daños. Los *crackers*, en cambio, tienen como principal objetivo producir daños que en muchos casos suponen un problema de extrema gravedad para el administrador del sistema. En cuanto a los piratas, su actividad se centra en la obtención de información confidencial y *software* de manera ilícita.

[1] ¿Qué es un hacker? (consulta en internet: bbs.seker.es.html.). México, 07/07/2001, 11:25 A.M.

Es muy difícil establecer perfiles de estas personas, porque salvo en los casos en que han saltado a la luz pública como resultado de sus actividades, en su conjunto forman un círculo cerrado e impenetrable. Una aproximación podría ser la de un joven, bastante inteligente, con necesidad de notoriedad, inclinaciones sectarias, y en muchos casos, algo de inadaptación social. Su principal motivación es la de acceder a sistemas protegidos de forma fraudulenta, en una escala que va desde la mera constancia de su éxito, hasta la destrucción de datos, obtención de información confidencial, colapso del sistema, etc. Normalmente los objetivos más apetecibles son los sistemas relacionados con la seguridad nacional, defensa e instituciones financieras, pero ante las posibles consecuencias legales de estos actos optan por otros organismos públicos, las universidades y las empresas.

Existe una serie de grupos que tienen un carácter supranacional, y que se extiende a través de su hábitat natural: Internet. A través de este medio intercambian información y experiencias, al mismo tiempo que logran un cierto grado de organización. Esto ha disparado la alarma en algunos ámbitos gubernamentales, dado que una acción coordinada que afectará a varios sistemas estratégicos de un país puede ser igual de desestabilizadora que las actividades terroristas.

"En España tenemos ejemplos recientes, como es el caso de *Hispahack*, que realizó ataques a varios sistemas, incluidos los de algunas universidades. También se ha creado en la Guardia Civil un grupo especializado en todo tipo de delitos informáticos para identificar e investigar a estos modernos delincuentes.

En la ULL, en cambio, hasta este momento no ha existido un riesgo importante ya que, por una parte, había un gran retraso tecnológico en nuestras infraestructuras y, por otro, los sistemas formaban parte de redes que por sus características eran impermeables a dichos ataques. Pero la situación ha cambiado: la ejecución del Plan Integral de Comunicaciones ha elevado tanto

nuestras posibilidades que nos permite la integración en una única red de todos nuestros sistemas informáticos, con lo que conlleva a la hora de prestar servicios a los usuarios. Esto tiene su contrapartida, y es que el número de servicios que se ofrecen es directamente proporcional a los riesgos que se asumen, y sobre todo porque el primer enemigo al que habría que considerar podrían ser los propios usuarios.

De todas formas, el exceso de prudencia es contrario a la innovación y, por tanto, se están adoptando medidas que garanticen una cobertura suficiente: la adquisición de herramientas de *software* para la gestión de red, *firewalls* (cortafuegos, programas especializados en la protección de redes y sistemas), y *software* de auditoría; la elaboración de planes de seguridad tanto física como lógica y de las políticas correspondientes; y, por último, la mentalización de los usuarios para el correcto uso de los servicios que se prestan. De todas formas, la total seguridad nunca se podrá alcanzar, a menos que coloquemos los sistemas detrás de un muro infranqueable. Pero entonces nos encontraríamos con una red que es una auténtica autopista, pero por la que sólo circularían el correo electrónico y las páginas *web*.

Además, esto significa un incentivo para que los administradores de los sistemas y responsables de seguridad seamos mejores en nuestro trabajo, ya que cada ataque con éxito pone en evidencia nuestras deficiencias". [2]

1.2.- DEFINICIÓN DE INTRUSIÓN CIBERNÉTICA.

Es la conducta desarrollada por el sujeto activo (hacker), consistente en la entrada a un ordenador o sistema de cómputo sin autorización, previo el derrumbe del sistema de seguridad que se tenga, con la finalidad de modificar, sustraer o destruir información.

[2] Actividad del hacker (consulta en internet: http://mundo internet.iespana.es/) México 07/07/2001, 11:30 A.M.

1.3. DEFINICIÓN DE DOLO.

"Es mala fe, es decir, una disposición de ánimo de quien realiza cualquier acto jurídico con el propósito de obtener una ventaja injusta en perjuicio de alguien, que el derecho sanciona en todo caso.

En materia penal es la voluntad consciente y voluntario de cometer un acto delictivo"[3]

La definición legal la encontramos en el artículo 9 fracción I del código penal federal mexicano diciendo:

"Art. 9.- Obra dolosamente el que, conociendo los elementos del tipo penal, o previendo como posible el resultado típico, quiere o acepta la realización del hecho descrito por la ley".[4]

1.4. TEORIA DEL DELITO

Previo al desarrollo de este apartado, resulta indispensable definir al derecho penal, ya que el delito es parte integrante de esta materia.

Para el jurista Luis Jiménez de Asúa en su obra la ley y el delito expone que el derecho penal es el "conjunto de normas y disposiciones jurídicas que regulan el ejercicio del poder sancionador y preventivo del Estado, estableciendo el concepto de delito como presupuesto de la acción estatal, así como la responsabilidad del sujeto activo y asociado a la infracción de la norma una pena finalista o una medida aseguradora".[5]

En mi opinión el derecho penal es el conjunto de normas jurídicas que regula el actuar de las personas mediante la amenaza de una sanción con la finalidad de mantener un orden y así lograr la convivencia en sociedad de las personas que la integran.

---

[3] PINA VARA, Rafael de, "Diccionario de derecho", 26ed., editorial, Porrúa, S.A., 1998.
[4] Código Penal Federal, edit. Sista, S.A. de C.V., México, 2002, p. 3.
[5] JIMÉNEZ DE ASÚA, Luis, "la ley y el delito", edit. Sudamericana, Buenos Aires, 1990, p.18.

Una vez definido el derecho penal, es necesario ubicar esta rama del derecho dentro del mundo jurídico. Para ello recordemos que el derecho se divide en tres grandes grupos: el público, privado y social. El derecho penal es parte integrante del derecho público ya que se destaca la posición del Estado como entidad soberana investida de poder público, porque tiene la característica de que en casos de incumplimiento se de una sanción, la cual no es otra cosa que la pena estipulada en la norma jurídica impuesta por el Estado, para salvaguardar los intereses de los particulares; es decir que el Estado es el único capaz de crear normas que definan delitos y sus respectivas sanciones aplicadas por sus órganos encargados de administrar justicia.

El derecho público se divide en interno y externo. El interno también llamado derecho nacional, esta constituido por el conjunto de disposiciones que integran a un determinado Estado; es decir, de una nación particularmente considerada como por ejemplo Francia, México, etc. El derecho externo, llamado internacional, es aquel que se aplica a las relaciones de Estado a Estado como entidades soberanas, estableciendo además la forma de llevar al cabo la aplicación extraterritorial de las leyes dictadas por un Estado, teniendo como fuente principal a los tratados internacionales.

Una vez ubicado el derecho penal, corresponde el desarrollo de la teoría del delito, comenzando por definir que es el delito, ante esta interrogante, el doctrinario Raúl Carrancá y Trujillo, menciona que "es siempre una conducta (acto u omisión) reprobado o rechazado (sancionado). La reprobación opera mediante la amenaza de una pena (por las leyes penales). No es necesario que la conducta tenga eficaz secuencia en la pena, basta con que ésta amenace, es decir, se anuncie como la consecuencia misma, legalmente necesaria".[6]

"La definición más aceptada es la que nos menciona Francesco Carrará diciendo que es la infracción de la ley del estado, promulgada para proteger la

[6] CFR. CARRANCÁ Y TRUJILLO, Raúl/ Raúl Carrancá y Rivas, "Derecho penal mexicano, parte general", 19 ed., edit. Porrúa S.A., 1997, P.22.

seguridad de los ciudadanos, resultado de un acto externo del hombre ya sea positivo o negativo, moralmente imputable y políticamente dañoso."[7]

EL código penal federal mexicano nos da una definición de delito en su artículo 7 diciendo que es "el acto u omisión que sancionan las leyes penales".[8]

Para que un delito llegue a existir, es necesario que tenga lo que se ha denominado elementos del delito, éstos se han dividido en positivos y negativos, los primeros son llamados así porque, de darse todos, surgirá el delito y los segundos son porque teniendo alguno, no nace el delito. Estos elementos son:

- "El primer elemento positivo del delito es la conducta, esta es el actuar del hombre dirigido a un fin o propósito. Su aspecto negativo es la ausencia de conducta, esta se presenta cuando en torno al obrar del sujeto activo se da una transformación en el mundo externo, sin que para ello intervenga la voluntad del mismo; es decir, cambia el mundo externo pero no puede serle atribuido al sujeto activo. La conducta es dable solo en una de sus dos formas que se presente, es decir, por acción o por omisión. La acción, se da mediante un hacer positivo del hombre y se manifiesta por la infracción a normas de carácter prohibitivo. La omisión, se da por la inactividad del hombre, es decir, mediante un comportamiento de abstinencia. La omisión, puede ser propia e impropia, la primera basta la inactividad para que se llegue a la consumación de un delito, por ejemplo el abandono de hogar. La segunda, es también llamada de omisión por omisión, es dable cuando se infringen normas de carácter dispositivo y prohibitivo, en la circunstancia de que la inactividad es determinante para que se de el delito, por ejemplo en la muerte por inanición.

- El segundo elemento positivo del delito es la tipicidad, la cual se ha definido como el encuadramiento de la conducta a la descripción del tipo penal. Su

[7] MANCILLA OVANDO, Jorge A., " Teoría legalista del delito", edit. Porrúa, S.A., 1989, PP. 48-50.
[8] Código Penal Federal, op. Cit, p.6.

aspecto negativo es la atipicidad que es la falta de encuadramiento de la conducta al tipo penal. La tipicidad esta muy ligada a la constitución, ya que se contempla una garantía en el artículo 14 párrafo tercero, esta es el principio de la exacta aplicación de la ley, que también se le conoce con el nombre de principio de reserva y que se identifica a su vez con la máxima nullum crimen nulla poena sine lege.

- El tercer elemento positivo del delito es la antijuridicidad, la cual es, la conducta realizada por el agente contraria a la ley o a las exigencias que esta marca. Su aspecto negativo son las causas de licitud o de justificación, que se identifican con la juridicidad, es decir, con aquello que esta conforme a derecho, siendo las hipótesis previstas por la ley que impiden el nacimiento de la antijuridicidad.

- El cuarto elemento positivo del delito es la imputabilidad que se define como la capacidad de entender y querer en el ámbito del derecho penal: es el mínimo de salud mental para que el estado se encuentre en la posibilidad de atribuir responsabilidad de carácter penal a quien ha realizado una determinada conducta. Su aspecto negativo es la inimputabilidad, es decir, la falta de salud mental exigible para que le Estado pueda atribuir responsabilidad de carácter penal.

- El quinto elemento positivo del delito es la culpabilidad, siendo ésta, el nexo intelectual y emocional que liga al sujeto con su acto, es decir un desprecio que se hace al ordenamiento jurídico, así como a sus prohibiciones. Su aspecto negativo es la inculpabilidad, presentándose cuando se hace inexistente el delito al operar excluyentes como el estado de necesidad, miedo grave, obediencia jerárquica y caso fortuito.

- El sexto elemento positivo del delito son las condiciones objetivas de punibilidad, es decir condiciones que determinados tipos penales los

requieren. Cabe mencionar que su aspecto negativo, es decir la falta de condiciones objetivas de punibilidad, el 99% de los delitos son así.

- El séptimo elemento positivo del delito es la punibilidad, la cual es el merecimiento a la aplicación de una sanción desprendiéndose como consecuencia a la realización de una conducta delictiva. Es decir estar sancionando a el delito por las leyes penales. Su aspecto negativo son las excusas absolutorias, éstas constituyen la punibilidad, siendo las hipótesis previstas por la ley en los que el Estado por política criminal decide no imponer sanción, por ejemplo cuando por violación se permite el aborto".[9]

La teoría del delito ha elaborado una clasificación del mismo, teniendo como finalidad, saber como se persigue, cuantos sujetos intervienen en el delito, si es federal o local, etcétera.

La clasificación es:

" Por su gravedad los delitos se clasifican en:

- Faltas.- son infracciones a los reglamentos, como por ejemplo a los de tránsito que caen en el ámbito administrativo y que no constituyen delito. Otro ejemplo lo constituyen también los reglamentos internos de las dependencias o empresas.
- Delitos.- es la infracción penal por excelencia, en virtud de que en el momento en que se manifiesta, ya nos ubicamos en el campo del derecho penal. Estos obedecen a la exigencia que de manera social se presenta cotidianamente y por lo mismo pueden cambiar según el momento y lugar.
- Crimenes.- son aquellos que afectan intereses de validez universal o que son válidos intrincicamente, son validos en sí mismos.

Atendiendo a la conducta del sujeto activo, los delitos se clasifican en:

[9] CFR. MANCILLA OVANDO, Jorge A. "Teoría legalista del delito", op cit p.7, pp.35-47.

- De acción.- son aquellos que implican, un hacer positivo del agente que propicia la violación a normas de carácter prohibitivas.
- De omision.- son aquellos que implican una inactividad, es decir un no hacer. La omisión de subdivide en:

--Omisión propia, siendo aquella que se da por el no hacer, solo infringen normas de carácter dispositivo y el simple obrar negativo basta para que se colme la conducta.

--Omisión impropia, también llamada omisión por omisión, esta infringe normas de carácter dispositivo y prohibitivo, con la circunstancia de que el no hacer es inicial, pero este se convierte en factor determinante para que se de un cambio en el mundo externo y surja la violación a la norma prohibitiva.

Atendiendo al número de sujetos, los delitos se clasifican en:

- Unisubjetivos porque basta un solo sujeto para su comisión.
- Plurisubjetivos; cuando necesariamente se requiere de la intervención de dos o más sujetos para su comisión.

Atendiendo al número de actos, los delitos se clasifican en:

- Unisubsistente, en el cual basta un solo acto para la integración del delito.
- Plurisubsistente, el cual para su consumación necesita de varios actos.

Atendiendo a su resultado, los delitos se clasifican:

- Formales, también conocidos como delito de preferente conducta , son aquellos en que la conducta por si misma estimase suficiente para que se colme el tipo sin ser susceptible de que se de un cambio en el mundo externo.
- Materiales, son aquellos en los que además de la conducta se requiere que se presente un cambio en el mundo externo.

Atendiendo al daño que produce, los delitos se clasifican en:

- Daño, siendo aquellos que para su integración requieren de una afectación de un menoscabo o disminución del bien que se proteja.
- Peligro; aquellos que nos ubican dentro de la posibilidad del menoscabo de la destrucción del bien jurídico.

Por su elemento interno o culpabilidad, los delito se clasifican en:

- Doloso, aquellos que por su naturaleza o esencia solo se pueden cometer de manera intencional, es decir aquellos que forzosamente el sujeto activo tenga como propósito su comisión.
- Culposos, los que se presentan de forma intencional, es decir cuando el sujeto no se propone su comisión.

Por su estructura, los delitos se clasifican en:

- Simples, son aquellos que dentro de su regulación protegen de manera exclusiva a un interés.
- Complejos, aquellos que dentro de su configuración protegen dos o más bienes jurídicos, en una solo descripción típica.

Por su factor temporal, los delitos se clasifican en:

- Instantáneos; aquellos que cuando tan luego se agota la conducta lo mismo ocurre con el bien jurídico y se obtiene la consumación respectiva.
- Continuados; aquellos que se manifiestan por una discontinuidad en su ejecución, pero con unidad de lesión, en cuanto al bien jurídico y en cuanto al propósito en cuanto al agente mismo.
- Permanentes; aquellos que surgen de momento a momento, es decir, aquellos que requieren para su consumación el transcurso de cierto lapso.

Atendiendo a su persecución, los delitos se clasifican en:

- Oficio; aquellos en los que la denuncia es presentada por cualquier persona o la noticia de que se ha cometido un delito es suficiente para que se ponga en movimiento la maquinaria del estado, tendiente a investigarlo y el resultado de la misma dará lugar o no al ejercicio de la acción penal.
- Querella.- siendo aquellos que para la intervención del Estado necesita de la decisión del ofendido, ya que no puede intervenir cualquiera no aún teniendo noticia de su comisión".[10]

1.5. DEFINICIÓN DE TIPIFICAR.

" Es el adoptar un conjunto de normas jurídicas para regular una conducta humana, presentándose cuando el Estado capta alguna conducta no regulada por el derecho penal, es decir no tipificada, éste tiene la obligación de describir esa conducta y dar su penalidad, una vez aprobada esa conducta, se convierte en una ley regulada en un ordenamiento jurídico, en este caso es en el código penal.

En el caso concreto del intruso cibernético se tiene que adoptar un conjunto de normas jurídicas para regular esta conducta y así disminuir este delito."[11]

1.6. DEFINICIÓN DE SISTEMA DE SEGURIDAD DE COMPUTO.

"Son programas para computadora (softwears) que se adquieren con la finalidad de impedir que algunas personas lleguen a entrar a un sistema de computo. Se han catalogado como filtros que impiden el paso de personas que no pertenezcan a ese sistema, es decir a extraños.Estos softwears tienen una clave especial designada, consistente por lo regular en letras y números o su combinación designados al momento de adquirir ese softwear".[12]

1.7. DEFINICIÓN DE DAÑO.

"Es la pérdida o menoscabo sufrido en el patrimonio por la falta de cumplimiento de una obligación (art. 2108 del código Civil Federal). Debe de

---

[10] CASTELLANOS TENA, Fernando, "Lineamientos elementales de derecho penal", 36 ed., edit. Porrúa, S.A., México, 1991, pp.135-146.
[11] ¿Qué es tipificar?, (consulta en internet: bbs.seker.es/aluy.html), México, 07/07/2001, 14:35 P.M.
[12] "Qué es sistema de seguridad de cómputo?, (consulta en internet: bbs.secker.es/aluy.html), México, 07/07/2001, 14:37 P.M.

entenderse esta definición en el sentido de daño material. El daño puede ser también moral.

Daño moral es aquel que afecta a la vida de una persona, a su bienestar a su honor, etc."[13]

1.8.- DEFINICIÓN DE PROPIEDAD.

La propiedad es el derecho real por excelencia. El derecho real es aquel que con relación al aprovechamiento o disposición de una cosa se tienen contra todo el mundo o en contra de un sujeto indeterminado, es decir, ese poder que se tiene sobre las cosas con un derecho absoluto de disposición y que se ejerce directamente sobre una cosa.

En el derecho romano, la propiedad se contemplaba en tres frases:

A) IUS UTENDI: es el derecho a usar el objeto.

B) IUS FRUENDI: es el derecho de aprovechar el objeto.

C) EUS ABUTENDI: es el derecho a disponer del objeto.

Esto significa que el derecho de propiedad era de forma exclusiva, absoluta y perpetua. Exclusivo, porque, solo el titular de ese derecho podía disponer del bien inmueble; absoluto, porque, nadie podía oponerse a ese derecho que tenia el titular y perpetua porque, era un derecho para siempre.

Este concepto de propiedad prevaleció por muchos años, hasta que en el código civil de 1932, cambio el concepto por que se contempla un derecho de propiedad en función social, dejando de ser el derecho de propiedad absoluto y perpetuo.

En el código civil en su articulo 830, se nos dice la definición de propiedad, diciendo que es "el derecho de gozar y disponer de un bien con las limitaciones y modalidades que fijen las leyes".[14]

---

[13] PINA VARA, Rafael de, "Diccionario de derecho", op. Cit, p.

[14] Cogido Civil Federal actualizado hasta el 10 de julio del 2002 (Consulta en internet: http://info.juridicas.unam.mx/infor/ley) México, 13:00 P.M., 28/08/ 2002.

1.9.- DEFINICIÓN DE INTERNET.

"Internet es un conjunto de redes de ordenadores u equipos físicamente unidos mediante cables que conectan puntos de todo el mundo. Estos cables se presentan en muchas formas: desde cables de red local (varisa máquinas conectadas en una oficina o campus) a cables de teléfonos convencionales, digítales y canales de fibra óptica que forman las carreteras principales. Esta gigantesca red se difumina en ocasiones porque los daños pueden transmitirse vía satélite, o a través de servicios como la telefonía celular, o porque a veces no se sabe muy bien a dónde está conectada.

Esto en cierto modo, no hay mucha diferencia entre Internet y la red telefónica que todos conocemos, dado que sus fundamentos son parecidos. Basta que cualquier cosa a la que se pueda acceder a través de algún tipo de conexión, como un ordenador personal, una base de datos en una universidad, un servicio electrónico de pago (como CompuServe), un fax o un número de teléfono, pueden ser, y de hecho forman parte de internet.

El acceso a los diferentes ordenadores y equipo que están conectados a internet puede ser público o estar limitado. Una red de cajeros automáticos o terminales de banco, por ejemplo, puede estar integrados en internet pero no ser de acceso público, aunque formen parte teórica de la red. Lo interesante es que cada vez más de estos recursos están disponibles a través de internet: fax, teléfono, radio, televisión, imágenes de satélites o cámaras de tráfico son algunos ejemplos.

En cuanto a su organización, internet no tiene en realidad una cabeza central, ni un único organismo que la regule o al que pedirle cuentas si funciona mal. Gran parte de la infraestructura es pública, de los gobiernos mundiales, organismos y universidades. Muchos grupos de trabajo laboran para que funcione correctamente y continúe evolucionando.

Otra gran parte de internet es privada, y la gestionan empresas de servicios de internet (que dan acceso) o simplemente publican contenidos"[15]

"¿Cómo funciona el internet?, este es básicamente, millones de ordenadores conectados entre sí independientes unos de otros. Para que todos estos ordenadores puedan coexistir y comunicarse entre ellos, deben ponerse de acuerdo. Con este motivo fueron creados los Protocolos, que son reglas de comunicación que han de adoptarse para ser entendido por los otros ordenadores de la red. Los dos protocolos más importantes son Protocolo de control de Transmisión y el protocolo de internet. Usualmente se trata a estos dos protocolos como si fuera uno solo. Un ordenador, si maneja estos dos protocolos, no tendrá ningún problema para se entendido por los demás ordenadores de Internet.

Todos los ordenadores que componen internet no están conectados unos con otros: solo se esta conectado con los más cercanos. Si realizas una petición de cierta información a un ordenador que se encuentra a cientos de kilómetros de donde estas tú, se accede a este ordenador a través de otros ordenadores, formando una especie de cadena. Para saber donde esta el ordenador al que quieres acceder, debes saber también donde se encuentra. Para saber donde esta se utilizan las direcciones, que son una especie de DNI de los ordenadores, que está compuesto por una combinación de números entre 0 y 255, y se utiliza para identificar a cada ordenador dentro de una red.

Una vez sabido esto, la información que hemos solicitado al ordenador lejano, nos llega a nosotros en pequeños paquetes que una vez en nuestro ordenador, se enlazan mostrándonos nuestra petición en pantalla.

En internet, los ordenadores que están conectados a la red no tienen siempre los mismos propósitos o poseen las mismas capacidades. En internet existen dos tipos de ordenadores, los clientes y los servidores.

[15] ¿Qué es internet? (consulta en internet; http: bbs.sker.es/aluy), México, 07/08/2001., 13:30 P.M.

Los servidores forman parte de un esqueleto de Internet. Un servidor es un gran ordenador encargado de atender las peticiones de otros ordenadores (por esos u nombre). Por poner un ejemplo, si se escribe en un navegador www.google.com, lo que se realiza en una petición a un servidor para que muestre la página de Google. Quien realiza la petición de la página es el cliente. También existen otro tipo de servidores, que son los ISP (proveedor de servicios en internet). Estos sevidores son los encargados de ofrecer una conexión de acceso a Internet para los ordenadores clientes y será el enlace de estos con los demás ordenadores de internet. Un ejemplo de ISP puede ser terra, es mas, wanadoo, entre otros.

Los servidores tienen un tipo de conexión a Internet que se denomina dedicada, que quiere decir que siempre está conectado a Internet. Los clientes pueden tener una conexión a internet dedicada o no dedicada. La conexión no dedicada quiere decir que la conexión es por un tiempo limitado, no permanente. Un ejemplo de conexión dedicada en clientes es cuando se posee una línea ADS, y una conexión no dedicada, una conexión vía modem.

Ahora explicaremos todo lo anterior con un ejemplo : Usted se encuentra en su casa conectado a internet vía MODEM (usa una conexión no dedicada y es un cliente) y solicita desde su navegador la visualización de una página web (la solicita a un servidor). Pues bien, su navegador genera un paquete con la dirección del servidor donde se encuentra la página que solicitó. Este paquete es enviado a su ISP, que es el encargado de enviarlo de servidor en servidor hasta su destino.

Una ves en su destino, el servidor que ha recogido la petición, genera y envía otro paquete con la información que solicitaste hasta su ISP, que es el encargado de enviárselo a usted. Una vez que su ISP lo envía a su ordenador, su navegador interpreta el paquete y se lo muestra en pantalla.

Este ejemplo resume lo que se hace todos los días cuando se entra a navegar en el internet para obtener información (muy variada), que puede ser tanto nacional o extranjera y de cualquier parte del mundo.

Visto así, internet parece una cosa fácil y sencilla, pero detrás de este proceso se encuentra la mayor infraestructura tecnológica de la era moderna, imposible de explicar en tan poco espacio". [16]

Desafortunadamente en este mundo tan fascinante se pueden realizar un gran número de delitos.

1.10.- DEFINICIÓN DE CIBERESPACIO.

" Se utiliza en la actualidad para referirse al conjunto de información digital y a la comunicación que se realiza a través de las redes, un espacio en el que casi todo lo que contiene es información Es una palabra cuyo origen esta en la ciencia ficción y hace referencia a la dimensión generada por el mundo digital. "[17]

Se entiende como toda la información contenida en el mundo cibernético. El cibernauta es el apelativo con el que se reconoce a los usuarios de la red. Este proviene de ciberespacio. "[18]

El cibernauta es el apelativo con el que se reconoce a los usuarios de la red. Este proviene de ciberespacio. Es decir, ciberespacio es toda la información que contienen el internet, siendo tanto información escrita como fotografías o conferencias y la persona que utiliza el ciberespacio es conocido como cibernauta.

1.11. DEFINICIÓN DE PERSONA.

"El vocablo persona deriva del verbo personare que en latín significa producir sonido. El vocablo persona en su aceptación común, denota al ser humano, es

---

[16] ¿Cómofuncionelinternet?(consultaeninternet:http://mundointernet.iespana.es/mundointernet/como_funciona.htm) México, 10/07/2001, 13:45 P.M.
[17] ¿Qué es ciberespacio? (consulta en internet: http: bbs.sker.es/aluy), México, 07/07/2001, 13:30 P.M.
[18] ¿Qué es ciber nauta? (consulta en internet: http: bbs.sker.es/aluy), México, 07/07/2001, 13:30 P.M.

decir, tiene igual connotación que la palabra hombre que significa individuo de la especie humana de cualquier edad o sexo.

El vocablo persona denota al ser humano dotado de libertad, capaz de realizar una conducta encaminada a determinados fines. La persona es el sujeto de derechos y obligaciones, es decir, en la medida en que las relaciones humanas interesan al derecho, la persona humana se convierte en persona en el mundo de lo jurídico como un sujeto de derechos y obligaciones"[19]

El derecho no toma al ser humano para calificarlo como persona, en toda la amplia y variada gama de fines íntimos, religiosos, éticos, sociales, económicos, políticos, etc., que el ser humano puede proponerse durante su existencia.

Al derecho sólo le interesa una porción de esa conducta del hombre, aquella parte de la conducta que el derecho toma en cuenta, para derivar de ella consecuencias jurídicas; es decir, lo que se toma en cuenta son esquemas genéricos y tipos de conducta dibujados en la norma y aplicables en principio a todos los sujetos.

El derecho a creado a la persona moral o también llamada colectiva como son las sociedades, asociaciones, etc. Se trata de un concepto elaborado por la técnica jurídica que sirve para deslindar un conjunto de cualidades requeridos por la norma, para que el agente de una cierta conducta humana, se repute capaz de derechos y obligaciones, deberes y facultades, es decir de relaciones jurídicas.

1.12.-DEFINICIÓN DE PERSONA IMPUTABLE PARA EL DERECHO PENAL.

"Es la aptitud para ser sujeto pasivo o activo de relaciones jurídicas se designa con al palabra personalidad es decir, capacidad jurídica que se desdobla en la aptitud para ser titular de derechos y obligaciones, así como tener capacidad para obrar, es decir, capacidad para dar vida a actos jurídicos.

[19] GALINDO GARFIAS, Ignacio, "Derecho civil, parte general", 14 edc., edit. Poorúa. S.A., México, 1995.

Las disposiciones que contiene las diversas leyes penales, como los códigos, solo se aplican en nuestro país a los mayores de edad que es de dieciocho años por regla general, aunque algunas entidades han reducido la edad requerida, para la responsabilidad penal a dieciséis años.

Los menores de edad están sujetos a reglas distintas, por ello cuando un menor comete un ilícito se le somete a un sistema exclusivo para jóvenes infractores.

En el distrito federal, se ha creado el consejo tutelar para menores infractores que tiene por objeto promover la readaptación de los menores mediante el estudio de su personalidad y medio social, procurando dar medidas correctivas de protección y vigilancia durante su tratamiento".[20]

1.13.- DEFINICIÓN DE IMPUTABILIDAD.

"Es la capacidad del sujeto para conocer del ilícito de su conducta y determinarse espontáneamente a esa comprensión, la inimputabilidad supone consecuentemente, la ausencia de dicha capacidad.

Lo anterior quiere decir que es la capacidad de entender y querer en el ámbito del derecho penal: es el mínimo de salud mental exigible para que el Estado se encuentre en la posibilidad de atribuir responsabilidad de carácter penal a quien ha realizado una determinada conducta. "[21]

1.14.-DEFINICIÓN DE PATRIMONIO.

"El investigador Guillermo Floris Margadant, dice que es el "conjunto de cosas que pueden ser tanto corporal como incorporales y también las deudas que correspondan a una persona. Por regla general cada persona tiene un patrimonio y cada patrimonio pertenece a una persona, sin embargo existen excepciones como son las fundaciones"[22]

---

[20] LÓPEZ BETANCOURT, Eduardo, "Introducción al derecho penal", 2ª.ed., edit. Porrúa, S.A., México, 1994, p.100.
[21] PAVON VASCONCELOS, Francisco, "Manual de derecho penal mexicano, parte general",10ª ed. Edit. Porrúa S.A., México, 1991, p.159.
[22] FLORIS MARGADANT, Guillermo," Derecho romano privado", 22ª. Edi, edit. Esfinge, S.A, de C.V, 1997, p. 531.

1.15.-DEFINICIÓN DE REFORMA.

"La palabra reforma quiere decir corregir o restaurar un precepto legal con la finalidad de hacerlo más eficaz. Por lo regular, es modificar todo un capítulo a una ley".[23]

1.16.DEFINICIÓN DE DELITO.

Delito deriva del latín delictum, del verbo delinquere, a su vez compuesto de linquere, dejar y el prefijo de, en la connotación peyorativa, se toma como linquere viam o rectam, dejar o abandonar el buen camino.

Para el doctrinario Luis Jiménez de Asúa, el delito es "el acto típicamente antijurídico culpable, sometido a condiciones objetivas de punibilidad, imputable a un hombre y sometido a una sanción penal".[24]

El código penal federal mexicano, nos da la definición legal, mencionando que es el acto u omisión que sancionan las leyes penales.

1.17.-DEFINICIÓN DE DELITO GRAVE.

Lo proporciona el articulo 194 del Código Federal de Procedimientos Penales: "Articulo 194.- Se califican como delitos graves, para todos los efectos legales, por afectar de manera importante valores fundamentales de la sociedad, los previstos en los ordenamientos legales siguientes:

I.- Del Código Penal Federal los delitos siguientes:

1)Homicidio por culpa grave, previsto en el articulo 60, párrafo tercero;

2) Traición a la patria, previsto en los artículos 123, 124, 125 y 126;

3) Espionaje, previsto en los artículos 127 y 128;

4) Terrorismo, previsto en el articulo 139, párrafo primero;

---

[23] CFr. PINA VARA, Rafael de, " Diccionario de derecho". Op cit. P.6.

[24] JIMENES DE ASÚA, Luis, "Principios de derecho penal, la ley y el delito",edit. Abelardo-perrot, Buenos Aires, 1990, P.129.

5) Sabotaje, previsto en el articulo 140, párrafo primero;

6) Los previstos en los artículos 142, párrafo segundo y 145;

7) Piratería, previsto en los artículos 146 y 147;

8) Genocidio, previsto en el articulo 149 bis;

9) Evasión de presos, previsto en los artículos 150 y 152;

10) Ataques a las vías de comunicación, previsto en los artículos 168 y 170;

11) Uso ilícito de instalaciones destinadas al tránsito aéreo, previsto en el articulo 172 bis párrafo tercero;

12) Contra la salud, previsto en los artículos 194, 195, párrafo primero, 195 bis, excepto cuando se trate de los casos previstos en las dos primeras líneas horizontales de las tablas contenidas en el apéndice i, 196 bis, 196 ter, 197, párrafo primero y 198, parte primera del párrafo tercero;

13) Corrupción de menores o incapaces, previsto en el articulo 201; y pornografía infantil, previsto en el articulo 201 bis;

14) Los previstos en el articulo 205, segundo párrafo;

15) Explotación del cuerpo de un menor de edad por medio del comercio carnal, previsto en el articulo 208;

16) Falsificación y alteración de moneda, previsto en los artículos 234, 236 y 237;

17) Falsificación y utilización indebida de documentos relativos al crédito, previsto en el articulo 240 bis, salvo la fracción iii;

18) Contra el consumo y riqueza nacionales, previsto en el articulo 254, fracción vii, párrafo segundo;

19) Violación, previsto en los artículos 265, 266 y 266 bis;

20) Asalto en carreteras o caminos, previsto en el artículo 286, segundo párrafo;

21) Lesiones, previsto en los artículos 291, 292 y 293, cuando se cometa en cualquiera de las circunstancias previstas en los artículos 315 y 315 bis;

22) Homicidio, previsto en los artículos 302 con relación al 307, 313, 315, 315 bis, 320 y 323;

23) Secuestro, previsto en el artículo 366, salvo los dos párrafos últimos, y trafico de menores, previsto en el artículo 366 ter;

24) Robo calificado, previsto en el artículo 367 cuando se realice en cualquiera de las circunstancias señaladas en los artículos 372 y 381, fracciones vii, viii, ix, x, xi, xiii, xv y xvi;

25) Robo calificado, previsto en el artículo 367, en relación con el 370 párrafos segundo y tercero, cuando se realice en cualquiera de las circunstancias señaladas en el artículo 381 bis;

26) Comercialización habitual de objetos robados, previsto en el artículo 368 ter;

27) Sustracción o aprovechamiento indebido de hidrocarburos o sus derivados, previsto en el artículo 368 quater, párrafo segundo;

28) Robo, previsto en el artículo 371, párrafo ultimo;

29) Robo de vehículo, previsto en el artículo 376 bis;

30) Los previstos en el artículo 377;

31) Extorsión, previsto en el artículo 390;

32) Operaciones con recursos de procedencia ilícita, previsto en el artículo 400 bis, y

33) En materia de derechos de autor, previsto en el artículo 424 bis.

II. De la ley federal contra la delincuencia organizada, el previsto en el artículo 2.

III. De la ley federal de armas de fuego y explosivos, los delitos siguientes:

1) Portación de armas de uso exclusivo del ejército, armada o fuerza aérea, previsto en el artículo 83, fracción III;

2) Los previstos en el artículo 83 bis, salvo en el caso del inciso i) del artículo 11;

3) Posesión de armas de uso exclusivo del ejército, armada o fuerza aérea, en el caso previsto en el artículo 83 ter, fracción III;

4) Los previstos en el artículo 84, y 5) introducción clandestina de armas de fuego que no están reservadas al uso exclusivo del ejército, armada o fuerza aérea, previsto en el artículo 84 bis, párrafo primero.

IV. De la ley federal para prevenir y sancionar la tortura, el delito de tortura, previsto en los artículos 3o. y 5o.

V. De la ley general de población, el delito de tráfico de indocumentados, previsto en el artículo 138.

VI. Del código fiscal de la federación, los delitos siguientes:

1) Contrabando y su equiparable, previstos en los artículos 102 y 105 fracciones i a la iv, cuando les correspondan las sanciones previstas en las fracciones ii o iii, segundo párrafo del artículo 104, y

2) Defraudación fiscal y su equiparable, previstos en los artículos 108 y 109, cuando el monto de lo defraudado se ubique en los rangos a que se refieren las fracciones ii o iii del artículo 108, exclusivamente cuando sean calificados.

VII.- De la ley de la propiedad industrial, los delitos previstos en el artículo 223, fracciones II y III.

La tentativa punible de los ilícitos penales mencionados en las fracciones anteriores, también se califica como delito grave.

VIII. De la ley de instituciones de crédito, los previstos en los artículos 111; 112, en el supuesto del cuarto párrafo, excepto la fracción V, y 113 bis, en el supuesto del cuarto párrafo del artículo 112;

IX. De la ley general de organizaciones y actividades auxiliares del crédito, los previstos en los artículos 98, en el supuesto del cuarto párrafo, excepto las fracciones IV y V, y 101;

X. De la ley federal de instituciones de fianzas, los previstos en los artículos 112 bis; 112 bis 2, en el supuesto del cuarto párrafo; 112 bis 3, fracciones I y IV, en el supuesto del cuarto párrafo; 112 bis 4, fracción I, en el supuesto del cuarto párrafo del artículo 112 bis 3, y 112 bis 6, fracciones II, IV y VII, en el supuesto del cuarto párrafo;

XI. De la ley general de instituciones y sociedades mutualistas de seguros, los previstos en los artículos 141, fracción I; 145, en el supuesto del cuarto párrafo, excepto las fracciones II, IV y V; 146 fracciones II, IV y VII, en el supuesto del cuarto párrafo, y 147, fracción II inciso b), en el supuesto del cuarto párrafo del artículo 146;

XII. De la ley del mercado de valores, los previstos en los artículos 52, y 52 bis cuando el monto de la disposición de los fondos o de los valores, títulos de crédito o documentos a que se refiere el artículo 3o. de dicha ley, exceda de trescientos cincuenta mil días de salario mínimo general vigente en el distrito federal;

XIII. De la ley de los sistemas de ahorro para el retiro, los previstos en los artículos 103, y 104 cuando el monto de la disposición de los fondos, valores o documentos que manejen de los trabajadores con motivo de su objeto, exceda de trescientos cincuenta mil días de salario mínimo general vigente en el distrito federal, y

XIV. De la ley de quiebras y suspensión de pagos, los previstos en el artículo 96."[25]

1.18.-DEFINICIÓN DE TRATADO INTERNACIONAL.

El tratado es la fuente más importante del Derecho Internacional Público, ya que con ellos, obra el consentimiento expreso de los Estados intervinientes en su carácter de altas partes contratantes.

Las relaciones que corresponden a los tratados internacionales está reconocido en el preámbulo de la carta de las Naciones Unidad cuando se asevera la decisión de los pueblos tendientes a crear condiciones bajo las cuales puede mantenerse la justicia y el respeto a las obligaciones emanadas de los tratados y de otras fuentes del derecho internacional.

El tratado internacional es "el acto jurídico, regido por el derecho internacional que entraña el acuerdo de voluntades entre dos o más sujetos de la comunidad internacional, principalmente Estados, con la intención licita de crear, transmitir, modificar, extinguir, conservar, aclarar, certificar, detallar, etc., derechos y obligaciones.

Los elementos de la definición son:

1.- Acto jurídico, por ser la manifestación de la voluntad hecha con la intención licita de producir consecuencias de derecho.

2.-Regido por el derecho internacional, porque excluye aquellos acuerdos de voluntad que están sometidos al derecho interno.

[25] CFr., Código Pernal federal, Ediciones fiscales ISEF, S.A., México, 2002, p.45-48..

3.- Sujetos de la comunidad internacional, porque el tratado no es celebrado exclusivamente por los Estados, aunque principalmente lo celebran estos. El tratado también lo celebran los organismos internacionales entre ellos o con los Estados.

4.- Intención licita, porque se excluyen actos que vulneran las normas jurídicos de derecho internacional.

5.- El objeto de los tratados internacionales son la fijación de derechos y obligaciones recíprocas. Se mencionan los infinitivos de crear, transmitir, modificar, extinguir, conservar, aclarar, certificar, detallar, etc., porque en los tratados internacionales hay una amplia gama de consecuencias de derecho que no es posible encerrar en los infinitivos crear, transmitir, modificar, extinguir derechos y obligaciones". "[26]

1.19.- DEFINICIÓN DE EXTRADICIÓN.

La palabra extradición deriva de las palabras EX que significa fuera y de TRADICTIO O TRADICTIONES que quieren decir entregar desde afuera.

La ley de extradición internacional define a la extradición como "el acto mediante el cual un gobierno entrega a otro que lo ha reclamado, a un sujeto al que se le atribuye la comisión de un delito común, para que sea juzgado y, en su caso condenado previa la tramitación del debido proceso.

De acuerdo con la ley de extradición de la república mexicana, la extradición tendrá lugar:

1.-En los casos y formas que determinan los tratados internacionales.

2.- A falta de estipulación internacional se observarán las disposiciones de esta ley.

[26] ARELLANO GARCIA, Carlos," Primer curso de derecho internacional público" 3ª ed., edit., Porrúa, S.A., México, 1986., p. 632.

El artículo segundo de dicha ley preceptúa que solo podrán motivar la extradición los delitos internacionales del orden común en sus cuatro grados de actos punible, delito intentado, delito frustrado y delito consumado.

Son excepciones de extradición:

1.- Los hechos que no tengan calidad de punibles en el Estado que demanda la extradición.

2.- Los que solo sean punibles con la pena de multa o prisión hasta de un año.

3.-Los que, según la ley aplicable al Estado requirente, no tengan mayor pena de la pecuniaria, de destierro o de un año de prisión.

4.- Los que hayan dejado de ser punibles por prescripción de la acción o de la pena.

5.- Los que hayan sido objeto de absolución, indulto o amnistía del acusado, o respecto de los cuales se haya cumplido la condena.

6.- Los delitos dentro de la jurisdicción de la república mexicana". [27]

La ley reglamentaria del artículo 114 constitucional dispone que las autoridades de un entidad federativa, cuando fueren requeridos, en los términos por ella establecidos, por las autoridades de otras, tienen la obligación de entregar sin demora a estos últimos, a los reos condenados que traten de evadir la acción de la justicia o presuntos responsables contra quienes se haya dictado orden de aprehensión siempre que el exhorto o la
requisitoria se ajusten a las prescripciones legales, los delincuentes políticos no pueden ser objeto de extradición.

La definición denota la posibilidad que tienen los Estados de ejercer acción penal fuera del territorio de un Estado como consecuencia de la celebración de los tratados o acuerdos internacionales que existen entre dos o más países.

---

[27] "Ley de extradición internacional (consulta en internet: www. Info.jurídicas.UNAM.mx) México, 14:00P.M. 01/08/2002.

CAPITULO 2 PROBLEMA.

2.1.- LAS FORMAS DE ACTUACIÓN DEL INTRUSO CIBERNETICO, NO SOLO CAUSAN DAÑO A LOS BIENES MATERIALES, SINO QUE ORIGINAN TAMBIÉN UN PELIGRO INMINENTE Y GRAVE QUE PRODUCE INQUIEDTUD U ZOZOBRA A LAS PERSONAS EN SU INTEGRIDAD O EN SUS BIENES Y DE AHÍ QUE SE DIGA QUE ALTERA AL MISMO TIEMPO LA PAZ Y LA SEGURIDAD SOCIAL.

Las formas de actuación del intruso cibernético (sinónimo de hacker, el cual es el termino mundialmente conocido), fueron conocidas desde 1971, aunque hay que aceptar que desde esa fecha hasta ahora han tenido cambios considerables y radicales que han dado como consecuencia una conducta ilícita.

Los primeros intrusos cibernéticos fueron aficionados en computación, quienes adoptaron el termino mundial de intruso hack, que es un sinónimo para aquellas personas que trabajan en una computadora necesitando un determinado nivel de conocimientos en esta materia.

La característica de la segunda oleada de los intrusos cibernéticos, era que desesperadamente buscaban computadoras y los sistemas de las mismas para hacerlas accesibles a todos los ciudadanos y que no solo pertenecieran a aquellas personas que tuvieran un cierto nivel de conocimiento en esta nueva materia. En la segunda parte de los ochentas, se adoptó el término de intruso en un sentido malicioso cambiándose así radicalmente su denominación.

De esa fecha en adelante lo que predomina es el ordenador clandestino para realizar la intrusión cibernética, logrando así realizar varias de sus conductas que hoy en día son conocidas, tales como, robo, destrucción de información, espionaje, sabotaje, entre otros.

Al respecto se han dado hasta la fecha cuatro generaciones de intrusos cibernéticos, los cuales muestran claramente como se ha desvirtuado este término:

- GENERACIÓN 1.- Son aficionados, definiéndose como aquel quien se desarrolla o se desenvuelve en las técnicas de los programas de computadoras.
- GENERACIÓN 2.- Son definidos como aquellos que se dedican a desarrollar programas y aquellos elementos que integran a la computadora que se pueden ver y tocar (hardwears) como el ratón, quemadores de discos compactos, entre otros, para computadoras, es decir, los inventan y sacan al mercado
- GENERACIÓN 3.- La palabra intruso cibernético es usada solamente para describir una adicción, esto para realizar una treta o artimañas, como por ejemplo un juego en computadora
- GENERACIÓN 4.- El término intruso cibernético es usado para quien acceda ilícitamente a computadoras de otras personas. Esta generación representa la co –opción de pericia para manipular la computadora comercial, se caracterizan por ser perspicaces.

En 1996 se realizó un estudio a más de ochenta intrusos cibernéticos y sus asociaciones en Estados Unidos y Europa. Este estudio arrojó como resultado que en la primera generación se distinguía por su honradez, pero desafortunadamente esto desapareció.

Hoy en día, esta cultura ha empleado regularmente al intruso cibernético malicioso o malévolo, encaminando su actuar en afectar a otras personas. Este tipo de delincuentes se deleitan en presentar por si mismos publicaciones idealistas como si fueran dioses, la razón es para amedrentar o asustar a su posible victima.

Dentro del internet, al respecto, aparecen frases como "así que empiezas a navegar en el internet y a relacionarte con el correo electrónico y los buscadores,

sobre todo a recordar tu clave para ingresar a tu correo electrónico y a no confundirlos con otros, y te das cuenta de que, si no tiene cuidado alguien podría descubrir el tuyo y leer tu correo. Es cierto, la mayor de las veces no escribes nada importante, pero realmente tampoco quieres ser espiado. De repente te das cuenta que si supieras la clave podrías espiar a todo el mundo: a tu novia, tus amigos, tus profesores y especialmente a quien no te cae bien. Y es así como comienzas a pensar en los intrusos cibernéticos (hackers). Así que eres bienvenido a este mundo, ya que los intrusos cibernéticos están aquí.

Desafortunadamente dentro de las filas de estos delincuentes existen muchos menores de edad que aparentan ser mayores, son caracterizados por una actitud idealista e inmadurez excesiva, (sin embargo se debe de reconocer que jugando es como se convierten en expertos). Estos menores de edad sus actos son parecidos a lo juegos de ladrones en un mundo fantástico que encierra repentinamente un torno verdadero cuando ellos son cautelosos al actuar. Invariablemente este tipo de intruso cibernético son maliciosos por lo cual convendría ponerlos a la par de los adultos y así poderlos castigar igual.

El intruso cibernético requiere de varios grados de conocimiento para poder realizar sus conductas y explicar sus actos así como su técnica que utilizan para poder atacar a diversos sistemas de cómputo. Generalmente la información que necesitan la obtienen de otros intrusos o de estudios de sus victimas disponibles en la red o de diversas materias.

Los métodos más comunes para obtener información son sus propias futuras victimas o sus sistemas de computación. Los intrusos requieren de un status alto en conocimientos de computación y para pertenecer a un circulo hacker deben de cumplir con la cantidad de conocimientos y herramientas que se acuerdan poseer para pertenecer a este circulo y así poder tener acceso a cualquier lugar del ciberespacio.

Son pocas las personas que se las arreglan para vivir dentro de este circulo y obtener así posiciones respetables en lo que se refiere a la información

tecnológica. Estos individuos tienen dones o al menos así piensa la mayoría de las personas, siendo así inteligente y talentoso y por lo mismo pueden realizar varias actitudes logrando lo que se propongan hacer.

Estudios realizados en Estados Unidos, indican que el intruso cibernético tiene mucho miedo a la cárcel, esto es porque, la actividad de estos sujetos disminuye cuando se sabe de un arresto y aún más de su condena. El derecho de Estados Unidos obliga a la policía, como a la Agencia Federal de Investigación de Estados Unidos de Norteamérica (F.B.I.) y en algunos casos al servicio secreto para que a través de sus conocimientos en computación puedan capturar legalmente a los intrusos cibernéticos, desafortunadamente no siempre la sentencia es la que podrían merecer, esto por falta de ley uniforme en todo Estados Unidos.

"En México, los intrusos cibernéticos aparecen en 1998, era el grupo llamado X-PLIT TEAM, fueron relacionados con el ejercito zapatista de liberación nacional, aunque este grupo siempre lo negó.

Este grupo contaba con miembros que lograron entrar a sitios estratégicos del gobierno mexicano, entre ellos al Senado de la Republica, donde alteraban el contenido de la pagina y en su lugar instalaban imágenes de Zapata y textos subversivos pro-EZLN. Pronto corrió el rumor que estos intrusos cibernéticos habitaban en el árido norte mexicano, cerca de la frontera con Estados Unidos.

Este grupo ha declarado que solo actúan para gravar su nombre en un sitio web y de identificarse con la intrusión política". [28]

Por lo tanto la inquietud u zozobra de las personas se presenta:

1.- Porque no se sabe como, ni que daños cause el ataque del intruso cibernético. Ya que el intruso cibernético puede entrar a un determinado sitio web para insertar graffiti y no hacer nada mas; hasta sustraer información confidencial

[28] ¿X-PLOIT? (Consulta en internet: www. Xploit.htm) México. 14:30. 10/10/2001.

de un determinado estado o destruir una serie de computadoras a través de un virus.

2.- Porque el usuario no esta protegido debidamente por el derecho en caso de un ataque, el cual, como ya se menciono puede consistir en varias cosas o actos.

3.- Por no existir a nivel internacional acuerdos de cooperación para capturar al intruso cibernético.

2.2.- LA INTRUSIÓN CIBERNÉTICA SE REALIZA UNICAMENTE POR MEDIO DEL INTERNET.

Las personas que realizan este tipo de delitos son sumamente complejas y necesitan saber muchas cosas, como por ejemplo el tipo de seguridad que utilizan las computadoras para llevar a cabo su conducta; la seguridad es una guerra en contra de este tipo de personas, no únicamente podría ser una solución, sino que es más bien para poner control y un poco en aprietos el actuar de estos intrusos cibernéticos. Las tecnologías y la ejecución de la ley los han catalogado como los reyes del delito cibernético. El intruso cibernético ataca de manera exterior a otras computadoras, tan solo por placer, curiosidad, desafío, experiencia o por aviso o advertencia de que la sociedad es vulnerable a este tipo de ataques y de que las nuevas tecnologías dan entrada a quienes son presumiblemente motivados por avaricia o codicia.

Son conocidos básicamente por sus penetraciones a ordenadores. La ética del intruso esta basada en el aprendizaje y en la formación libre y abierta. Cuando esta persona se para al bando contrario y es pagado por un tercero para obscuras intereses es tildada como un intruso malvado o delincuente.

Desafortunadamente este estereotipo son simplemente punteros en este siglo de avances tecnológicos y por lo tanto de este tipo de delitos, la continuidad la aseguran estas personas contratando empleados y adiestrándolos en estos mundos de delincuentes. Estas amenazas hacen frágil al sistema de computación

y a la fila de información que contiene; para el intruso cibernético es fácil conseguir cualquier tipo de información incluyendo los de oficina. Las múltiples formas de actuar le han dado su propio nombre a estos sujetos, tales como terroristas, espías, etc., que son emigrantes para no ser atrapados y poder ejercitar mejor sus roles.

El perfil inapropiado de un intruso cibernético se presenta por un mal joven que es, el delincuente genio en computadora que entra a una casa o a una matriz para obtener información con solo usar la línea telefónica. La tecnología incluye muchos programas para computadoras que son usados para robar información o dinero, directamente han usado en las computadoras técnicas exótica como el caballo de trolla "trojan hourse" y también bombas lógicas para atacar.

Estos programas utilizados por los intrusos cibernéticos (necesarios mencionarlos porque mas adelante se hará menciona a ellos), son:

- SPOOFING.-Es definido cono un tipo de engaño impersonal, usado en las computadoras. Spoofing en internet consiste en enviar recados disfrazados y repetidos con direcciones falsas para facilitar o hacer imposible rastrear a la original. Los ataques en internet son anónimos para las victimas, siendo esta vía la más confiable, ya que por ejemplo si mandas una extorsión en una carta en el correo normal, no se asegura, primero que llegue a donde vaya dirigido, segundo al que se desea extorsionar se proteja ya sea por el derecho o a través de una agencia; pero si lo haces por internet es seguro que se cumpla la extorsión por no dar tiempo a que se proteja. Este programa tiene la característica de que no deja huella o rastro en las computadoras y en algunas ocasiones deja huellas o rastros falsos para engañar y nunca ser encontrado. Si los delincuentes usan la falsificación de la dirección, es seguro que la victima responda al ataque.

- WEB SPOOFING.-Es realmente un método nuevo para delinquir, el cual es más difícil de detectar, aunque no es muy acertado porque falta afinarlo; los

hackers ya trabajan en eso y en un futuro no muy lejano será una arma muy destructiva. ¿Cómo funciona?, el delincuente necesita tener el control de una página, cualquiera que sea en el internet para alterarla y adquirir él la posición de intermediario. Esta alteración requiere de grandes habilidades en lo que se refiere a la programación de computadoras y de las páginas de internet. Alternativamente una web engañada podría atentar en contra del usuario por la instalación de un softweare falso para obtener la información requerida, ya que este softweare se introduce en el disco duro y ordena a la computadora realizar determinadas acciones que el hacker le mande como si fuera él el usuario. Es muy difícil para la victima descubrir este ataque, siendo así casi imposible detectarlo; los delincuentes usan esta técnica para robar o alterar información confidencial.

- SPAMMING.-Es un término usado para describir la técnica de inundación de computadoras con muchos mensajes de correos electrónicos, mandar virus o cosas deseadas, como por ejemplo insultos o imágenes ofensivas a los usuarios. Aunque esta es una de las formas más extremas para atacar existen otras y por desgracia, día a día surgen nuevas.
- FLOODING AND PINGING.-Este ataque es directo a los servicios que proporciona el internet, este tipo de ataque satura la comunicación siendo vulnerables los sitios que proporciona el internet, lo saturan con nombres y números de líneas telefónicas anónimas de productos o servicios falsos.

- SNIFEER ATTACK.-Conocido como ataque para husmear, es un programa para computadora que sirve para buscar paquetes de datos individuales, pasando directo al ataque que necesitan desconectando la red del internet. Los hackers usan este ataque para obtener información que ellos necesitan para molestar o fastidiar a sus victimas y así lograr su propósito ilícito. Este programa opera con notas secretas no

autorizadas, es como si fuera una sombra, es similar al programa de Caballo de trolla para burlar al softweare.

- PASSIVE HACKENG.- Es un programa nuevo muy poderoso para poder curosear en una página web que ejecuta el programa java, el cual a través de un código permite al hacker intentar su ataque. La visita a esa web trae graves daños, por ejemplo mandar un indeseable regalo como un virus o ejercer dominio en su computadora.

- IDENTITY THEFT.- Se refiere al uso ilegal por alguien usando una identidad que no le corresponde o de otra persona para tomar ventaja de la victima en cuanto a su crédito o reputación. Este tipo de ataque es muy bueno, porque obtienen confidencialidad e información personal de su victima. Este programa es solo el comienzo de un robo como el de una cartera o una bolsa, esto es común por ejemplo en las cajas de ahorros; es como escuchar a escondidas en el internet. También es usado para difundir información confidencial, aunque esto no es nuevo en el mundo del hackeo.

- E-MAIL SPOOFING.- Es el término aplicado para la falsificación de recados de correo electrónico, este ataque es considerado como una epidemia en el internet. Aunque existe una cantidad considerable de e-mails spoofings algunos son inofensivos pero otros son graves. Si el delicuente es el afortunado para entrar y usar el e-mail legitimamente, debe de tener previamente un conocimiento para usarlo y así obtener la información y contraseña requerida para ingresar sin problema y las veces que quiera.

- THE SALAMI FRAUD.- Es un programa mediante el cual se engaña a la base de datos de un banco con la unica finalidad de transmitir dinero de una cuenta a otra, pero con la peculiaridad de maquillar esta acción para que no den cuenta de este ilícito.

- THE TOJAN HOURSE.- Es un programa utilizado para engañar al disco duro de la PC y así poder tener el control de la máquina. Es usado más que nada para mandar virus a través del correo o de sitios webs a otros usuarios que esa máquina infectada tenga registrados para mandar correos. El intruso cibernético utiliza el lenguaje de la criptografía, esto consiste en transformar un mensaje inteligible en otro que no lo sea en absoluto, para después devolverlo a su forma original sin que nadie que vea el mensaje cifrado, sea capaz de entenderlo.

El internet es una red mundial que contiene mucha información de particulares, de empresas y de gobiernos de todo el mundo, contando con servicios como el e-mail, chat room, ciber conferencias, entre otras cosas. Para contar con esta maravilla es necesario contar con una línea telefónica y una PC o computadora, este avance tecnológico tiene ventajas y desventajas, la primera es la gran cantidad de información que se puede consultar desde cualquier parte del mundo en la comodidad del hogar de cada usuario pero la desventaja son los delitos que se pueden cometer, siendo uno de ellos la intrusión cibernética.

Esta actividad es solo realizable en el internet porque es el único medio para poder tener contacto con la información de otras personas, llámense estado, particulares o empresas tanto públicas como privadas, y así poder realizar sus diversas conductas que se convierten en delitos, cabe hacer mención que la intrusión cibernética se puede llevar a cabo desde cualquier parte del mundo a otra parte del mundo, es decir no solo es dentro de un estado o a nivel local, sino que es de estado a estado. Esta tecnología es grandemente usada por estos delincuentes para realizar sus diferentes conductas gracia s a la proliferación de la P.C e internet que es su vehículo, lo más usado por los intrusos cibernéticos para realizar sus propósitos son:

1.- CITOS WEB O PÁGINAS EN INTERNET.- Usado ilícitamente para fraudes, divulgación y falsificación de información, proliferación de virus, uso de imágenes ilícitas, etc.

2.- E- MAIL.- Llamado correo electrónico usado por personas anónimas para distribuir información confidencial, fraudes de tarjetas de crédito por medio de falsos servicios, distribución ilícito de material confidencial y la proliferación de virus cibernéticos.

3.- NÚMEROS TELEFONICOS.- Son usados por una persona o una organización regularmente anónimos para realizar fraudes con tarjetas de crédito.

El delito más frecuente por el intruso cibernético es el fraude en tarjetas de crédito, ya que las compras por medio del internet son a través de la tarjeta de crédito.

La aplicación que tienen el internet es información importante, por ejemplo muchas organizaciones usan este medio electrónico para poner información privada, esto para facilitar la comunicación entre sus empleados, para hacer ventas, pagos y otro tipo de transacciones más.

En el USENET o IRC que se encuentran en el internet, existen este tipo de servicios conteniendo casi toda la información de personas, organizaciones y áreas geográficas.

Las personas usan este medio electrónico para comunicarse, explorar nuevas ideas y realizar compras desde la comodidad de su hogar. Esta combinación de actividad social y financiera hacen la aplicación adecuada y el sitio atractivo para que se cometa el delito hacia cualquier tipo de personas por que se encuentran varios nombres, direcciones, números telefónicos y direcciones electrónicas.

Dada la magnitud de la información que se encuentra en le internet, es crucial el saber buscar efectiva y eficazmente; existen muchas herramientas para realizar

una investigación adecuada incluyendo búsqueda de manera general o de alguna materia en específico. Algunos excelentes buscadores son:

- Alta vista: http://www.altavista.com.
- Hotbot: http://www.hotbot.com.
- Excite: http://www. Excuse.com.
- Infoseck: http://www.infoseck.com

El internet proporciona toda una hilera de nuevas oportunidades para el delito y otras ocasiones para el negocio o su combinación. Los delincuentes aprecian el anonimato proporcionado por las computadoras, además que la intrusión cibernética siempre utiliza apodos o pseudónimos.

El anonimato es muy ventajoso porque les permite la perpetración del delito y así operar fuera de los requerimientos de las leyes.

A través del las diversas conductas del intruso cibernéticos se pueden obtener varias cosas como fraudes, robos, engaños, amenazas, infecciones de virus, todo ello encaminado a producir un daño que en ocasiones es muy fuerte.

A pesar de que el internet es un gran avance tecnológico muy importante; hoy en día no es seguro ya que tiene muchos usuarios, se ha estimado que son más de un millón y medio de usuarios en todo el mundo. Debido a esto es muy grande su fuerza y por lo mismo es muy vulnerable para realizar abusos y ataques de varias formas como terrorismo, pornografía, pedofilia, robo de números y nombres de tarjetas de crédito, entre otros.

Se han dado una serie de abusos y un mal uso del intenet, trayendo como consecuencia o dando como resultado varios tipos de delitos.

Sobresaliendo la intrusión cibernética por la especialización con la que deben de contar las personas que realizan esta actividad y desafortunadamente día a día aumenta la frecuencia y alcance de esta conducta.

2.3.- LOS NOMBRES DE LOS INTRUSOS CIBERNÉTICOS DE ACUERDO A LA FORMA DE ACTUAR SON:

Antes de entrar a decir las diversas conductas del intruso cibernético es necesario para entenderlas mejor, referirse primero a la manera de operar de estos delincuentes.

La manera de operar se refiere a la conducta que es cometida por un delincuente que tiene la intención de cometer un ataque; es tradicional realizar investigaciones exhaustivas en casos relevantes para saber aplicar correctamente la ley y por lo tanto también saber que hacer para evitar estas conductas.

Sin embargo en las investigaciones se ha sabido que algo relevante del ataque es la técnica utilizada que caracteriza a una disciplina en particular o un campo nuevo de conocimiento; esto incluye conductas que pertenecen a un simple delincuente o aun criminal.

Es muy característico que estos ataques vayan dirigido a una o más de tres intenciones:

- Proteger la identidad de las personas que realizan el ataque.
- Garantizar el acertado cumplimiento del delito.
- Facilitar la identidad para escaparse; de este punto es que los intrusos cibernético siempre utilizan apodos.

El comportamiento para realizar las conductas y cometer un delito en el internet, incluye que no hay limites en cuanto a:

- Importante cantidad de intentos antes de cometer el delito, esto se refiere a lo que se pueda saber de la victima por ejemplo: notas tomadas en un día de la victima, investigar la información contenida en su PC o en su correo electrónico.
- Materiales usados para la ofensa en la comisión de una conducta específica por ejemplo, gravar sistemas o conversaciones.

- Presuponiendo de la victima el delito y la escena de la misma: por ejemplo, manteniendo a las victimas visitando su página web para saber sus principales ocupaciones, contactando a las victimas directamente usando un amigo para poder realizar su conducta.
- Selección del lugar de la ofensa, por ejemplo, conversación en el chat o por medio de distribución de materiales ilícitos.
- Uso de un arma durante el delito, por ejemplo un virus que destruye o programas de PC o un correo electrónico para engañar a la victima.
- Actos precautorios ofensivos por ejemplo, el uso de un alias, el robo de un sistema privado para usarlo como base de su operación.

Cuando un sitio en internet es atacado, es común y notable por causar un daño menor en muchos casos, por ejemplo insertando graffiti o imágenes pornográficas en un página determinada o alterando el texto para transmitir amenazas o provocar al poseedor de la página por medio de insultos.

Invariablemente es notable e inofensivo el acto por erosionarse la confianza en cuanto a la autenticidad de la página e introducir el ataque para mostrar como dañar con los diversos tipos de ataques. El intruso cibernético se esmera cada vez más para darle autenticidad a la página y así poder tomar una victima más.

El ataque sufrido a una página para provocar la pérdida de autenticidad de ese sitio (por ejemplo en negocios, modificando sus listas de precios o insertando productos y servicios ficticios) genera graves daños para el que otorga el servicio como son perdidas de dinero importantes y por lo mismo la quiebra.

2.3.1. EL INTRUSO CIBERNÉTICO DE CORAZÓN.

Es llamado así dentro del mundo de los intrusos cibernéticos a aquel que, disfruta del desafío intelectual de superar las dificultades de forma creativa, así también como el que disfruta explorando los sistemas y programas sabiendo por lo mismo como sacarles el máximo provecho, al contrario que la mayoría de los usuarios que prefieren conocer solo lo indispensable.

Lo que distingue a este tipo de intrusos cibernéticos de los demás es que no causa un daño, es decir, no roba, no modifica información. Su conducta la realiza únicamente para demostrarse a él mismo que si puede derribar las barreras de seguridad y entrar a cualquier sistema o página web.

Este tipo de intrusos cibernéticos son catalogados como principiantes o aquellos que se encuentran en la etapa larval, ya que solo tienen conocimientos básicos.

La característica, es que deja un mensaje en la computadora como su podo, o diciendo que su sistema de seguridad no era tan bueno, etc.; pero no sustraer ni alterar la información que se encuentra en esa página que logró entrar.

También son llamados así a los intrusos cibernéticos que se dedican a no hacer daño y su misión es el de descubrir cuando sus programas están dañados; o de revisar los sistemas de cómputo para su reparación, es decir, usar sus conocimientos para lograr que toda la computadora como los sistemas de la misma trabajen bien, así como entrar a las diferentes paginas en internet y lograr su reparación para su buen funcionamiento.

2.3.2. EL INTRUSO CIBERNETICO QUE MANDA MEGA VIRUS A LOS USUARIOS.

Los virus de una computadora es actualmente un tipo específico de códigos maliciosos que se reproducen al instante y se han hecho copias o nuevas versiones de virus en otros programas; cuando esto es ejecutado se infecta todo un programa. En muchas ocasiones se insertan ellos mismos en la tarjeta de programas dando así instrucciones para transferir el control al virus, con un almacenamiento en alguna parte de la memoria.

Cada ves que el programa da instrucciones es ejecutado y por ello transfiere el control al programa del virus, con ello se reemplazan instrucciones y se inserta en

otros programas para poder infectar y así llegar a una fila o cadena de infecciones que abarcan varios programas y de diferentes usuarios.

El virus se considera un parásito, porque deja que el programa siga funcionando normalmente para poder infectar a más sistemas y así poder llegar a una destrucción masiva.

Hasta la fecha se han presentado más de 10,000 infecciones del sistema operativo de la PC.

Este tipo de intrusos cibernéticos se caracteriza por ser obsesivos en programación, ya que elaboran ordenes para ejecutarlos de manera específica para un programa. Estas personas disfrutan en dañar a muchos usuarios y computadoras ya que la infección se puede transmitir de manera automática a través del correo electrónico.

Para llevar a cabo esta conducta, utilizan el programa llamado caballo de trolla para confundir a las computadoras y así aceptar las ordenes que allí se encuentran.

La forma preferida para atacar es por medio de el correo electrónico, ya que a través de él, el virus se reproduce tan solo al enviar un correo a otra persona; o si no es así se mandan solos a las direcciones que se tienen registrado en la bandeja de entrada. No obstante también pueden usar los citios webs, aunque sería la infección más lenta, ya que se necesita que alguien entre a este sitio.

Los programas utilizados preferentemente es el e-mail spoofing y el caballo de trolla por no dejar huella o si la dejan es falsa.

La actividad de crear virus, gusanos, troyanos o bombas lógicas se llama virucking.

Si bien es un ataque que puede se ingresado al sistema por un dispositivo externo (diskettes) o a través de la red (correo electrónico u otras formas) sin

intervención directa del atacante. Dado que el virus tiene como característica propia su auto reproducción, no necesita de mucha ayuda para propagarse a través de una LAN o WAN rápidamente, si es que no esta instalada una protección de antivirus en los servidores, estaciones de trabajo y los servidores de correo electrónico.

Existen distintos tipos de virus, como aquellos que infectan archivos ejecutables (.exe, .com, .bat, etc) y los sectores de boot-partición de discos y diskettes, pero aquellos que causan en estos tiempos mas problemas son los macro virus que, están ocultos en simples documentos o planilla de calculo, aplicaciones que utiliza cualquier usuario de PC, y cuya difusión se potencia con la posibilidad de su transmisión de un continente a otro a través de cualquier red Internet. Y además son multiplataforma, es decir, no están atados a un sistema operativo en particular, ya que un documento do MS-WORD puede ser procesado tanto en un equipo windows, como en otras.

Cientos de virus son descubiertos mes a mes, y técnicas mas complejas se desarrollan a una velocidad muy importante a medida que el avance tecnológico permite la creación de nuevas puertas de entrada. Por eso es una nueva amenaza.

El ataque de virus es el mas común para las empresas, que en un gran porcentaje, responden afirmativamente cuando se les pregunta si han sido victimas de algún virus en los últimos cinco años.

2.3.2. EL INTRUSO CIBERNETICO QUE ENTRA A UN SISTEMA SOLO POR VENGANZA.

Este tipo de intruso cibernético tal ves sea el más peligroso, ya que cuenta con sentimientos encontrados, y por lo mismo va a realizar lo posible por acabar con su victima.

Estudios realizados en Estados Unidos de Norte América, revelan que afortunadamente son pocos los casos que se han registrado; el principal motivo han sido despidos injustificados, afortunadamente se han presentado en empresas de personas particulares, los cuales muchos ya han desaparecido, esto por lo terrible del ataque, otro motivo es por riñas y en el caso de la agencia federal de investigación de los Estados Unidos (F.B.I.), es por coraje de haber sido detenidos o por el simple hecho de demostrar que son mejor que ellos.

Se ha revelado que en estos ataques, lo usado es el programa de caballo de trolla combinado con el spoofing para no dejar rastro.

Los ataques a las empresas consisten principalmente en el aspecto psicológico de las personas a las que van dirigidos, pudiendo consistir en notas de amenazas de muerte, otro aspecto al que va dirigido es al referente al del dinero, es decir, ofrecen servicios y promociones que no pueden resistir o simplemente hacen transferencia de dinero a varias cuentas.

Por supuesto esto es siempre con el programa de salami fraud, es usado por engañar a la base de datos de un banco, con la finalidad de burlarlo para obtener dinero.

2.3.4. EL INTRUSO CIBERNETICO QUE DESTRUYE SISTEMAS DE SEGURIDAD.

Este tipo de intruso cibernético recibe el nombre de crackers, definiéndose de la siguiente manera:

"1.- Es alguien que disfruta explorando los sistemas y programas , sabiendo como sacarles provecho, al contrario que la mayoria de los usuarios que prefieren conocer solo lo imprescindible. Siendo experto en los diferentes sistemas de seguridad, en ocasiones se han adelantado a los nuevos modelos de seguridad, convirtiéndose en expertos en estos sistemas antes de que salgan al mercado.

2.- Una persona que es buena programando de forma rápida.

3.- Es una mala persona que trata de descubrir información secreta.

4.- Es un término acuñado en 1985 y se refiere al que rompe la seguridad de un sistema. Los crackers forman pequeños grupos secretos y privados adentrándose en el mundo de lo ilegal.

5.-Comprende la obtención por fuerza bruta de aquellas claves que permiten ingresar a servidores, aplicaciones, cuentas, etc. Muchas claves de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario, que además nunca la cambia. En este caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y diccionarios que prueban millones de posibles claves hasta encontrar la correcta.

Es muy frecuente crackear una clave explotando agujeros en los algoritmos de encriptación utilizados, o en la administración de las claves por parte de la empresa.

Por ser el uso de la clave la herramienta de seguridad mas cercana a los usuarios , es aquí donde hay que poner énfasis en la parte humana con políticas claras y una administración eficiente.

La utilización de los términos intruso cibernético como cracker refleja una fuerte repulsión contra el roba y vandalismo perpetuado por estos circulos. Todos los intrusos cibernéticos, tienen habilidades de sobra para convertirse en crackers. Cuando un intruso cibernético responde al llamado de su lado oscuro de su fuerza se convierte en un cracker o en un dark side hackers, es decir, el lado oscuro y secreto de un intruso cibernético."[29]

[29] ¿Qué es un cracker? (consulta en internet: http://cracker, conductas y definición.com) México, 14:30 , 10/10/2001.

Esta es una forma de decirle al intruso cibernético delincuente, este tipo de intrusos para llevar a cabo su ilícito, utilizan los programas más sofisticados para lograr su objetivo: son expertos en saber como están compuestos los diversos sistema de seguridad para poder ejecutarlos y poderse meter al sistema que deseen.

Para lograr ser un buen intruso cibernético y entrar a cualquier pagina web y delinquir se tiene que pasar por varias etapas, siendo esta la primera, es decir, el saber quitar la seguridad y el dejar un mensaje en el sitio que entraran.

2.3.5. EL INTRUSO CIBERNETICO QUE COPIA, MODIFICA O DESTRUYE INFORMACIÓN CONTENIDA EN DETERMINADOS SISTEMAS DE COMPUTO O SERVIDORES DE INTERNET.

Como ya se dijo, la conducta del intruso cibernético se realiza por el internet, debido a la gran cantidad de información que éste tiene. La intrusión cibernética se realiza para tener acceso a la información que se requiere y hacer con ella lo que se desee.

Este tipo de intruso cibernético aprovechan los avances tecnológicos para ser usados por ellos mismos y para su beneficio. Estas personas ganan mucho dinero, pueden ser uno solo o un grupo de personas los que se dediquen a esta actividad.

Estos intrusos cibernéticos se denominan phreakers, siendo aquellos que están dentro del mundo de lo ilegal con la finalidad de irrumpir redes de servidores para internet y líneas telefónicas, siendo además expertos en todo tipo de seguridad, incluso van un paso delante de lo que ya existe en el mercado.

Este tipo de intrusos cibernéticos son englobados y llamados comúnmente como terroristas ya que se dedican a obtener información política, religiosa o social. La información que es la más interesante para este tipo de intruso

cibernético son la militar para tener un control de armas, la financiera y en algunos casos información de hidrocarburos que el país tenga.

Al respecto existen estudios que son limitados por que muchos casos de estos son de un alto secreto sobre todo cuando el ataque va dirigido a un estado y en muchas ocasiones no se tiene acceso.

Para adquirir victimas utilizan el ciberespacio buscando en páginas web, hojean páginas, buscan chat para buscar información confidencial y así poder intimidar.

Esta conducta la realiza en algunas ocasiones para hacer pasar un mal rato a un país determinado, la información copiada, modificada o destruida por lo regular es usada por otro estado para aprovecharse de los avances que este país tenga, sobre todo en tecnologías o en estrategias ya sean militar, política y económicos.

Dentro de las conductas del intruso cibernético, la destrucción de información es la más grave, porque su ataque va dirigido por lo regular a los Estados, dejándolo así sin información de ningún tipo, tanto financiera como política y militar, afortunadamente estos ataques aún no han sido registrados pero es una posibilidad latente, ya que día a día los intrusos cibernéticos obtienen más y más fuerza por la impunidad que tienen.

Estudios realizados en Estados Unidos indican que este tipo de delincuentes son pagados o retribuidos, ya sean por Estados, empresas o particulares, dependiendo a quien vaya dirigido este ataque. Las razones son muy variadas ; por venganza que seria el caso de un particular a otro, es decir por ejemplo, un intruso cibernético entra a la computadora de Juan Pérez y lo intimida; por remuneración, que en este caso, la mayoría van dirigidos a empresas ya sea para obtener información de sus avances, políticas, o la mejora de sus productos, etc. Teniendo casos aunque pocos (importando aquí que se realizan) a los Estados, esto es para saber sus políticas, economía, avances, etc.

En este ultimo punto, no existe acceso a esta información, ya que las páginas que contienen esto, están encriptadas y siendo rastreadas por la agencia federal de investigación de Estados Unidos por se posibles terroristas.

2.3.6 EL INTRUSO CIBERNÉTICO QUE REALIZA ESPIONAJE.

Al respecto no existen muchos estudios o son limitados ya que muchos casos de espionaje no se han resuelto ni reportado.

En realidad muchos ofensores combinan la tradicional forma de espiar y acosar, quienes telefoneando la victima, obteniendo así su dirección y número de teléfono. Muchos ciber espías obtienen victimas por el internet y otros por información personal de sus victimas.

En general, los espías carecen de una fuerza poderosa hacia sus victimas. Los espías usan información semejante a números telefónicos, direcciones y referencias personales para dañar a sus victimas.

En este apartado son encerrados todos los intrusos cibernéticos, ya que lo que ellos hacen es husmear un sistema que no es el suyo, la diferencia radica en el grado de daño que cause, porque no es lo mismo entrar a un sistema sin hacer nada a robar información o destruir a empresas.

Estudios que se ha elaborado recientemente al respecto señalan que las materias que son más espiadas son:

- Militar.
- Financiera
- Industrial
- Inventos, aquí se incluye las patentes y marcas así como con derechos de autor.

Una vez expuesto la manera de llamar a cada intruso cibernético de acuerdo a su actuar y de saber los softwears que puede llegar a utilizar en sus ataques, es necesario, antes de entrar al siguiente apartado de este capítulo, mostrar la manera de cómo aparecen en la red, es decir, en el Internet, así como, las noticias que se tienen sobre estos delincuentes, ya que, día a día su actuar se propaga en todo el mundo, esto es, la mayoría de las veces para crear pánico en los sitios que han realizado la intrusión cibernética, teniendo así lo siguiente:

Atacan hackers a Microsoft

Descubren desvío de contraseñas desde Rusia; podrían haber obtenido códigos fuente de Windows y Office

AP

Nueva York, Estados Unidos.-Intrusos cibernéticos irrumpieron hoy en la red de computadoras de la compañía Microsoft, obteniendo acceso a los códigos fuente de las últimas versiones de Windows y Office, dijo el ejecutivo de la empresa Steve Ballmer.

Los atacantes informáticos podrían tener el código fuente de Windows y Office / Foto: LUIS VÁZQUEZ

La intrusión de los hackers fue descubierta por expertos en seguridad de Microsoft en la empresa ubicada en Redmond, tras percatarse que ciertas contraseñas eran dirigidas hacia un correo electrónico ubicado en San Petersburgo, Rusia. El hecho está siendo investigado por la empresa y el FBI, ante la sospecha de que pudiera tratarse de un caso de espionaje industrial.

Las pistas indujeron la sospecha que las contraseñas enviadas se estaban usando para transferir el código fuente de los programas, que contiene sus secretos de fabricación.

"Lograron acceso a los códigos básicos", dijo Ballmer durante una reunión realizada en Estocolmo. "Les aseguro que esto es un asunto de capital importancia. También les aseguro que sabemos que no ha habido erosión alguna de la integridad de los códigos básicos, que no han sido alterados en modo alguno".

La compañía dijo que la incursión no afectará los consumidores, los negocios y las oficinas gubernamentales que utilizan las computadoras de Microsoft. El vocero del FBI, Steve Berry, confirmó que la agencia ha iniciado una investigación acerca del caso, pero declinó entrar en detalles.

El código fuente de Windows y Office es uno de los secretos mejor guardados en el mundo informático, y el director general de Microsoft, Bill Gates, ha advertido en repetidas ocasiones que su divulgación sería una seria amenaza para la compañía. Con acceso a los códigos básicos, otras empresas pueden

crear fácilmente programas que compitan con Microsoft en las diversas aplicaciones de los productos de la compañía.

"Estamos estudiando el caso todavía", dijo el vocero de Microsoft Rick Miller. "Estamos tratando de determinar cómo ocurrió. Esto es un acto deplorable de espionaje industrial y vamos a proteger nuestra propiedad intelectual".

Si bien no se ha mencionado motivo alguno para la incursión, los hackers han utilizado métodos similares en el pasado para extorsionar a las empresas afectadas con la amenaza de publicar la información obtenida mediante su incursión cibernética.

Esta noticia, es desplegada de la agencia federal de investigación de Estados Unidos de Norte América, siendo de relevancia porque, esta empresa de Microsoft, es una de las más fuertes en cuestiones de seguridad, ya que de ahí surgen y son probados los sistemas de seguridad nuevos que saldrán al mercado o que ya están a la venta.

Los intrusos cibernéticos que entran a estos lugares son rastreados y localizados con el único propósito de que trabajen para ellos, ya que, estas personas han descubierto la vulnerabilidad de estos sistemas de seguridad que se llaman orificios y para subsanarlo, ponen lo que se denominan parches para que ya no sea presa de violarse.

Microsoft tiene la idea de que teniendo a su favor a los intrusos cibernéticos y utilizarlos en algo útil como lo antes mencionado, frenaran a esta conducta delictiva que puede causar mucho daño.

Este sitio web o página de internet, muestra la manera de cómo aparecen en la red estos intrusos cibernéticos, en la imagen se aprecia el titulo de la misma, después muestra la barra de herramientas de internet; mostrando en la barra la dirección que es el lugar donde se encuentra localizada dentro del mundo del ciberespacio esta sitio, y por último muestra el contenido de la página.

Sobresale la nota de que no se hace responsable de lo que se realice con lo publicado, pero en realidad, aunque fuera responsable , no existe la manera de cómo castigarlo, porque, en primera es anónima y no se sabe el lugar donde se pública la página, aparte de que con lo publicado en donde dice conviértete en un

hacker, muestra todos los pasos que se requieren para realiza esta conducta, este link se muestra así:

CONVIÉRTETE EN UN HACKER EN UNOS MINUTOS

Aprendiz hacker:

Sigue estos diez pasos, eso si, paso a paso:

1) Tú no puedes llamarte de cualquier manera (Fernando, José, Enrique...), sino que debe escoger un nick apropiado como: Kojjin, RiÑa, mArTeS13 o algún otro nick parecido.

2) Debes buscarte una cuenta de correos que vaya acorde con tu nick, y, por supuesto, mas falso que una moneda de 26 Ptas., como por ejemplo: RiÑaen(arroba)puticlub.com.

3) Desde luego, tu no usas un ordenador, sino una máquina que corre bajo UNIX o LINUX.

4) A partir de ahora, antes de mandar correos electrónicos, cambia las letras Q por letras K (Quien-Kien) y además di que te encanta INTOZIKAZION EHTILIKA, JENOZIDAS HAGUERRIDOS...

5) Usa el Netscape o el Outlook Express.

6) Que no se te ocurra preguntar nada, tu lo sabes todo. Cuando te consideren "gurú" pides el crack del WINZIP o cualquier otra cosa y dices que es para un colega tuyo que usa Windows.

7) En algunas de tus charlas dices que te colaste en un "root" y que, deduciendo password dejaste tu huella de tu paso en ese ordenador.

8) Ni se te ocurra decir que bajar shareware, Ethek... ni mucho menos de Microsoft.

9) Estas suscrito a todos los grupos 2600, warez, hacking y fucking, y por aquí solo vienes a contar que nunca es alabado ni valorado lo suficiente.

10) Contesta a todos los que pidan serial number, drivers, crack...

Al poco tiempo te habrás hecho un hacker y verás que hay muy poca gente como tú, sino que hay un puñado de "retrasados" a los que hay que ignorar.

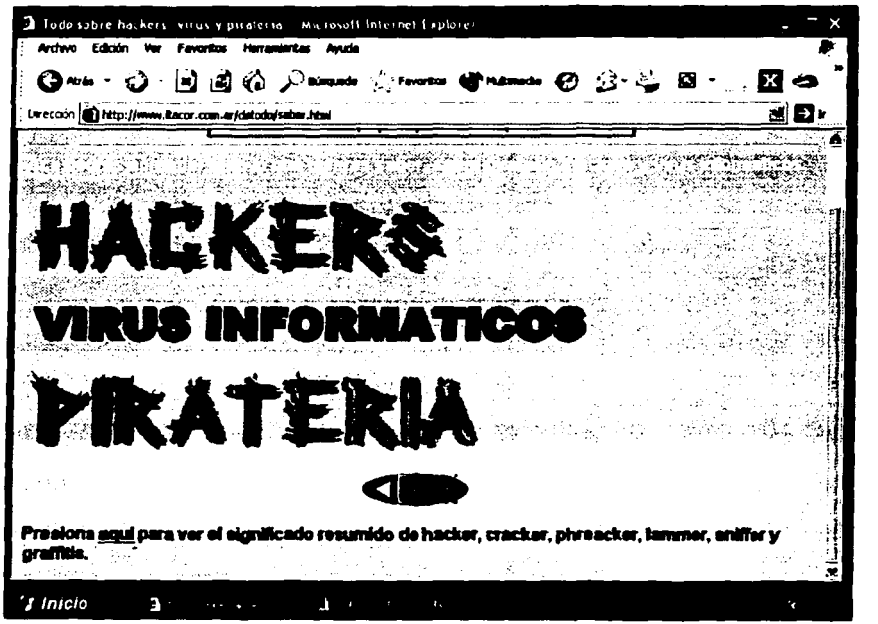
Advertencia: Yo no me hago responsable del mal uso de estos datos, sino que los publico para el uso educativo y/o científico.

Este link, esta desplegado porque mostrarlo como la imagen no salen todos los pasos que se mencionan para ser un buen hacker, cabe hacer mención que en páginas de Estados Unidos de Norte América, muestran los pasos para delinquir, en particular para ingresar al departamento del tesoro de Estados Unidos, esta página mencionada, no se puede imprimir ni copiar, solo se puede ver, es por ello que no la muestro en esta tesis, pero si quieren observar esta página, necesitan, buscar el servidor de yahoo, después, seleccionar que la página lo busque en todos los idiomas, acto seguido, poner lo siguiente en donde dice dirección: "the word black on hacker", darle un clic en busca y aparecerá la página, la cual contiene una introducción, mientras pasa esto, el hacker que realizó esa página, lee todo el disco duro de la computadora y se lo da a conocer al que visita esa página, después da las instrucciones para entrar al departamento del tesoro, ofreciendo una especie de recompensa para que se comprometa uno a realizar esa conducta y desde la entrada sea atractivo.

En este caso se tiene que tener cuidado porque la agencia investigadora correspondiente para la investigación de delitos cibernéticos en Estados Unidos, rastrea esta página por introducirse a ese departamento y en un dado caso que se muestra su responsabilidad, puede ser juzgado en Estados Unidos por terrorismo, puesto que este tema en Estados Unidos, es catalogado como causa de seguridad nacional, debido a los ataques del once de Septiembre pasado, de acuerdo a un proyecto de ley, podrá ser castigado hasta con pena de muerte.

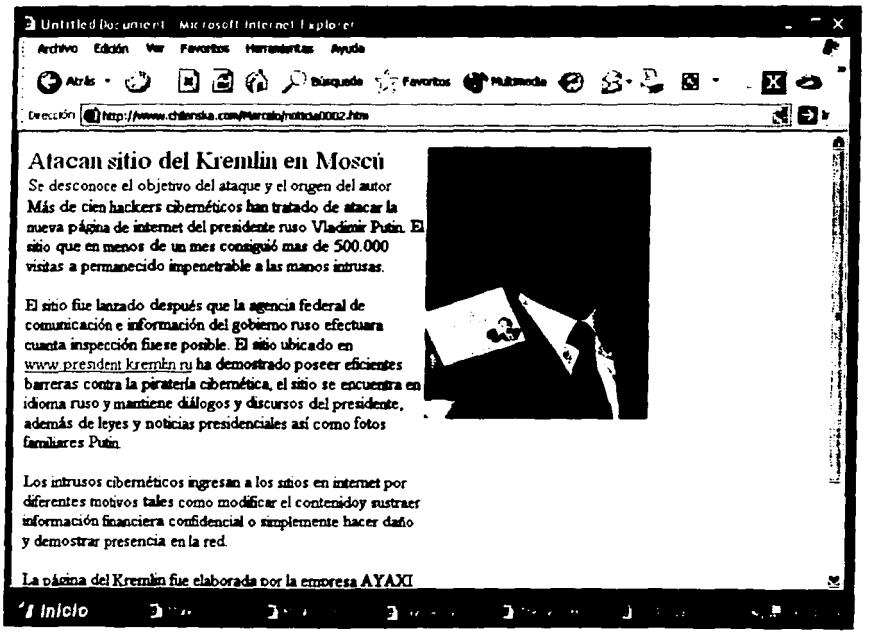
A continuación se mostrará otra página que muestra lo mismo de la primera, solo que en esta página se muestra la manera de cómo crear un virus y distribuirlo en la red, y dentro del link de piratería da unos sitio para tener canciones en su servidor de manera permanente, así como la forma de burlar la seguridad de los sitios que contienen esa información.

Estas páginas están desplegadas porque, no se pueden copiar ni guardar ,si se quiere tener esa información, es necesario abrir esa página y abrir los link para poder ver su contenido. Dentro de la página se debe tener cuidado porque puede infectarse la computadora con un virus.



A continuación se pondrá un ejemplo de un ataque a un sitio oficial del gobierno de Moscú, el cual ha demostrado tener una seguridad muy poderosa. La finalidad de poner este sitio, es para demostrar que la intrusión cibernética se puede realizar desde y hacia cualquier país del mundo vía internet.

Al ser información confidencial solo se puede copiar la introducción del caso, que es lo que se muestra en la imagen, lo demás únicamente se puede ver, si se quiere conocer los detalles hay que ir al sitio. **www.presidentkremán.**, este sitio cuenta con dos idiomas, el ruso y el ingles.



2.4.- LAS DEFICIENCIAS DE LA LEGISLACIÓN PENAL VIGENTE EN MÉXICO.

El capítulo segundo del código penal federal habla del acceso ilícito a sistemas y equipos de informática diciendo en sus artículos 211 bis al 211bis 7 lo siguiente:

"Capítulo 11 Acceso ilícito a equipos de informática.

Art. 211 bis 1.- Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis a dos años de prisión y de cien a trescientos días de multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días de multa.

Art. 211 bis 2.- Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de cien a seiscientos días de multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días de multa.

Art. 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente modifique, destruya o provoque perdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días de multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente copie información que contengan, se le impondrán de

uno a cuatro años de prisión y de cincuenta a cuatrocientos cincuenta días de multa.

Art. 211 bis 4.- Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún medio de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días de multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Art. 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque la perdida de información que contengan, se le impondrán de tres meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. Las penas previstas en este articulo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Art. 211 bis 6.- Para los efectos de los articulos 211 bis 4 y 211 bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 bis de este código.

Art. 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno"[30].

Como puede observarse en el artículo 211 bis 1, bis 2 y bis 4, se intentó frenar un poco el entrar a un sistema protegido por algún equipo de seguridad, con la finalidad de provocar perdida, destrucción o modificación de información solo que con esto no se frena al intruso cibernético, por que en la redacción del artículo se omitió:

I. Decir la vía utilizada par atacar, la cual para el intruso cibernético es únicamente el internet;
II. Decir que pasa cuando el intruso cibernético no destruye información, no la modifica, no la copia, solo la infecta con un virus que no es destructor, esto es con la finalidad de infectar a otras máquinas o sistemas;
III. Mencionar otra conducta, ésta es la del pirateo de softwear para engañar a la máquina y poderlo manipular a su gusto cuando quiera o lo desee;
IV. Mencionar la manera de cómo localizar al intruso cibernético y a cargo de quien está esta localización;
V. Decir que pasa cuando el intruso cibernético engaña al propietario de este sitio para que le de información que el intruso cibernético necesita;
VI. Darle una proyección internacional, no tan local, esto es decir que sucede en caso de que la conducta del intruso cibernético se realice desde fuera de la república mexicana.

Para que quede claro, pondré el siguiente ejemplo:

Las computadoras que se encuentran en red, es decir, unidas unas a otras, como seria el caso de la UNAM o de la PGR, tienen sus sistema de seguridad, la cual consiste en una contraseña o una clave para poder acceder, siendo sus empleados los únicos que conocen esas claves.

[30] Código Penal Federal, ediciones fiscales ISEF, México, 2002, p. 53, 54

En el supuesto de que se descomponga una de las computadoras de la PGR, mandan llamar a un técnico cualquiera, este no trabaja ahí, es decir es un extraño, pero como con sus conocimientos sabe que están en red, este puede investigar la clave e ingresar al disco duro de la computadora central, una vez allí copia la información que necesita, con esto se cumple lo que dice la ley y en ningún momento existió la intrusión cibernética, porque no buscó a su victima, no le puso trampas o mensajes para que tuviera información, no utilizó uno de los programas para burlar la computadora o al sistema para ingresar a obtener información y nunca tuvo el control de su disco duro y ni mucho menos utilizó su página que se podría encontrar en la red, es decir en el internet.

De los artículos que menciona que al que este autorizado a tener acceso a información y utilice esta autorización para modificar, copiar o destruir información, esta parte mucho menos es intrusión cibernética, porque una de las características de esta actividad ilícita es que no tienen permiso o consentimiento para acceder al sistema, esto es más bien un abuso de confianza tipificado ya en el Código Penal Federal en su artículo 382: es abuso de confianza porque, la conducta delictiva en este delito se encuentra expresada en la ley por el verbo disponer, el cual equivale al de apropiar usado en otras legislaciones y determina el momento consumativo del delito, ya la disposición sea para sí o para otra persona, tal disposición cae sobre la cosa ajena mueble, respecto de la cual el agente tiene la tenencia y no el dominio.

Existe disposición o apropiación cuando el activo del delito incorpora a su dominio privado esta disposición sin el ánimo de restitución. En términos generales el abuso de confianza debe de entenderse como la disposición ilícita de cosa ajena mueble, con el ánimo de dominio por quien lo ha recibido de otro en posesión o en virtud de un acto jurídico. Es un delito catalogado en contra del patrimonio.

La posesión significa la tenencia, no significando necesariamente tener la posesión, debiéndose distinguir con claridad el acto de entrega al de su custodia;

tratándose de dos cuestiones distintas ya que existe custodia a virtud de circunstancias diversas, como la es la relación entre el sujeto activo y el sujeto pasivo.

VII.- En el reglamento a la ley orgánica de Procuraduría General de la Republica, no existe una fiscalía que investigue este delito, ya que de acuerdo a la constitución, este ilícito al ser federal, se perseguirá por la Procuraduría.

VIII.- Tampoco existe una preparación especial para los funcionario encargados de investigar este delito, ya que al ser en materia cibernética, deben tener una preparación adecuada.

IX.- No existe un centro de quejas donde se les de el seguimiento respectivo cuando se sufra un delito de esta índole, y

X.- La falta de acuerdos internacionales para facilitar la detección, captura y en su caso extradición del intruso cibernético, porque, recordemos que esta conducta delictiva es realizable desde cualquier parte del mundo.

2.5.- LA REGLAMENTACIÓN FUE HECHA PARA REGULAR LA CONDUCTA DE MANERA INTERNA, ES DECIR, SOLO EN NUESTRO PAÍS, LO CUAL DEBE CAMBIAR, PORQUE TIENE QUE REGULARSE DE MANERA INTERNACIONAL, ESTO CON EL FIN DE PODER CASTIGAR A ESTOS DELINCUENTES CUANDO SE ENCUENTREN EN OTROS TERRITORIOS QUE NO SEA EL DE MÉXICO.

La única vía que tiene un intruso cibernético para atacar es el internet, ya que al ser éste una red que llega a todo el mundo, este delincuente por lo mismo su ataque lo puede hacer hacia y en cualquier parte del mundo.

El intruso cibernético no siempre realiza su conducta en el país de donde es originario, si no que lo puede hacer hacia cualquier parte del mundo a donde llegue el internet.

Esto dificulta tanto el arresto como el castigo hacia el intruso cibernético, aumentando aún más la dificultad porque no se tienen leyes para reglamentar esta conducta; salvo sus excepciones como la moción existente en la Unión Económica Europea o las leyes penales de algunos Estados de Estados Unidos de Norte América.

Aunque estos países aventajan por tener ya una ley, tiene el problema de que su regulación es interna que en el caso de la Unión Económica Europea les ha servido por la gran cantidad de países que son miembros; mientras que en Estados Unidos de Norte América tienen dificultad porque su ley cambia de un Estado a otro.

El problema que se presenta a nivel mundial es que no existe un acuerdo para poder capturar y castigar al intruso cibernético.

Para subsanar este problema se tiene que hacer un tratado internacional de carácter multilateral, esto no quiere decir que los países que formen parte del acuerdo adopten una ley que imponga un país, sino que el acuerdo sería principalmente para quedar de acuerdo en la captura y extradición para poderlos castigar.

Debe de ser un acuerdo internacional porque es la fuente más importante que tiene el derecho internacional para crear derechos y obligaciones a los países que intervengan, ya que en estos obra el consentimiento expreso en carácter de altas partes contratantes, es decir, que en este caso los Estados que se comprometan a la celebración del acuerdo crearan sus formas y maneras de cómo participar para capturar y en su caso extraditar al intruso cibernético, lo anterior sería como los acuerdos firmados por varios países para el caso de narcotráfico, enriquecimiento ilícito, etc.

Debe de ser un acuerdo internacional multilateral, porque, como menciona el jurista Carlos Arellano García "los tratados multilaterales son aquellos en los que intervienen más de dos Estados o más de dos organizaciones internacionales"[31]

Lo que se pretende es que el acuerdo sea a nivel mundial o si no es posible esto, por lo menos que la mayoría de los países se comprometan con este acuerdo. En el caso de México, éste acuerdo facilitaría el castigo a este tipo de delincuentes, ya que en el artículo 4 del Código Penal Federal, se menciona que:

"Los delitos cometidos en territorio extranjero por un mexicano, contra mexicanos o contra extranjeros; o por un extranjero contra mexicanos, serán penados en la república mexicana, con arreglo a las leyes federales, si concurren los siguientes requisitos:

1.- Que el acusado se encuentre en la república mexicana;

2.- Que el reo no haya sido definitivamente juzgado en el país en que delinquió y;

3.- Que la infracción de que se le acuse tenga el carácter de delito en el país en el que se ejecutó y en la República"[32]

El artículo antes mencionado da requisitos que se deben tener en cuenta para castigar a un delito, razón por la que nos presenta problema para castigar a la intrusión cibernética, porque:

1.- Primero pide para poder castigar a un delito una tipificación que regule esta conducta, porque de otra manera no hay delito por no existir ley que regule ese actuar.

---

[31] ARELLANO GARCÍA, Carlos, "Derecho internacional público", ed. 14ª., edit. Porrúa, S.A. de C.V., México, 1998, p. 188.

[32] Código Penal Federal, edit. Sista, S.A., México, 2002.pp.1,2.

2.- En el caso de la fracción primera no tiene problema, porque, una vez tipificada la conducta es necesario solamente que el intruso cibernético se encuentre en la republica mexicana.

3.- La fracción segunda no representa problema, porque Será Juzgado en el país en el que delinquió el intruso cibernético, y

4.- En la fracción tercera ya representa problema por que no basta que en México exista este delito, sino que debe existir también en el país en el que se ejecuto, por ello se debe de realizar un acuerdo internacional donde se regule esta conducta y exista este delito en los países signatarios del acuerdo. También debe de existir un consenso para ponerse de acuerdo en cuanto a facilitar la detección, captura y extradición del delincuente para castigarlo.

Por las razones antes mencionadas es que se debe de realizar el tratado internacional, para que se regule y no quede más impune la conducta del intruso cibernético, ya que sus conducta puede ser muy grave y necesita un castigo.

2.6. LA CONDUCTA DEL INTRUSO CIBERNÉTICO ES DOLOSA.

Recordemos que el intruso cibernético es un experto en materia de computación, ya sea programando, en materia de seguridad entre otras.

Por este motivo, el intruso cibernético al realizar su conducta para cometer el ilícito sabe de antemano que es lo que va a pasar con ello y más que nada esta consiente de que su actuar esta fuera de la ley por lesionar el derecho a la intimidad que los usuarios deben tener.

Por ello su actuación es de mala fe, es decir, tienen un ánimo de disposición para realizar su acto y con ello obtener una ventaja, la cual es siempre en perjuicio del usuario o de quien posee una página en internet.

Por lo antes mencionado se cumplen los requisitos que debe de presentar el dolo, el cual lo da el artículo 9 del Código Penal Federal diciendo:

"Obra dolosamente el que, conociendo los elementos del tipo penal o previniendo como posible el resultado típico acepta la realización del hecho descrito por la ley"[33]

Esta definición quiere decir que es la voluntad consiente y voluntario de cometer el acto delictivo; es decir, actuar de mala fe, porque existe una disposición de ánimo de quien realiza cualquier conducta con el propósito de obtener una ventaja injusta en perjuicio de alguien, que el derecho sanciona en todo caso.

Para que quede claro el dolo pondremos un ejemplo real de un ataque por un intruso cibernético a un banco en Estados Unidos, este ataque consistió en que se transfirió dinero de una cuenta a otra para cobrarse después por quien atacó.

"En este ejemplo el intruso cibernético buscó a varias posibles victimas, su búsqueda fue dirigida al banco de datos de la computadora por varios días; después que encontró su victima, transfirió dos millones de dólares a su cuenta, (cabe aclarar que su cuenta la abrió en el banco sin presentarse al mismo) dos días después se presentó en el banco para retirar todo el dinero. El banco se puedo dar cuenta dos semanas después, cuando el cliente quiso cobrar un cheque. Este ataque sucedió en 1999 y hasta el 2000 pudieron dar con el lugar donde se realizó la transacción desafortunadamente el intruso cibernético anda prófugo por encontrarse en otro país". [34]

En este ejemplo la mala fe se da desde el momento en que decide realizar esa conducta, y siguiendo con la búsqueda de la victima; indudablemente que el intruso cibernético sabia lo que iba a suceder, estaba consiente de que cometería un delito y obtendría una ventaja por ser experto para entrar al sistema de ese banco. Desde un principio existía una voluntad consiente y voluntaria de cometer un delito que consistió en el traslado de dinero de una cuenta a otra para después retirarla, motivo por el cual debe la intrusión cibernética ser dolosa.

---

[33] Idem

[34] Cfr. CASEY EOGHAN, "Digital evidence on computer crime", San Francisco California, 2000, pp. 182-187.

2.7. LA CONDUCTA DEL INTRUSO CIBERNÉTICO ES UN DELITO GRAVE.

En al artículo 194 del Código Federal de Procedimientos Penales se nos menciona que es lo que se considera delito grave, diciendo éste artículo que:

"Se consideran delitos graves para todos los efectos legales, a aquellos que afecten de manera importante valores fundamentales de la sociedad"[35]

El problema que presenta la definición legal, es la de saber que es un valor; de acuerdo a las diversas teorías filosóficas y más precisamente a la axiología, que es en sí la disciplina que estudia a los valores, se sabe que desde Platón se ha estudiado este tema. Al valor en un principio lo dirigían hacia el bien y hacia el mal, es decir, eran esencias y por lo tanto se pensaba en realidades e irrealidades.

Posteriormente se descubrió que los valores no existen en sí mismos, sino que necesitan a un depositario; así se creyó que el valor era una cualidad que se daba a ciertos objetos llamados bienes y que se captaban a través de los sentidos.

"Este concepto de valor fue evolucionando hasta llegar a decir que el hombre crea el valor con su agrado, deseo o interés; descubriendo ese valor para quien es valioso. Siguió evolucionando el concepto hasta que se dijo que el valor lo tiene cada individuo al captarlos por medio de sus vivencias al percibir los sentimientos y de acuerdo a la necesidad en que se encuentre, de ahí surgió lo que se llama la jerarquía de los valores, porque no todo individuo le da el mismo valor a una cosa que a otro, depende de sus necesidades y situación en que se encuentre".[36]

Para despejarnos la duda de cuáles son los valores fundamentales de la sociedad; el investigador Eduardo López Betancourt dice: "que la ley penal tiene una importante misión de proteger valores vitales para la convivencia humana como lo son:

---

[35] Código Federal de Procedimientos Penales, ediciones fiscales ISEF, México, 2002, p.45.

[36] CFr. FRONDIZI Risiere, "¿Qué son los valores?", Fondo de cultura económica, México, 1995, 14ª. ed.

1) La vida humana.
2) La integridad corporal.
3) El patrimonio.
4) La libertad personal.
5) La paz pública y

6)La seguridad interior y exterior.

Esta protección se hace al través del poder coactivo del Estado, valiéndose de las penas y medidas de seguridad"[37]

Los valores antes mencionados por Eduardo López, se cumplen en la redacción del artículo 194 del Código Federal de Procedimientos Penales; es por ello que debe de considerarse la conducta del intruso cibernético como un delito grave, ya que con su actuar lesionan valores importantes como son:

- La seguridad nacional y exterior, porque, con el ciberterrorismo y el ciberespionaje, las naciones no tienen seguridad en cuanto a que en cualquier momento su información confidencial puede ser tomada o que este tipo de conductas pueden ocasionar un conflicto entre dos o más países.
- El patrimonio, porque con su actuar, pueden sustraer dinero o pasar el mismo de una cuenta a otra, dejando así sin nada de capital a un particular o al mismo Estado. Otro daño patrimonial es el referente a el pirateo que realizan tanto de softwers como de música, marcas, etc.
- La integridad corporal, porque con su actuar, se ha demostrado que la persona que sufre un ataque por parte del intruso cibernético muchas veces sufre de enfermedades, como riesgo a infartos, diabetes, entre otras, con esto pueden atentar en contra de la vida humana.

[37] LÓPEZ BETANCOURT, Eduardo, "Introducción al derecho penal", segunda edición, edit. Porrúa, S.A., 1994, pp. 86y 87.

Por lo antes expuesto es necesario que se tome como delito grave, incluyendo con esto una penalidad ejemplar y el derecho a reparar el daño cuando sea posible repararlo y por lo mismo no debe de otorgarse el derecho a fianza, más cuando atentan en contra de un Estado, tanto en sus finanzas, como en lo militar.

CAPITULO 111. SOLUCIÓN AL PROBLEMA.

La solución posible para combatir eficazmente esta conducta delictiva es realizar una adición al Código Penal Federal, en la cual se describan las conductas de los intrusos cibernéticos, así como sus posibles penas; adicionar al reglamento de la ley orgánica de la Procuraduría General de la República, para crear una fiscalía especializada para el rastreo, ubicación del intruso cibernético. Así como su detención, la cual la puede llevar al cabo la Policía Federal Preventiva; realizar un convenio internacional para afinar cuestiones de extradición.

3.1.- REALIZAR UNA ADICIÓN AL CÓDIGO PENAL FEDERAL.

La adición consiste en agregarle un capítulo en el cual se tenga regulada las diversas conductas de los intrusos cibernéticos, así como su posible penalidad. La propuesta es:

TITULO VIGESIMOQUINTO.

CAPITULO 1.

INTRUSOS CIBERNÉTICOS.

ART. 414.- Al que sin autorización por cualquier vía o medio electrónico, se apodere ,utilice o modifique en perjuicio de tercero, datos reservados de carácter personal o de cualquier otro tipo que se encuentren registrados en soportes o ficheros informáticos, electrónicos, o en cualquier otro tipo de archivo o registro, se le aplicará una pena de 1 a 4 años de prisión.

Si se difunde, revela o ceden a terceros los datos o imágenes descritos en la fracción anterior, se le impondrá una pena de 2 a 5 años de prisión.

Si los hechos descritos en este articulo se realizarán en complicidad con personas encargadas de los ficheros, soporte informático o de cualquier otro tipo

de archivos o registro se le impondrá a los cómplices una pena de 3 a 5 años de prisión, más la separación del cargo.

ART. 415.- A la persona que sin autorización, vía internet viole los sistemas de seguridad de un usuario particular y con ello provoque modificación, destrucción o pérdida de información contenida en ese servidor, se le impondrá una pena de 1 a 2 años de prisión, más la reparación del daño cuando sea posible.

ART. 416.- A la persona que sin autorización vía internet, viole los sistemas de seguridad contenida en un servidor para ingresar a un sitio en internet y copie o modifique información contenida en ese sitio, ya sea para uso personal o para el de un tercero, se le impondrá una pena de 2 a 4 años de prisión.

ART. 417.- A la persona que sin autorización vía internet, viole el sistema de seguridad de un servidor del Estado mexicano y con ello provoque la pérdida, modificación o destrucción de la información contenida en ese sitio, se le impondrá una penalidad de 1 a 4 años de prisión.

ART. 418.- A la persona que sin autorización, vía internet viole los sistemas de seguridad de uno o de varios sitios del Estado mexicano con la finalidad de ingresar a ella para copiar, modificar o destruir información, ya sea para uso personal o para un tercero, se le impondrá una sanción de 6 a 8 años de prisión.

ART. 419.- A la persona que sin autorización, vía internet viole los sistemas de seguridad de uno o varios sitios de las diferentes secretarías de Estado mexicano con la finalidad de copiar, modificar, destruir o perder información que contengan esos sitios ya sea para su uso personal o un tercero, la penalidad será de 8 a 12 años de prisión.

ART. 420.- A la persona que sin autorización vía internet, viole los sistemas de seguridad de los diversos servidores del sistema financiero mexicano y con ello provoque pérdida, destrucción de la información contenida en esos sitios, se le impondrá una pena de 1 a 4 años de prisión.

ART. 421.- Al que sin autorización, vía intenet, viole los sistemas de seguridad contenida en los diversos servidores del sistema financiero con la finalidad de entrar a ese sitio para copiar, modificar o destruir información contenida en esos sitio con la finalidad de usarlo él o un tercero con fines lucrativos o para dañar, se le impondrá una pena de 8 a 12 años de prisión.

ART. 422.- Si el intruso cibernético obtiene la información mencionada en los artículos anteriores con la ayuda de algún funcionario de las dependencias mencionadas, se le impondrá las penas previstas en los artículos correspondientes, más la inhabilitación de su cargo el tiempo que marque la ley federal de responsabilidad de los servidores públicos, más la reparación del daño cuando fuere posible.

ART. 423.- En el caso de que su conducta se realice en contra de tema catalogados como temas de seguridad nacional, se aumentará la penalidad hasta una mitad más.

ART. 424.- A o las personas que sin autorización por medio del internet , logren obtener números confidenciales de tarjetas de crédito o para acceder a cuentas bancarias y realicen con ello transacciones, compras transferencias, fraudes o clonación de las tarjetas de crédito, se le impondrá una pena de 15 a 20 años de prisión, más la reparación del daño a sus víctimas.

En el caso de que lo descrito anteriormente lo realice con ayuda de alguien, se aplicará el artículo 414 párrafo tercero.

ART. 425.-A la persona que mande virus cibernéticos y con ello provoque la destrucción o el deterioro de la computadora y la información que se encuentra en ella, tendrá una pena de 8 meses a 2 años de prisión, más la reparación del daño causado.

ART. 426.- Al intruso cibernético que con ánimo de lucro y en perjuicio e tercero, reproduzca, plagie, distribuya o comunique en todo o en parte, una obra

literaria, artística o científica o su transformación, interpretación o ejecución artística, fijada en cualquier tipo de soporte electrónico y que no tenga la autorización de sus titulares o de sus cesionarios para llevar al cabo la conducta antes mencionada se le impondrá una pena de dos a cuatro años de prisión.

ART. 427.- Para proceder por los delitos previstos en este capitulo es necesaria la denuncia de la persona agraviada o de su representante legal.

No será necesaria la denuncia de la persona agraviada cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.

3.2.- ADICIONAR AL REGLAMENTO DE LA LEY ORGANICA DE LA PROCURADURÍA GENRAL DE LA REPÚBLICA.

La conducta del intruso cibernético por ser un ataque a las vías generales de comunicación y por lo que marca la Constitución Política de los Estados Unidos Mexicanos en su artículo 28, es considerado como un delito federal.

De acuerdo a la Constitución Política de los Estados Unidos Mexicanos en su artículo 21, la persecución de este tipo de delitos le corresponde al ministerio público de la federación, el cual para el despacho de sus asuntos tiene a la Procuraduría General de la República, motivo por el cual es necesario adicionar a la ley orgánica de la Procuraduría General de la República, en la cual se mencione la creación de una fiscalía especial para la persecución de estos delitos cibernéticos.

Lo anterior es viable porque, de acuerdo a la ley orgánica de la Procuraduría General de la República; al ministerio público federal le corresponde entre otras cosas la pronta, expedita y debida procuración de justicia; así como perseguir los delitos del orden federal, lo cual comprende:

- ✓ La recepción de denuncias o querellas sobre un acto que constituya un delito.

- ✓ Investigar los delitos del orden federal con ayuda de sus auxiliares como la Policía Federal Preventiva, la Policía Judicial federal, Peritos, entre otros.
- ✓ Practicar las diligencias necesarias para la acreditación del delito y la responsabilidad del delincuente.
- ✓ Detener y retener a los responsables del delito.
- ✓ Asegurar y tramitar los instrumentos, objetos y producto del delito.
- ✓ Solicitar ordenes de cateo, arraigo, aseguramiento o embargo de bienes indispensables para la averiguación previa.
- ✓ Poner a disposición del Consejo de Menores, a los menores que hubiesen cometido un delito tipificado por las leyes federales.
- ✓ Aportar las pruebas y promover las diligencias para comprobar el delito.
- ✓ Solicitar la imposición de las penas y medidas de seguridad correspondientes, así como la reparación del daño cuando sea posible.

La conducta del intruso cibernético, la puede realizar desde cualquier parte del mundo; motivo por el cual el Ministerio Público de la Federación puede intervenir en la extradición internacional, así como aplicar las tratados celebrados conforme a la Constitución Política de los Estados Unidos Mexicanos.

La creación de la fiscalía especializada para este tipo de delitos, tiene su fundamento en la Ley Orgánica de la Procuraduría General de la República en su artículo 14 párrafo tercero, el cual menciona: "se podrá contar con fiscalías especiales para el conocimiento, atención y persecución de delitos específicos que por su trascendencia, interés y características así lo ameriten"[38].

Estableciéndose en el reglamento su organización y funcionamiento. Esta agencia debe de contener tres áreas muy importantes:

[38] Ley Orgánica de la Procuraduría General de la República, ediciones fiscales, ISEF, S.A., México,2002. p. 9, 10.

1.- **La área técnica**, la cual estará integrada por especialistas en el uso y manejo del internet, esto con la finalidad de poder rastrear al intruso cibernético y por lo mismo saber su ubicación, así como para guardar y juntar todas las pruebas necesarias y no destruirlas o borrarlas.

2.- El área jurídica, compuesta por abogados encargada de llevar a cabo el procedimiento jurídico respectivo hasta sus ultimas consecuencias.

3.- **El área de policía cibernética,** encargada de llevar al cabo la detención de los intrusos cibernéticos, esta policía debe de contar con una capacitación especial en cuanto al manejo de internet, esto con la finalidad de poder identificar el lugar donde se encuentre el delincuente, llevando al cabo esto, no solo se combatirá a esta conducta delictiva, sino a todas las demás que en un momento dado se presenten vía internet.

La fiscalía especializada para los delitos vía internet, debe de contar con los siguientes funcionarios:

1.- **Titular de la dependencia**, el cual será nombrado por el titular de la Procuraduría General de la República.

2.- **Área jurídica**, integrado por licenciados en derecho para llevar al cabo la integración del expediente y llevar el procedimiento respectivo ante las autoridades competentes.

3.- **Área técnica**, conformado por expertos en computación y en el uso y manejo de internet para el rastreo y ubicación del intruso cibernético.

4.- **Área de Policía Especializada**, puede llamarse como en Estados Unidos de Norte América "policía cibernética", la cual podrá ser integrado por miembros de la Agencia Federal de Investigaciones (A.F.I.), ya que las instalaciones de esta agencia cuentan con tecnología de punta, banco de datos, banco de información,

persecución de delitos federales en los que se verá lo que es al análisis fáctico y la coordinación de investigación. Es encargado de perseguir del federales como secuestro, narcotráfico, terrorismo, lavado de dinero, robo, etc.

"La Agencia Federal de Investigaciones cuenta con líneas directas de comunicación con los enlaces policiacos de todos las Procuradurías Generales de Justicia de las entidades federativas y en materia de colaboración internacional se podrán realizar enlaces directos con los representantes de los cuerpos policiacos internacionales tales como la policía española, colombiana y estadounidense, como la DEA; la agencia de aduanas y la Agencia federal de Estados Unidos de Norteamérica (F.B.I.).

La misión de la AFI es ser un auxiliar del Ministerio Público de la Federación, para la investigación y persecución de delitos del orden federal y de aquellos que siendo del fuero común afecten la seguridad nacional o son atraídos por el ámbito federal y cuya aclaración deberá ser con estricta observancia a la legalidad y respeto a los derechos humanos"[39]

Los cuales tendrán que llevar una capacitación especial de manejo de PC y de internet para ser más eficaces.

Atribuciones de los funcionario de la fiscalía:

1.- **Titular de la dependencia**, sus atribuciones son:

I. Coordinar la fiscalía.
II. Recibir las denuncias de este tipo de delitos para su investigación y entregarlo a su personal para la investigación y su integración.
III. Coordinarse con el personal auxiliar para la investigación del delito.
IV. Solicitar a la autoridad competente, ordenes de aprehensión, retención, cateo, aseguramiento de bienes; extradición, exhorto.

[39] AFI (consulta en internet: http://.pgr.gob.mx/afi/prof.htm) México, 13:22 P.M., 06/08/2002.

V. Presentar al titular de la Procuraduría General de la República el expediente integrado para que, se presente al juez competente y se le de el curso legal correspondiente.

VI. Con el apoyo de todos los funcionarios de la fiscalía, planear y coordinar estrategias a seguir para hacer más eficaz a la fiscalía.

2.- **Área Jurídica**, sus atribuciones son:

I. Representar al titular de la fiscalía y por lo tanto a la misma fiscalía.

II. Integrar el expediente respectivo para presentarlo en tiempo y forma al titular de la dependencia para darle el curso legal correspondiente.

III. Llevar el procedimiento respectivo ante el juez competente, esto comprende desde la denuncia hasta sentencia y cuando sea pertinente promover recursos que estén autorizados por la ley.

IV. Pedir al titular de la dependencia, las órdenes de cateo, aprehensión, retensión, aseguramiento de bienes; extradición, exhortos y todo aquello que juzgue pertinente para la integración jurídica del expediente.

V. Coordinarse con los demás funcionarios de la fiscalía para planear y coordinar estrategias para la integración jurídica del expediente.

3.- **Área técnica**, sus atribuciones son:

I. Una vez recibida la autorización correspondiente, rastrear al intruso cibernético para saber su ubicación.

II. Recabar y guardar pruebas que se encuentran en computadoras, servidores, páginas en internet, softwears piratas para tener el control sobre las computadoras y en si todo aquello que pueda servir de prueba que se encuentre en el mundo cibernético.

III. Presentar las pruebas a el área jurídica para su integración, valoración y manejo pertinente.

IV. Coordinarse con la policía especializada para dar su ubicación y así poder aprehenderlo.
V. Coordinarse con los demás funcionarios para planear estrategias con la finalidad de hacer más eficaz a la fiscalía.

4.-**Área de Policía Especializada**, sus atribuciones son:

I. Una vez autorizado por el titular de la dependencia, capturar al intruso cibernético.
II. En caso de que el delincuente se encuentre fuera de la República Mexicana, coordinarse con las autoridades y policías del lugar donde se encuentre para lograr su aprehensión.
III. Coordinarse con las autoridades estatales y municipales de la República Mexicana con la finalidad de obtener coordinación para detener a los intrusos cibernéticos.
IV. Cuando fuera posible recabar y guardar las pruebas que se encuentren en el lugar donde fuese la aprehensión del intruso cibernético.
V. Coordinarse con los demás funcionario de la fiscalía para planear estrategias para hacer más eficaz a la fiscalía.

Pensando en todos los delitos que se pueden cometer por medio del internet, esta fiscalía, no solo sería exclusiva para el intruso cibernético (hacker), si no que sería útil también para perseguir pornografía infantil (pedofilia), secuestros, prostitución, robos, fraudes, y todos los demás delitos que se pueden cometer por esta vía.

En el caso de que el delincuente fuese menor de edad, el ministerio público de la federación, tiene la obligación de ponerlo ante el consejo de menores, para que se le siga el procedimiento que marca la ley y así lograr encausar su conducta a poner en práctica sus conocimientos en la materia de computación a beneficio de la sociedad.

Lo que se le debiera de quitar a la ley para el tratamiento de menores infractores, es que cuando exista la posibilidad de reparación del causado, este menor sí reparara el daño, ya sea él mismo o su padre o tutor, los cuáles son responsables del menor y olvidarse de ir a los tribunales civiles para pedir este derecho que tiene el afectado.

Con respecto a la extradición es necesario tipificar esta conducta, ya que para que se exista esta es necesario que se cumpla el requisito establecido en al artículo seis de la ley de extradición internacional, que dice:

" Darán lugar a la extradición los delitos dolosos o culposos, definidos en la ley penal mexicana, si concurren los requisitos siguientes:

1.- Que tratándose de delitos dolosos, sean punibles conforme a la ley penal mexicana y a la del estado solicitante, con pena de prisión cuyo termino medio aritmético por lo menos sea de un año; y tratándose de delitos culposos, considerados como graves por la ley , sean punibles, conforme a ambas leyes con pena de prisión.

II.- Que no se encuentren comprendidos en alguna de las excepciones previstas por la ley".[40]

3.3.- REALIZAR UN CONVENIO INTERNACIONAL.

Esta conducta delictiva se puede cometer no solo en el territorio nacional, sino que la puede llevar a cabo desde cualquier parte del mundo.

Al respecto la legislación penal mexicana en su artículo cuarto menciona que cuando es cometido un delito fuera del territorio nacional es necesario para su persecución y castigo que exista el delito en los dos países afectados y que para traer a un delincuente que realizó su conducta fuera del territorio nacionales

[40] Ley de extradición internacional (consulta en internet: www.info jus. com) México, 08/08/2002, 14:30 P.M.

necesario un tratado de extradición, motivo por el cual es necesario realizar un tratado internacional al respecto.

El tratado es definido en la ley sobre la celebración de tratados como " el convenio regido por el derecho internacional publico, celebrado por escrito entre el gobierno de los Estados Unidos Mexicanos y uno o varios sujetos de derecho internacional publico. Los acuerdos interinstitucionales solo podrán ser celebrados entre una dependencia u organismo descentralizados de la administración pública federal, estatal o municipal y uno o varios órganos gubernamentales extranjeros u organizaciones internacionales"[41]

El tratado debe de ser multinacional porque intervendrían más de dos países, recordemos que dentro del derecho internacional público, la fuente más importante para la creación de derechos y obligaciones son los tratados o acuerdos internacionales, ya que en ellos se contiene el consentimiento expreso de los Estados intervinientes en su carácter de partes contratantes.

Por otro lado, los tratados internacionales tienen la virtud de concretar con precisión y claridad por escrito, las normas jurídicas que vinculan a los estados participantes.

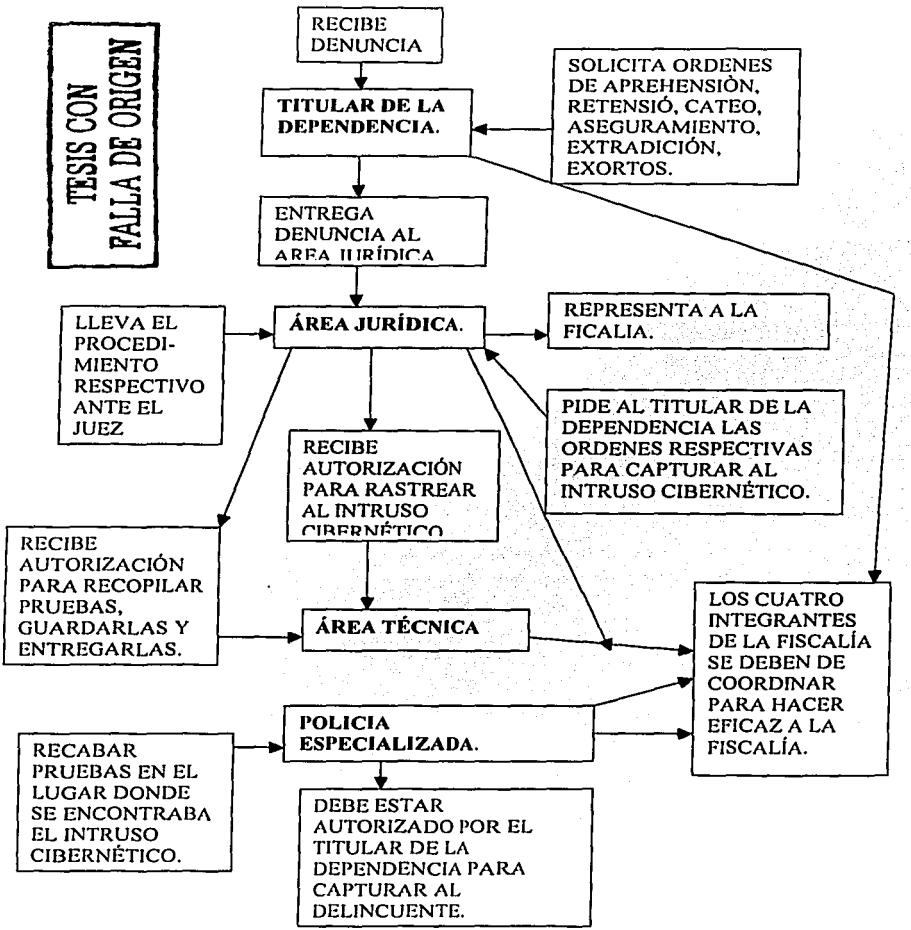
"La importancia que tiene los tratados internacionales, esta reconocido en el preámbulo de la carta de las Naciones Unidas, cuando se asevera la voluntad de los pueblos tendientes a crear condiciones bajo las cuales puedan mantenerse la justicia y el respeto a las obligaciones emanadas de los tratados y de otras fuentes del derecho internacional"[42]

---

[41] Ley sobre la celebración de tratados internacionales (consulta en internet: www.info jus.com) México, 08/08/2002. 15:25 P.M.

[42] ARELLANO GARCIA, Carlos, "primer curso de derecho internacional público", 3ª. Edi., edit. Porrúa, S.A., México, 1986, p. 186.

ORGANIGRAMA DE LA FISCALIA PROPUESTA EN ÉSTA TESIS



CAPITULO IV. DEMOSTRACIÓN DE LA SOLUCIÓN.

Para poder demostrar la solución planteada en el capítulo anterior, es necesario revisar las legislaciones de los países que se encuentran más adelantados en este tema, para que con ello, nos demos una idea de la magnitud del problema; la solución que han dado y algo muy importante, como es el saber en que han fallado, para que México no cometa esos mismos errores y su ley sea práctica y confiable.

Así pues, comenzaré en el continente americano con el gigante de este tema que es Estados Unidos de Norte América, ya que es el más avanzado; así como Argentina por ser después de Estados Unidos quien ha estado abordando este tema.

En el continente europeo, el gigante por sus avances en este tema y por su economía es la Unión Económica Europea, ya que como comprende varios países, estos han logrado tener uniformidad en sus leyes que penalizan al intruso cibernético; a nivel de Estados Europeos; se verá a España, por ser uno de los más avanzados en congruencia de sus leyes internas con las existentes en la Unión Económica Europea.

4.1. EN AMERICA LATINA:

4.1.1.- ESTADOS UNIDOS DE NORTE AMÉRICA.

Este pais, en lo concerniente a las intrusos cibernéticos se ha dividido en dos, la primera parte va desde finales de los setentas y principios de los ochentas hasta el 2001, con la creación de una ley para intervenir los aparatos telefónicos, en esta época era solo de control y para prever algunas conductas delictivas y la mayoría de estas conductas eran delitos menores, llamados felonías, los cuales eran sancionados con multa y la reparación del daño causando. Existía un poco más de libertad, ya que se encontraban en proceso leyes para combatir estos delitos.

La segunda etapa que comienza a partir del 11 de septiembre del 2001, año en que es burlada la seguridad y derriban las torres del centro mundial del comercio y el ataque al Pentágono y los continuos ataques con ántrax, Estados Unidos ha entrado en una nueva era de terrorismo que toma como blanco tanto a civiles como a soldados, en una guerra sin reglas y sin un final claro. Ha habido un constante avance hacia este punto mediante eventos tales como el estallido en 1998 del vuelo 103 de Pan Am sobre Lockerbie, en Escocia; el caso de los intrusos cibernéticos ha Hannover en 1998; el caso de fraude en el Citibank en 1994, y el atentado dinamitero de la ciudad de Oklahoma en 1995.

Aunque los medios y los fines hayan evolucionado a través de la historia, los elementos esenciales del terrorismo (miedo, pánico, violencia y dislocamiento) han cambiado poco. Mientras el mundo entra en el siglo XXI, el terrorismo sigue siendo un problema exasperante humano e inhumano en el Tercer Milenio como lo fue antes, en los albores de la historia escrita. Si bien en una ocasión los terroristas utilizaban actos de terrorismo como medio de hacer propaganda a sus causas, los objetivos operativos de los ataques más recientes se concentraron en producir el máximo de destrucción.

"Hoy, un potencial destructivo tremendo cabe en paquetes fácilmente transportables (bombas, gas neurotrópico o de nervios y agentes biólogos), y las computadoras conectadas con la internet pueden ser atacadas desde cualquier punto de la tierra. La amenaza de represalias, efectiva contra las naciones, no lo es tanto contra grupos pequeños y evasivos que golpean anónimamente y no tienen territorios que retener a su propio riesgo.

La necesidad de aumentar la seguridad de las operaciones críticas ha crecido marcadamente en años recientes, como resultado del enorme aumento del uso de la tecnología de la información para mejorar el desempeño, las presiones competitivas incrementadas resultantes de la supresión de regulaciones y la mundialización y la concentración de operaciones en un número menor de

instalaciones para así reducir costos, con la reducción resultante de redundancia y capacidad de reserva.

El instituto de seguridad de computadoras (CSI), que lleva a cabo una encuesta mundial del crimen y la seguridad en las computadoras, con participación de la escuadra de intrusión en computadoras de la Oficina Federal de Investigaciones (F.B.I.) en San Francisco, ha informado en su encuesta del 2001 que las pérdidas que sufrieron ciento ochenta y seis de los que respondieron a la encuesta totalizaron aproximadamente trescientos setenta y ocho millones de computadoras detectadas principalmente por grandes corporaciones, agencias de gobierno y universidades.

Las violaciones de seguridad detectadas por los que respondieron a la encuesta incluyen una gama de ataques tales como: acceso no autorizado por parte de personal de la misma entidad, negativa de servicio, penetración de sistemas por parte de elementos ajenos a la entidad, robo de información protegida por derechos de propiedad intelectual, fraude financiero y sabotaje de datos y redes. Los sistemas de control, supervisión y adquisición de datos (SCADA) son particularmente vulnerables cuando usan la internet para vigilar y controlar procesos en sitios distantes. Tal práctica la emplea una variedad de industrias, entre ellas la química, petroquímica, petróleo y gas, elaboración de alimentos, pulpa y papel, productos farmacéuticos, agua y gas servidas, transporte, administración de energía y otras aplicaciones manufactureras.

Las pérdidas financieras, por supuesto, no se restringen al robo de información protegida por derechos de propiedad intelectual, el fraude financiero y otros delitos.

A medida que se lleva a cabo un mayor volumen de comercio en línea, aumentan las demandas civiles en la que los demandantes procuran, en orden vertical descendente, indemnización por daños debidos a intrusiones en las redes,

basándose en teorías legales tales como falta de debida diligencia en la relación con los accionistas, clientes, proveedores y otros terceros inocentes.

En respuesta a estas crecientes vulnerabilidades de la infraestructura crítica, el presidente Clinton estableció en 1998 la comisión del presidente sobre la protección de la infraestructura crítica (PCCIP), con el objeto de estudiar las infraestructuras críticas que constituyen los sistemas de apoyo vitales de Estados Unidos, determinar vulnerabilidades y proponer una estrategia para protegerlas.

El informe, puesto en práctica en 1998 mediante la Directiva de Decisión Presidencial (PDD) 63 sobre Protección de la Infraestructura Crítica, declara que las instalaciones federales deben estar entre las primeras en adoptar las mejores prácticas, administración activa del riesgo y planificación de seguridad mejorada, con lo cual presentarían un modelo para que la industria lo siga voluntariamente. La PDD exige la creación de una firme asociación con la comunidad empresarial y los gobiernos de Estados y localidades para maximizar la alianza a favor de la seguridad nacional.

La directiva estipulo en el establecimiento del Centro Nacional de Protección de la Infraestructura, mediante la conversión del centro de evaluación de la Amenaza a la infraestructura e investigación de computadoras en el núcleo del NIPC. El NIPC une a representantes de la agencia federal de investigación de Estados Unidos (F.B.I.), los departamentos de Comercio, recursos energéticos, la comunidad de inteligencia y otras agencias federales con el sector privado, en un esfuerzo de intercambio de información que no tiene precedentes.

La misión del NIPC consiste en detectar, dar la alarma, responder e investigar intrusiones en computadoras que amenazan la infraestructura crítica. No sólo provee una respuesta de reacción a un ataque que ya ha ocurrido, sino que busca de modo activo procurar descubrir los ataques que se planean y dar la voz de alerta antes de que ocurran.

Esta labor requiere la recopilación y análisis de información recogida en todas las fuentes disponibles y la diseminación entre las victimas potenciales de análisis y llamados de alerta contra posibles ataques, ya sea que pertenezcan al gobierno o al sector privado". [43]

Por lo antes expuesto, todo cambio y ahora son más estrictos tanto en sus leyes como en sus procedimientos como se verá a continuación:

A) LEY PARA PODER INTERVENIR LAS LINEAS TELEFÓNICAS.

Llamada " Telephone Consumer Protection Act". Ahora abarca:

- Sistemas de teléfonos automáticos; fijos y celular;
- Máquina de fax;
- Intervención de solicitudes de nuevas líneas telefónicas.

La finalidad es de que se tienen bases de datos de todos los usuarios o posibles usuarios para tenerlos bajo vigilancia y así tener un control para poder saber cuando podrían realizar una conducta delictiva , sobresaliendo de manera especial el terrorismo.

El fundamento legal para dar paso a esta intervención telefónica, es la que se encuentra en el artículo 18 de la Constitución de Estados Unidos de Norteamérica, el cual consagra el principio de seguridad nacional; agregando lo concerniente al derecho a la protección de la intimidad y la restricción a la garantía de expresión y comunicación.

"Esta ley establece que habrá una comisión para investigar las llamadas telefónicas, fax o correos eléctronicos sospechosos, así como al intruso cibernético que entra a determinados sitios webs.

[43] Agenda de la política exterior de Estados Unidos de Noviembre del 2001. "Protección contra el terrorismo cibernético en Norte América" [Trad. Gelacio Cortés Ramírez.], (consulta en internet: http://www.usinfo.state.gov/journals/jourpa.htm) México, 15:00 P.M., 10/10/2001.

En el dado caso de que se encontraré una llamada, fax o correo electrónico que sea sospechosa, la comisión correspondiente le dará aviso a las autoridades para que se le persiga y enjuicie en las cortes de jurisdicción federal, las cuales podrán sancionar con cárcel o con multa o con cárcel sin multa sobresaliendo que siempre se da la reparación del daño causado.

Sobresaliendo además lo expedito de este procedimiento, porque no se necesita denuncia, basta con la identificación de la llamada para iniciar el procedimiento y juzgarlo para dictarle sentencia.

Donde se han intensificado más esta práctica es en las zonas rurales, donde existe una policía específica para estos lugares, ya que por lo alejado de las grandes ciudades o por la ignorancia de estas personas del campo, pueden ser más vulnerables para este tipo de ataque, lo que le da vida a esta policía es el "formland protection policy" o protección de la policía rural; encontrándose en el capítulo VII de la ley de intervención telefónica.

Esta ley es importante porque, el intruso cibernético realiza sus diferentes conductas delictivas por medio del internet, el cual se proveer por línea telefónica, ya sea fija o móvil; esta ley regula las intervenciones a estos sistemas de comunicación". [44]

B) LEY DE ESPIONAJE ECONÓMICO.

Aprobada el 17 de septiembre de 1996, penaliza el desarrollo y el intercambio de conocimientos y otorga poder al servicio secreto de inteligencia para actuar en todo el mundo con el fin de proteger los derechos de propiedad intelectual de las empresas estadounidenses, a los que considera vitales para la seguridad nacional.

---

[44] "Telephone consumer protection act", [Trad. Gelacio Cortés Ramírez], (consulta en internet: www.legislation.hmso.gov.uk) México, 12:00P.M., 11/10/2001.

A esta ley le surge una paradoja, porque considera propiedad intelectual a la información pirata otorgada de sociedades no occidentales y comunidades indígenas. En Estados Unidos, el poder imperial siempre se ha apoyado en la conjunción similar en torno a la defensa del comercio y ahora se esta dando una conjunción similar en torno a la defensa de los intereses comerciales en un periodo de globalización y del llamado libre comercio, con la intromisión del servicio secreto en lugar del poder militar.

Estados Unidos que edificó su poderío económico y capacidad manufacturera librándose del monopolio británico, ahora no esta dispuesto a permitir a través de esta ley, del congreso y de las empresas, que ese espíritu de libertad y desarrollo económico se de en otras partes del mundo. Cabe recordar que las empresas estadounidenses han pirateado innovaciones indígenas y tercermundistas y ahora con esta ley dicen que es propiedad intelectual y hacer lo mismo esta ya penado.

Si alguien quisiera hacer lo mismo que Estados Unidos, con esta ley sería arrestado en cualquier parte del mundo y encarcelado mínimo 15 años, o multado con hasta 10 mil dólares.

Esta ley establece en su introducción que el desarrollo y la información económica de carácter patrimonial es parte integral del bienestar económico de Estados Unidos, por otra parte los intrusos económicos de la nación son para Estados Unidos, parte integrante de su seguridad nacional. Por lo tanto toda acción al interés económico de la nación es una amenaza a la seguridad vital de la nación.

"Menciona la ley que el espionaje típicamente consiste en un procedimiento bien organizado por parte del gobierno de un país con el fin de obtener información vital para la seguridad nacional. Con esto redefinen la transferencia de tecnología como espionaje económico o industrial.

A Estados Unidos se le olvido con esta ley que el desarrollo científico y tecnológico depende del libre intercambio de conocimiento, tecnológico e ideas y sobre todo en ese intercambio que se ha definido como espionaje" .[45]

C) LEY PARA PROTEGER EL CORREO ELECTRÓNICO (E-MAIL)

Esta ley se auspicio bajo el dicho de dime que correo electrónico usas y te diré como te tratará la ley. La finalidad es el de proteger el correo electrónico, permitiendo a los patronos revisar los correos electrónicos de sus trabajadores. Esta ley responde a las ya varias iniciativas al respecto y sobre todo a la creciente delincuencia del correo electrónico (e-mail).

La ley define lo que se debe de entender por correo electrónico, diciendo que "es toda correspondencia, mensaje, archivo, dato u otra información electrónica que se transmite a una o a más personas por medio de una red de interconexión entre computadoras y lo equipara a los efectos legales, a la correspondencia epistolar".[46]

El artículo 153 de esta ley menciona que la penalidad por este tipo de delitos es de 15 días a 6 meses de prisión, el que obtuviera indebidamente una carta, un correo electrónico, un pliego cerrado o un despacho telegráfico, telefónico o de otra naturaleza que no le este dirigido; o se apoderé indebidamente de una carta, de un correo electrónico, de un pliego, de un despacho o de otro papel privado, aunque no esté cerrado, o suprimiere o desvíe de su destino una correspondencia que no le esté dirigida.

Se le aplicará prisión de 1 mes a 1 año, si el culpable comunicaré a otro o publicare el contenido de la carta, correo electrónico, escrito o despacho.

---

[45] Cfr. "Análisis jurídico de la ley de espionaje económico" (consulta en internet: www.law.cornell.edu/) México, 13:00 p.m., 11/10/2001.
[46] "Ley para proteger el e-mail". [Trad. Gelacio Cortés Ramírez], (consulta en internet: www.finlaw.com) México, 16:30 P.M., 11/10/2001.

El artículo 155 menciona que, el que se hallaré en posesión de una correspondencia, un correo electrónico, un pliego cerrado o un despacho telegráfico, telefónico o de otra naturaleza no destinados a la publicidad, los hiciere publicar indebidamente, aunque hayan sido dirigidos a él, será reprimido con multa de 1.500 a 90.000 dólares, si el hecho causare o pudiere causar perjuicios a terceros.

D) **COMISIÓN FEDERAL DE COMERCIO.**

Publica lo que se llama " top ten the swindle the cybercrimen" (top 10 de las estafas informáticas), ya que desafortunadamente, el internet no solo es un medio de información y entretenimiento, sino que se ha convertido en el vehículo propicio para cometer crímenes y estafas informáticas, las siguientes son las estafas más comunes en Estados Unidos de Norteamérica, ya que han tenido más de 285,000 quejas:

"1.- FRAUDE UN SUBASTAS:

Después de enviar el dinero, el vendedor recibe el pago, el comprador recibe un producto de menor valor o de ningún valor en absoluto.

2.- ESTAFAS DE PROVEEDORES DE SERVICIOS DE INTERNET:

El usuario puede encontrarse atrapado en un contrato de larga duración para acceso a Internet, con graves penalizaciones por rescisión.

3.- DISEÑO/ PROMOSIONES DE SITIOS WEB:

El usuario recibe cargos en su factura de teléfono por servicios que nunca ha aceptado ni solicitado.

4.- ABUSO DE TARJETAS DE CRÉDITO:

Se le solicita al usuario su número de tarjeta de crédito, argumentando que se hace exclusivamente para verificar su edad y luego se le pasan cargos difíciles de cancelar.

5.-MARKETING MULTINIVEL/ ESTAFAS DE PIRÁMINES:

Se le promete hacer dinero a través de productos y servicios que el usuario venderá, así como a través de los vendidos por gente que él reclute. A la hora de la verdad, resulta que sus clientes son otros distribuidores, no el público y sus beneficios se evaporan.

6.- OPORTUNIDADES DE NEGOCIOS Y ESTAFAS "TRABAJE DESDE CASA":

Se le proporcionan a la victima grandes cantidades en un negocio del que el usuario será su propio jefe, ganado cantidades fabulosas de dinero.

Por supuesto, después de que él invierta sus ahorros en esta maravillosa oportunidad de negocio, resulta que todo era humo.

7.- ESQUEMAS DE INVERSIÓN Y ESTAFAS TIPO "HAGASE RICO RAPIDAMENTE":

El navegante puede perder su dinero al confiar en programas o servicios de inferior calidad a la pagada, o le cargan por conceptos que no aparecían en el contrato.

8.- FRAUDE EN VIAJES/ VACACIONES:

Compañías fraudulentas le mienten a los usuarios respecto a sus paquetes de viajes al ofrecerle alojamiento y servicios de inferior calidad a la pagada, o le cargan por conceptos que no aparecían en el contrato.

9.- FRAUDES TELEFÓNICOS:

Sin que el usuario lo sospeche, mientras ve toneladas de fotos y videos porno utilizando un programa que debe instalar en su computadora, el módem se conecta silenciosamente y marca un número internacional, para acceder a internet a tráves de un ISP en el extranjero.

10- FRAUDES DE ATENCIÓN SANITARIA:

¿Qué sufre de una enfermedad incurable?, no se preocupe, aceite de serpiente a la venta a módico precio que curará ésta y cualquier otra dolencia incurable... Este tipo de mensajes se convierten muchas veces en la versión cibernética de los famosos culebros".[47]

E) AGENCIA FEDERAL DE INVESTIGACIONES DE ESTADOS UNIDOS DE NORTE AMÉRICA (FBI) Y SUS TROYANOS.

"El titulo de una enmienda que le da autorización al F.B.I. (Federal Bureau of Investigation) para desarrollar su propio programa de caballo de trolla, este programa es usado para ser puesto en los discos duros de las computadoras vía correo electrónico y así poder investigar sin que el usuario se de cuenta: este programa es para desarrollar el terrorismo.

La idea del programa es robar las contraseñas de todo aquel, en principio sospechoso, que use el correo electrónico encriptado para sus comunicaciones.

Este troyano, conocido como " magic lanterna" o linterna mágica, podría enviarse a cualquier sospechoso, como un adjunto a un mensaje aparentemente inocente.

Aprovechándose de algunas vulnerabilidades, podría incluso instalarse sin el conocimiento del destinatario y a partir de allí capturaría las contraseñas usadas por el supuesto terrorista, enviándolas a las oficinas del F.B.I. Linterna mágica es llamado cyber knight o caballero cibernético, el cual incluye una base de datos que permitiría al F.B.I. cruzar información proveniente de correos electrónicos, salas de platica, mensajeros instantáneos tipo ICQ y llamadas telefónicas por internet.

[47] "Comisión federal de comercio" . [Trad- Gelacio Cortés Ramírez.], (consulta en internet: www.usdoj.gov/criminal/cybercrimen/search-does/toc htm) México, 17:30 P.M., 11/10/2001.

El uso de una herramienta como la antes descrita, no sería lo más apropiado, puesto que resultaría hasta trivial que los antivirus detectaran algo así y esperar que los terroristas no se preocupen de tener un antivirus al día, sería un acto irresponsable.

Por otro lado se encuentran las libertades individuales, ya que organizaciones norteamericanas que defienden los derechos civiles de los ciudadanos ya han reaccionado ante lo que consideran un claro abuso a este principio.

Linterna mágica no deja de ser peligroso, en el sentido que no pasaría de ser un troyano más, con mayor o menor sofisticación, pero troyano al fin. Casi sería como combatir al ántrax con ántrax. La USA Patriot Act (constitución de Estados Unidos de Norte América), habilitan al F.B.I. para este tipo de acción, pero se debe de recordar que no todos los ciudadanos son norteamericanos". [48]

F) **CENTRO DE QUEJAS.**

El centro de quejas para fraudes en internet (IFCC "The intenet fraud complaint center) es co-patrocinado por el FBI y la NW3C (centro nacional de delitos de cuello blanco " national whit collar crime center). Las quejas que hacen en estos sitio webs son procesados y encausados al derecho aplicable o a las agencias reguladoras para su investigación. Toda información es confidencial por parte de la agencia que recibe la denuncia.

La clasificación de quejas por el IFCC, no permite por ningún motivo que la notificación, queja o denuncia, así como las pruebas aportadas, se de a cualquier persona, proporcionando garantía para que su información sea confidencial por encriptar la información recibida .

La IFCC usa los datos que voluntariamente se proporcionan para ayudar a las víctimas del internet, una vez recibida la información , esta la mandan a el NW3C,

[48] "Fedral Boureau of Investigation". [Trad. Gelacio Cortés Ramírez], (consulta en internet: www.findlaw.com/fbi) Méxiso, 11:30 A.M. 12/10/2001.

para su integración, luego se manda al FBI, para su persecución y detención así como llevarlo a juicio.

Su funcionamiento es que en la red del internet existen sitios webs o sitios de ayuda a las personas que han sufrido un daño por un delito cibernético.

La información que se da en este sitio es encriptada, es decir, se pone bajo resguardo por parte de la agencia correspondiente, con una clave, la cual puede ser números, cifras, letras o su combinación de estas y por medio de esto nadie puede modificar la información que se tenga; se puede solo leer, pero se corre el peligro de que la agencia correspondiente le suelte el programa de caballo de trolla para investigarlo por ser sospechoso de terrorismo, no importando que se encuentre en otro país, pudiendo investigar lo que quiera sin que el usuario se de cuenta y en el momento de que su actuar sea sospechoso, va el F.B.I., lo detiene y lo lleva a juicio, todo esto fundado en el principio de seguridad nacional.

Cabe mencionar que lo dicho antes, Estado Unidos, lo puede llevar al cabo en cualquier parte del mundo, pero para meterse a detener a un sospechoso solo no lo hace en la Unión Económica Europea y en los países asiáticos de China y Japón, ya que en estos países, se tiene que pedir extradición y permiso para entrar a detener, pero en el resto del mundo, Estados Unidos no lo respeta.

"Sobresalta la detención casi indefinida de los no-ciudadanos (inmigrantes). Las detenciones policiales pueden durar desde las 48 horas hasta los 7 días, antes de ser puestos en los destinos a disposición judicial.

Se minimiza la supervisión judicial sobre las escuchas telefónicas e internet, se habilita al gobierno para realizar investigaciones secretas, fuera del control judicial. El F.B.I. tendrá amplio acceso a datos recogidos por empresas sobre individuos que a tenor del FBI resulten sospechosos de realizar actividad delictiva. Dichas escuchas tienen una justificación legal, evitar el control judicial es por tanto

peligroso para el ciudadano, ya que la autoridad al poder evitar los controles puede, también, caer en la arbitrariedad.

A esta forma de actuar le da vida la Provide Apropiate Tools Required to Intercept and Obstract Terrorism Act".[49]

G) **DEPARTAMENTO DE JUSTICIA DE ESTADOS UNIDOS**:

"Este departamento ha endurecido la legislación relacionada con el cibercrimen ya que se le ha otorgado al gobierno la potestad de incrementar las penas para los crímenes relacionados con el intruso cibernético, o las conductas desplegadas por el intruso cibernético, proporcionan directrices para determinar las sentencias diferenciando los delitos para lucro personal de aquellos que pueden afectar a la defensa y la seguridad nacional.

El departamento de justicia contará con el NII (National Information infraestructure "el centro nacional de información"), la cual proporciona y organiza los records de fraudes de tarjetas de crédito y da la garantía de protección federal.

La general accounting office "la oficina general de contabilidad", se encarga de recabar información de mal uso de computadoras y que este mal uso sea un delito, presenta testimonio a la casa de operaciones gubernamentales, al comité de información, al de justicia, al de agricultura y a la de transportación para que se integran los expedientes respectivos y poder llevarlos a juicio.

Su función principal de la GAO es evaluar la información para poder entregarla a las demás agencias e iniciar el procedimiento. El departamento de justicia esta dividido en subsecciones, cada una tiene su función especifica, sus funciones son:

- SUBSECCION A: Usada solamente cuando se tenga la intención de causar un daño a los Estados Unidos y con ello se tenga la posibilidad de sacar ventaja una nación extranjera.

[49] "The internet fraud complint center". [Trad. Gelacio Cortés Ramírez], (consulta en internet: www.findlaw.com) México, 14:00 P.M. 12/10/2001.

- SUBSECCION B: Es encargada de proteger la confiabilidad de las datos de computadoras del gobierno coordinándose con el comité judicial del senado.
- SUBSECCION C: Encargada de proteger las computadoras usadas por el gobierno cuando éste no sea necesariamente el usuario u operador y se pueda presentar confusión.

- SUBSECCION D: Es encargado de asegurar la sanción aplicando cuando se use una computadora y no se esta autorizado o se exceda en esa autorización y con ello se cause un delito.

- SUBSECCIÓN E: Encargado de dar protección federal a los sistemas que contienen finanzas del gobierno para luchar contra el mal uso, en especial, darle más cuidado a la intrusión cibernética para la transferencia de fondos o de recursos.

Si alguien entra y no esta autorizado es responsable de su actuar y de sus consecuencias causando un delito y además un daño a su victima, aumentando con ello la penalidad. Siendo además un delito grave cuando cause un daño o un perjuicio y a parte obtenga una ganancia con ese mal uso o con la entrada ilegal a ese web y así un estado pueda obtener ventaja en diversos ámbitos.

- SUBSECCION F: Es el encargado para saber cuando se tengan amenazas contra computadoras o cadenas de computadoras. Las amenazas por lo regular deben de llevar o ir acompañadas de una extorsión o una amenaza de extorsión y destrucción del sistema económico norteamericano.

La creación de estas subsecciones tienen su fundamento en el artículo 18 de la constitución norteamericana, ya que se prevee el derecho a la privacidad, así

pueden gravar todo lo que pueda ser sospechoso, cuidando sobre todo los fraudes de tarjetas de crédito". [50]

H) UNIDAD DE INVESTIGACIÓN DE LA DELINCUENCIA EN TECNOLOGÍA DE LA INFORMACIÓN.

"El cuerpo nacional de policía ha sido creado para perseguir los delitos informáticos. Entre las funciones de la nueva Unidad de Investigación de la Delincuencia en Tecnologías de la Información se encuentra la investigación de: Estafas, amenazas, calumnias e injurias, revelación de secretos, defraudaciones Contra la Propiedad Intelectual, etc. Que se realizan principalmente a través de internet. También la Unidad investiga delitos de fraude en el uso de las telecomunicaciones, telefonía etc.

En muchas ocasiones se viene hablando de nueva delincuencia, sería más correcto hablar de nuevas formas para cometer delitos ya clásicos, tal es el caso de las infracciones penales contra la propiedad intelectual, de manera especial aquellos que tienen por objeto el enriquecimiento por medio de la copia y la distribución no autorizada de programas y soportes lógicos de ordenador, así como la mera tenencia de dispositivos que permitan eliminar las protecciones de dichos programas, actividad delictiva conocida como piratería informática, la cual supone pérdidas millonarias del sector, el debilitamiento de la industria y a la postre la perdida de competitividad y de puestos de trabajo.

Otro tanto cabe destacar del delito de daños mediante destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas operativos informáticos, tristemente populares con el del virus melisa o el más reciente I love you, con resultados de perdida multimillonarias en sectores claves de la economía mundial por medio de los modernos sistemas de comunicación, en

[50] "Departament of Justice" . [Trad. Gelacio Cortés Ramírez], (consulta en internet: www.justice departement home page) México, 17:00 P.M., 12/10/2001.

estos casos la Unidad de la policía se encarga de rastrear la pista de la amenaza a través de la red utilizando técnicas innovadoras.

El esfuerzo investigador del cuerpo nacional de policía se concreta en el desarrollo de la unidad de investigación de la delincuencia en tecnologías de la información, la cual cuenta con una estructura central y otra territorial.

En la estructura central se destacan tres secciones claramente diferenciadas. De una parte el área de Delitos cibernéticos se encargará de la investigación de los delitos contra la libertad sexual, pornografía infantil, amenazas, calumnias e injurias cometidas a través de la red.

Por otro lado la sección de delitos de telecomunicaciones atenderá las investigaciones de los delitos cometidos por medio de telefonía fija o móvil, los locutorios clandestinos y en las comunicaciones mediante el uso de tarjetas de prepago.

Finalmente la sección de investigación y desarrollo es la competente en el ámbito de las relaciones internacionales, el conocimiento y difusión de la legislación sobre la materia, la elaboración de los estudios e informes para la mejora en la toma de decisiones, así como el estudio y el análisis permanente de nuevos medios y tecnologías de interés policial.

La novedad de la apuesta de la dirección general de la policía radica en la creación en cada jefatura superior de una estructura de investigación integrada en el área de policía judicial permanente coordinada con la unidad de investigación".[51]

Estados Unidos de Norteamérica, para realizar sus leyes se han basado una parte en su constitución, pero la mayor parte de estas legislaciones son en base a

[51] "Unidad de investigación de la delincuencia en tecnología de información" (consulta en internet: www.find law.com) México, 10:00A.M., 13/10/2001.

la convención americana sobre los derechos humanos, la cual es suscrita en San José de Costa Rica el 22 de noviembre de 1969, esto es por lo mencionado en el preámbulo de dicha convención, así como en algunos de sus artículos, los cuales dicen:

"PREAMBULO

Los Estados americanos signatarios de la presente Convención,

Reafirmando su propósito de consolidar en este Continente, dentro del cuadro de las instituciones democráticas, un régimen de libertad personal y de justicia social, fundado en el respeto de los derechos esenciales del hombre;

Reconociendo que los derechos esenciales del hombre no nacen del hecho de ser nacional de determinado Estado, sino que tienen como fundamento los atributos de la persona humana, razón por la cual justifican una protección internacional, de naturaleza convencional coadyuvante o complementaria de la que ofrece el derecho interno de los Estados americanos;

Considerando que estos principios han sido consagrados en la Carta de la Organización de los Estados Americanos, en la Declaración Americana de los Derechos y Deberes del Hombre y en la Declaración Universal de los Derechos Humanos que han sido reafirmados y desarrollados en otros instrumentos internacionales, tanto de ámbito universal como regional;

Reiterando que, con arreglo a la Declaración Universal de los Derechos Humanos, sólo puede realizarse el ideal del ser humano libre, exento del temor y de la miseria, si se crean condiciones que permitan a cada persona gozar de sus derechos económicos, sociales y culturales, tanto como de sus derechos civiles y políticos, y

Considerando que la Tercera Conferencia Interamericana Extraordinaria (Buenos Aires, 1967) aprobó la incorporación a la propia Carta de la Organización

de normas más amplias sobre derechos económicos, sociales y educacionales y resolvió que una convención interamericana sobre derechos humanos determinara la estructura, competencia y procedimiento de los órganos encargados de esa materia, Han convenido en lo siguiente:

Artículo 2. Deber de Adoptar Disposiciones de Derecho Interno

Si en el ejercicio de los derechos y libertades mencionados en el artículo 1 no estuviere ya garantizado por disposiciones legislativas o de otro carácter, los Estados partes se comprometen a adoptar, con arreglo a sus procedimientos constitucionales y a las disposiciones de esta Convención, las medidas legislativas o de otro carácter que fueren necesarias para hacer efectivos tales derechos y libertades.

Artículo 13. Libertad de Pensamiento y de Expresión

1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar:

a. el respeto a los derechos o a la reputación de los demás, o

b. la protección de la seguridad nacional, el orden público o la salud o la moral públicas.

3. No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de

información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones.

4. Los espectáculos públicos pueden ser sometidos por la ley a censura previa con el exclusivo objeto de regular el acceso a ellos para la protección moral de la infancia y la adolescencia, sin perjuicio de lo establecido en el inciso 2.

5. Estará prohibida por la ley toda propaganda en favor de la guerra y toda apología del odio nacional, racial o religioso que constituyan incitaciones a la violencia o cualquier otra acción ilegal similar contra cualquier persona o grupo de personas, por ningún motivo, inclusive los de raza, color, religión, idioma u origen nacional.

Artículo 26. Desarrollo Progresivo

Los Estados partes se comprometen a adoptar providencias, tanto a nivel interno como mediante la cooperación internacional, especialmente económica y técnica, para lograr progresivamente la plena efectividad de los derechos que se derivan de las normas económicas, sociales y sobre educación, ciencia y cultura, contenidas en la Carta de la Organización de los Estados Americanos, reformada por el Protocolo de Buenos Aires, en la medida de los recursos disponibles, por vía legislativa u otros medios apropiados"[52].

Una vez expuestas las leyes que regulan a la intrusión cibernética, es necesario conocer, cuantos casos se han resuelto y en que sitios se han sufrido más ataques por parte de estos delincuentes. Al respecto las Agencia Federal de Investigaciones de Estados Unidos de Norte América (F.B.I.), ha publicado una lista de nombres de intrusos cibernéticos y el lugar que llevaron a cabo la intrusión cibernética, así como lo que hicieron es esa páginas, asimismo como los casos anónimos famosos no resueltos, teniendo como única finalidad, demostrar lo difícil que es el encontrar a estos delincuentes.

[52] C.F.R., www. Pintos y Salgado/Jurídicos/Convención Americana sobre derechos humanos

Además como cuales son los delitos reconocidos por la O. N. U., ya que la importancia y trascendencia de este organismo, es importante conocer su opinión, estas son:

ESTE ES UN RESUMEN DE LOS ACTOS DE "CIBERVANDALISMO" MÁS CONOCIDO EN EL CIBERESPACIO:

Pagina	Hacker	Date	Informacion acerca:
Telia	The Kevin Mitnick Liberation Front	3/17/96	La compañía mas grande de telecomunicaciones y Internet fue hackeada por segunda vez en el mismo día, después de asegurar en radio nacional la imposible de violar la seguridad. Piden la liberación de Kevin Mitnick.
Department of Justice	???	8/18/96	Hackeada como protesta contra la proposición de censar el Internet y hacer ilegal transmitir pornografía en la red.
CIA	Power Through Resistance	9/20/96	¡Este sitio hizo noticia en el CNN!. El Fiscal Sueco, Bo Skarinder, proceso la semana anterior a 5 personas por hackear. Modificaron la pagina y pusieron: "Bienvenidos a la Agencia Central de Estupidez"
Kriegsman	The Ghost Shirt Factory	11/12/96	Una fabrica que vende abrigos de pieles fue hackeada por un activista de los derechos de los animales, colocando vínculos a paginas a favor de la fauna.
Nethosting	01001000 00110111	11/27/96	Nethosting tiene su pagina electrónica y todos sus las paginas de sus 1500 clientes fueron hackeadas en un día, solo para darse a conocer.
Labour	???	12/12/96	El partido británico del trabajo fue hackeado. "Misma política, mismas mentiras". Además de declaraciones en contra de los políticos.
NASA	\\StOrM\\	12/23/96	El encabezado de la pagina decía "La NASA patrocina a los hackers". Además de criticas, vínculos a playboy y otras paginas.
NASA	\\StOrM\\	12/30/96	De nuevo una semana después. "No

			emociona explorar el Challenger.."
U.S. Air force	???	12/30/96	El título de la página fue "Bienvenidos a la verdad", además se colocaron criticas contra el gobierno e imágenes fuertes.
Employment Network	???	1/8/97	Se colocaron criticas al gobierno, y esta pagina se mantuvo por casi una semana.
Republic of Indonesia	TOXYN	2/11/97	La pagina del Dpto. de Asuntos exteriores de Indonesia fue hackeada. Esto fue hecho para protestar contra la ocupación de Indonesia en el East Timor.
NASA	H4G1S	3/5/97	Criticas al gobierno EUA. Además de comentarios a favor de la liberación de Kevin Mitnick y Ed Cummings
Cyber promotions	???	3/19/97	"¡Finalmente! La pagina de Cyberpromotions del gordo cerdo Sanford Wallace's fue hackeada. Este es el tipo que llena tu buzón con basura y hace dinero por eso". .
Amnesty International	4 man dream team	4/26/97	Amnistía Internacional fue hackeada, "¿Quien ríe al ultimo?".
Conservative	Circle of Deception	4/27/97	El partido Conservador británico fue hackeado, "ahora tienen, por lo menos algo en común con el partido del trabajo".
Jurassic Park	hackers(?)	5/27/97	La pagina "El Mundo Perdido" fue hackeada 4 días después del estreno de la película, duró 12 horas con una figura parecida a un pato.
LAPD	P.A.R.A.	5/29/97	"Bienvenidos a la pagina de LADP, el escuadrón de la muerte", siendo encabezado de una foto de la golpiza a Rodney King.
Geocities	fr0lic	6/25/97	La pagina principal de Geocities fue hackeada.
C.S.I.S.	???	7/15/97	¡¡El servicio canadiense de seguridad fue hackeado!!
Crack Mac	Starfire	8/18/97	"Gran concurso para hackear la pagina".
Value Jet	???	10/1/97	"¡Vuela con nosotros, porque estrellarse es divertido!".
Pentagon	Chameleon	10/4/97	El Centro Armado de Inteligencia Artificial de EUA fue hackeado.
Whitepower	L.O.U.	10/11/97	Esta pagina a favor del poder blanco fue

			"cómicamente" hackeada.
Spice Girls	Team CodeZero	11/14/97	La pagina oficial de las Spice Girls fue hackeada, y fuertes criticas fueron publicadas con referencia a la calidad del grupo.
China Agricultural University	LSD	11/26/97	Esta pagina fue hackeada con criticas en contra de la ocupación del Tibet por China. Y en contra de la prueba de armas nucleares.
Yahoo	PANTZ/ H4GiS	12/8/97	Este popular buscador fue hackeado durante alrededor de 15 minutos, y solo fue visto por algunas personas. "Liberen Kevin Mitnick".
FOX	???	12/11/97	El canal de TV FOX, fue hackeado. (Son los únicos que pasan los Expedientes X en USA). Así se mantuvo mucho tiempo.
China Agricultural University	W1n{} Dose & 1-s-d	12/31/97	El mismo servidor Chino fue hackeado. "¿Por qué EUA comercializa con China y no con Cuba?, Saquen a esa gente del Tibet".
Janet Jackson	Team CodeZero	1/2/98	La pagina oficial de Janet Jackson. Modificaron la apariencia de la pagina al cambiar la foto.
Rolling Stones	Team CodeZero	1/2/98	Pagina oficial de los Rolling Stones, se une a las Spice Girls, Janet Jackon, La Red de Defensa de Sistemas de Información de EUA, etc.
BMW	???	1/2/98	La pagina de los automóviles alemanes fue hackeada.
UNICEF	D.A.M.M.	1/7/98	El UNICEF fue hackeado. "Liberen a Kevin Mitnick".
Indonesia	LithiumError/ ChiKo-Torremendez	1/18/98	"Bienvenido a lo cruel, violento y corrupto". Cerca de 15 paginas de Indonesia fueron hackeadas al mismo tiempo. Esto como parte de la anticampaña a Suharto (para presidente).
International Church of Christ	???	1/18/98	Pagina de la Iglesia Internacional de Cristo, modificada, con criticas en contra. "Vida eterna a cambio de todo tu dinero, si, nosotros lo prometemos".
legislate	No|d Crew	1/21/98	"Buenas declaraciones" (www.legislate.com).

Saatchi& Saatchi	Trix&Vertex	2/19/98	Saatchi&Saatchi, fueron premiados por innovaciones en comunicación.
One Live Crew	???	2/22/98	Pagina en protesta sobre el abuso sexual a infantes.
Universidad Turca	Gr Power	3/5/98	En protesta a la presencia turca en Chipre..
NAMBLA	74074	3/6/98	En protesta al abuso a menores, NAMBLA.
US Army	No|d Crew	3/8/98	Ya van 3 paginas de diferentes servidores de los EUA que son hackeadas.
US Navy	No|d Crew	3/9/98	La pagina del Comando del Espacio Naval fue hackeada. Criticas al gobierno.
Korean Heritage College	RaPtoR 666	4/14/98	La pagina de "The Korean Heritage College of North America" fue hackeada.
Leonardo DiCaprio	D3str0, Fouk0, Lunat1c	4/19/98	La pagina de oficial del actor Leonardo DiCaprio's fue comicamente modificada, alterando la fotografia de inicio.
Motorola	H4CK1NG F0R G1RL13Z	8/21/98	Motorola fue hackeada 2 veces el mismo día. Una fue a la división de semiconductores y la otra fue la pagina principal de Motorola Japonesa. El seudónimo utilizado es "Hackeando por mujeres".
Arsenal F.C.	Cumbrian Alliance	8/30/98	La pagina oficial del Club de Football Arsenal Football fue hackeada en protesta por la expulsión del entrenador.
New York Times	H4CK1NG F0R G1RL13Z	9/12/98	Otro golpe de "Hackeando por mujeres". En protesta a las declaraciones hechas por un reportero en relación a Kevin Mitnick.
id Software	rd	9/24/98	id Software's, fue hackeada. La pagina fue modificada muchas veces. Pero no estuvo disponible por mucho tiempo.
SCO	ax	11/7/98	SCO (Santa Cruz Corporation) tiene muchos servidores hackeados en diferentes paises. SCO's sitio Mexicano en http://www.sco.com.mx.
Jack Daniels	FLUXX	12/14/98	La pagina de Jack Daniels fue hackeada.
Calgary Public Library	the leprechaun	1/25/99	La biblioteca publica fue hackeada como medio para comunicar la opresión en el norte de Irlanda. Sin tener relación con el

			hecho.
Greenpeace	???	1/27/99(?)	La pagina de la asociación internacional Greenpeace fue hackeada. Liberen a Kevin Mitnick.
Front National	RaPtoR 666	1/28/99	El partido Fascista francés "Front National" fue hackeado.
200 Cigarettes	MagicFX	2/20/99	Película de Hollywood hackeada.
Dominos Pizza	Cyrus	2/28/99	Dominos Pizza fue hackeada. "Yo charlo en irc"..
Monica Lewinsky	Magic FX	3/5/99	Mónica Lewinsky.com fue hackeada. Y modificaron la pagina.
Pussy-Power	???	3/5/99	Mas acerca de Mónica Lewinsky.
Ministerio Griego de Asuntos Exteriores	Kalamata Hacking	3/23/99	Pagina del Ministerio de asuntos exteriores en Gracia. Fue hackeado en protesta por los asuntos relacionados con el asentamiento turco, el gobierno, además del crimen.
Hot Bot	???	3/25/99	HotBot, una de los 5 mejores motores de búsqueda fue hackeado, colocando su autor un mensaje relacionado con la falta de raíces en las culturas y la influencia de los EU en eso.
Playboy Sprint Yellowpages Sony Music	???	4/4/99	Muchas paginas han sido hackeadas y remplazadas por la misma pagina electrónica. También, la pagina de Barbra Streisand, Oreilly.com, Umd.edu, hornyrob.com, sun.ca, y muchas otras.

Este cuadro fue arduamente traducido de una pagina muy completa que esta en http://www.onething.com/archive/ y tiene el archivo de las paginas "espejo",que hicieron los hackers en los lugares antes mencionados.

XII. CASOS ANONIMOS SONADOS DE CRIMEN POR COMPUTADORA.

En 1988, varios hackers consiguieron entrar en los ordenadores de siete universidades de Gran Bretaña, la de Londres incluida. Para resolver este crimen, la policía necesito la ayuda técnica de un asesor informático, Robert Jones. Una vez arrestado un sospechoso, las pruebas se analizaron durante un año y medio

antes de presentarlas ante el tribunal, que lo condeno a un año de prisión. Después de varias colaboraciones más, Scotland Yard propuso la creación de un centro universitario dedicado a la investigación de estos casos. El Centro de Investigación de Delitos Informáticos, adscrito al Queen Mary & Westfield College, se creó a principios de 1996 y el abogado Ian Walden, experto en la legislación de tecnología de la información, es su director. El Centro obtiene fondos del Gobierno y se dedica a la investigación y la asesoría en el campo de los delitos informáticos, así como a impartir cursos de formación en la materia para policías, fiscales, abogados y cualquier interesado.

En 1989 la justicia alemana detiene a un grupo de crackers germanos que habían copiado durante años miles de programas de acceso no legal y passwords de ordenadores en departamentos de la administración de EEUU. El destinatario de la información era el KGB soviético.

También en 1993 la compañía discográfica Frank music Corporation vence en su demanda contra Compuserve, el mayor proveedor de Internet, por permitir que sus abonados copiaran más de 500 canciones sometidas a derechos de autor. Otras 140 discográficas han denunciado a Compuserve por idéntica razón.

En 1993 la revista Play Boy gana un juicio contra George Frena, que había distribuido ilegalmente en su BBS fotos de desnudos procedentes del web de esta publicación. En 1993 y 1994, Play Boy denunció a 12 BBS más por el mismo motivo.

Todos estos asaltos no suelen tener consecuencias importantes, pero lo peor de todo es cuando lo efectúan los "chicos malos": crackers o hackers de contraseñas. Uno de los casos más destacados es el que se produjo en 1994, cuando varios "piratas" consiguieron introducirse en el sistema de seguridad de la Florida State University, violándolo y llevándose consigo varias copias de prueba de Windows 95, uno de los más potentes sistemas operativos de Microsoft, que en aquel entonces no era comercial ni público.

En 1994 crackers americanos se hacen vía Internet desde Mallorca con 140.000 números de tarjetas de crédito telefónicas de EEUU.

Usuarios de todo el mundo llaman a cuenta de las víctimas. El fraude llega a los 140 millones de dólares perdidos por compañías como Bell Atlantic, MCI o AT&T.

En agosto de 1995, Adam Back (británico), Eric Young (australiano) y David Byers (sueco), demuestran en Internet como pueden violarse en cuestion de minutos los algoritmos de seguridad de Netscape Navigator, el programa de acceso a WWW más usado mundialmente. Al mes siguiente, los cyberpunks americanos David Wagner y Ian Goldberg crean un método para violarlo en sólo 25 segundos.

En 1996 Public Access Networks Corp., una de las grandes empresas dedicadas al suministro de acceso a la red de Estado Unidos, que controla las páginas de más de 1,000 empresas en la World Wide Web, sufrió un feroz ataque por parte de piratas informáticos. Estos llevaron a la locura a los ordenadores de la empresa mediante el continuo envío de solicitudes de información adulteradas, mas de 150 por segundo.

Como ejemplo, tenemos lo que sucedió el 19 de Septiembre de 1996, cuando la CIA sufrió los ataques de un grupo de Hackers suecos, que desmantelaron su servidor de Información en Internet, modificando el mensaje de presentación "Bienvenidos a la Agencia Central de Inteligencia" por "Bienvenidos a la Agencia Central de Estupidez". Entre la maraña de contenidos de la Web, colocaron también varias conexiones directas a otros lugares de Internet, como a las revistas Flashback o Playboy.

La CIA experimentó una grave derrota, con lo que tuvo que retirar su maltrecho servidor.

En 1996 el Grupo Antipiratería de la empresa de software Novell, informaba de la captura de un individuo que respondía al alias de "El Pirata". Con la colaboración de la Policía de Zurich, Novell consiguió atrapar a este cracker que ofrecía productos de la compañía a usuarios de Internet de forma ilegal por valor de 60.000 dólares, junto con software comercial de otros miembros de la BSA (Business Software Aliance). Se localizaron también instrucciones para realizar operaciones fraudulentas con tarjetas de crédito.

Sus acciones le pueden llevar a ser condenado un máximo de tres años y/o una multa de 10 millones de pesetas por ellIo. Martin Smith, el Director de Programas de Licencias de Novell para Europa, Oriente Medio y África, lo valora así: "Éste es un caso clave para el futuro de la industria del software. Desde hoy los individuos y organizaciones que distribuyen software ilegal en Internet saben que pueden ser capturados y procesados".

En Mayo de 1997, un grupo de hackers ("cortadores") asalta la pagina de una de las películas más taquilleras de la fabrica Spilberg: Jurassic Park, cambiando durante 18 horas el logotipo del dinosaurio por otro en el que apare cía un pato. Los servicios de inteligencia están protegidos por poderosas "articulaciones" de los estados, y gozan d e una fama y d e un prestigio internacionales, pero los hackers logran con su espontaneidad bajarle los humos al brazo armado del poder, y perpetuar el carácter secreto y anárquico de sus organizaciones, consiguiendo de paso, unos buenos "titulares".

Nadie está fuera del alcance de estos saqueadores, ni siquiera el todopoderoso Bill Gates, que vio cómo la Homepage de Microsoft fue atacada por varios hackers en junio de 1997. Estos hackers, accedieron al sistema operativo por un bug de Windows Nt 4.0, el cual era el servidor bajo el que se ejecutaba la Web de Microsoft. Hay muchas formas de dar publicidad a actos "presumiblemente ilegales", pero algunas son más ingeniosas que otras.

Algunos hackers consiguen que sus hazañas sean universalmente conocidas, dejándose "atrapar" por la justicia, o incluso en ocasiones, llegando a

negociar las penas de cárcel por escuchas y accesos ilegales. Este es el caso de J.C Ardita, un hacker argentino (antes mencionado) que en Diciembre de 1997 se confesaba culpable de los cargos que se le imputaban, y volvía voluntariamente a Estados Unidos para que se le juzgara por los delitos cometidos.

Una de las hazañas más sorprendentes de intercambio de información entre hackers fue el caso Price. En esta ocasión, se investigó la acción de un joven hacker que accedía gratuitamente al sistema telefónico chileno y desde allí conseguía entrar en los ordenadores del Ministerio de Defensa de los Estados Unidos.

Llegó a copiar archivos que no eran materia reservada, pero sí investigaciones de temas delicados. Su centro de trabajo era su casa, en Londres, y desde allí causó uno de los mayores desastres informáticos de la década. No trabajaba solo, por lo que intercambió todos los documentos que había obtenido con hackers de distintos países, vía Internet.

El caos fue total, llegando incluso al cierre temporal de la red norteamericana. Estos grupos tienen una forma de operar muy estricta, y la exclusión de uno de sus miembros significa la recesión total de privilegios, y la condena al ostracismo virtual. Fidelidad, confidencialidad y tenacidad son los rasgos más comunes entre los hackers.

Pero lo que más sorprende al mundo del underground, y más aún, a los ciudadanos de a pie es que, estos asaltos, en más de una ocasión, no son perpetrados por "gurús" de la informática, ni por miembros de la "elite hacker" sino más bien por principiantes, por iniciados al hacking.

En 1997 se publica el libro "Takedown" de Tsutomu Shimomura y John Markoff de la editorial El País-Aguilar de 464 páginas. En el se relatan la busqueda y captura de un escurridizo hacker que domina el arte del "IP-spoofing", que consiste en producir falsos números IP para ser reconocido por otras máquinas conectadas y pasearse por su interior. Es un reportaje novelado, contado en

primera persona por el experto en seguridad Tsutomu Shimomura, que fue saqueado por el hacker en plena navidad del 94 y dedicó medio año a detenerle. Lo escribió junto a John Markoff, un periodista del New York Times que había seguido el caso.

Microsoft ha anunciado firmes avances en su lucha contra el delito informático durante el año fiscal de 1997, que incluye el embargo de cerca de 100,000 copias ilegales o programas falsos, CD-ROM y dispositivos hardware, procedentes de canales de distribución europeos y con un valor de más de 23 millones de dólares.

TIPOS DE DELITOS INFORMATICOS RECONOCIDOS POR NACIONES UNIDAS.

a).- Fraudes cometidos mediante manipulación de computadoras.

- Manipulación de los datos de entrada. Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a funciones normales de procesamiento de datos en la fase de adquisición de los mismos.
- La manipulación de programas.Es muy difícil de descubrir y a menudo pasa inadvertido debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas que existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado "Caballo de Troya", que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

- Manipulación de los datos de salida. Se efectúa fijando un objetivo al funcionamiento del sistema informático.

El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usa ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

- Fraude efectuado por manipulación informática. Aprovecha las repeticiones automáticas de procesos de computo. Es una técnica especializada que se denomina técnica del salchichón en la que rodajas muy finas apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

b).- Falsificaciones informáticas.

- Como objeto. Cuando se alteran datos de los documentos almacenados en forma computarizada.
- Como instrumento. Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas a color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original y los documentos que producen son de tal claridad que solo un experto puede diferenciarlos de los documentos auténticos.

c).- Daños o modificaciones de programas o datos computarizados.

- Sabotaje informático. Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de

obstaculizar el funcionamiento normal del sistema. Algunas de las técnicas que permiten cometer sabotajes informáticos son: virus, gusanos, bomba lógica o cronológica, etc.

- Acceso no autorizado a servicios y sistemas informáticos. Por motivos diversos que van, desde la simple curiosidad, como es el caso de muchos piratas informáticos (hackers o crackers) hasta el sabotaje o espionaje informático.
- Reproducción no autorizada de programas informáticos de protección legal. Esta puede entrañar una perdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con él trafico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones moderna.

4.1.2.- ARGENTINA:

El llamado delito informático, no constituye en su ordenamiento positivo por si mismo una categoría delictiva, sino que se trata de usos indebidos de cualquier medio informático.

En este marco es importante tener en cuenta si los tipos penales descriptivos dentro de nuestro código penal y leyes especiales se adecuan a éstos.

Sin duda, poseen avanzados conocimientos de informática y programación y producen importantes daños económicos.

La posibilidad de cometer el ilícito desde cualquier ordenador conectando a la red da una gran dificultad de detectar el delito. Según otros datos, solo el uno por ciento de los delitos informática son descubiertos, entra otras cuestiones, por la falta de denuncia por el desprestigio que significa la vulnerabilidad del sitio.

Los delitos que pueden cometerse en la red, los más comunes cometidos son:

- Delitos de daño: Es el más típico entre los delitos informáticos. El artículo 183 del código penal reprime el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañaré una cosa mueble total o parcialmente ajeno siempre que el hecho no constituya un delito grave.

Se trata de un delito instantáneo que se consuma con la destrucción, inutilización, desaparición o daño de la cosa o animal sobre los que recaen esas acciones. No admite la tentativa, ni la figura culposa, porque se trata de un delito doloso.

Es preciso que la alteración subsista de manera indudable o considerablemente fija, de tal manera que su retrogradación a su estado anterior requiere de algún tipo de esfuerzo o trabajo apreciable o gasto.

La acción de dañar esta constituida por todo ataque a la materialidad, utilidad o disponibilidad de las cosas, que elimine o disminuya su valor de uso o de cambio, se ataca su utilidad cuando se elimina su aptitud para el fin que estaba destinado y se ataca su disponibilidad cuando el acto del agente impide que el propietario pueda disponer de ella. El resultado deseado deberá ser el detrimento de su materialidad o funcionalidad futura.

En virtud de la reforma al artículo 2311 del código civil por la ley 17.711; la energía eléctrica y magnética apropiada en forma de información contenida en un soporte digital es asimilable a una cosa. Por lo tanto, dicho bien es susceptible de ser dañado.

Así se puede decir que es aplicable la norma en cuestión toda vez que el sujeto activo maliciosamente destruya, inutilice o de cualquier forma hiciera desaparecer cualquier tratamiento de información, bancos de datos, en todo o en parte.

Las formas de daño más comunes del intruso cibernético son:

- Introducir virus al sistema. Los virus son elementos informáticos que tienden a reproducirse y a extenderse dentro del sistema al que acceden, se contagian de un sistema a otro, exhiben diversos grados de malignidad y son, eventualmente, susceptibles de destrucción mediante un antivirus adecuados frente a los cuales pueden incluso desarrollar resistencia

- Borrado o destrucción de un programa de computación: sin perjuicio de que alguna jurisprudencia haya establecido que el borrado o destrucción de un programa de computación no es un delito, en virtud de que se trata de una conducta aprehendida por los tipos penales especiales de la ley 11.723. Del mismo modo podría encuadrarse el agravante del mismo lícito cuando se ejecuta en archivos y registros digitales, bibliotecas digitales tal como prevé el artículo 184 inciso 5 del código penal.

- Piratería de softweres y banco de datos: Como todo delito contra objetos protegidos por el derecho de autor, requiere inexcusablemente la existencia, en su aspecto subjetivo, del dolo del agente.

4.2. EN EL CONTINENTE EUROPEO.

4.2.1. ESPAÑA.

En el derecho penal español, el capitulo concerniente a este tipo de delitos, se integra dentro del delito de daños, y que se describe en el artículo 263 como causar daños en propiedad ajena.

En este sentido el código penal actual supone una regresión injustificada y que se debe a un desconocimiento por parte del legislador de lo que está regulando.

El artículo 263 establece la pena para el delito de daños genérico (multa de seis a veinticuatro meses), mientras que el artículo 264 establece un subtipo agravado (prisión más multa).

En el derecho penal existe lo que se denomina principio de graduación de las penas, que consiste en que la pena de un hecho grave debe de ser mayor que la de un hecho leve. Pues bien, todo daño cometido utilizando un ordenador, sin siquiera verificar en que consiste, lleva adherida la mayor pena aplicable al delito de daños, lo cual no tiene sentido: borrar una fotografía de un ordenador tiene la misma pena que arruinar a una persona.

La acción de destruir, alterar, inutilizar o dañar. No puede ser lo mismo destruir que alterar, ya que la primera implica la desaparición del objeto protegido, mientras que la alteración implica la pervivencia del objeto.

La consistencia de la redacción vigente es que borrar una imagen contenida en un archivo gráfico conlleva la misma pena que alterar esa imagen difuminándola. Si puede invertirse la modificación de esa misma imagen difuminándola, la pena aplicable sigue siendo la misma, pese a que no ha existido ningún daño para el perjudicado por el delito. Llegando así a la penalización de conductas cuyo perjuicio puede deshacerse con un mero clic.

El medio utilizado para cometer la acción puede ser cualquier medio, con ello se engloba cualquier posibilidad, ya sea mediante una destrucción externa de un ordenador o mediante una entrada ilícita. La norma jurídica iguala, por tanto, un acto de destrucción física a un acto de manejo de un ordenador.

La norma amplia las acciones prohibidas incorporando al tipo penal la expresión " o de cualquier modo". Así pues el tipo penal se expande a todas las posibilidades posibles mediante la utilización de una formula de cajón de sastre. Esta técnica punitiva no es propia ni del derecho penal ni del estado de derecho, ya que un código penal debe ser un catálogo cerrado de acciones.

El objeto protegido consiste en datos programas o documentos electrónicos. También esta relación debe de ser criticada por su redundancia. Para que se complete el tipo penal, los datos, programas o documentos electrónicos deben hallarse en redes, soportes o sistemas informáticos. Contener implica almacenar y necesariamente tiene dos objetos uno el continente y otro el contenido. El objeto contenido son datos en formato electrónico por lo que obviamente el contenido son datos electrónicos en una red que están en un sistema de almacenamiento.

No coincide el bien jurídico protegido con la sede en que se incorpora al tipo penal, correspondiente al delito de daños, que protege tradicionalmente una propiedad física. Se equipara penológicamente conductas totalmente diferentes como son la destrucción material de un ordenador y el borrador de los datos que contiene. Se engloban con una misma pena conductas de alteración y de destrucción, lo cual atenta con el principio de graduación de las penas.

En su relación con el delito de daños en el que se integra dicha conducta se equipara a los delitos de daño más graves, sin que pueda defenderse lógicamente esa equiparación.

La mayor ventaja de los delincuentes consiste èn la incultura informática de los usuarios, incultura informática que es lógica, puesto que un ordenador es un herramienta de trabajo, no una universidad que todos debemos de conocer.

Existe cierta controversia sobre la definición de virus, definiéndolo como un programa de ordenador que puede infectar otros programas modificándolos para incluir una copia del mismo. Según algunos autores los virus se han clasificado en:

I. Virus de acción directa, en el momento en que se ejecutan, infectan a otros programas.

II. Virus residentes, al ser ejecutados, se instalan en la memoria del ordenador, infectando a los demás programas a medida que son ejecutados.

III. Virus que infectan el sector de arranque, estos son residente en la memoria

Existe una tercera categoría pero corresponde a los virus que infectan archivos y al sector de arranque, por lo que se puede decir que es la suma de las categorías anteriores. En función a su comportamiento, todos los virus pueden clasificarse a su vez en otros dos grupos:

1) Virus uniformas, que producen una replicación idéntica a sí mismos.
2) Virus polimorfos, que su aplicación producen una mutación de sí mismos, para así evitar ser detectados por los antivirus.

Nos encontramos con una categoría de virus que afecte al sistema operativo o nos encontramos con otra que afecte a ficheros, las acciones que pueden cometerse son: la creación de virus, modificación de virus, propagación de virus.

Las empresas especializadas en antivirus, suelen experimentar con los mismos para sí proveer su aparición, así mismo la creación de un virus puede realizarse en el ámbito de estudio de los mismos. También son comunes las acciones en las que se modifican los virus, ya sea con carácter preventivo, ya sea con intenciones maliciosas. En la aparición de un virus nuevo siempre se produce un efecto rebote consistente en modalidades del mismo.

A los efectos penales dos son por tanto las cuestiones de se debe tener en cuenta: Si el virus afecta al sistema operativo o simplemente a archivos; o son la conducta del delincuente ha sido la de crear, modificar o propagar virus.

El código penal español actual castiga, en su artículo 263.2, y dentro del capítulo "de los daños", con la pena de prisión de uno a tres años de prisión de uno a tres años y multa al que por cualquier medio destruya, altere o inutilice o de

cualquier otro modo dañe los datos, programas o documentos electrónicos contenidos en redes, soportes o sistemas informáticos.

La propagación maliciosa de un virus de ordenador queda integrada dentro de este tipo penal.

Nuestro ordenamiento jurídico ha recibido una importante actualización con el Código Penal de 1995, que incluye una buena parte de las dinámicas comitivas.

1.Hacking (INTRUSIÓN CIBERNÉTICA)

En el apartado correspondiente a los delitos contra la intimidad se introduce la interceptación de correo electrónico, que queda asimilada a la violación de correspondencia.

"El artículo 197 extiende el ámbito de aplicación de este delito a las siguientes conductas:

1.-Apoderamiento de papeles, cartas, mensajes de correo electrónico o cualquier otro documento o efectos personales.

2.- interceptación de las telecomunicaciones, en las mismas condiciones utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, en las mismas condiciones de invasión de la intimidad y vulneración de secretos.

Estas actividades deben producirse sin consentimiento del afectado y con la intención de descubrir sus secretos o vulnerar su intimidad.

La pena que se establece es de prisión, de uno a cuatro años y multa de doce a veinticuatro meses (Con el nuevo concepto de días-multa, un día equivale a un mínimo de 200 pesetas y un máximo de 50.000 pesetas)

También quedan tipificados los actos consistentes en apoderarse, utilizar, modificar, revelar, difundir o ceder datos reservados de carácter personal que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos.

El Código Penal de 1995 introduce el concepto de la estafa electrónica, consistente en la manipulación informática o artificio similar que concurriendo ánimo de lucro, consiga una transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

El Código Penal anterior exigía la concurrencia de engaño en una persona, lo cual excluía cualquier forma de comisión basada en el engaño a una máquina.

El artículo 248 y siguientes establecen una pena de prisión de 6 meses a 4 años para los reos del delito de estafa, pudiendo llegar a 6 años si el perjuicio causado reviste especial gravedad.

En el delito de daños se contemplan los supuestos de destrucción, alteración, inutilización, o cualquier otra modalidad por la que se dañen los datos, programas o documentos electrónicos contenidos en redes, soportes, o sistemas informáticos.

El Código Penal anterior sólo preveía la destrucción de bienes materiales, por lo que los daños causados en bienes inmateriales no quedaba incluida en dicho delito.

El artículo 239 considera llaves falsas las tarjetas magnéticas o perforadas así como los mandos o instrumentos de apertura a distancia, considerando por lo tanto delito de robo la utilización de estos elementos, el descubrimiento de claves y la inutilización de sistemas específicos de alarma o guarda con el fin de apoderarse de cosas muebles ajenas.

2.Cracks

El artículo 270 incluye en la categoría de los delitos contra la propiedad intelectual la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinado a facilitar la supresión no autorizada o la neutralización

de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador.

3.Phreaking

Además de la aplicación del régimen correspondiente a las defraudaciones y a las estafas electrónicas, este tipo de delitos podría encuadrarse en el artículo 256, que castiga el uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular". [53]

4.2.1.1. LA OBTENCIÓN DE PRUEBAS EN INTERNET

La Comisión Europea está analizando la posibilidad de publicar unas recomendaciones para la protección de las personas físicas en relación con la recogida y el tratamiento automatizado de datos personales a través de las autopistas de la información.

La Comisión se ha propuesto promover la protección de la intimidad en las redes de telecomunicaciones como Internet. Los puntos que serán objeto de una especial atención serán los siguientes:

1. Los riesgos específicos que la capacidad de proceso suministrada por Internet genera para el derecho a la intimidad y los datos personales.

2. El principio de que el uso de los datos personales debe reducirse al mínimo.

3. Las condiciones bajo las que los datos personales pueden ser divulgados a terceros, por razones de seguridad nacional o prevención de delitos.

---

[53] "Código Penal Español" (consulta en internet: http://www.pintos&salgado/análiss/ código penal español.) México, 17:00 P.M., 12/10/2001.

4. El flujo transfronterizo de datos

"La percepción de las redes telemáticas como un nuevo espacio en el que los delitos acostumbran a quedar impunes carece de fundamento. Las mismas ventajas que permiten al delincuente moderno aumentar la efectividad de sus acciones, pueden ayudar a los técnicos que participan en la investigación a obtener pruebas evidentes de la identidad y ubicación del presunto infractor. Las nuevas dinámicas comisivas generan otro tipo de huellas y evidencias que pueden resultar inequívocas para determinar la autoría de un delito, pero exigen al investigador un conocimiento específico de la materia.

Por otro lado, la gran innovación que Internet aporta a las técnicas de investigación, es la posibilidad de obtener una copia exacta de todos los elementos que han participado en una transacción ilícita. Desde los mensajes transmitidos por los participantes hasta los propios efectos del delito".[54]

4.2.1.2. Pruebas digitales

En las actuaciones presenciales, la intervención de un alijo de droga puede impedir que la investigación llegue a determinar quién era el beneficiario final de la transacción. Resulta difícil obtener una evidencia clara de la existencia de un material ilícito sin que el buen curso de la operación se vea afectado. Los efectos del delito acostumbran a ser únicos e irrepetibles.

La tecnología digital utilizada en las redes telemáticas provoca la desaparición del concepto "original". Los bienes que circulan por Internet han perdido el carácter de irrepetibles, ya que un objeto digital puede ser reproducido hasta el infinito sin merma de su calidad y sin huellas que permitan apreciar diferencias entre las distintas copias.

En el caso de los programas de ordenador, por ejemplo, el órgano judicial que haya ordenado la intervención, puede obtener una copia completa y fehaciente de

[54] Idem

las aplicaciones informáticas transferidas ilícitamente, sin que las partes que participan en la transacción lleguen a saberlo.

Los mensajes y datos adjuntos que se transmiten a través del correo electrónico, de una lista de distribución, un grupo de noticias o una sesión chat, pueden ser intervenidos en tiempo real y, en algunos casos, incluso unos días después.

4.2.1.3. Sistemas de identificación

Durante los primeros años de las redes telemáticas, la información era escasa y estaba limitada a usuarios con privilegios para acceder a la misma. Al mismo tiempo, los diferentes protocolos de transferencia de datos hacían difícil una búsqueda global. En la actualidad, organizaciones públicas y privadas, personas físicas y jurídicas se han lanzado a nutrir la red de datos de toda índole. Los propietarios de contenidos han abierto sus sistemas y han permitido el acceso al público y a los robots o motores de búsqueda que permiten localizar la información.

Esta situación, que todavía debe ser calificada como incipiente, a la vista del prometedor futuro que nos depara el cable, los satélites, los nuevos sistemas de compresión de datos y el acceso global a un mayor número de bases de datos, permite la localización e identificación de un servidor o de un usuario de forma sencilla y rápida.

En las investigaciones que se han llevado a cabo hasta ahora en nuestro país, la propia red ha suministrado los datos necesarios para completar la identificación de los presuntos infractores.

En una primera aproximación, las bases de datos WHOIS, de acceso público y gratuito, permiten conocer la titularidad de un dominio, y con ello, los datos del responsable administrativo, técnico y financiero de un servidor o de una sede web en la que se están cometiendo actos ilícitos. La información suministrada consta

del nombre y los apellidos, el domicilio y el teléfono, así como el IP del servidor primario y secundario.

También existen herramientas que permiten conocer el origen de un mensaje, analizando la cabecera del mismo y la ruta que ha seguido.

La dirección de correo electrónico puede ser suficiente para conocer la identidad de una persona. Pero un PSI no puede revelar la identidad del titular de una cuenta sin el correspondiente requerimiento judicial que ordene el suministro de dichos datos y si este hecho llega a conocimiento del presunto infractor, se perderá la posibilidad de obtener más pruebas con posterioridad.

Sin embargo, existen numerosas fuentes de información, de acceso público, que permiten asociar una dirección de correo electrónico a una persona concreta sin alertar a su titular. Además de las bases de datos en las que el propio usuario registra sus datos con el fin de que sus amistades puedan conocer su dirección de correo electrónico (p.e. LISTIN.COM), existen anuncios gratuitos, clubs de usuarios, asociaciones deportivas, universidades, etc., donde es fácil encontrar el nombre y la dirección e-mail juntos. Por ejemplo, recientemente, el titular de una cuenta de correo electrónico ha sido identificado a través de una lista de usuarios que se adhirieron a la campaña "Tarifa plana en Infovia". Los datos obtenidos en esta lista pública fueron: nombre, apellidos y DNI.

En el caso de nicknames o alias, el presunto infractor puede ser víctima de su propio pasado. En una investigación realizada en abril de 1997, la búsqueda basada en el alias utilizado en los chats, arrojó un resultado sorprendente, ya que esta persona había sido miembro de un club universitario en la que los estudiantes tenían sus propias páginas personales y el investigado había incluido dos fotos suyas, en un alarde de premonición: una de frente y otra de perfil.

El uso de remailers anónimos o de sistemas de correo gratuito como Hotmail no suponen un obstáculo para conocer la identidad de un usuario, ya que los

propietarios de este tipo de servidores están obligados a facilitar los datos de sus usuarios a la autoridad judicial que lo requiera.

Finalmente, la identificación a través de IP's dinámicos exige el concurso de los PSI a través del correspondiente requerimiento judicial que ordene el análisis de los logs del sistema antes de que el transcurso del tiempo lo impida.

4.2.1.4. Sniffers

España fue el primer país europeo en aplicar la técnica de los sniffers en la investigación de delitos en Internet. La intervención tuvo lugar en diciembre de 1996, a raíz de una denuncia por distribución no autorizada de programas, obras multimedia y bases de datos jurídicas a través de Internet. El mandamiento judicial recogió cada uno de los pasos necesarios para la interceptación de los mensajes de correo electrónico del presunto infractor y su grabación automática en el disco duro de un ordenador habilitado al efecto.

Los treinta días de la intervención telemática arrojaron pruebas concluyentes de la infraccion, ya que, junto a los mensajes transferidos se hallaron catálogos, pedidos, órdenes de transferencias de fondos, cracks y los propios programas distribuidos ilícitamente.

4.2.1.5. Obstáculos

"Los problemas que impiden la práctica de las citadas diligencias de investigación en la actualidad son, principalmente, los que se enumeran a continuación:

- Escasez de medios técnicos dedicados a la actividad investigadora.
- Ventaja tecnológica de los delincuentes profesionales.
- Exceso de tiempo transcurrido entre la solicitud de un mandamiento de intervención electrónica y su concesión y trámite.
- Uso de contramedidas, como el cifrado de la información y los sistemas de anonimato real.

- Problemas de jurisdicción en los delitos transfronterizos.

La mayor asignación de recursos por parte de la Administración, la progresiva especialización de los cuerpos policiales, la creación de grupos específicos para la persecución de este tipo de delitos, unidos a la práctica judicial y a la creación de jurisprudencia en esta materia, ayudarán a mejorar la eficacia de los métodos de investigación y obtención de pruebas.

Pero la sensibilización de los usuarios de Internet, su colaboración y su comportamiento diario serán los que, en definitiva, deberán reducir las conductas delictivas en la red a un simple e irrisorio dato estadístico". [55]

4.2.2. COMUNIDAD ECONÓMICA EUROPEA.

Dentro del gran bloque que forma la Unión Económica Europea existe un convenio llamado "CONVENIO EUROPEO SOBRE EL CIBERCRIMEN", este acuerdo es del 23 de noviembre del 2001, se firmó en Budapest y bajo el paraguas del consejo de Europa, el Convenio Europeo sobre el cibercrimen.

"El convenio se estructura en cuatro capítulos: definiciones, medidas a ser tomadas en los ordenamientos internos de los firmantes, cooperación internacional y disposiciones finales.

El objetivo del convenio es doble. Por un lado consiste en establecer la cooperación internacional para la prevención y persecución de los delitos cometidos mediante o a través de las redes y ordenadores. Por otro lado, establece un mandato a las partes signatarias para desarrollar una legislación nacional coherente entre todos ellos y represiva de los siguientes delitos.

1. Acceso ilegal.
2. Interceptación ilegal.

[55] Idem

3. Interferencia de datos.
4. Mal uso de los propios aparatos.
5. Modificación de datos.
6. Pérdida de propiedad por modificación o interferencia ilegítima de datos.
7. Pornografía infantil.
8. Delitos contra la propiedad intelectual.

Si esta legislación que las partes se obligan a desarrollar deberá ser aplicable no sólo en el territorio de los Estados signatarios del tratado, sino en los buques y aeronaves con bandera del Estado matriculados en el mismo, y a los nacionales de dicho estado, siempre que cometan el delito en un territorio que sea punible o en un territorio fuera de los estados signatarios. No obstante el convenio permite que sean los propios Estados los que desarrollen el ámbito de aplicación.

Las partes establecen unos procedimientos y líneas generales para la colaboración entre todas ellas con un funcionamiento 24/7, esto es, veinticuatro días de la semana. La asistencia mutua en las medidas cautelares provisionales y en las facultades de investigación, el procedimiento de extradición de los delincuentes y la comunicación directa entre autoridades forman parte de este nuevo sistema de colaboración que se pretende implantar y que no se limita a los Estados miembros del consejo de Europa sino que pretende la adhesión de todos aquellos Estados que lo consideren oportuno.

Un total de 30 países firmaron en Budapest la convención internacional contra el cibercrimen, un documento en el que se pretenden coordinar la lucha para erradicar el terrorismo que a su vez será el primer documento jurídico que incorpora a internet como objeto de obligaciones y sanciones.

Estados Unidos, Japón, Canadá y Sudáfrica, son algunos de los firmantes de este documento , junto a 26 de los 43 países miembros del Consejo de Europa, entre ellos todos los comunitarios, excepto Luxemburgo, Irlanda y Dinamarca, que

aplazan su participación en el por razones de su calendario. Aún así los responsables del Consejo de Europa, calificaron la ratificación de este texto por parte de 30 países como un acontecimiento sin precedentes.

Uno de los temas más controvertidos fue el del respeto a los derechos humanos, sobre todo la inviolabilidad de la correspondencia, cuya garantía exigía el consejo de Europa entrando así en conflicto con la prioridad de ka seguridad.

La convención si permite reunir pruebas electrónicas sobre infracciones relacionadas con el terrorismo si se cometen actos terroristas contra los sistemas informáticos.

El texto cubre lagunas legales en cuanto a fraudes informáticos, atentados contra la confidencialidad y la integridad de los sistemas y delitos relacionados con la propiedad intelectual (plagios e imitación) y los contenidos (pornografía infantil).

Así mismo en su artículo nueve la convención prevé una serie de medidas para sancionar la posesión y distribución de imágenes pornográficas de menores en internet y la prostitución infantil.

En términos económicos, el texto constata el elevado precio del cibercrimen; así los fraudes con tarjetas de crédito reportaron 400 millones de dólares a sus autores en 1999, mientras que los gastos derivados de la acción de virus informáticos costaron cerca de 12,000 millones de dólares.

Por su parte las empresas victimas de la piratería dejan de ganar unos 250,000 millones de dólares cada año.

El consejo de ministros de telecomunicaciones de la Unión Europea ha alcanzado un acuerdo político sobre Directiva referente a la privacidad en las comunicaciones electrónicas.

La norma aprobada compromete a organismos públicos y privados a destruir o hacer anónimos los datos personales que obtengan a través de sus comunicaciones en internet, excepto si consideran que estos afectan la seguridad pública o del Estado. Se establece el principio universal de la destrucción inmediata de los datos personales, pero permite almacenarlo si el usuario ha sido informado o si fuera necesario para la protección de la seguridad pública, la Defensa, la seguridad del Estado, incluido el bienestar económico, o la aplicación del ordenamiento penal". [56]

[56] "Convention on cybercrimen". [Trad. Gelacio Cortés Ramírez], (consulta en internet: www.pintos&salgado/legislation/convention on cybercrimen) México, 12:30 P.M., 15/10/2001.

CONCLUSIONES.

Primera.- La tecnología va desarrollándose muy rápido, dando lugar a acciones que en otra época eran irrealizables o difíciles de realizar, siendo hoy en día una realidad, es por ello que sin duda este delito va a ir en aumento día a día, motivo por el cual se tiene que regular de manera efectiva en nuestro derecho positivo, porque de no hacerlo, los usuarios mexicanos de internet no tendrán protección jurídica para defenderse cuando sufran un ataque por parte de estos delincuentes.

Segunda- La intrusión cibernética al lesionar valores importantes de la sociedad como son el patrimonio; la seguridad tanto interna como externa así como la paz pública, es necesario que esta conducta sea catalogada como un delito grave en el Código Penal Federal mexicano.

Tercera.- La conducta desplegada por el intruso cibernético, lo realiza con toda la intención de hacer daño y por el grado de especialización con el que deben contar, saben los alcances de su actuar, con la cual obtienen una ventaja en perjuicio de otra persona, motivo por el cual la intrusión cibernética debe considerarse como dolosa

Cuarta.- Al ser la conducta del sujeto activo (intruso cibernético) un delito federal, es necesario realizar adiciones al Código Penal Federal y al reglamento de la ley orgánica de la Procuraduría General de la República para que quede establecido en la ley sustantiva este delito y en la ley adjetiva la manera de cómo se va a actuar para la persecución de este delito, dándose la creación de una fiscalía cibernética, la cual para actuar necesita de una preparación especial.

Quinta.- Se requiere una capacitación general del personal que labore en la fiscalía; la capacitación debe de contener la manera de cómo usar el internet, como rastrear al intruso cibernético,de cómo recuperar pruebas, para estar en la posibilidad de erradicar a este tipo de delincuentes.

Sexta.- La fiscalía debe estar integrada por tres partes que son fundamentales para estar en la posibilidad de atacar este delito: la primera porción es la especializada en computación, compuesta por ingenieros en cibernética; la segunda esta integrada por abogados para llevar al cabo el procedimiento judicial respectivo; y la última parte esta integrada por los agentes judiciales encargados de la captura de este tipo de delincuentes.

Séptima Al instituirse esta fiscalía, su utilidad no solo será para luchar contra la intrusión cibernética, sino que se aprovecharía para todos los demás delitos informáticos, como por ejemplo, la pornografía infantil, los abusos en los chat, estafas, etc.

Octava.- Urge crear un centro de atención y quejas tanto en el internet como en la dependencia con la finalidad de recibir todas las denuncias y darle un seguimiento. Lográndose con ello la facilidad y rapidez para denunciar y por lo mismo actuar de una forma sencilla y rápida.

Novena.- El centro de quejas que se encuentre en el internet, necesita contar con seguridad para no alterar las denuncias recibidas y así hacer confiable toda la información que se proporcione, es por ello que, se debe de contar con criptografía, la cual es, la más confiable.

Décima.- . Al desarrollarse la intrusión cibernética desde cualquier parte del mundo gracias al internet, es necesario que México celebre tratados con otros países para que entre todos los signatarios exista un acuerdo de cooperación para facilitar la localización, extradiciones, captura del delincuente como hoy en día lo esta llevando acabo la Comunidad Económica Europea.

Décima primera.- Es necesario que se le de más importancia al derecho cibernético, ponerlo al día con los avances que tenga, ya que al ser un campo novedoso para el derecho, cada día existe algo nuevo y por lo tanto que no esta

regulado, porque sino estamos en desventaja con la diferente gama de delitos que se llevan a cabo a través del internet.

Décima segunda.-Con la regulación se tendrá la oportunidad de disminuir esta conducta delictiva y así se estará ganando una batalla más en contra de este delito y logrando así la finalidad del derecho en general.

Décima tercera.- Al ser este delito novedoso y por lo mismo difícil para integrar los elementos para llevar al cabo el proceso judicial, se le tiene que dar a los postulantes la oportunidad de contar con tiempo para integrar los elementos necesarios, estudios hechos en el extranjero muestran que este tiempo es de cinco años a partir de la fecha en que se tenga conocimiento del ilícito por parte de la agencia investigadora.

BIBLIOGRAFÍA JURÍDICA.

1.- ARELLANO GARCÍA, Carlos, " Derecho internacional público", 12ª edición.,editorial Porrúa, S.A,, México, 1996.

2.- BARRIO GARRIDO GABRIELA, MUÑOZ DE ALBA MARCIA Y PEREZ BUSTILLO CAMILO, Internet y derecho en México, Mc. Graw Hill, México, 1997.

3.-BOXIR CLAUS, "Culpabilidad y prevención en el derecho penal", editorial. Reus, S.A., Madrid, España, 1981.

4.- CARRNCÁ Y TRUJILLO, Raúl/ Raúl Carrancá y Rivas, "Derecho penal mexicano, parte general",19 ª edición, editorial, Porrúa, México, 1997.

5.- CASEY EOGHAN, Digital evidence on computer crime, 2a. edición, San FRANCISCO, 2000, 279 p.

6.- CASTELLANOS TENA, Fernando, " Lineamientos elementales de derecho penal", 31ª. Edición, editorial Porrúa, S.A., México, 1992.

7.-BOGUER, Christina, "Cybercrime-cyberterorism-cyberwafare-averting an electronic waterloo. Global organized crime proyect, Washington D.C., 1998.

8.- GALINDO GARFIAS, Ignacio, " Derecho civil", 14ª. Edición, editorial Porrúa, S.A., México, 1995.

9.- GARCÍA RAMÍREZ, Sergio, "Derecho penal", UNAM, 1990. 83p.

10.- GONZÁLEZ DE LA VEGA Francisco, "Derecho penal mexicano", 25ª. edción, editorial Porrúa, S.A., México, 1992.

11.- GUERRERO M. MA. FERNANDA, "Delitos por computadora", Santa Fé de Bogotá Colombia, ediciones jurídicas Gustavo Ibáñez, 1999.

12.- HAFNER, KATIE, "Cyberpunk; out laws on the computer fronter", editorial Touchstone, Nueva York, 1995.

13.- JIMÉNEZ DE AZÚA, Luis " Principios de derecho penal", 3ra. Edición, editorial Depalma, Buenos Aires, 1990., 186p.

14.- KNIGHTMARE, Secrets of a super hacker, Washington, 1994

15.- LÓPEZ BETANCOUT, Eduardo, "Introducción al derecho penal", 2ª. Edición, editorial Porrúa, S.A., México, 1994, 281p.

16.- LÓPEZ BETANCOURT, Eduardo, "Teoría del delito", edtotial Porrúa, S.A, México l994, 303p.

17.- LOPEZ Y MIGUEL-GUÑI MUÑOZ," Informática jurídica documental", Madrid, Dias de Santos S.A., 1984.

18.- MANCILLA OVANDO, Jorge A, " Teoria legalista del delito", editorial Porrúa, S.A., México, 1989.

19.- ROBERETI RAQUEL," Llaneros solitarios; hackers, la guerrilla informática", Buenos Aires: Esposa Calpa, 1995.

20.- PARERAS LUIS, Intenet y derecho, Barcelona, 1998.

21.- PERZ LUÑO Y Enrique Antonio, "Manual de informática y derecho", Barcelona, Ariel S.A. 1996. 207p.

22.- PINA VARA, Rafael de, "Diccionario de derecho", 26ª. Edición, editorial Porrúa, S.A., México, 1998.

23.- SEARA VAZQUEZ, Modesto, " Derecho Internacional Público", 13ª. Edición, editorial Porrúa, S.A., México, 1991.

24.- SEPÚLVEDA Cesar, " Derecho internacional", 16edición, editorial Porrúa, S.A., México, 1991.

25.- SUSSKIND RICHARD," The future of law", Oxford university, 1996.

26.- TAYLOR PAULA, "Hackers, Crime in the digital sublime", Londres, 1999

27.- WASIK MARTIN," Crimen and computer", Oxford, 1991.

LEGISLACIONES MEXICANAS.

1.-Constitución Política de los Estados Unidos Mexicanos.
2.- Código Federal de Procedimientos Penales.
3.-Código Penal Federal.
4.- Ley de la Policía Federal Preventiva.
5.- Ley Orgánica de la Procuraduría General de la República.
6.- Reglamento a la ley orgánica de la Procuraduría General de la República.

LEGISLACIONES EXTRANJERAS.

1.- Constitución de los Estados Unidos de Norte América. (USA CODE).
2.- Convention on cybercrime. (convención contra el delito cibernético).
3.- Cybercrime act. (ley contra el delito cibernético).
4.- Terrorism act. (ley contra el terrorismo).

BIBLIOGRAFÍA INFORMÁTICA.

1.-www.usdoj.gov/criminal/cybercrime/search-does/toc.htm.

2.-www.usdoj.gov/criminal/cybercrime/supplement/ssgssup.htm.

3.-www.hcvc.org/infolink/info46.htm.

4.-www.uaonlim.org.

5.- www.law.cornell.edu/

6.-www.findlaw.com

7.-www.gahtan.com/techlaw/

8.-www.lawcrawler.com

9.-www.virusprot.com.

10.-www.cnnenespanol.com/2001/eeuu/canada/07/17/feb.

11.- www.mailer.fsu.edu/-6+1553/ccrr/cases.htm.

12.- www.legislation.hmso.gov.uk/acts/acts 2000/20000011.htm

13.- www.lawcrawler.findlaw.com/scripts/ic.pl?entry=hacker&sites=findlaw.

14.-www, pintos&salgado/unión económica europea/legislaciones.

15.- www.info jus.UNAM.mx.

16.- www.pgr/afi.com

17.-www.dgbiblio.UNAM.mx.

18.- www.bbs.sekr.es/

19.- www.nsi.org/library/composec/

A N E X O .

Este anexo que contiene la tesis, es para a conocer las noticias referentes al actuar del intruso cibernético o hacker, pretendiendo con ello demostrar lo que se esta realizando para luchar en contra de estos delincuentes, así como el mostrar el daño que puede causar un ataque de ésta naturaleza, no lo económico, sino también social y emocional.

Estas noticias con pocas, porque es un tema novedoso, también por ser los países llamados primer mundistas los que han recibido más ataques de esta naturaleza, es por ello que, estos países en sus proyectos de leyes y las leyes existentes son de las más avanzadas en este tema, sobresaliendo Estados Unidos de Norte América y la Unión Económica Europea.

Cabe resaltar que los ataques de los intrusos cibernéticos no son exclusivos de estos países, porque se tienen noticias que han atacado sitios webs como el de México, Colombia, Argentina, etc., lo que si se debe tomar en cuenta es que cada vez más lugares están siendo atacados por estos delincuentes y que se tienen que tomar las medidas pertinentes para combatirlo ya que es una situación actual que esta teniendo día a día mucha fuerza.

La primer noticia llamada "Cybertheft: un crimen cada día", es tomada de la página en internet que publica el diario estadounidense llamado New York Times del día 28 de Julio del 2002. Esta nota da a conocer los daños sufridos por compañías que pierden mucho dinero por el pirateo se programas o (softweares) para computadora: así como de canciones que se toman todos los días del internet; recordemos que en el contenido de la tesis se menciona esta conducta que realiza el intruso cibernético, utilizando los programas pirateados para engañar al disco duro de la computadora y así poder introducirse para saber el contenido de la información que se tiene en la computadora.

La segunda noticia llamada "Intrusos cibernéticos se enfrentan a penas más duras", fue tomada de internet, publicada por iblews. Com, que es una agencia de noticias de Estados Unidos de Norte América.

La tercera noticia llamada " Nace la agencia Europea para luchar contra el cibercrimen", fue tomada de internet, publicada por Euro sur, noticias de Europa para América Latina y Mercosur", la dirección electrónica donde se puede localizar esta nota es http:// www.Euro Sur /noticias.

Cybertheft: an every day crime crime

For some, Internet is a freeway to all kinds of information. Others think differently. Especially the software companies that lose billions of dollars because of copyright violation. But try as they might, the free-riders are hard to fight. . .

Paul's room is in a terrible mess. Full of floppys, diskdrives, wires and computer magazines. After an hour of silence, and dialing several bulletin board numbers on his PC, the law student suddenly jumps out of his chair and shouts out: "Bingo, I told you."

Paul, 21, a computer freak for at least ten years, has finally found what he was looking for: the new version of a high-tech game, worth hundreds of dollars. The place to be? The Internet, a vast international network of networks, linking as many as 40 million computers worldwide.

Each year companies lose billions of dollars because of theft in Cyberspace By some estimates, more than 2 billion dollars - approximately 4.6 billion Ecu - were stolen last year from copyrighted software alone. This is almost a quarter of the total 7.4 billion dollars which the Software Publishers Association (SPA) believes was lost to computer crime in 1994. According to the popular scientifical magazine New Scientist, the SPA have at their disposal a list that includes the names of at least 1,600 bulletin boards, which are used for illegal activities. The economical consequences of theft on the net are big, not to say enormous. Microsoft for instance, one of the world's largest software companies, lost more than an estimated 500 million dollars last year because of software theft.

Imprisonment

It is not only individuals, like Paul, who are involved in theft in Cyberspace. In 1993 CompuServe, the major online information service, were allegedly involved in a huge fraud. The Frank Music Corporation sued the American company for allegedly permitting subscribers to download more than 500 copyrighted songs. More recently, CompuServ was again in the middle of an immense Cyberspace fight. The service was sued by 140 music publishers for giving Internet-users the chance to copy popular songs.

A judicial break through

Richard Kenadek, from Milburry, Massachusetts, was recently grounded for six months, because of the illegal distribution of Lotus 1,2,3, Wordperfect and Norton Utilities. These programmes could be freely downloaded by anyone who paid Kenadek a membership of 100 U.S. dollars. It took investigators four months to track him down.

Last year different European countries, like France, Germany and the Netherlands, changed, or were considering changing, their laws concerning computer crime. In the Netherlands for example, illegal copying of protected software will, in the near future, be punished with a maximum imprisonment of six months or a fine of up to 25,000 guilders (approximately 57,000 Ecu). In Germany one of the many regulations is that providers (also of Internet), if requested, are forced to give police investigators all the information they have on their 'customers'.

Piracy

Despite these new regulations, several other cases of theft on the net have occured. A few months ago, Newsweek Magazine reported on a piracy ring operating out of Mallorca, Spain. One of the leaders pleaded guilty to a brand of fraud destined to become commonplace. US investigators found out that the criminal organization stole 140,000 telephone credit card numbers, which were sold to computer bulletin boards in the United States and Europe. This was not only a case of piracy but, because hackers used the phone numbers to make a huge 140 million dollars worth of long-distanced phonecalls, it became also a matter of copyright violation.

Considering all these incidents, is it reasonable to question whether theft in Cyberspace will ever disappear? "The consequence of Internet is that it has just become easier to commit copyright violation and harder to prove," said Michael Schneider, lawyer and head of department of the new telecommunication carrier Communications Network International (CNI) in Frankfurt. "We have to consider a concept to traditional copyright. Because if this development continues, publishing houses will eventually disappear. If no one is going to pay for copyrighted software anymore, how will publishers survive?"

Not a lost cause

Despite the enormous losses, the Business Software Alliance (BSA), the international 'watchdog' that safeguards worldwide software companies against any kind of computer crime, is still convinced that the fight against theft on the net is not a lost case. "With a lot of effort we can protect the net from becoming a free place for illegal activities. But we realise that we'll never be able to stop the total illegal distribution. If people want to get the new version of Windows for example, they'll eventually find it," said J. Ranselaar of BSA Holland. He denies that Microsoft, one of the founders of BSA, is frequently offering bounties for information leading to the arrest and conviction of distributors. "It only happened once, but that was more of a reward. The only way we can fight copyright violation is co-operating with Interpol and other countries. It is a worldwide problem."

Fanatics

Even though organised theft is the main cause of the enormous losses to software companies, there is more to it than meets the eye. For example people are down loading without realising that they are dealing with protected software.

Steven Fishman, author of Nolo's 'The Copyright Handbook' published on Internet, says copyright violation is not always a matter of premeditation. He said: "Users would probably think about copyright rules only if they wanted to republish a chapter of a book, a play or a song they liked. But they're easy to overlook when you're dealing with electronic media. These bits of information fly around so rapidly and can be reproduced so easily, that it's hard to remember that someone out there probably owns the right to determine when and how many copies are made and used."

The only effective way to fight theft of copyrighted ware, seems to be on the net itself. More passwords, codes and 'gates' could be the key. But what about that old Internet-spirit? That anarchistic ethic, stated most precisely in Steven Levy's 'Hackers', says that all information should be free. Anything found on the net, is still considered as information for everyone. At least, that is what 'sharing' is all about, according to pioneers of Cyberspace. And they will not give up that privilege very easily.

Michael de Roo

Pages created by: Wilhelm Lagercrantz: lagwil@imk.su.se - 21-06-95.

Cybertheft: un cada crimen de crimen de dia

> **Para algunos, Internet es una autopista a todos los tipos de información. Otros piensan diferentemente. Sobre todo las compañias del software que pierden billones de dólares debido a violación del derechos de propiedad literaria. Pero intenta cuando ellos pueden, los libre-jinetes son duros luchar. . .**

El cuarto de Paul está en un enredo terrible. Lleno de floppys, diskdrives, alambres y revistas de la computadora. Después de una hora de silencio, y marcando varios tablón de anuncios numera en su PC, el estudiante de derecho salta de repente fuera de su silla y gritos fuera: "Bingo, yo le dije."

Paul, 21 años, un monstruo de la computadora durante por lo menos diez años, han encontrado lo para que él estaba pareciendo finalmente: la nueva versión de un juego alto tecnología, valor ciento de dólares. ¿El lugar para ser? La Internet, una inmensa red internacional de redes, uniéndose tantos como 40 millones de computadoras mundial.

Cada compañías del año pierden billones de dólares debido a robo en el Ciberespacio. Por algunas estimaciones, más de 2 mil millones de dólares - aproximadamente 4.6 mil millones Ecu - se robó el año pasado exclusivamente del software propiedad registrado. Éste es casi un cuarto de los 7.4 mil millones dólares totales que la Asociación de Publicadores de Software (S.P.A.) cree se perdió a crimen de la computadora en 1994. Según la revista del scientifical popular el Nuevo Científico, el S.P.A. tiene a su disposición una lista que incluye los nombres de por lo menos 1,600 tablones de anuncios que se usan para las actividades ilegales. Las consecuencias baratas de robo en el precio neto son grandes, no decir enorme. Microsoft por ejemplo, uno de las compañías del software más grandes del mundo, perdido más de un estimó 500 millones de dólares último año debido a robo del software.

Encarcelamiento

No sólo es individuos, como Paul que está envuelto en robo en Ciberespacio. En 1993 CompuServe, el servicio de información en línea mayor, estaba según se alega envuelto en un fraude grande. La Frank Música Corporación demandó la compañía americana por permitirles según se alega a subscriptores transmitir más de 500 canciones propiedades registradas. Más recientemente, CompuServ estaba de nuevo en el medio de una inmensa lucha del Ciberespacio. El servicio se demandó por 140 publicadores de música por darles la oportunidad a Internet-usuarios para copiar las canciones populares.

Un descanso judicial a través de

Richard Kenadek, de Milburry, Massachusetts, se conectó con tierra recientemente durante seis meses, debido a la distribución ilegal de Loto 1,2,3, Wordperfect y Utilidades de Norton. Estos programas podrían transmitirse libremente por cualquiera que le pagó un número de miembros de 100 dólares americanos a Kenadek. Tomó a investigadores cuatro meses para rastrearlo abajo.

En el último año países europeos diferentes, como Francia, Alemania y Países Bajos, cambiaron, o estaba considerando cambiando, sus leyes acerca del delito de la computadora. Por ejemplo, en Países Bajos ilegal que copia de software protegido quiere, en el futuro cercano, se castigue con un encarcelamiento máximo de seis meses o una multa de a a 25,000 florines (aproximadamente 57,000 Ecu). En Alemania uno de las muchas regulaciones es que los proveedores (también de Internet), si pidió, se obliga a darles toda la información a los investigadores policíacos ellos llevan puesto su ` clientes.

Piratería

A pesar de estas nuevas regulaciones, varios otros casos de robo en el precio neto tienen occured. Hace unos meses, Revista de Newsweek informó en un anillo de piratería que opera fuera de Mallorca, España. Los investigadores americanos averiguaron que la organización delictiva robó 140,000 teléfono crédito tarjeta números que se vendieron a tablones de anuncios de la computadora en los Estados Unidos y Europa. Éste no sólo era un caso de piratería pero, porque los hackers usaron los números de teléfono para hacer un 140 millones de dólares valor grande de phonecalls largo-distanciado, también se volvió una materia de violación del derechos de propiedad literaria.

¿Considerando todas estas casualidades, es razonable a pregunta si robo en Ciberespacio alguna vez desaparecerá? "La consecuencia de Internet es que se ha puesto más fácil simplemente de comprometer violación del derechos de propiedad literaria y más difícilmente para demostrar", dijo Michael Schneider, abogado y cabeza de departamento de las nuevas Comunicaciones de portador de telecomunicación Conectan una red de computadoras Internacional (CNI) en Francfort. "Nosotros tenemos que considerar un concepto al derechos de propiedad literaria tradicional. Porque si este desarrollo continúa, editoras desaparecerán en el futuro. Si nadie va a ya pagar por el software propiedad registrado, cómo publicadores sobrevivirán? "

No una causa perdida

A pesar de las pérdidas enormes, la Alianza del Software Comercial (BSA), el internacional ` el perro guardián' eso salvaguarda las compañías del software mundiales contra cualquier amable de crimen de la computadora, todavía se convence que la lucha contra robo en el precio neto no es un caso perdido. "Con mucho esfuerzo nosotros podemos proteger el precio neto de volverse un lugar libre para las actividades ilegales. Pero nosotros comprendemos que nosotros nunca podremos detener la distribución ilegal total. Si las personas quieren conseguir la nueva versión de Windows por ejemplo, ellos lo encontrarán" en el futuro, dijo J. Ranselaar de BSA Holanda. Él niega que Microsoft, uno de los fundadores de BSA, frecuentemente esté ofreciendo liberalidades por información que lleva al arresto y convicción de distribuidores. "Sólo pasó una vez, pero ése era más de un premio. La única manera que nosotros podemos luchar que violación del derechos de propiedad literaria está cooperando con Interpol y otros países. Es un problema" mundial.

Fanáticos

Aunque el robo organizado es la causa principal de las pérdidas enormes a compañías del software, hay más a él que se encuentra el ojo. Por ejemplo las personas están mal cargando sin realising que ellos están tratándose del software protegido.

Steven Fishman, autor de Nolo ` El Manual del Derechos de propiedad literaria' publicó en Internet, dice violación del derechos de propiedad literaria no siempre es una cuestión de premeditación. Él dijo: "Usuarios probablemente pensarian sólo sobre reglas del derechos de propiedad literaria que si ellos quisieran un capítulo de un libro, una obra o una canción que les gustó. Pero ellos son fáciles pasar por alto cuando usted está tratándose de los medios de comunicación electrónicos. Estos

momentos de mosca de información alrededor de tan rápidamente y puede reproducirse tan fácilmente, que es duro recordar que alguien fuera allí posee el derecho para determinar probablemente cuando y cuántas copias son hecho y usadas."

La única manera eficaz de luchar robo de mercancías propiedad registrada, parece estar en el propio precio neto. Más contraseñas, códigos y ` verjas podría ser la llave. ¿Pero eso que sobre ese Internet-espíritu viejo? Ese anarquista ético, el más precisamente declaró en Steven Leva ` Computomaníacos, dice que toda la información debe ser libre. Algo encontró en el precio neto, todavía es considerado como información para todos. Por lo menos, ése es eso que ` compartiendo' es por todas partes, según pioneros de Ciberespacio. Y ellos no dejarán ese privilegio muy fácilmente.

Michael de Roo

Páginas creadas por: Wilhelm Lagercrantz: lagwil@jmk.su.se - 21-06-95.

En 1997, un adolescente que entró en la red de la compañía telefónica Bell Atlantic hizo que el sistema se cayera dejando a 600 hogares, un aeropuerto regional y los servicios de emergencia sin comunicación telefónica y afectando las comunicaciones de tráfico aéreo durante seis horas, informa Reuters.

Miércoles, 14 agosto 2002
IBLNEWS, Agencias

El joven se declaró culpable y fue sentenciado a dos años de libertad condicional, una multa de 5.000 dólares y a servicio comunitario. Pero en un futuro cercano, la sentencia podría ser de cadena perpetua si alguien muere por un accidente de avión o por la demora en contactar los servicios de emergencia.

"Ese es un escenario realista", dijo William Reilly, abogado de la firma Cyber Security Law, con sede en San Francisco.

Los fiscales y jueces en Estados Unidos están enfrentando los delitos cibernéticos con más agresividad que nunca, afirmó Reilly. Los atentados con aviones secuestrados el 11 de septiembre han sido utilizados para justificar un tratamiento más duro en nombre de la seguridad nacional, afirman expertos.

Esa realidad oscureció el ambiente en la décima conferencia anual de intrusos cibernéticos DefCon, celebrada el fin de semana en Las Vegas, a pesar de las celebraciones que incluyeron una fiesta con música tecno, cerveza barata y desnudistas.

Esta es la mayor reunión en el mundo de los anarquistas del ciberespacio y programadores renegados, que prefieren operar bajo nombres falsos.

"El acto de la intrusión por sí mismo tiene una dimensión política", dijo Richard Thieme, escritor, ex sacerdote episcopal y la figura paterna de muchos intrusos

cibernéticos. "Antes del 11 de septiembre, no podía ser definido como un acto de terrorismo por sí mismo".

Aunque la mayoría de los asistentes a la conferencia mantuvo su instintiva desconfianza hacia la autoridad, algunos han estado ofreciendo su servicios al gobierno estadounidense desde los atentados.

"Hay mayor conciencia de que todos estamos juntos en esto", dijo Thieme, quien fue uno de los oradores en la conferencia. "Son mucho más realistas. Han perdido su sueño".

Nuevas leyes contra el ciberdelito

Una de las preocupaciones de muchos intrusos es el Acta Patriótica que entró en vigor el año pasado y un nuevo proyecto de ley llamado "Acta de Mejoramiento de la Seguridad Cibernética", aprobado el mes pasado por abrumadora mayoría en la Cámara de Representantes.

El Acta Patriótica elevó la pena máxima por entrar en una red de computadoras de cinco a 10 años de prisión. El nuevo proyecto propone un máximo de cadena perpetua para los intrusos que causen o intenten causar la muerte de alguien.

"Lo que era un delito menor antes del Acta Patriótica podría ser ahora un delito mayor con una sentencia de cinco a 10 años", dijo un hombre que se identificó como "Simple Nomad", orador en la conferencia y que trabaja en la empresa de seguridad BindView Corp. "Eso amedrenta a mucha gente".

Como resultado, los intrusos que antes actuaban por aburrimiento o para buscar un reto, están ahora dirigiendo sus energías al uso de la tecnología para perseguir fines políticos.

Por ejemplo, ahora hay más investigación para proteger el anonimato en Internet. Esas tecnologías incluyen la "esteganografía", que consiste en ocultar mensajes en objetivos como imágenes digitales, dijo "Simple Nomad".

El desarrollo de tales tecnologías de evasión enfrenta aún más a los intrusos con los agentes de la ley, que en la década de 1990 perdieron todas las batallas para evitar la disponibilidad de sistemas de criptografía, utilizados para mantener los mensajes en secreto.

La Oficina Federal de Investigaciones (FBI) y otras agencias han aumentado la supervisión en Internet tras encontrar información relacionada con la Web en computadoras decomisadas a Al Qaeda, el grupo al que Washington responsabilizó por los atentados del 11 de septiembre.

Los intrusos están ahora "más preocupados por las consecuencias políticas y la posibilidad de que el gobierno les quite más de sus derechos", dijo un intruso que se identificó como Rain Forest Puppy.

Patriotismo renovado

Para algunos, sin embargo, los atentados del 11 de septiembre acarrearon un renovado sentido de patriotismo. Por ejemplo, Thieme dice que conoce a varios intrusos que están usando sus habilidades para ayudar a los servicios de inteligencia de Estados Unidos.

"Hubo una enorme necesidad y de repente la CIA y todos esos tipos ya no eran más los enemigos", dijo Thieme.

Para Simple Nomad, "ha habido destellos de patriotismo que muchos intrusos no habían experimentado nunca".

Al menos un agente federal del gobierno estadounidense está de acuerdo.

"Creo que veremos más de esto porque el mundillo subterráneo de la computación tiende a ser bastante patriótico", dijo Don Cavender, agente especial de la unidad de

entrenamiento en computadoras de la FBI.

"En los tres meses posteriores al 11 de septiembre, podría haber acudido a la comunidad clandestina y haber obtenido una mejor respuesta que antes", dijo Cavender, uno de los pocos agentes federales presentes en la conferencia que no ocultó su identidad.

Encuesta

¿Ud. cree que, finalmente, Europa apoyará a los Estados Unidos en la guerra contra Irak?

Indicadores UE

Alemania

Austria

Bélgica

Dinamarca

España

Finlandia

Francia

Gran Bretaña

Grecia

MEDIOS E INTERNET - 6/6/2001 14:06GMT

Nace la agencia europea para luchar contra el "cybercrimen"

Por Martino Rigacci

(ANSA) - BRUSELAS, 6 JUN - Los hábiles y dañinos "hackers" que se mueven en la red a la busca de nuevas víctimas están advertidos. Dentro de poco nacerá en Bruselas la "Agencia europea para la lucha al cybercrimen" que tendrá tres objetivos principales: luchar contra los ataques informáticos, frenar la difusión de los virus y combatir los fraudes on-line.

La propuesta de la nueva Agencia fue presentada hoy a la Comisión Ejecutiva, que probablemente la aprobará cuanto antes.

Los expertos del sector afirman que los europeos -tanto los privados, como las empresas o las estructuras públicas- están cada vez más expuestos a las ofensivas vía internet, no sólo a raíz de los virus o los fraudes, sino también en el frente de las crecientes interceptaciones de las comunicaciones y los mensajes del correo

home

Lea más sobre Medios e Internet

Italia: brigada antiterrorismo allanó domicilios de periodistas italianos

Italia-Argentina: RAI dedicará programa al retorno de residentes italianos

Italia-América latina: "el modelo ha fracasado", afirma diario L'Unita

Irlanda

Italia

Luxemburgo

Países Bajos

Portugal

Suecia

CALCULADORA

Foro

Newsletter

nombre:

e-mail:

electrónico, además del robo de la identidad de los internautas.

Según las últimas estadísticas de las que dispone la Comunidad Ejecutiva, en Europa hay un creciente aumento de la difusión de los virus, visto que sobre la base de los datos de febrero el 11% de los navegantes de la red ha sido víctima de un programa "asesino" recibido desde el exterior, frente al 9% de octubre pasado.

Pese al gigantesco volumen de negocios del mercado del "software" para la seguridad de los sistemas -casi US$ 500 millones en el 2000- los usuarios europeos de internet no son muy receptivos en este frente, visto que sólo el 5% utiliza los servicios on-line que brindan programas de seguridad, frente al 25% de lo que ocurre en Estados Unidos.

Pese al elevado nivel del uso de programas anti-virus (el 80% de los navegantes) en Europa hay muy poca difusión de los sistemas para la decodificación de los datos (menos del 18%), el uso de las firmas electrónicas (el 6%) o los sistemas "firewall" que impiden el acceso a los datos de las redes o de las computadoras (menos del 3%).

Italia: Valeria Mazza en la TV con Mijail Gorbachov

Italia: cierran dos programas políticos en la RAI

Medios: Murdoch visita Italia para sondear adquisición de Tele+

"Torre de Babel": nuevo manual de comunicación italiano

Premio Príncipe de Asturias a los "padres" de Internet

Los expertos europeos han, por otra parte, advertido que las cosas están destinadas a empeorar con el lanzamiento de las conexiones a la red activas 24 horas sobre 24 y con el creciente uso de las aplicaciones internet para rubros como por ej. los sistemas de seguridad, antiincendios o de alarmas.

De una u otra manera, los temibles "hackers" tendrán así nuevos flancos para poder dar rienda libre a su fértil fantasía.(ANSA)

Ansa-Valle d'Aosta: nuevo sitio Internet de turismo

Redacción de semanario político es invadida en Roma

Operación internacional contra explotación paidofílica

Italia: falta tecnología informática para "e-commerce"

Internet: aumenta número de usuarios en Europa

Italia tiene 20 millones de internautas

Mediaset negó estar implicado con Premiere World

Intrusos ciberméticos se enfrentan a penas más duras

En 1997, un adolescente que entró en la red de la compañía telefónica Bell