Hacking y ciberdelito

Autor: Vicente Miguel Giménez Solano

Director: Juan Vicente Oltra Gutiérrez

ÍNDICE

1. Objeto y objetivos

El objeto del presente Proyecto de Fin de Carrera es la obtención del título de Ingeniero Técnico en Informática de Gestión, expedido por la Universidad Politécnica de Valencia.

En lo que respecta a objetivos, el presente Proyecto alberga dos de la misma envergadura e importancia.

El primero de ellos es dar a conocer al lector, que se supone, en primera instancia, ajeno al mundo de la informática, conceptos referidos al *hacking*, ya sean básicos, medios, avanzados y de carácter histórico.

El segundo objetivo es, partiendo de dos grandes conjuntos como son la informática y el mundo de las leyes, realizar una intersección entre ellos y proyectarla al lector. Pretendemos, pues, en este segundo objetivo, que el lector quede notablemente marcado y concienciado por la problemática que presenta la intersección mencionada y, asimismo, que adquiera unos conocimientos medios sobre las leyes que se ocupan de la informática,

de cómo se regula, de qué delitos existen relacionados con el mundo de las tecnologías de la información, de sus repercusiones, de las consecuencias jurídicas, de los tipos de fraudes, etc.

Deseamos, pues, y sobretodo, que el lector se encuentre cómodo leyendo estas memorias y tenga la sensación, y que así sea, de que está adquiriendo conocimientos útiles y actualizados en lo que concierne a los temas mencionados.

2. Introducción

El mundo de la Informática ha avanzado a pasos agigantados en los últimos veinte años. Son muchas las ventajas que conlleva la Informática al desarrollo tecnológico. Por ejemplo, al campo de la Medicina, a la Biología, a la Geología, a la Arquitectura, a la Ingeniería, etc. Pero todo este gran avance no está exento de ser controlado, y no escapa al poder de la Ley. Nos referimos en este caso a Internet y al desarrollo de programas, básicamente.

Con la llegada de Internet, la Informática y las comunicaciones van de la mano, y con ellas ha nacido la posibilidad de realizar *ciberdelitos*. No sólo porque ahora la Informática es un medio ideal para la realización de delitos, sino porque la propia Informática puede ser el objeto de delito.

Nos referimos, concretamente, a delitos contra la **propiedad intelectual**, la **propiedad industrial**, el **derecho a la intimidad** (interceptación de comunicaciones), el **patrimonio** (estafas, apropiación indebida y fraudes), la **libertad** y **amenazas**, el **honor** (calumnias e injurias), el **mercado** y los **consumidores** (revelación de secretos, publicidad engañosa y falsedades documentales), la **libertad sexual** y **prostitución**. Asimismo, delitos de **sabotaje informático**, **convencionales** (espionaje, espionaje industrial y terrorismo informático), del **mal uso de la red** (*cybertorts*, usos comerciales no éticos, actos parasitarios y obscenidades). Y, por último, delitos tradicionalmente denominados "**informáticos**" (acceso no autorizado, destrucción de datos,

ciberterrorismo, infracción de los derechos de autor, infracción del *copyright* de bases de datos, interceptación de e-mail, estafas electrónicas, transferencia de fondos y *phising*).

¿Qué dice la legislación al respecto? ¿Hay alguna ley que trate este tipo de delitos? ¿Cuenta el Código Penal Español con alguna ley o leyes referidas a ellos? Veremos que sí, y veremos también que, además de los delitos mencionados, también pueden producirse infracciones de la Ley de Protección de Datos y de la Ley de Propiedad Intelectual.

Hace 30 años nadie se preocupaba de si alguien podía acceder a su sistema informático de manera ilegítima y causar daños y, en general, de los *ciberdelitos*. Ahora, el desarrollo acelerado de la Informática se ha encargado de hacer patente dicha preocupación, y es por ello que es un tema que debe cogerse a conciencia por profesionales de la Ley a la par que por profesionales de la Informática y buscar una solución o, lo que se está llevando a cabo, ir adaptando la actual legislación en términos de Informática y de Tecnologías de la Información en general.

Por la importancia de este tema es por lo que hemos decidido elaborar un Proyecto Final de Carrera (en el que, además, se desarrollará una web de apoyo), que describa esta problemática en términos de actualidad, haciendo especial hincapié en las repercusiones legales que pueda tener el uso ilegítimo de la Informática unido a la posibilidad de llevar a cabo delitos o faltas sancionables. Haremos una clasificación de la legislación vigente y de las posibles infracciones que se pueden llevar a cabo. Asimismo, aprenderemos conceptos básicos relacionados con los delitos informáticos y en particular del *hacking*. Haremos un repaso de los *hackers* más importantes de la historia, veremos noticias relacionadas, analizaremos sentencias de casos reales y presentaremos el actual abanico legislativo que se ocupa de lidiar con este tema.

Hemos estructurado estas memorias en dos bloques. En el primero de ellos, el BLOQUE I, el lector va a poder conocer todo lo relacionado con el *Hacking*. Y en el segundo, el BLOQUE II, presentaremos el ámbito legislativo referente al *Hacking* y a los Sistemas de Información en general, como hemos anunciado en el párrafo anterior.

3. Metodología y herramientas

Para el desarrollo de este Proyecto Final de Carrera se ha recabado una gran cantidad de información a través de Internet, ha sido filtrada, revisada y, en muchos casos, resumida y/o esquematizada.

Otro punto de apoyo importante han sido proyectos finales de carrera de años anteriores de características similares o que trataran parcialmente las temáticas que aquí vemos.

Y, por supuesto, algunos libros y apuntes de asignaturas han supuesto la base, los cimientos para construir a partir de ellos y desarrollar el proyecto y ayudar en el desarrollo de estas memorias.

Las herramientas empleadas han sido:

Para el Proyecto

- Navegadores de Internet (Firefox y Google Chrome)
- Internet (con todo lo que ello conlleva: artículos, libros online, vídeos, apuntes, sitios web, etc.)
- Buscadores
- Legislación
- Literatura gris
- Apuntes
- Otros proyectos

Para el desarrollo de las memorias

- Open Office (Writer)

Para el desarrollo de la web

- Adobe Photoshop CS5
- Adobe Dreamweaver CS5
- Macromedia Freehand MX
- Open Office (Writer)

4. *Hacking*

Llamamos ***hacking*** a un conjunto de técnicas para acceder a un sistema informático sin autorización. Existe autorización cuando se dispone de un control de acceso mediante el uso de identificadores de usuario y *passwords*. Es un término tradicionalmente ligado a la libertad de Información de Internet. En sus códigos está el respetar la vida privada, pero eso después de aprender cómo funcionan los sistemas y dónde están los datos. Entre sus medios destacan los *Sniffers* o escaneadores de puertos, programas que buscan claves, *passwords* y puertos abiertos. Actúan conjuntamente con otras aplicaciones como reventadoras de claves y nukeadores.[1]

4.1. Qué es un *hacker*

En general se tiene la idea de que un ***hacker*** es un pirata informático que se infiltra en sistemas

1 DE MIGUEL, María del Rosario y Juan Vicente Oltra. *Deontología y aspectos legales de la informática: cuestiones éticas, jurídicas y técnicas básicas.* Valencia : Ed. UPV, 2007. p. 119 ISBN 978-84-8363-112-6

informáticos sin autorización, ilegalmente, para robar, modificar o destruir información. Esta visión, en realidad, es errónea. De esa definición se desprende el concepto de ***cracker***.

Un *hacker* es un entusiasta de la informática con un gran interés en aprender acerca de los sistemas informáticos y de cómo usarlos de formas innovadoras. Esto les lleva a penetrar en sistemas, normalmente a través de Internet, en busca de esa información que los lleve a encontrar más conocimientos. Una vez dentro, se limitan a dejar su marca, un "yo estuve aquí". Suelen escribir alguna versión de la ética del *hacker*, código que les lleva a no hacer daño, sólo a borrar sus huellas, y que además refleja una fuerte repulsión contra el vandalismo de los *crackers*. No se estropean los datos de los demás y la libertad de información no debe atentar contra el derecho a la vida privada. Suelen ser personas inteligentes. Aunque queda claro que no son *crackers*, se supone que cualquier *hacker* auténtico ha jugado con algún tipo de *crackeo* y conoce muchas de las técnicas básicas. Sus características podrían ser: personas que disfrutan investigando detalles de los sistemas y cómo aprovechar para sacarles jugo; no como la mayoría de los usuarios, que sólo aprenden lo imprescindible. Disfrutan del reto intelectual de superar o rodear las limitaciones de forma creativa. Programan de forma entusiasta (incluso obsesiva) y rápida. Son sociales, en contra de la opinión generalizada, pues se reconocen los méritos entre sí mismos.[2]

Según la Wikipedia, un ***hacker*** es una persona que pertenece a una de estas comunidades o subculturas distintas pero no completamente independientes:

- Gente apasionada por la seguridad informática. Esto concierne principalmente a entradas remotas no autorizadas por medio de redes de comunicación como Internet ("Black hats"). Pero también incluye a aquellos que depuran y arreglan errores en los sistemas ("White hats") y a los de moral ambigua como son los "Grey hats".

- Una comunidad de entusiastas programadores y diseñadores de sistemas originada en los sesenta alrededor del Instituto Tecnológico de Massachusetts (MIT), el Tech Model Railroad Club (TMRC) y el Laboratorio de Inteligencia Artificial del MIT. Esta comunidad se caracteriza por el lanzamiento del movimiento de software libre. La World Wide Web e Internet en sí misma son creaciones de *hackers*. El RFC 1392 amplia este significado como "persona que se disfruta de un conocimiento profundo del funcionamiento interno de un sistema, en particular de computadoras y redes informáticas".

2 DE MIGUEL, María del Rosario y Juan Vicente Oltra. *Deontología y aspectos legales de la informática: cuestiones éticas, jurídicas y técnicas básicas.* Valencia : Ed. UPV, 2007. p. 118 - 119 ISBN 978-84-8363-112-6

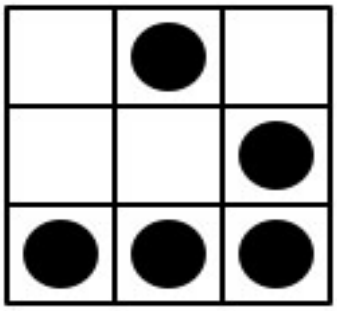


Figura 1. Emblema hacker

- La comunidad de aficionados a la informática doméstica, centrada en el hardware posterior a los setenta y en el software (juegos de ordenador, *crackeo* de software, la demoscene) de entre los ochenta/noventa.

En la actualidad se usa de forma corriente para referirse mayormente a los criminales informáticos, debido a su utilización masiva por parte de los medios de comunicación desde la década de 1980. A los criminales se le pueden sumar los llamados "script kiddies", gente que invade computadoras, usando programas escritos por otros, y que tiene muy poco conocimiento sobre como funcionan. Este uso parcialmente incorrecto se ha vuelto tan predominante que, en general, un gran segmento de la población no es consciente de que existen diferentes significados.

Mientras que los *hackers* aficionados reconocen los tres tipos de *hackers* y los *hackers* de la seguridad informática aceptan todos los usos del término, los *hackers* del software libre consideran la referencia a intrusión informática como un uso incorrecto de la palabra, y se refieren a los que rompen los sistemas de seguridad como "*crackers*" (analogía de "*safecracker*", que en español se traduce como "un ladrón de cajas fuertes").[3]

3 http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Hacker, Agosto/2011

4.2. Conceptos básicos[45]

4.2.1. *Newbie*

Muchas ganas, pero en fase de adquisición de conocimientos.

4.2.2. *Hacker*

Amplios conocimientos de redes (TCP/IP), sistemas operativos (Windows, Linux), programación (Java, ensamblador).

4.2.3. Experto

Conocimientos muy avanzados sobre todo lo relacionado con la informática. Pueden ser seniors, administradores de sistemas...

4.2.4. *Lamer*

Carecen prácticamente de conocimientos, psicológicamente perdidos, ayer quisieron ser 007, hoy *hackers*. Buscan información para presumir de ella o para plagiarla.

Estas definiciones no incluyen a los *hackers* malignos que deliberadamente rompen sistemas y borran ficheros, simple y llanamente porque ese es un mal uso del término. Se tiende a confundir a los *hackers* con: ***phreakers*** (piratas de software), ***carders*** (los que hacen un uso ilegal de tarjetas de crédito) y ***crackers***. Vemos sus definiciones a continuación.

4.2.5. *Luser*

Es el término despectivo con el que los *hackers* aluden a los usuarios comunes de los ordenadores e Internet. Proviene de dos palabras inglesas: loser (perdedor) y user (usuario).

4.2.6. *Phreaker*

Es una persona que investiga los sistemas telefónicos, mediante el uso de tecnología por el placer de manipular un sistema tecnológicamente complejo y en ocasiones también para poder obtener algún tipo de beneficio como llamadas gratuitas. Phreak es una conjunción de las palabras phone (teléfono en inglés) y freak, algo así como pirado por los teléfonos y surgió en los Estados Unidos en los años 1960. Entre los phreakers más conocidos destaca el Capitán Crunch, a quien veremos más adelante en el capítulo dedicado a *hackers* importantes.

---

4 DE MIGUEL, María del Rosario y Juan Vicente Oltra. *Deontología y aspectos legales de la informática: cuestiones éticas, jurídicas y técnicas básicas.* Valencia : Ed. UPV, 2007. p. 119 - 122 ISBN 978-84-8363-112-6

5 GIJÓN, Jesús. *Hackers, crackers y sus implicaciones sociales y mediáticas.* Valencia UPV. p. 15 - 23

4.2.7. *Carder*

Se le llama de esta forma al *hacker*, que con propósitos de *cracking* o *preaking*, realiza transacciones con tarjetas creadas o adulteradas. Se aprovecha de las múltiples vulnerabilidades que poseen las compañías de tarjeta de crédito. Subsisten bastante en el sistema, debido a que las compañías no efectúan las denuncias correspondientes, a fin de no perder credibilidad en el mercado. Es mediante técnicas de ingeniería social y troyanos como consigue el carder los números de tarjetas.

4.2.8. *Cracker*

(Black hat)[6] En contraposición a los *hackers* coexisten los *crackers* que son aquellos expertos o aficionados en las nuevas tecnologías de la información que de forma consciente y voluntaria usan su conocimiento con fines maliciosos, antimorales o incluso bélicos, como intrusión de redes, acceso ilegal a sistemas gubernamentales, robo de información, distribuir material ilegal o moralmente inaceptable, piratería, fabricación de virus o herramientas de *crackeo*, es decir, usan sus conocimientos para el beneficio propio, para lucrarse o para causar daños en un objetivo. Los *crackers* forman pequeños grupos, secretos y privados (se adentran en el terreno de lo ilegal), que tienen muy poco que ver con la cultura abierta (open source) que se describe en el mundo *hacker*.

Pero dentro de esta nueva cibersociedad, no sólo son *hackers* o *crackers*, ya que dentro de cada una de estas categorías existen diferencias entre sus miembros, existen aprendices, existen especialistas *hackers* contratados por las empresas,… Pasemos ahora a nombrar las categorías más importantes y los términos designados para cada eslabón de la nueva sociedad, los términos aparecen por orden alfabético con el fin de tener un manual de consulta.

4.2.9. Pirata del software

El pirateo está en auge y la causa más importante son los altos beneficios económicos que proporciona a sus autores. Es tal el volumen de pérdidas que supone para las empresas la piratería, que lo que empezó siendo una simple gamberrada, se ha convertido en un serio problema a combatir. Todo esto sin contar el descenso en los puestos de trabajo y las pérdidas por dejar de recaudar dinero en las arcas del Estado. Por estas causas, apareció en 1995 el Grupo de Delitos Informáticos (cuenta con el apoyo del Servicio de Informática y con el Servicio de Telecomunicaciones. También cuentan con colaboradores externos de instituciones privadas o públicas, los cuales se ven afectados de manera directa e indirecta por estas actividades), dentro de la Comisaría General de la Policía Judicial. Este grupo depende de la Brigada de Delincuencia Económica, pues en la mayoría de casos los piratas se mueven por fines económicos. En la

6 Los conceptos de *Black, White y Grey Hat* los vemos más adelante, en el apartado 7. *Hacking* ético

actualidad, el CD-ROM e Internet son dos de las plataformas más utilizadas para piratear; no se trata de nuevos delitos, sino de nuevos medios para cometerlos. Está muy relacionado además el pirateo con el empleo de *cracks*.

Hay que recordar que tanto la venta como la compra de software ilegal están penadas. El Código Penal hace que el pirata se exponga a años de cárcel y multas considerables. Comprar software pirateado es denominado como el delito de receptación, pero queda la duda; *¿se conocía o no la ilegalidad de ese programa antes de comprarlo?* Recordemos el caso *Vesatec*. Esta empresa ofrecía alojamiento a través de la página web «El Jamón y el Vino» a software copiados y *cracks*, entre otros productos. Tras un registro sorpresa en esta compañía, fue clausurada la página web. Emitieron un comunicado donde lanzaba una serie de críticas a la BSA (*Business Software Alliance*), promotora de esta investigación, por ir contra los particulares y dejar impunes a grandes empresas que piratean software mientras se investiga a las pequeñas y medianas empresas.

Estas críticas, realmente difíciles de rebatir, nos hacen pensar que hay que distinguir entre grandes y pequeños piratas. Los más abundantes son los pequeños, los usuarios particulares, aunque siempre que pensamos en piratas pensamos en esa persona que se dedica a realizar cientos o miles de copias de un programa. Las empresas pretenden reducir el micropirateo abaratando los precios.

4.2.10. Bucanero

Son peores que los Lamers, ya que no aprenden nada ni conocen la tecnología. Comparados con los piratas informáticos, los bucaneros sólo buscan el comercio negro de los productos entregados por los *Copyhackers*. Los bucaneros sólo tienen cabida fuera de la red, ya que dentro de ella, los que ofrecen productos "*crackeados*" pasan a denominarse "piratas informáticos". El bucanero es simplemente un comerciante, el cual no tienen escrúpulos a la hora de explotar un producto de *cracking* a un nivel masivo. El bucanero compra al *CopyHacker* y revende el producto bajo un nombre comercial. En realidad es un empresario con mucha afición a ganar dinero rápido y de forma sucia.

4.2.11. *Ciberokupa*

Este término ha sido ampliamente usado en los medios de comunicación para referirse al registro de dominios de marcas comerciales de forma ilegítima. En definitiva, un *ciberokupa* es una persona que se dedica a comprar y reclamar los derechos de determinados dominios de Internet relevantes o buscados por grandes empresas, celebridades emergentes u otros, con el fin de revendérselos a los interesados a un precio desorbitado. En muchas ocasiones ocupan el dominio

mediante páginas web de contenido poco apropiado con el objetivo de meter presión al interesado.

También los *ciberokupas* registran nombres de páginas web muy parecidos a los originales, son los llamados 'Typosquatters', consiste en prever los errores tipográficos más probables que cometerán los visitantes de direcciones URL famosas: por ejemplo, escribir "microsft" en lugar de "microsoft". Este es el caso de Googkle.com un sitio con forma de buscador pero que en realidad (es decir en su código fuente) tenía dos acciones, una oculta y una visible. La oculta es que al entrar en el servidor incorrecto, descargaban en la máquina-víctima dos virus, tres troyanos y un ejecutable que anulaba las actualizaciones de los antivirus *McAfee*, *Norton* y *Karspersky*. La visible es que luego de mostrar una advertencia falsa de que la máquina estaba infectada, te redirigía a una página de una empresa proveedora de soluciones antivirus. Otro ejemplo de *typosquartters* sobre google es la página *www.goggle.com*, que nos presenta una sospechosa página de regalos.

Otra técnica también utilizada es conocida con el nombre *cibersquatting*, consiste en registrar los mismos nombres de dominio de sitios bien conocidos y únicamente cambiar la extensión (.com en lugar de .org, por ejemplo) o bien añadir una palabra. Este es el caso de es el sitio *whitehouse.com*, que no tiene nada que ver con el sitio Web de la Casa Blanca (*whitehouse.gov*) y que conduce a los usuarios a un sitio de contenido pornográfico.

4.2.12. *Ciberpunk*

Jóvenes intelectuales, no necesariamente expertos en informática, que apuestan definitivamente por una red libre, sin control y con tarifa plana y a los que les vale cualquier cosa con tal de no profanar estos principios básicos.

Apuestan por aprender a hacer las cosas por si mismos, llegan a defender la libertad de información a niveles extremos como podría ser la divulgación de manuales de construcción de bombas atómicas caseras o *hacking* sobre satélites, apoyándose en el principio de que la información en sí no es mala.

4.2.13. *Copyhacker*

En cuanto a ingeniería social, se trata del grupo más experto, pues su objetivo es aprovecharse de los propios *hackers* y que éstos les expliquen cómo *crackear* cualquier software o hardware. Después, venden el software a los bucaneros.

4.2.14. *Geek*

Es una persona que comparte una gran fascinación, quizás obsesiva, por la tecnología e informática. Es más un estilo de vida y una forma de ser que una afición concreta por algo poco habitual. Su objetivo es hacer las cosas por diversión y por el reconocimiento, casi siempre por el simple placer de hacerlo. En el idioma español este término esta relacionado solo a la tecnología a diferencia del uso del término *geek* en el idioma inglés, que tiene un significado más amplio y equivalente al término español *friki*.

Según el *Jargon File* un *geek* es una persona que ha elegido la concentración en lugar del conformismo, alguien que persigue la habilidad (especialmente la habilidad técnica) y la imaginación, en lugar de la aceptación social de la mayoría. Los *geeks* habitualmente padecen una versión aguda de neofilia (sentirse atraídos, excitados y complacidos por cualquier cosa nueva). La mayor parte de los *geeks* son hábiles con los ordenadores y entienden la palabra *hacker* como un término de respeto, pero no todos ellos son *hackers*. De hecho algunos que son *hackers* de todas formas se llaman a sí mismos *geeks* porque consideran (y con toda la razón) que el término «hacker» debe ser una etiqueta que otras personas le pongan a uno, más que una etiqueta alguien se ponga a sí mismo.

Una descripción más completa aunque algo más larga incluiría a todos los jugones, apasionados, aficionados a la ciencia ficción, *punks*, pervertidos, *nerds*, especies de cualquier subgénero y *trekkies*. El tipo de personas que no va a las fiestas del colegio, promociones y otros eventos. Y que incluso se sentiría ofendida por la simple sugerencia de que tal vez estuvieran interesados.

4.2.15. Gurú

Se trata del experto en un determinado tema, normalmente muy complicado o extenso (como conocer en profundidad alguna distribución de GNU/Linux). A un Gurú se le puede preguntar cualquier cosa al respecto: es la opinión y palabra final. Ha llegado a esta etapa del conocimiento sin esfuerzo aparente alguno, y su sabiduría es tal, que no se debería abusar de su paciencia, y las preguntas deben ser planteadas correctamente. No se debe esperar grandes demostraciones de afecto por parte de un Gurú: cuando habla, no lo hace personalmente sino al mundo a través de sus comentarios en su propio blog o en las listas de correo. Tampoco habla mucho: lo hace certeramente y con educación cada vez que lo hace, y si está irritado u ocupado puede utilizar pocas palabras o acrónimos.

4.2.16. *Phiser*

También se le llama *Ingeniero Social*. Es un *hacker* que se aprovecha de una de las más grandes vulnerabilidades que poseen los sistemas: los humanos. Habitualmente el Ingeniero Social consigue contraseñas a través de aprovechar descuidos del personal, tales como dejar contraseñas escritas, llamar por teléfono haciéndose pasar por un servicio técnico, conectarse a puertos con contraseñas “default” o “test” para solicitar servicios o suponiendo contraseñas como “123” o “111”. Aunque parezca raro, en un informe de una consultora de Europa, el 85% de casos de vulnerabilidades en los sistemas se producen por medio de la Ingeniería Social desde adentro de la empresa, por
los mismos empleados. También se hacen pasar por empresas de confianza en correos electrónicos pidiendo los datos por ejemplo de la tarjeta de crédito o creando también sitios web clones de entidades bancarias donde obtienen los datos de usuario y contraseñas. En los últimos años están aumentando los casos de phising de una forma alarmante. Pueden existir más formatos de phising pero en estos momentos sólo mencionamos los más comunes:

• SMS (mensaje corto); La recepción de un mensaje donde le solicitan sus datos personales.

• Llamada telefónica; Pueden recibir una llamada telefónica en la que el emisor suplanta a una entidad privada o pública para que usted le facilite datos privados. Un ejemplo claro es el producido con la Agencia Tributaria, ésta advirtió de que algunas personas están llamando en su nombre a los contribuyentes para pedirles datos, como su cuenta corriente, que luego utilizan para hacerles cargos monetarios.

• Página web o ventana emergente; es muy clásica y bastante usada. En ella se simula suplantando visualmente la imagen de una entidad oficial, empresas, etc. pareciendo ser las oficiales. El objeto principal es que el usuario facilite sus datos privados. La más empleada es la "imitación" de páginas web de bancos, siendo el parecido casi idéntico pero no oficial. Tampoco olvidamos sitios web falsos con señuelos llamativos, en los cuales se ofrecen ofertas irreales y donde el usuario novel facilita todos sus datos, un ejemplo fue el descubierto por la Asociación de Internautas y denunciado a las fuerzas del Estado: Web-Trampa de recargas de móviles creada para robar datos
bancarios. Es el caso del phising realizado a la entidad bancaria caja Madrid.

• Correo electrónico, el más usado y más conocido por los internautas. El procedimiento es la recepción de un correo electrónico donde simulan a la entidad o organismo que quieren

suplantar para obtener datos del usuario novel. Los datos son solicitados supuestamente por motivos de seguridad, mantenimiento de la entidad, mejorar su servicio, encuestas, confirmación de su identidad o cualquier excusa, para que usted facilite cualquier dato. El correo puede contener formularios, enlaces falsos, textos originales, imágenes oficiales, etc., todo para que visualmente sea idéntica al sitio web original. También aprovechan vulnerabilidades de navegadores y gestores de correos, todo con el único objetivo de que el usuario introduzca su información personal y sin saberlo lo envía directamente al estafador, para que luego pueda utilizarlos de forma fraudulenta: robo de su dinero, realizar compras, etc.

4.2.17. Samurai

Un *hacker* 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, está amparado por la primera enmienda estadounidense o cualquier otra razón de peso que legitime acciones semejantes. Los *samurais* desdeñan a los *crackers* y a todo tipo de vándalos electrónicos. En definitiva se puede decir que un *samurai* es un *cracker* que está amparado por la ley.

4.2.18. *Sneaker*

Es aquel individuo contratado por las propias empresas para romper los sistemas de seguridad de ellas con la intención por parte de las empresas de subsanar dichos errores y evitar por lo tanto posibles ataques dañinos.

4.2.19. *Spammer*

Son los responsables de los millones de correos basura no solicitados que saturan cada día los buzones electrónicos de todo el mundo. En la actualidad, casi el 70% de todos los correos electrónicos que circulan en el mundo son spam, una auténtica plaga que puede llegar a dificultar el uso del correo electrónico como herramienta útil de comunicación.

Los spams no son código dañino, pero sí molesto. Se basa en enviar repetidas veces un mismo correo electrónico a miles de direcciones. Algunas empresas lo utilizan en una equivocada política de marketing agresivo.

Los receptores pueden ser particulares o grupos de noticias, listas de distribución, etc. Siendo la solución para estas últimas el moderarlas, mientras los primeros tendrían que emplear programas anti-spam, que detectan el código identificativo y los filtran al llegar antes de ser bajados al buzón.

La Ley de Servicios de la Sociedad de la Información prohíbe el spam de modo que, siempre que

se envíe publicidad, el asunto del mensaje debe anunciarlo con la misma palabra "publicidad" seguida del lema del anuncio. El problema será cuando esta publicidad no llegue desde la Unión Europea, sino desde otros países donde no se controla.

4.2.20. *Uebercracker*

Variante de *cracker*. Son los *crackers* de sistemas que han ido más allá de los métodos de intrusión tradicionales. No se motiva normalmente para realizar actos violentos. Las víctimas se escogen deliberadamente. Es difícil de detectar, de parar, y casi imposible mantenerlo alejado de cualquier site.

4.2.21. Administrador o *root*

Individuo que se encarga del mantenimiento de un sistema informático y tiene el control total sobre el mismo. También se encarga de la seguridad.

4.3. Modo de actuación de un *hacker*[7][8]

Todos los sistemas son inseguros, puesto que están creados por humanos. Incluso sistemas como el de la NASA o el Pentágono tienen debilidades.

Una forma típica de obtener información es buscando usuarios inexpertos o cándidos, ya que en ocasiones puede resultar sencillo engañarles para que te revelen sus palabras de acceso (contraseñas). Esto es lo que se conoce como: ingeniería social, a la cual ya hemos hecho referencia en el punto anterior.

Realmente un ordenador no corre peligro mientras no lo conectemos a Internet ni instalemos nada a través de disquetes o CD's no comerciales. El problema surge cuando el ordenador se conecta a Internet y se nos asigna una IP para identificarnos en la Red. Una vez hecho esto, el ordenador pasará a ser un elemento más de la red de redes. Los usuarios demandamos servicios de la Red, cada vez, estos servicios son más y por eso es necesario diferenciarlos gracias a los puertos. Imaginaros un edificio de oficinas, éste tiene una puerta de entrada al edificio (que en nuestro caso sería la IP) y muchas oficinas que dan servicios (que en nuestro caso serian los puertos). Eso nos lleva a que la dirección completa de una oficina viene dada por la dirección postal y el

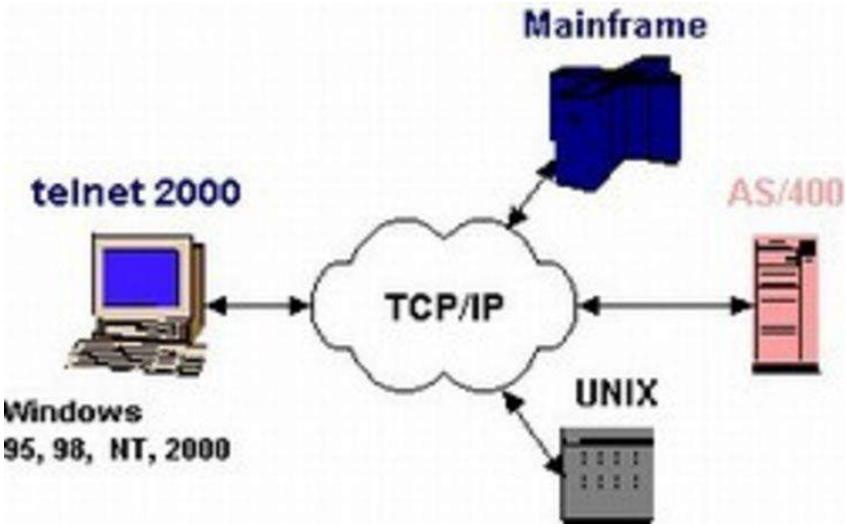
7 GIJÓN, Jesús. *Hackers, crackers y sus implicaciones sociales y mediáticas.* Valencia UPV. p. 24 - 26

8 DE MIGUEL, María del Rosario y Juan Vicente Oltra. *Deontología y aspectos legales de la informática: cuestiones éticas, jurídicas y técnicas básicas.* Valencia : Ed. UPV, 2007. p. 122 ISBN 978-84-8363-112-6

número de la oficina. En el caso de Internet viene dado por la dirección IP y por el número de puerto. Cuando solicitas un servicio de Internet, por ejemplo una página web, haces tu solicitud de la página mediante un puerto de tu ordenador a un puerto del servidor web. Existen más de 65000 de puertos diferentes, usados para las conexiones de red, y son éstos los culpables de muchas de las intromisiones de los *hackers*/*crackers*. Es por esto que los puertos deben permanecer cerrados. Por ello, si utilizamos un servidor nada más que para ofrecer servicio de correo, es un error dejar abiertos los otros puertos. Resumiendo, podemos afirmar (y lo volveremos a repasar en el tema de *Hacking ético*) que todo buen ataque *hacker* debe constar de los siguientes pasos[9]:

1. Introducirse en el sistema que tengamos como objetivo. (Telnet, SSH y FTP)

El *hacker* debe identificar el objetivo: saber a quién atacar, es decir, hacerse con la dirección IP de la máquina que se asaltará. A la hora de elegir un objetivo, un *hacker* tiene dos alternativas: o decidirse por un sistema concreto, o encontrar uno al azar. En muchas situaciones las víctimas son elegidas de forma totalmente aleatoria.

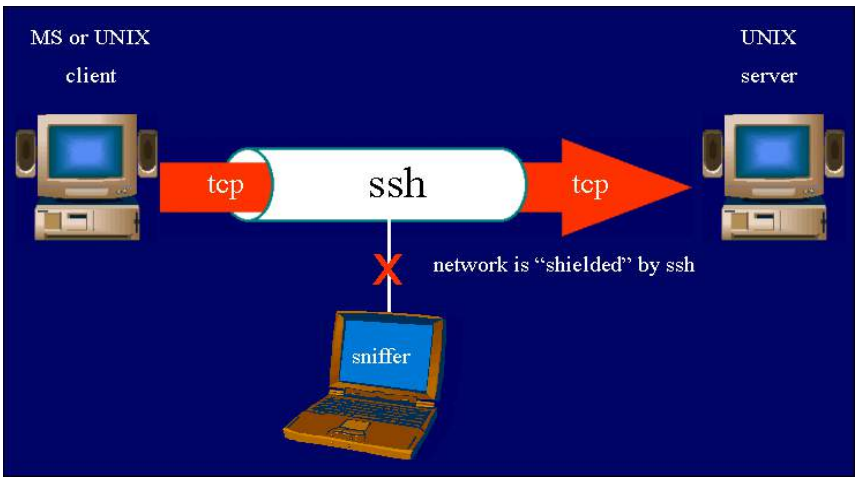


Telnet

Una vez que sabe a quién atacar, es decir, conoce cuál es su dirección IP, debe recopilar la cantidad máxima de información sobre el blanco: sistema operativo, servicios a la escucha y versión de los mismos, topología de red, información sobre la organización y sus usuarios, etc. En esta fase utilizará herramientas de exploración de puertos, como netcat, nmap o cheops, que permiten detectar qué puertos están abiertos en una máquina, o lo que es lo mismo, permiten saber qué servicios están activos. Llegado a este punto, el *hacker* cuenta en su poder con una carpeta rebosante de datos sobre su objetivo: topología de la red, tipo y versión de sistema

9 Estos conceptos los vemos más adelante, en el apartado 7. *Hacking* ético, resumidamente.

operativo instalado en los servidores y cortafuegos, servicios de Internet en ejecución y su versión, información de algunos usuarios, información de la organización, etc. Es el momento de estudiarla y analizarla concienzudamente con el fin de identificar vulnerabilidades, puntos de acceso y puertas de escape. A partir de ahí, comienza el ataque.

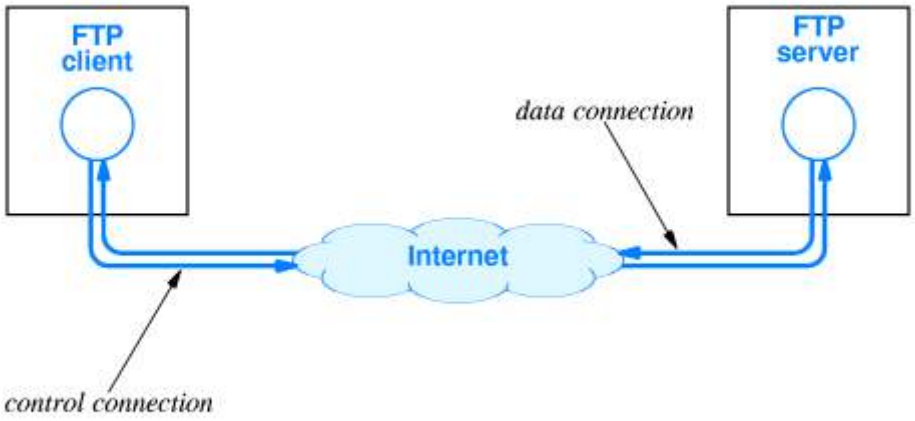


Secure Shell (SSH)

Para poder hacer uso de servicios como Telnet, ssh o ftp y entrar en otros equipos, hay que introducir un nombre de usuario (login) y una contraseña (password).

En los servidores suelen correr sistemas operativos multiusuario como Windows NT, Unix o algún derivado suyo: AIX, Linux, donde cada usuario tiene un espacio de trabajo y unos privilegios determinados, como cambiar la configuración de éste.

Para entrar en los equipos, los *hackers* intentarán conseguir el fichero passwd. Este fichero guarda el login (nombre de identificación) de cada usuario en el sistema, así como su password (contraseña de acceso) encriptado. Para ello, exploran los puertos buscando las posibles entradas, y acceden a ellos para conocer la versión del protocolo utilizado, en busca de emplear los bugs (fallo de programación) conocidos de éste que faciliten la entrada, por lo tanto usarán los fallos de seguridad de las aplicaciones que corren en la máquina, como servidores de páginas Web, puertos de red mal configurados como el FTP, SMTP, HTTP... que son las llamadas backdoors o puertas traseras.



File Transfer Protocol (FTP)

Una vez obtenido el fichero passwd, buscarán mediante un "*cazaclaves*" o *crackeador* (más adelante hablaremos de ellos) el login y el password de algún usuario. Dada la facilidad de entrar en el sistema que suponía el uso del fichero passwd, se elaboró el método de claves shadow, que hace invisibles los passwords encriptados para los usuarios; sin embargo, no es una protección segura, y cualquier *hacker* con ciertos conocimientos y algo de paciencia será capaz de romperla.

Otra forma de obtener información es buscando usuarios cándidos a los que engañar o convencer para que te revelen sus contraseñas. Los medios más comunes son el IRC y el correo falsificado o de un servidor gratuito (hotmail, latinmail). Haciéndonos pasar por el administrador, podemos informar al usuario de que debemos conocer su password para una reestructuración del sistema. Es la llamada “Ingeniería Social”.Otro medio es buscar sistemas con administradores con poca experiencia o excesivamente confiados, que no quiten el permiso de escritura a ficheros que solo debían ser suyos, o no eliminaran las cuentas con login y password por defecto, o el usuario típico para ftp, “anonymous” cuya contraseña es el login o guest, invitado, convidat...

2. Una vez conseguido el acceso, obtener privilegios de root (superusuario).

Lo ideal para entrar en un sistema es hacerlo como administrador, lo cual proporciona suficientes privilegios como para alterar cualquier cosa sin ningún problema.

Conseguidos el nombre y contraseña de un usuario, el *hacker* ya puede entrar al ordenador, y ahora su objetivo será pasar de ser un simple usuario a alcanzar los privilegios del root. El root o

superusuario dispone de poder absoluto dentro del sistema, pudiendo hacer cosas tan peligrosas como instalar cualquier tipo de programas, leer el correo electrónico de los usuarios o alterar la configuración del sistema. Para lograrlo, el *hacker* utiliza los exploits, programas que se aprovechan de los agujeros de seguridad de los propios sistemas operativos o de las aplicaciones que corren sobre él.

Si la versión del sistema operativo que ha sido atacado es antigua y no está parcheada, puede haber muchas formas de obtener privilegios de root.

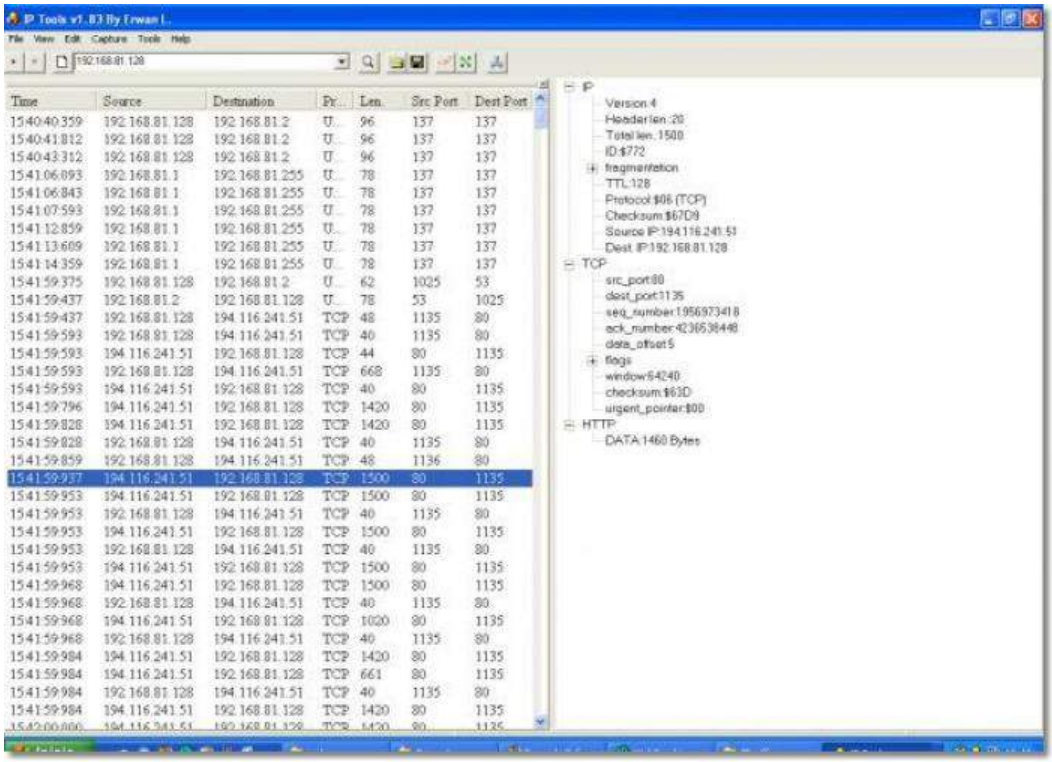
3. Borrar las huellas.

Si ya se es root, probablemente el *hacker* deje un mensaje de bienvenida, para que el administrador sea consciente de los errores de seguridad de su sistema. Éste es el momento cumbre del *hacker*; ha conseguido su objetivo, demostrar que es superior al administrador. Debido a que las figuras del *hacker*/*cracker* se suelen confundir, llega el momento de borrar las huellas dejadas por el ataque en los registros logs.

También con el objetivo de crear confusión pueden dejar pistas falsas: cuando van a obtener el root de un ordenador no penetran directamente en él, sino que van dando saltos de un ordenador a otro con lo que su rastro se hace más difícil de seguir.

4. Poner un sniffer para conseguir logins de otras personas.

Un *sniffer* es un programa que se encarga de recoger toda la información que circula a través de una red mediante una técnica que es poner la tarjeta de red en un modo llamado "promiscuo", para su posterior tratamiento. Los ordenadores conectados a una red utilizan un canal de comunicación compartido esto significa que los ordenadores pueden recibir información proveniente de otras maquinas aunque de dicha información no sea el destinatario. Los *hackers* instalarán estos programas para capturar de forma automática las contraseñas enviadas en claro (sin encriptar) y nombres de usuario de la red. Obteniendo continuamente contraseñas y logins de usuarios, consiguen tener acceso siempre que lo deseen al sistema atacado, e incluso a otros sistemas ya que muchos usuarios utilizan las mismas claves por motivos de comodidad. Una navegación lenta en Internet nos puede indicar que hay un *sniffer* en línea.



Ejemplo de IP Sniffer

4.4. Recomendaciones ante posibles ataques[10]

Presentamos a continuación 13 recomendaciones para estar a salvo de intromisiones ilegítimas por parte de *hackers*:

• No mantener información comprometedora y no necesaria en un ordenador, si ésta no va a ser utilizada nunca y en cambio a un *hacker* le puede ser de gran utilidad.

• Al instalar software nuevo, asegurarse de que si posee un demonio, servicio o TSRs, éste este en su última versión, correctamente actualizado. Varios fallos de seguridad se producen en el demonio de gestión de servicios web (httpd) si éste no esta actualizado, siendo así una puerta de entrada para posibles intrusos.

• Cerrar los puertos no utilizados (systat, netstat, finger, rlogin, etc.)

• Mantener el telnet y ftp solamente en caso necesario.

• Eliminar/bloquear las cuentas que el sistema tiene por defecto (guest, system,…), o si son

10 GIJÓN, Jesús. *Hackers, crackers y sus implicaciones sociales y mediáticas.* Valencia UPV. p. 26- 27

necesarias eliminarles privilegios que puedan afectar a la vulnerabilidad del sistema. Así como asegurarse de que el fichero de contraseñas está protegido frente a accesos externos.

• Enviar los logs a otros servidores y consultarlos periódicamente para poder detectar un ataque con prontitud.

• Informarse de los bugs que aparecen constantemente para parchearlos. Hay listas de correo (también usadas por los *hackers*, naturalmente, pero con otros propósitos) que nos mantienen constantemente informados de los agujeros encontrados en los distintos sistemas.

• Visitar páginas de *hackers*, ya que en ellas pueden encontrar utilidades y textos importantes escritos por otros *hackers*, muchos de ellos también administradores.

• Obtener software de recorrido de puertos, con el objetivo de realizar un “scan” de los puertos para saber de la existencia de demonios o servicios no permitidos como es el caso de los nukenabber que son programas que controlan todos nuestros puertos y su estado y son capaces de detectar una intrusión o Nuke en cualquiera de los puertos seleccionados.

• Tener un adecuado y actualizado software Criptográfico. Emplear siempre que se pueda el protocolo SSL en sus comunicaciones, y si fuese posible usar software criptográfico que no funcione con claves de 40 bits, de fácil desencriptación para los *hackers*. Desgraciadamente, todas las versiones internacionales del software producido en Estados Unidos llevan este tipo de claves, debido a las leyes sobre exportación de material criptográfico que posee este país.

• Contra ataques de diccionario para descubrir passwords, hay sistemas operativos que permiten la no ejecución de una ventana terminal de forma remota, impidiendo así que el *hacker* ejecute el terminal, sólo pudiéndose ejecutar éste desde un acceso físico al ordenador. Este punto es de gran importancia para ordenadores conectados a Internet.

• Cambiar periódicamente de contraseñas y al hacerlo utilizar contraseñas seguras, usando tanto números como letras como caracteres permitidos.

• Realizar backups de forma continua de los datos importantes y críticos, para así si por alguna casualidad un *cracker* vulnerase su sistema y borrase sus archivos, poder recuperarlos.

4.5. El concepto de *hacktivismo*[11]

La palabra *hacktivismo* proviene de *hacking* y activismo[12], la utilización de las técnicas *hackers* para una causa política, generalmente promoviendo políticas tales como la libertad de expresión, derechos humanos y ética de la información.

El término *hacktivismo* lo impuso el renombrado grupo de *hackers* "Cult of the dead cow" en 1996 tomando como base las líneas de dos Artículos Internacionales. El Artículo 19 de la Declaración Universal de los Derechos Humanos: "Todo individuo tiene derecho a la libertad de opinión y expresión; este derecho incluye la libertad de sostener opiniones sin interferencia y a buscar, recibir e impartir información e ideas a través de cualquier medio y sin consideración de fronteras", y el Artículo 19 del Convenio Internacional sobre los Derechos Civiles y Políticos: "Todo individuo tendrá el derecho de sostener opiniones sin interferencia.

Los orígenes del *hacktivismo* fueron bastante funestos. Los *hackers* de comienzos de los 90 criticaron el *hacktivismo* por su uso dañino de la Red y sus técnicas primitivas, "sois peores que *script-kiddies*, tecnológicamente patéticos" dijeron los *hackers*.

Desde el activismo tampoco fueron vistos con buenos ojos, existía por aquel entonces un fuerte movimiento primitivista y neoludita (quienes se oponen a quienes tejemos digitalmente redes de comunicación con ayuda de un ordenador) que entendía la tecnología como un instrumento del poder, totalmente contrario a la lucha activista.

Un ejemplo de *hacktivismo* español a favor del derecho al acceso a la cultura lo inauguró la campaña de comunicación CompartirEsBueno.Net.

---

11 GIJÓN, Jesús. *Hackers, crackers y sus implicaciones sociales y mediáticas.* Valencia UPV. p. 28 - 33

12 Según la wikipedia: El concepto de **activismo** se puede generalizar como la acción o la actividad sostenida con intención de efectuar un cambio de índole social o política, usualmente dirigida a favor de una postura particular dentro de una disputa o controversia.

Aún así, Ricardo Domínguez y otros *hacktivistas* cercanos a la Desobediencia Civil Electrónica siguieron trabajando en herramientas sencillas de usar, continuando con su idea de acercar herramientas de interacción tecno-políticas a la gente corriente.

El ejemplo más claro de la aplicación del *hacktivismo* en sus inicios fueron las manifestaciones en la Red o *netstrikes*[13]. Con un programa muy sencillo, utilizable desde cualquier ordenador personal, un *hacktivista* realiza continuas peticiones a una misma página web intentando colapsarla (denegación de servicio). Si este ataque se combina desde diferentes fuentes, se puede perjudicar seriamente la accesibilidad de un sitio web. El fundamento es similar al de congregar en la puerta de un banco a 200.000 personas para que traten de ser atendidas en la ventanilla de ese banco. Realmente no está ocurriendo nada ilícito, pero a efectos prácticos el resultado es que cualquier cliente "legítimo" de ese banco no podrá acceder a la ventanilla durante ese día, porque está saturada intentando atender a las miles de peticiones extra que se han generado con el ataque.

13 Según la wikipedia, un **netstrike** o **sentada virtual** es una forma pacífica y ordenada de protesta social que se lleva a cabo en la red, utilizando un ordenador y una conexión a Internet. Consiste en la interacción consensuada de multitud de personas desde diferentes lugares y distintos horarios sobre un sitio web, con objetivo de ralentizar su servicio, llegando en ocasiones a saturar la web establecida como objetivo. Esto se produce porque el ancho de banda contratado por el sitio web es rebasado debido a la carga de visitantes, con lo que deja de dar el servicio habitual, quedando inutilizado.

En 1998, Ricardo Domínguez y otros miembros de la *Critical Art Ensemble*[14] decidieron crear una herramienta de activismo, que recargaba varias veces un sitio web. Unas 80.000 personas participaron en una manifestación virtual contra el servidor que alojaba la página web del entonces presidente de México durante aquellas fechas, consiguiendo que dejara de dar servicio durante varios días.

El mayor *netstrike* registrado en España fue organizado por un grupo de *hacktivistas* el 22 de febrero de 2006 sobre el sitio web de la Sociedad General de Autores y Editores (SGAE), tuvo lugar entre las 20:00 y las 00:00 y contó con una participación aproximada de 6.500 personas. El *netstrike* consistía en descargarse el programa "acomodador-SGAE.zip" el cual se pondrá a recargar repetidas veces la página web de la SGAE con objetivo de ralentizarla. El servidor web fue incapaz de soportar tal avalancha de transferencia de datos, quedando por tanto inutilizado, esto sucedió hasta en al menos 12 ocasiones.

Con el uso del Software Libre como uno de sus pilares fundamentales y en paralelo con la actividad *hacktivista* desarrollada sobre todo dentro de los países anglófonos, surge el movimiento de *hacklabs*[15] a finales de los años 90 en Italia. En el año 1998 se convocó en Florencia el primer *hackmeeting* italiano, pretendiendo reunir en él a *hackers*, *hacktivistas* y *artivistas* (activistas del arte) para compartir impresiones, realizar talleres u organizar acciones conjuntas. Dado el éxito de la convocatoria, se decidió repetirla de forma anual y desde esa fecha se han venido produciendo *hackmeetings* cada año en diferentes partes de la geografía italiana. Gracias a la cohesión y organización surgida de cada uno de estos encuentros, los *hacktivistas* italianos se han ido organizando en *hacklabs*, laboratorios de *hackers*, o más bien de *hacktivistas*, con un marcado carácter técnico y político, en continua sinergia.

Debido a la intensa interacción entre el movimiento telemático antagonista de Italia y de España, el fenómeno del *hackmeeting* se exporta a Barcelona en el año 2000. El Centro Social Ocupado Autogestionado Les Naus acoge la primera edición de un encuentro que desde entonces no ha hecho sino crecer en cuanto al número de sus asistentes y de actividades organizadas durante el mismo. Los *hackmeetings* han servido también para ir generando, en las ciudades donde ha tenido lugar, grupos locales más o menos fuertes que han derivado en la creación de *hacklabs*.

14 Según la wikipedia, **Critical Art Ensemble** (CAE) es un galardonado colectiva de cinco medios tácticos profesionales de diversas especialidades como informática gráfica y diseño web, cine / vídeo, la fotografía, el arte de texto, libros de arte, y el rendimiento. Para CAE, los medios tácticos es la situación, lo efímero, y la auto-terminación. Se fomenta el uso de cualquier medio de comunicación que contratar a un determinado contexto socio-político con el fin de crear intervenciones molecular y los choques semiótica, que en conjunto podría disminuir la intensidad creciente de la cultura autoritaria.

15 Según la wikipedia, ***Hacklab*** o laboratorio hacker es un espacio físico donde se reúne un grupo de personas para investigar, debatir y difundir temas relacionados con Internet, las nuevas tecnologías y los derechos civiles en esos ámbitos, desde un punto de vista social.

Los *hacklabs* tienen una vertiente muy social y eso se manifiesta en forma de proyectos. Con el software libre como bandera, los *hacklabs* organizan cursillos periódicos de formación sobre temas meramente técnicos como navegar por Internet, escribir correos electrónicos o instalar GNU/Linux en un ordenador o talleres con una vocación más activista como la creación de redes ciudadanas inalámbricas al margen de Internet, talleres de criptografía básica utilizando GnuPG, una herramienta libre de cifrado (como disponemos del código fuente de esta herramienta, ningún gobierno podrá introducir software espía o puertas traseras en ella, como ocurre con software privativo de Microsoft u otros fabricantes) o el uso de sistemas de navegación para evitar la censura de determinadas páginas web. Además pretenden realizar una labor constante de concienciación social en temas relacionados con las nuevas tecnologías, entre los que destacan la lucha contra las Patentes de Software, que golpean en la línea de flotación del Software Libre, o la reivindicación de una socialización de la cultura y un cambio del modelo de explotación de la misma, fomentando licencias libres para la documentación o el arte como el movimiento Copyleft o las licencias "Creative Commons", un traslado de la idea de las tierras comunales (commons) al plano creativo.

A grandes rasgos podemos distinguir tres áreas donde los *hacktivistas* actúan: la contra-información, los *hacklabs* y las redes wireless:

1. La contra-información: Bajo esta denominación se agrupan un conjunto de prácticas orientadas a “sacar a la luz informaciones obviadas o manipuladas por los medios convencionales”. Los colectivos que realizan estas actividades reconocen que los medios de comunicación se han convertido en espacio privilegiado de la política. Pero, además, denuncian que solo unos pocos grupos mediáticos pueden informar a nivel global y que este fenómeno vuelve homogéneos los contenidos distribuidos, uniforma la visión de mundo proyectada y anula las perspectivas alternativas.

Los proyectos que se llevan a cabo en esta materia incluyen la producción de textos impresos, programas radiales libres, recursos audiovisuales y servidores telemáticos.

Como ejemplo más importante en España tenemos a la web sindominio.net que nació como iniciativa para combatir contra las empresas que proporcionan acceso web, correo, listas de distribución, publicidad,…frente a esto se crea un espacio libre en Internet, donde no hubiese empresarios ni clientes, donde las posibilidades de utilización de Internet como medio no estuviesen limitadas a lo que pagas, dónde toda la gente participase en la toma de decisiones de una forma horizontal.

Existen muchos colectivos vinculados a sindominio, entre otros destacamos a la Asociación de Alumnos de la UNED o la Asociación de Seguimiento y Apoyo a Presos/as de Aragón.

2. Los *hacklabs*: los *hacklabs* son lugares físicos, organizados, autónomos y autogestionados. Su virtud es la de permitir la reunión de diversos actores y la generación de un colectivo donde se intercambian conocimientos y habilidades, se crea tecnología y se experimenta con ella. Este ejercicio de desarrollo tecnológico tiene una dimensión sociopolítica: está orientada a concienciar sobre uso de software libre, a reflexionar sobre las implicaciones sociales y políticas de la tecnología, a favorecer el acceso a Internet y a socializar la tecnología.

3. Las redes wireless: Las redes inalámbricas son un conjunto de equipos conectados entre sí por un medio que les permite compartir datos o dispositivos. Los enlaces no se hacen mediante cables o puntos fijos de conexión, sino a través del aire utilizando infrarrojos, láser o radio. Las redes inalámbricas son útiles para dar conexión en sitios donde el cableado resulta inconveniente, por ejemplo, lugares aislados, muy concurridos o protegidos por su carácter histórico. También se emplean para asegurar la conectividad a personas y colectivos en constante movimiento, o simplemente para no tener que instalar gran cantidad de cables en hogares u oficinas.

Los *hacktivistas* promueven la creación de lo que ellos llaman redes libres siendo el instrumento para conseguirlas la propia gente, estas redes libres inalámbricas son interesantes para el *hacktivismo* debido a:

• *Emplean los mismos protocolos de comunicación que se utilizan en Internet*. Esto hace que todos los servicios que funcionan en la Red de redes puedan instalarse y ejecutarse en una red inalámbrica, y que sea más fácil experimentar con ellos.

• *Buena parte del software empleado para montar las redes inalámbricas son aplicaciones libres.* Como ya se ha comentado en otros apartados, el software libre es apoyado y desarrollado por muchas experiencias de *hacktivismo*.

• *Montar y gestionar una red inalámbrica puede entenderse como un experimento* sociopolítico que intenta constituir nuevas formas de relación social y de gestión económica. En estas experiencias se juegan los principios de libertad, cooperación y autonomía que aprecian muchas comunidades *hacktivistas*.

4.6. El concepto de guerra informática o *ciberguerra*[16]

Según la wikipedia, Guerra informática, guerra digital o ciberguerra, se refiere al desplazamiento de un conflicto, en principio de carácter bélico, que toma el ciberespacio y las tecnologías de la información como escenario principal, en lugar de los campos de batalla convencionales.

También se podría definir como el conjunto de acciones que se realizan para producir alteraciones en la información y los sistemas del enemigo, a la vez que se protege la información y los sistemas del atacante. Los ataques informáticos no son considerados como ataques armados.La ciberguerra es la sucesora de la llamada guerra electrónica, por lo tanto vamos a definir este concepto antes de adentrarnos en el concepto de ciberguerra.

La guerra electrónica es aquella utiliza medios electrónicos para neutralizar los sistemas de mando y control enemigos, actuando sobre sus sistemas de comunicaciones y electrónicos, mientras que garantiza la integridad de sus propios sistemas. Este tipo de acciones existe desde que los militares comenzaron a utilizar el telégrafo, en 1850. Los equipos específicos de guerra electrónica comenzaron a surgir de manera eficiente y coordinada durante la Segunda Guerra Mundial, y constituyen, hoy, un componente común del arsenal de cualquier ejército.

El concepto de ciberguerra, si bien a veces es conocido de manera diferente con relación al concepto de guerra electrónica, puede ser considerado como parte íntegra de dicho concepto. Por lo tanto, la ciberguerra incluye la utilización de todas las "herramientas" disponibles al nivel de electrónica y de informática para derrumbar los sistemas electrónicos y de comunicaciones enemigos y mantener nuestros propios sistemas operacionales.

Los objetivos comunes de la ciberguerra son normalmente los ordenadores del enemigo, ya sean estos individuales o conectados en red. Tratar de penetrar en ellos y hacerse con el mando de programas de control de operaciones con el objetivo de usarlos para un beneficio propio. Los ordenadores o redes objetivo preferidos por los ciberguerreros suelen ser:

• Redes con funciones de distribución eléctrica.

• Redes con funciones de distribución de agua potable. El objetivo tanto de la luz y el agua es crear un gran malestar en la población además de desabastecer e ir mermando a la población.

16 GIJÓN, Jesús. *Hackers, crackers y sus implicaciones sociales y mediáticas.* Valencia UPV. p. 35 - 38

• Redes con funciones de desvío de carriles de tren.

• Redes con funciones de organizar el tráfico aéreo. En el caso de trenes y aviones el objetivo es claramente el de causar graves daños ya sea produciendo accidentes o retrasando sus trayectos.

• Redes con funciones de información de emergencia como pueden ser servicios de socorro inmediato, policía y bomberos.

• Redes bancarias, habilitando o deshabilitando al antojo cuentas bancarias, por ejemplo, cerrar las cuentas de todos los clientes de un banco de una determinada ciudad con el objetivo de sembrar el caos.

• Redes de comunicaciones como la televisión y la radio con el objetivo de difundir informaciones falsas.

• Enlaces de sistemas satélite de proveedores de teléfono, televisión, previsión del tiempo metereológico o los ahora tan importantes sistemas GPS.

• Ordenadores y redes de ministerios como el de defensa, interior o justicia, así como el banco central. En este apartado también podremos incluir sistemas de ordenación, tratamiento y recuperación de datos.

• Ataques que desfiguran páginas web, o de denegación de servicio (DNS). Esto normalmente se combate rápidamente y hace poco daño. Es conocido como vandalismo web. No es llevado a cabo por organismos militares, sino por simpatizantes del país, que atacan a webs enemigas.

Este sería el caso a mucha menor escala del leve conflicto que España tuvo con Marruecos debido a la intromisión de militares marroquíes en la isla Perejil cuya soberanía española discute Marruecos. Varios *hackers* marroquíes *hackearon* páginas españolas a los que *hackers* españoles reaccionaron *hackeando* la página web del Ministerio de Turismo Marroquí.

Pueden existir otros objetivos que serán aportados por los servicios de inteligencia estudiando cada caso en particular, por militares o agentes espías infiltrados en el país.
Como vemos las posibilidades son inmensas, ya que cada vez más, las actividades comerciales, los servicios y las personas dependen de los ordenadores y a su vez en los últimos tiempos de

Internet. Esto hace que los gobiernos se empiecen a plantear la creación de nuevos organismos encargados de la defensa cibernética del país, incluso hay muchos países que invierten mucho dinero en ciberejercitos, reclutando a los mejores *hackers* del mundo, como es el caso de EEUU.

Estos nos hace plantearnos cuestiones como si un ordenador es un arma, cuya respuesta es que en algunos casos si, ya que son capaces de disparar misiles o dejar a un hospital sin luz durante días, aunque un ordenador por si solo no tiene ningún peligro. Otra cuestión que nos planteamos es si los *hackers* actuales que han sido contratados por los gobiernos son militares. Esta pregunta es más difícil de responder, diría que no es un militar ya que no combate en el campo de guerra directamente, pero también diría que si en tanto que una acción suya puede ser considerada como una maniobra militar capaz da causar víctimas.

La ciberguerra no surge de *hackers* adolescentes. Entidades estatales y no estatales están formando expertos que hagan realidad las ciberguerras. Silenciosamente buscan maneras de incapacitar a naciones adversarias, infiltrando sus redes de computación.

Además, están creando equipos de especialistas para proteger a sus propias redes de la misma amenaza. Así nace una nueva generación de soldados: los guerreros cibernéticos.
Y Asia está emergiendo como su territorio de prueba, porque no es necesario ser rico ni estar bien armado para convertirse en una superpotencia del ciberespacio. Por eso no es llamativo que las principales potencias en materia cibernética, aparte de EEUU, son China, Corea del Sur y Corea del Norte.

El conflicto bélico en torno a la provincia serbia de Kosovo que tuvo lugar en 1999 es citado a menudo como la primera guerra peleada en forma paralela a través de Internet. Actores gubernamentales y no gubernamentales usaron la Red para diseminar información, difundir propaganda, demonizar a sus oponentes y solicitar apoyo para sus posiciones. Personas de todo el mundo usaron a Internet para debatir sobre el tema e intercambiar texto, imágenes y videoclips que no estaban disponibles a través de otros medios.

Los *hackers* hicieron oír sus opiniones tanto sobre la agresión de la OTAN como sobre la de Yugoslavia, interfiriendo servicios en computadoras gubernamentales y bloqueando sus sitios.

Manifestantes virtuales de ambos lados usaron "bombas de e-mail" (envío masivo de mensajes) contra sitios gubernamentales. Varios sitios fueron *hackeados* durante el conflicto de Kosovo. Según Fox News, El Boston Globe informó que un grupo estadounidense de *hackers* llamado

Team Spl0it ingresó a sitios gubernamentales serbios y puso carteles tales como "Díganle a su gobierno que detenga la guerra".

Otro caso sonado fue la ciberguerra emprendida entre EEUU y China. La causa del comienzo de esta ciberguerra fue la colisión el 1 de abril del 2001 entre un avión espía norteamericano y un caza chino que provocó la muerte del piloto oriental y la retención de la tripulación estadounidense durante once días.

Ciberguerra EEUU

Los ataques en el ciberespacio no se hicieron esperar, los grupos americanos de *hackers* atacaban a las páginas webs chinas, dejando la inscripción "We will hate China forever and we will *hack* its sites". Pero los *hackers* del país oriental no se quedaron atrás en ningún momento, fueron varios los ataques que lanzaron a páginas webs americanas: el día 4 de mayo, como ya informábamos, a la web de la Casa Blanca; el día 6, atacaban varías páginas oficiales de la alcaldía de Jacksonville (Florida) dejando mensajes antiestadounidenses. Durante estos últimos días, fue tal la alarma que tanto el FBI como las empresas tuvieron que tomar medidas preventivas para proteger los servidores oficiales y corporativos.

En general, han sido multitud las páginas webs que se han visto bajo los ataques de los piratas de ambos países: desde instituciones científicas, militares, gubernamentales, bancos, centros médicos, universidades, hospitales, etc... El FBI además vinculaba a China con el descubrimiento de un gusano de correo electrónico llamado Lion que enviaba contraseñas robadas de los equipos infectados a e-mails chinos.

Esta batalla política incluso ha llegado ha traspasar las fronteras chinas para llegar a Corea donde hace unos días se acusaba a un empleado de la Base aérea americana de Osan por *hackear* 113

páginas webs coreanas. El *hacker*, de 24 años y que podría formar parte del grupo WHP, utilizaba su PC oficial para realizar asaltos de los que luego alardeaba. En el momento de su detención, estaba realizando uno de los ataques.

Un ejemplo de esta ciberguerra es el ataque realizado por *hackers* chinos sobre la web iplexmarin.com, un foro de marines artistas en California. La web apareció con banderas chinas, frases políticas en inglés y en chino, el himno de fondo de China y con fotografías del piloto chino fallecido.

El comentario en inglés decía: “As we are Chinese, we love our motherland and its people deeply. We are so indignant about the intrusion from the imperialism. The only thing we could say is that, when we are needed, we are ready to devote anything to our motherland, even including our lives".

4.7. El concepto de *ciberterrorismo*[17]

El ciberterrorismo o terrorismo electrónico es el uso de medios de tecnologías de información, comunicación, informática, electrónica o similar con el propósito de generar terror o miedo generalizado en una población, clase dirigente o gobierno, causando con ello una violencia a la libre voluntad de las personas. Los fines pueden ser económicos, políticos o religiosos principalmente.

El término ha sido muy criticado, siendo considerado como un método de satanización para aquellas personas descontentas del orden establecido y que actúan en contra de éste es Internet, gracias a la libertad de ésta. Con el auge de las nuevas tecnologías y el nacimiento de los *hackers*, los gobiernos de países como EEUU han mostrado su preocupación con la posibilidad de que algún grupo terrorista pueda cometer atentados o actos de sabotaje empleando estas nuevas tecnologías como podrían ser dejar a los hospitales sin corriente eléctrica o manipular las coordenadas de los vuelos causando accidentes aéreos, surgirán los nuevos terroristas del siglo XXI: los ciberterroristas.

En los años 80, Barry Collin, un investigador senior del *Institute for Security and Intelligence* en California acuñó el término *cyberterrorism* para referirse a "la convergencia del ciberespacio con el terrorismo". Mark Pollit, un agente del FBI que se dedicó a estudiar el tema, desarrolló la siguiente

17 GIJÓN, Jesús. *Hackers, crackers y sus implicaciones sociales y mediáticas.* Valencia UPV. p. 39 - 40

definición operativa: "*El ciberterrorismo es el ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos que puedan resultar en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos".*

Para particularizar el caso a España vamos a desarrollar el *ciberterrorismo* utilizado por la organización separatista vasca ETA. Ante el hecho del uso de las altas tecnologías como Internet para darse publicidad, las páginas Web que apoyaban los pensamientos de la organización ETA, tras el asesinato del concejal de Ermua Miguel Ángel Blanco, sufrieron diversos ataques *hacker*. Un mes después del asesinato de Garrido se produjo un bombardeo de mensajes que intentó saturar al proveedor de servicios de Internet IGC (Institute for Global Communication) de San Francisco, en Estados Unidos. El objetivo fue intentar desalojar al Euskal Herria Journal, una controvertida publicación pro-ETA editada por un grupo de simpatizantes desde Nueva York. Los atacantes alegaban que IGC "fomentaba el terrorismo".

Como resultado de la acción, el servidor de e-mail de IGC se atascó. Muchos usuarios de IGC quedaron sin poder recibir su correo, y su línea telefónica de ayuda colapsó ante las llamadas de clientes enojados. Los atacantes también mandaron "correo basura" a los clientes y trabajadores de IGC, y colgaron sus páginas Web a base de órdenes de compra con números de tarjeta de crédito erróneos. Luego amenazaron con repetir estas acciones contra todos los que usaran los servicios de IGC. Para detener el ataque, IGC bloqueó el acceso de todos los servidores atacantes, medida efectiva pero imposible de sostener en el tiempo. IGC cerró el sitio del Euskal Herria Journal el 18 de Julio de 1997.

Un caso más reciente de *hacktivismo* anti-etarra se produjo el 23 de marzo de 2001, cuando piratas cibernéticos bloquearon la página principal del periódico vasco GARA (www.gara.net) donde la ETA publica con frecuencia sus pronunciamientos políticos o asume la responsabilidad por ataques perpetrados. Los piratas cibernéticos insertaron en el sitio el siguiente mensaje: "Esta web ha sido *hackeada* en recordatorio a las víctimas de ETA y sus familiares. Basta Ya. No somos *hackers*, somos españoles indignados".

Pero la banda terrorista ETA también cuenta entre sus filas con *hackers* que apoyan sus ideologías. Según un artículo publicado en el diario argentino La Nación, algunos *hackers* de ETA decidieron efectuar un "contraataque virtual". Con tal objetivo, se dedicaron a rastrear el origen de miles de mensajes que le reclamaban cesar con la violencia, y con esos datos en su poder, bloquearon las páginas de algunos de los manifestantes virtuales.

El caso más notorio de *hacktivismo* pro etarra tuvo lugar en abril del 2000, cuando un grupo de activistas modificaron la página oficial del museo Guggenheim. Durante varias horas cambiaron el aspecto del sitio del museo más emblemático de Bilbao y lo llenaron con slogans independentistas y fotos de miembros encarcelados de la ETA. Las pancartas, en inglés y francés, calificaban como "opresor" al gobierno español.

4.8. Los virus informáticos

Actualmente la informática va unida a las comunicaciones. Este es un campo de actuación perfecto para los creadores de virus informáticos. Se tiende a favorecer la interconexión de ordenadores por vía física o lógica, y esto a su vez convierte el medio en el más propicio para la proliferación de virus. La palabra "Virus" es realmente un acrónimo de: Vital Information Resources Under Siege (Recursos de Información Vital Bajo Acoso)[18].

Ante esta inminente amenaza, navegar sin la debida protección por Internet es un riesgo que puede salir bastante costoso y en el que se exponen los ordenadores, la información almacenada en éstos y los datos que se comparte a través de las redes. La lucha por combatirlos es cada vez más fuerte y los desarrolladores de programas de seguridad realizan actualizaciones o parches para tapar los agujeros por donde ya han entrado virus.

Hay un viejo dicho que dice: "Que no seas un paranoico no significa que no haya alguien que vaya a por ti". Este lema podría aplicarse claramente gracias a los escritores de virus. Y es por ello que un poco de paranoia vendría bien para empezar a protegernos de los virus. En el mundo de la informática, así como en el mundo biológico, una buena higiene es primordial para prevenirnos de infecciones. Y es mucho más sencillo prevenirnos de los virus que actuar reactivamente cuando ya estamos infectados. Hay una serie de puntos elementales que debemos cuidar y entender para atajar la problemática de la infección por virus informático:

- La versión del Sistema Operativo que estamos usando.
- Si tenemos o no instalados en nuestro ordenador programas de seguridad.
- Cuántas personas utilizan el ordenador.
- ¿A menudo visitamos muchas páginas web diferentes?
- ¿Visitamos páginas web que cambian la configuración de nuestro ordenador? De ser

18 DE MIGUEL, María del Rosario y Juan Vicente Oltra. *Deontología y aspectos legales de la informática: cuestiones éticas, jurídicas y técnicas básicas.* Valencia : Ed. UPV, 2007. p. 122 - 123 ISBN 978-84-8363-112-6

así ¿nos avisa nuestro propio sistema de esos cambios que van a realizarse?

- ¿Solemos leer y abrir e-mails de remitentes que no conocemos?
- ¿Entramos en URL's que vienen en estos e-mails de desconocidos?

Todos estos factores influyen directamente en la medida en que somos propensos a ser infectados por un virus informático.

¿Os suena? Éste era el aviso que mostraba *Blaster*.

Finalmente, es importante señalar que el modo en que nuestro ordenador está conectado a Internet es un elemento a destacar, ya que determina nuestra susceptibilidad frente a los virus. Si estamos conectados mediante banda ancha, y es una conexión permanente, los escritores de virus están intentando encontrarnos de manera activa (¡si no lo han hecho ya!). Mientras que conexiones discontinuas son habitualmente menos peligrosas (pero no están libres de peligro).[19]

4.9. Servidores y troyanos[20]

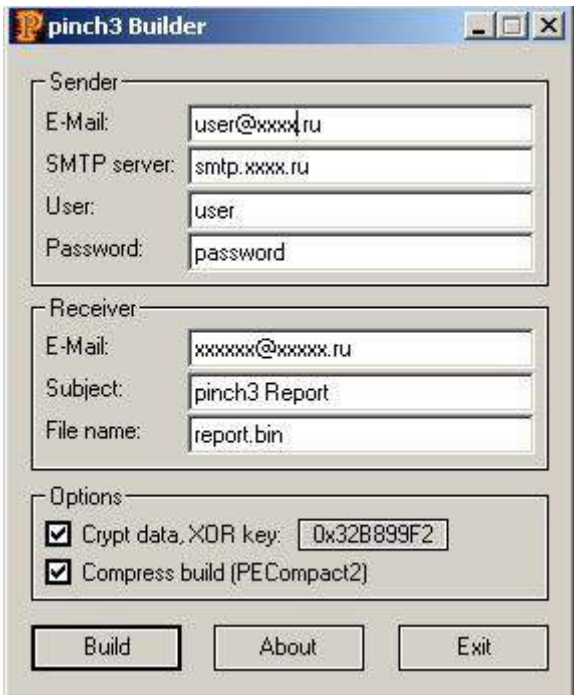
En realidad, no son virus como tales, puesto que lo que permiten es realizar acciones en una máquina remota.

Se les llama troyanos, como el caballo de Troya de Ulises, pues han de ser introducidos en el sistema para atacar. Existen distintas formas de penetrar en el sistema, por ejemplo adjuntándolos

19 GREGORY, Peter. *Computer Viruses for Dummies*. Indianapolis, Indiana: Wiley Publishing, Inc. ISBN: 0-7645-7418-3

20 DE MIGUEL, María del Rosario y Juan Vicente Oltra. *Deontología y aspectos legales de la informática: cuestiones éticas, jurídicas y técnicas básicas.* Valencia : Ed. UPV, 2007. p. 123 - 124 ISBN 978-84-8363-112-6

a un correo electrónico, con un applet de Java, mediante un send en el IRC, etc.



Troyano Pinch Builder

Lo recibido actúa como cliente de un programa servidor sito en la máquina atacante que, para ver si el cliente está activo, escanean el puerto configurado como de comunicaciones para esa aplicación concreta.

Estaban de moda en los años 80 para sistemas UNIX, reviviendo al hacerse populares para el entorno Windows.

4.10. Desarrolladores de virus y troyanos[21]

La opinión generalizada sobre ellos no es demasiado buena. Escribir virus se ha convertido en un hobby muy extendido. Este fenómeno tradicionalmente se ha estudiado desde el campo de la Informática, el Derecho y la Psicología, y ahora vamos a intentar dar una visión rápida sobre su perfil.

Los programadores descontentos, desde los 60's buscaban alterar el funcionamiento de las computadoras en las que trabajaban para obtener satisfacción moral. En los controles dispuestos

21 DE MIGUEL, María del Rosario y Juan Vicente Oltra. *Deontología y aspectos legales de la informática: cuestiones éticas, jurídicas y técnicas básicas.* Valencia : Ed. UPV, 2007. p. 124 - 125 ISBN 978-84-8363-112-6

para evitar los ataques veían estos primitivos creadores de virus un aliciente, un reto. Se trataba pues de profesionales en busca de varreras que batir, más que por malicia.

La catalogación hoy en día no es tan fácil, muchos virus tienen la intención de hacer tanto daño como puedan. Las motivaciones que los hacen nacer pueden ir desde la venganza o el fanatismo político, a un rencor enfermizo con la sociedad, pudiendo encontrarnos con las siguientes figuras, entre otras:

4.10.1. Terroristas

Su motivación puede ser política, religiosa o de cualquier tipo.

4.10.2. *Crackers*

Figura vista y que no hay que confundir con los *Hackers*. Son simples delincuentes virtuales que usan la informática en beneficio propio.

4.10.3. *Baby virus*

Estudiantes avanzados de informática que buscan demostrarse algo a sí mismos y a los demás.

4.10.4. Estados

Existen rumores de que la CIA y otras agencias desarrollan virus para ser utilizados como armas frente a otros estados o terroristas.

4.10.5. Creadores de antivirus

Sin confirmar tampoco, hay rumores que apuntan a que basta echar una ojeada a la cantidad de virus que circulan, frente al reducido número de antivirus que se comercializan.

4.11. Principios *hacking*[22]

Según Steven Levy, en su libro “La ética del *hacker*”, estos son los principios básicos que todo *hacker* que se precie debe seguir:

1. Entrégate siempre al imperativo de transmitir conocimientos. El acceso a ordenadores -y

22 LEVY, Steven. *Hackers.* Ed. Penguin, 2001. Capítulo: La ética del *hacker*.

cualquier otra cosa que pueda enseñarte sobre cómo funciona el mundo- debe ser ilimitado y total.

2. Toda la información debe ser libre.

3. Desconfía de la autoridad, promueve la descentralización.

4. Los *hackers* deben ser juzgados por su *hacking*, no por criterios falsos como títulos, edad, raza o posición.

5. Puedes crear arte y belleza en un ordenador.

6. Los ordenadores pueden cambiar tu vida a mejor.

Steven Levy escribió su primer libro, Hackers: Héroes de la revolución de la computadora , en 1984. En el Defcon conferencia de hackers en Las Vegas, habló de la palabra «hacker» y sus orígenes en medio de una multitud de jóvenes profesionales de la nave que no habían nacido cuando se publicó ese libro.

Otros principios:

- Va contra la ética del *hacker* alterar cualquier información. No se destruyen los datos ajenos como hacen los *crackers*. Sólo se explora el sistema y se aprende más.

- Compartir la información es poderoso, positivo y bueno, y es un deber ético del *hacker* compartir la suya escribiendo software gratis y facilitando el acceso de la información y los recursos en la medida de sus posibilidades.

- Invadir un sistema por diversión y exploración es éticamente aprobado siempre y cuando no se cometa robo, vandalismo o invasión de la confidencialidad.

- La libertad de información no debe atentar contra el derecho a la vida privada.

5. Los primeros *hackers*[23]

Quien dice primero, puede estar mintiendo, pero también es cierto que parece que todos apuntan a que fueron los chicos de MIT, los primeros en acuñarse la denominación *Hacker*. Estos eran un grupo de alumnos del prestigioso y conocido Massachusetts Institute of Technology (MIT), en su mayoría miembros del Tech Model Railroad Club (TMRC, Club de Modelos de Trenes) que en 1959 se apuntaron al primer curso de programación que la institución ofreció a sus alumnos, y que se enamoraron de los ordenadores y de lo que se podía hacer con ellos. Esta bella historia de amor "tecnológica" precipitó que los chicos pensaran de otra manera con respecto a la forma de funcionar con los ordenadores de aquellos días. Estos ordenadores eran unos aparatos demasiado caros y más que descomunales que, con un poco de suerte, ocupaban salas enteras que rápidamente impregnaban con un olor a chamuscado el ambiente de la sala. Para contrarrestar esto, los enormes ordenadores necesitaban complejos sistemas de aire acondicionado que los ventilaran continuamente. Además, estos gigantes de la informática necesitaban de una gran carga de suministro eléctrico para funcionar y subsistir, por lo que el acceso a éstos estaba realmente restringido para los estudiantes, lo que desembocaba en que en pocas ocasiones era el usuario final el que manejaba el ordenador directamente, sino que habitualmente se veía obligado a dar sus programas a los operadores, que a su vez se encargaban de introducirlos en el ordenador y de devolverle los resultados después.

23 HERNÁNDEZ, Claudio. *Hackers: Los piratas del Chip y de Internet.* 1999 - p. 22 - 23

Evidentemente, esto, a los chicos del TMRC, no les bastaba, y aparte de ingeniárselas para que en ocasiones les dejaran introducir directamente programas a ellos mismos y para tener tanto contacto como les fuera posible con el ordenador, no les suponía ningún problema el usarlo desde una sala de terminales a la que en realidad no tenían acceso de modo oficial colándose en ella por las noches. Lo que realmente les importaba a estos chicos, era poder usar el ordenador, sin preocuparse de las menudencias administrativas que dictaban una forma "oficial" de acceder a él.

Poco tiempo después de aquel curso llegó al MIT el TX-0, un ordenador revolucionario para la época, y el grupo de pirados de la informática del MIT tuvo la suerte de que Jack Dennis, un antiguo miembro del TMRC y ahora profesor del MIT, les diera acceso prácticamente ilimitado a esa máquina.

Para ellos, una de las principales ventajas que tenía ésta era que en lugar de interactuar con los usuarios mediante tarjetas perforadas, tenía un teclado gracias al cual era posible trabajar directamente con él, lo que les permitía ver directamente el resultado de su trabajo, con lo que cada vez empezaron a pasar más y más tiempo con el ordenador y pronto eran capaces de hacer cosas con él que ni sus diseñadores hubieran creído posibles. Fue en este entorno y en ese momento cuando el término *hacker* se empezó a aplicar a aquellos pirados de la informática capaces de hacer maravillas con un ordenador. En cualquier caso, la contribución más importante de este grupo de *hackers* a la historia de la informática no fue la de adoptar ese término sino la de ser los primeros en pensar diferente acerca de cómo se usaban los ordenadores y de lo que se podía hacer con ellos, y, sobre todo, la creación de una ética que regía su comportamiento que aún sigue vigente hoy en día y que todos los *hackers* siguen (o dicen seguir) en mayor o menor medida, sobre todo en la parte que mantiene que la información debe ser libre.

Esta historia, ha sido repetida una y otra vez, en la mayoría de los reportajes que se han escrito sobre *Hackers*, ya que de alguna manera se describe con certeza a los primeros *Hackers* o al menos, cuándo se acuñó este termino.

5.1. Richard Stallman[24]

Stallman brilla por su gran capacidad para programar. Todavía a día de hoy utiliza para trabajar, una máquina bastante antigua. Se trata de una DEC PDP-10. Stallman se integró en el laboratorio de Inteligencia Artificial del MIT en 1971, lo que le valió paracrear sus propias aplicaciones de Inteligencia Artificial. Stallman, por sus trabajos, fue recompensado con el premio McArthur Genius. En la actualidad Stallman se dedica a crear miles de utilidades gratuitas para entornos UNIX. Evidentemente, no los escribe él solo, para ello creó recientemente la Fundación Free Software en la que intervienen muchísimos programadores.

24 http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Richard_Stallman, Agosto/2011

5.2. Dennis Ritchie[25], Ken Thomson[26] y Brian Kernighan[27]



Estos tres mosqueteros del chip son buenos programadores y trabajan para Bell Labs. Es como si esta empresa sólo gestara buenos *Hackers*. Los tres están especializados en el entorno UNIX y en el lenguaje C. Estos hombres han tenido que ver, y mucho, con el nacimiento de Internet y su progreso. De no haber estado ellos en este proyecto, Internet quizás no existiría ahora, o de hacerlo, seria muchísimo más lenta. En la actualidad Ritchie esta trabajando en el Plan 9 de Bells Labs, un sistema operativo de última generación que vendrá a sustituir a UNIX. Thompson y Kernighan todavía siguen trabajando como *Hackers*, algo que siempre les motivó a seguir viviendo con cierta ilusión.

5.3. John Draper[28]

Conocido como el capitán Crunch, este hombre fue quien descubrió que con un silbato de los cereales Crunch se podía hacer Phreaking. Este silbato curiosamente generabaun silbido a 2.600 Hertzios. Esta frecuencia es la que se empleaba para cortar los contadores de los teléfonos de Bell. Este descubrimiento llevó a John a crear la primera "Blue Box", una caja electrónica mágica para los teléfonos.

25 http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Dennis_Ritchie , Agosto/2011
26 http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Ken_Thompson , Agosto/2011
27 http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Brian_Kernighan, Agosto/2011
28 http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/John_Draper, Agosto/2011

5.4. Paul Baran[29]

Hay quien lo cataloga como el mejor *Hacker* de todos. Esto es solo una objeción de otro *Hacker* bastante conocido, *Anonymous*. No obstante hay que reconocer que Baran estuvo enredado con Internet incluso antes de que esta existiese como tal, por lo que los principios de Internet se deben asignar a Baran. Baran comenzó a edificar lo que es hoy día, un Navegador. Baran tuvo un gran acierto con crear esta herramienta que a día de hoy, esta siendo utilizada por millones de internautas de todo el planeta.

5.5. Eugene Spafford[30]

Este profesor de Informática de la universidad de Purdue, ha descubierto e impulsado a varios estudiantes realmente brillantes, entre los que destaca Dan Farmer. Spaffor es el creador de COPS "Computer Oracle Password and Security System", un sistema de seguridad para Redes.

29 http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Paul_Baran, Agosto/2011
30 http://www.wikipedia.org, Wikipedia, http://en.wikipedia.org/wiki/Gene_Spafford , Agosto/2011

5.6. Mark Abene[31]

Con el alias Phiber Optik, este *Hacker* es uno de los miembros fundadores del grupo "Master of deception" un grupo dedicado exclusivamente al conocimiento profundo de los teléfonos. Su primer acercamiento a la tecnología fue con un Conmodore 64 y un sistema de *Radio Shack* TRS-80.

5.7. Johan Helsingius[32]

Alias Julf, es el más popular creador de correo anónimo, es decir, él fue quien creó este tipo de correo seguro a través de una cuenta llamada penet.fi. Julf se inició con un 486 con 200 megas de disco duro.

5.8. Wietse Venema[33]

En la actualidad, este hombre trabaja en la Universidad de Tecnología de Eindhoven. Es un

31 http://www.wikipedia.org, Wikipedia, http://en.wikipedia.org/wiki/Mark_Abene , Agosto/2011
32 http://www.wikipedia.org, Wikipedia, http://en.wikipedia.org/wiki/Penet_remailer, Agosto/2011
33 http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Wietse_Venema, Agosto/2011

programador prolífico que ha recibido multitud de reconocimientos por todo su trabajo. Venema es coautor con Dan Farmer de la herramienta SATAN. Pero fue el programa TCP Wrapper, el que le lanzó a la fama. Esta herramienta de seguridad es una de las más utilizadas en el mundo. Este programa controla y registra los paquetes que entran en una Red. Evidentemente, esto le mereció un premio a su trabajo.

5.9. Kevin Mitnick[34]

Mitnick es la leyenda viva. Se le conoce como el cóndor. Este apodo surge por la habilidad de éste, de ser el más escurridizo del FBI. Es el *Cracker* más famoso del mundo. Kevin comenzó sus andanzas con tan solo 10 años. Con esta edad, Mitnick fue capaz de violar el sistema de seguridad del sistema de defensa de los EE.UU. Sus principios se basan en el Phreaking, desde entonces ha violado todos los sistemas de seguridad imaginables, incluyendo los militares, empresariales o las grandes firmas. Su obsesión por recuperar un software de OKI, le llevo a invadir los ordenadores Tsutomu Shimomura en una noche de navidad. Shimomura era también otro *Hacker*. Esto le llevo a la ratonera más grande jamás creada. En la actualidad Mitnick ha cumplido condena y se encuentra libre, eso sí, le esta prohibido acercarse a un ordenador. Sin embargo se sabe que Mitnick actuó como asesor de seguridad contra el famoso Virus I Love You.

5.10. Kevin Poulsen[35]

Este hombre siguió los mismos pasos que Mitnick. A Poulsen se le conoce por su gran habilidad

34 http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Kevin_Mitnick, Agosto/2011
35 http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Kevin_Poulsen, Agosto/2011

para controlar el sistema telefónico de Pacific Bell. Una buena prueba de ello, es que Poulsen utilizó su talento para ganar un Porsche en un concurso radiofónico. Para ello intervino las líneas telefónicas, dándose prioridad a sí mismo. Pulsen ha violado prácticamente todos los sistemas de seguridad, pero parece que tienes mas interés en conocer los sistemas de la defensa militar. Esta filosofía le ha llevado a pasar por la cárcel, donde cumplió una condena de cinco años. En 1996 fue soltado y parece que hasta la fecha, Poulsen no ha hecho ninguna de las suyas, al menos que se conozca.

5.11. Justin Tanner Petersen[36]

Justin Tanner es también conocido como el Agente Steal. Su habilidad haciendo *cracking* le llevó a conocer perfectamente las tarjetas de crédito. Pero no empleó sus conocimientos sólo para fines educativos, ya que lo que verdaderamente le motivaba, era ganar dinero de una forma rápida y fácil. Esta falta de ética del *Hacker* verdadero, le llevo a una sucia jugada con el FBI para trabajar con ellos en la clandestinidad. Su colaboración con ellos, le llevo a denunciar entre otros *Hackers*, a Poulsen, pero al final fue incapaz de protegerse él mismo.

5.12. Vladimir Levin[37]

Vladimir Levin, un matemático ruso de 24 años, penetro vía Internet desde San Petersburgo en los sistemas informáticos centrales del banco Citibank en Wall Street. Una vez dentro, este *Hacker* logró transferir a diferentes cuentas de EE.UU, Rusia, Alemania, Israel y Suiza fondos por valor de

36 http://www.wikipedia.org, Wikipedia, http://en.wikipedia.org/wiki/Justin_Tanner_Petersen, Agosto/2011
37 http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Vladimir_Levin, Agosto/2011

10 millones de dolares. Pero finalmente el *Hacker* fue detenido en 1995. En Internet es fácil encontrar un documento titulado "Cómo robe 10 millones de dólares".

5.13. Grace Hooper[38]

Nacida en 1906. Se graduó de Vassar College con grados en matemáticas y física. Completó su maestría y doctorado en matemáticas en Yale. Durante la segunda guerra mundial se unió al Navy donde trabajó en el Bureau of Ordenance Computation. Trabajó en la primera computadora de automática secuencial digital a gran escala. En 1960 mostró por primera vez su versión de COBOL en dos camputadoras. Se le dio el premio Hombre del Año en las Ciencias de Cómputos por la Data Processing Management Association. Fue la primera mujer nombrada Distinguished fellow of the British Computer Society, y la primera y única mujer admirante en el U.S. Navy hasta ahora. Murió en 1992.

Por estas connotaciones, para muchos estudiosos, la almirante Grace Hooper es considerada la primera *hacker* de la era de la computación.

5.14. Robert Thomas, Douglas McIlroy y Victor Vysottsky[39]

Por el solo hecho de entretenerse crearon un juego al que denominaron CoreWar, inspirados en la teoría de John Von Neumann (famoso científico matemático de origen húngaro que en su presentaba la posibilidad de desarrollar pequeños programas que pudiesen tomar el control de otros, de similar estructura.) El juego CoreWar fue desarrollado en Assembler Pnemónico,

38 GIJÓN, Jesús. *Hackers, crackers y sus implicaciones sociales y mediáticas.* Valencia UPV. p. 41 - 47

39 GIJÓN, Jesús. *Hackers, crackers y sus implicaciones sociales y mediáticas.* Valencia UPV. p. 41 - 47

conocido como Red Code (código rojo) Puesto en la práctica, los contendores del CoreWar ejecutaban programas que iban paulatinamente disminuyendo la memoria del computador y el ganador era el que finalmente conseguía eliminarla totalmente. Robert Thomas Morris, Douglas McIlroy y Victor Vysottsky fueron los precursores de los virus informáticos.

5.15. Robert Tappan Morris

Hijo de Robert Thomas Morris uno de los precursores de los virus y recién graduado en Computer Science en la Universidad de Cornell, en 1988 difundió un virus a través de ArpaNet, (precursora de Internet) logrando infectar 6,000 servidores conectados a la red. La propagación la realizó desde uno de los terminales del MIT (Instituto Tecnológico de Massachussets). ArpaNet empleaba el UNIX, como sistema operativo. Robert Tappan Morris al ser descubierto, fue enjuiciado y condenado en la corte de Syracuse, estado de Nueva York, a 4 años de prisión y el pago de US $ 10,000 de multa, pena que fue conmutada a libertad bajo palabra y condenado a cumplir 400 horas de trabajo comunitario.

5.16. Chen Ing – Hou[40]

Es el creador del virus CIH, que lleva sus propias iniciales. Manifiesta que lo siente mucho por los graves daños causados por su creación viral, pero que ello fue motivado por una venganza en contra de los que llamó "incompetentes desarrolladores de software antivirus". Chen Ing-Hou nació en la ciudad de Kaohsiung, Taipei o Taibei, capital y principal ciudad de Taiwán, y creó su famoso virus en Mayo de 1998, al cual denominó Chernobyl, en conmemoración del 13 aniversario de la tragedia ocurrida en la planta nuclear rusa. Actualmente trabaja como experto en

40 GIJÓN, Jesús. *Hackers, crackers y sus implicaciones sociales y mediáticas.* Valencia UPV. p. 41 - 47

Internet Data Security.

5.17. David L. Smith

De 30 años, natural de Aberdeen, New Jersey y sospechoso de ser el autor del virus Melissa se declaró culpable en segundo grado de daño a computadoras el 09 de Diciembre de 1999. El jurado podría condenarlo a purgar una pena de 10 años en prisión.

El macro virus Melissa atacó a miles de usuarios y empresas el 26 de Marzo de 1999, después de haber sido esparcido como un documento de MS-Word infectado en un grupo de noticias de Usenet, que conformaban una lista de interés sobre páginas web porno. Después de las investigaciones correspondientes se arrestó a su supuesto autor.

El 8 de Abril de 1999, David L. Smith, de 30 años, natural de Aberdeen, New Jersey y sospechoso de ser el autor del virus Melissa hizo su primera aparición en público en la Corte Superior del condado de Monmouth para escuchar las acusaciones en su contra. Smith permaneció silencioso y cabizbajo cuando escuchó los cargos.

Las autoridades de New Jersey acusaron a Smith de interrupción de las comunicaciones públicas, conspiración para cometer el delito, intento de delito y robo de servicios de computadoras, en tercer grado. Todo esto lo haría enfrentar una posible pena de 40 años de cárcel y al pago de una multa de US $ 480,000.

Inicialmente David L. Smith, programador de computadoras, alegó su inocencia y manifestó que creó el virus en su departamento de Aberdeen y lo llamó así en memoria de una bailarina Topless, del estado de Florida, de la cual se había enamorado, pero sus relaciones sentimentales quedaron frustradas.

Ante el Juez John Riccardi que dirige la causa, un nervioso Smith leyó el siguiente argumento:
"Sí, yo admito esos sucesos ocurridos como resultado de la propagación del virus Melissa. Pero yo no esperaba o anticipé la enorme cantidad de daño que ocasionó. Cuando difundí el virus yo

supuse que algún daño material sería menor e incidental. De hecho, yo incluí instrucciones diseñadas para prevenir un daño substancial. No tuve idea de que habrían profundas consecuencias en contra de otros".

Cuando el Juez preguntó otra vez si Smith estaba de acuerdo de que causó significativos daños a los sistemas de computadoras en todo el país, Smith respondió: "Yo estoy de acuerdo, por cierto. Todo ello devino en esas consecuencias sin lugar a dudas"

El delito, que incluye "interceptación de las comunicaciones de computadoras y daños a los sistemas de computadora o a su información" es castigado con una carcelería de 5 a 10 años y hasta US $150,000 de multa. Como consecuencia de la acusación, Smith ha aceptado recibir la máxima pena por el delito, pero el Juez podría ignorar esta recomendación.

5.18. Reonel Ramones[41]

De 27 años, empleado bancario, quien vivía con su hermana y su novia Irene de Guzmán de 23, fueron acusados de ser los autores del virus LoveLetter, el mismo que según algunas evidencias, habría empezado como un conjunto de rutinas para penetrar en otros sistemas, con el objeto de sustraer la información de tarjetas de crédito de terceros. Las evidencias apuntaron a Reonel Ramonez, como cabeza del grupo que participó en la creación y difusión de este virus. Una corporación holandesa lo contrató con un sueldo muy atractivo, por considerarlo muy hábil y capaz en el desarrollo de sistemas de seguridad en Redes e Internet.

41 GIJÓN, Jesús. *Hackers, crackers y sus implicaciones sociales y mediáticas.* Valencia UPV. p. 41 - 47

5.19. Robert “Pimpshiz” Lyttle

De 18 años de edad, se encuentra bajo arresto domiciliario, por orden de una Corte Juvenil de ciudad Martínez, estado de California, acusado de ser uno de los miembros del grupo Deceptive Duo, que probadamente incursionaron ilegalmente y substrajeron información de los servidores del sistema de la Federal Aviation Administration de los Estados Unidos y descargaron información confidencial relacionada a las filmaciones de las actividades de los pasajeros de los aeropuertos. Al momento de su arresto Lyttle portaba una portátil IBM ThinkPad, un lector de huellas digitales del dedo pulgar y otros sofisticados dispositivos "The Deceptive Duo" (El dúo engañoso) ingresaron a un servidor de la FAA, empleado por la administración de Seguridad de la Aviación Civil de los Estados Unidos, encargada a partir de los fatídicos incidentes del pasado 11 de Septiembre del 2001, del monitoreo de las actividades de los pasajeros en todos los aeropuertos de ese país.

Cada sitio web incursionado por estos *hackers*, mostraba una supuesta "patriótica misión" en la cual preconizaban ser ciudadanos de los Estados Unidos de América, determinados a salvar al país de una "amenaza extranjera" al exponer los huecos de inseguridad en Internet. Incluso incluyeron el logo del grupo, consistente en dos armas de fuego delante de una bandera norteamericana. Cabe mencionar que Robert Lyttle, siendo un joven adolescente, de apenas 14 años formó la corporación Sub-Seven Software, que desarrolló herramientas tales como el Troyano buscador de puertos Sub- Net, el desinstalador Uninstall it Pro y Define, entre otros y que muchos usuarios consideramos de gran utilidad. Posiblemente se convierta en un héroe del "underground" en el ciber-espacio. En Febrero del 2002 descubrió una vulnerabilidad en el AOL Instant Messenger, y mucho antes hizo lo propio con varios sistemas de Microsoft.

6. Echelon, *Carnivore*, *Enfopol* y *Oseminti*[42]

Los gobiernos son capaces de "espiarnos" a todos con el objetivo, en un principio, de evitar por ejemplo ataques terroristas. Para ello cuentan con unas herramientas que vamos a explicar a continuación. Su modo de funcionamiento es que la información obtenida a través de estas herramienta puede ser usada por los países para lucrarse de una forma poco ética, por ejemplo facilitando datos a las grandes empresas que sostienen el país con el objetivo de que crezcan económicamente y a la par crezca el país.

Estas herramientas reciben los nombres de *Echelon* y *Carnivore* en el caso de EEUU y *Enfopol* y *Oseminti* en el caso de la Unión Europea.

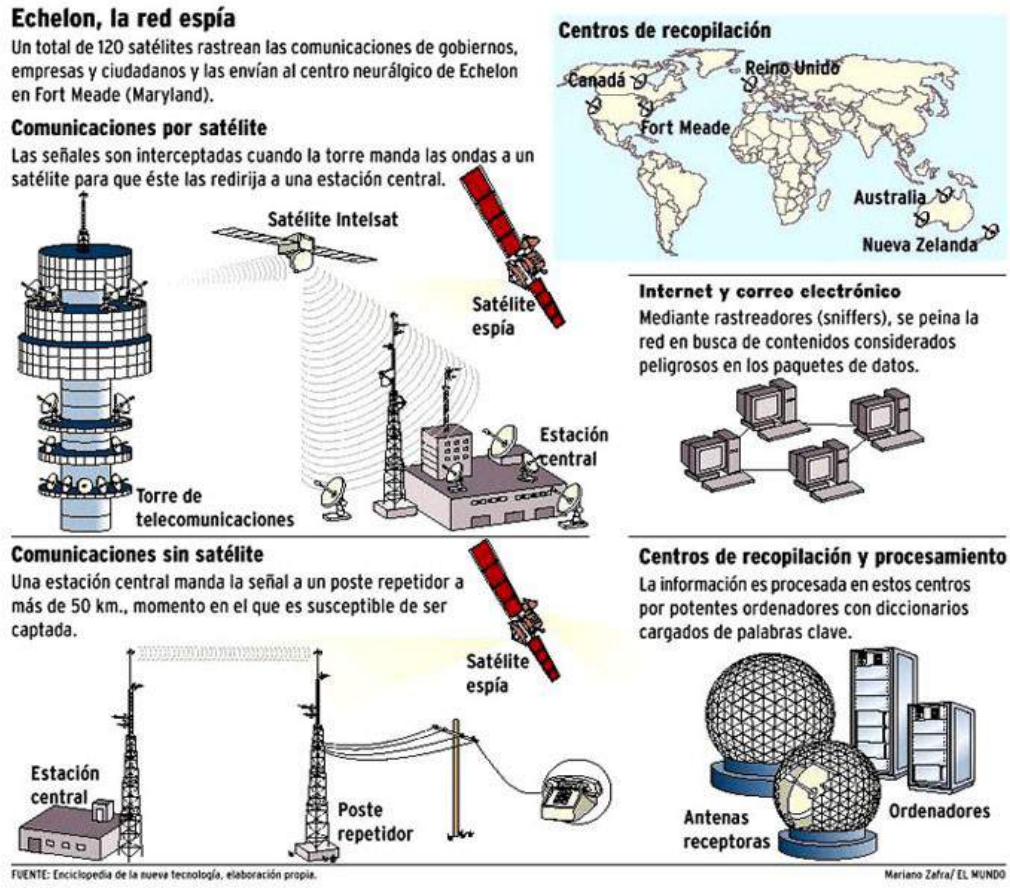
ECHELON es la mayor red de espionaje y análisis para interceptar comunicaciones electrónicas de la historia. Controlada por la comunidad UKUSA (Estados Unidos, Canadá, Gran Bretaña, Australia, Irlanda del Norte y Nueva Zelanda), ECHELON puede capturar comunicaciones por radio y satélite, llamadas de teléfono, faxes y e-mails en casi todo el mundo e incluye análisis automático y clasificación de las interceptaciones. Se estima que ECHELON intercepta más de tres mil millones de comunicaciones cada día.

42 GIJÓN, Jesús. *Hackers, crackers y sus implicaciones sociales y mediáticas.* Valencia UPV. p. 48 - 52

Echelon intercepta 3 mil millones de comunicaciones diarias

Echelon: el control total sobre las comunicaciones mundiales

A pesar de haber sido presuntamente construida con el fin de controlar las comunicaciones militares y diplomáticas de la Unión Soviética y sus aliados, se sospecha que en la actualidad ECHELON es utilizado también para encontrar pistas sobre tramas terroristas, planes del narcotráfico e inteligencia política y diplomática. Sus críticos afirman que el sistema es utilizado también para el espionaje económico y la invasión de privacidad en gran escala.



Resumen de Echelon

Los miembros de esta alianza de habla inglesa son parte de la alianza de inteligencia UKUSA, que lleva reuniendo inteligencia desde la Segunda Guerra Mundial. La existencia de ECHELON fue hecha pública en 1976 por Winslow Peck.

Varias fuentes afirman que estos estados han ubicado estaciones de intercepción electrónica y satélites espaciales para capturar gran parte de las comunicaciones establecidas por radio, satélite, microondas, celulares y fibra óptica. Las señales capturadas son luego procesadas por una serie de supercomputadoras, conocidas como diccionarios, las cuales han sido programadas para buscar patrones específicos en cada comunicación, ya sean direcciones, palabras, frases o incluso voces específicas.

El sistema está bajo la administración de la NSA (National Security Agency). Esta organización cuenta con 100.000 empleados tan sólo en Maryland (Estados Unidos) (otras fuentes hablan de 38.000 empleados a escala mundial), por lo que es probablemente la mayor organización de espionaje del mundo.

Red Echelon

A cada estado dentro de la alianza UKUSA le es asignado una responsabilidad sobre el control de distintas áreas del planeta. La tarea principal de Canadá solía ser el control del área meridional de la antigua Unión Soviética. Durante el período de la guerra fría se puso mayor énfasis en el control de comunicaciones por satélite y radio en centro y Sudamérica, principalmente como medida para localizar tráfico de drogas y secuaces en la región. Los Estados Unidos, con su gran cadena de satélites espías y puertos de escucha controlan gran parte de Latinoamérica, Asia, Rusia asiática y el norte de China. Gran Bretaña intercepta comunicaciones en Europa, Rusia y África. Australia examina las comunicaciones de Indochina, Indonesia y el sur de China, mientras que Nueva Zelanda barre el Pacífico occidental.

Según algunas fuentes el sistema dispone de 120 estaciones fijas y satélites geoestacionarias. Estos podrían filtrar más del 90 % del tráfico de Internet. Las antenas de Echelon pueden captar ondas electromagnéticas y trasmitirlas a un lugar central para su procesamiento. Se recogen los mensajes aleatoriamente y se procesan mediante los diversos filtros buscando palabras clave. Este procedimiento se denomina "Control estratégico de las telecomunicaciones".

ENFOPOL (del inglés «Enforcement Police», «policía de refuerzo») es un sistema de intercepción de las comunicaciones de la Unión Europea que surge como respuesta al megasistema ECHELON, propiedad de Estados Unidos, el Reino Unido y varios países miembros de la Commonwealth.

El 7 de Mayo de 1999, el Parlamento Europeo aprobó la Resolución del Consejo sobre

interceptación legal de las comunicaciones relativo a las nuevas tecnologías. Más conocido como Resolución Enfopol, abre el camino a un sistema de interceptación y vigilancia de las comunicaciones en todo el territorio de la Unión Europea. La extensión de los poderes otorgados a las policías europeas mediante este plan, unido al secretismo que ha rodeado su gestación y desarrollo, lo convierten en una grave amenaza potencial para la intimidad en la Europa del nuevo milenio.

OSEMINTI es un proyecto europeo llevado a cabo por Francia, Italia y España para crear un Carnivore Europeo.

El proyecto OSEMINTI debe lograr, según fuentes del Ministerio de defensa español, que "los servicios de Inteligencia, por medio de ordenadores, puedan identificar frases con significados concretos en cintas de grabación o en texto escrito y, a su vez, que dichos ordenadores aprendan, con el conocimiento que van generando en su interacción con las personas".

Francia lidera el proyecto, que durará dos años. España contribuye con 1.856.000 euros, el 30% del presupuesto. Según el Ministerio, "el campo natural de OSEMINTI es la inteligencia militar", aunque también otros "ámbitos de defensa y seguridad, tanto civil como militar".

Por su capacidad de entender el significado de un texto interceptado, OSEMINTI es un paso más en la evolución de los sistemas de espionaje telemático, cuyo representante más popular en el campo civil fue Carnivore, usado durante años por el estadounidense Federal Bureau of Investigation (FBI) para monitorizar comunicaciones a través de Internet.

Carnivore, según la Wikipedia, se instalaba en el proveedor de acceso (ISP) de la persona a espiar, previa orden judicial, y era capaz de discriminar la interceptación de sólo los datos autorizados por el juez, que copiaba al vuelo y mandaba a un ordenador central.

Su existencia se conoció en el año 2000, por una disputa legal con un ISP que se negaba a instalarlo, y desencadenó las protestas de grupos de libertades civiles de todo el mundo. Se hizo tan popular que hubo quien realizó obras de arte basadas en Carnivore, rebautizado después por el FBI como DCS-1000.

Carnivore era la tercera generación de los sistemas de espionaje de redes del FBI. El primero fue Etherpeek, actualmente un programa comercial. El segundo, Omnivore, usado entre 1997 y 1999 y sustituido por DragonWare y constaba de tres partes: Carnivore, que capturaba la información; Packeteer, que convertía los paquetes interceptados en textos coherentes, y Coolminer, que los

analizaba.

El sistema Carnivore provocó muchas controversias por sus fallos, como espiar a la persona equivocada, y porque se usó sin permiso judicial, según los grupos de libertades civiles. La ley USA Patriot acabó con la discusión, al decretar que el FBI podía monitorizar redes sin orden de un juez ni sospechas fundadas, mientras sólo captase la información del tráfico y no su contenido.

7. La conferencia *Defcon*[43][44]

Defcon es una de las convenciones de *hackers* más grandes del mundo. Tiene lugar todos los años en Las Vegas. La primera de ellas tuvo lugar en junio de 1993.

La mayoría de los asistentes de Defcon son profesionales en seguridad informática, periodistas, abogados, empleados del gobierno federal, *crackers*, cyber-criminales, investigadores en seguridad y *hackers* con un interés general en programación, arquitectura de computadores,

43 http://www.wikipedia.org, Wikipedia, http://en.wikipedia.org/wiki/DEF_CON, Agosto/2011
44 https://www.defcon.org, Defcon, https://www.defcon.org, Agosto/2011

phreaking, modificación de hardware y, en general, cualquier cosa que pueda ser *hackeada*.

El evento consiste en una serie de presentaciones de expertos en informática y en temas relacionados con el *hacking*, así como eventos sociales y todo tipo de concursos, creando una enorme conexión Wi-Fi y *crackeando* sistemas informáticos.

Se realizan otros concursos relacionados con desbloqueos, robótica, arte, etc. Pero el concurso más difundido es posiblemente el denominado "Capture the flag", algo así como "Capturar la bandera enemiga". El concurso, en el que compiten equipos, consiste en *hackear* a los demás equipos y evitar que los demás los *hackeen* a ellos.

8. Hacking ético[45]

8.1. ¿Puede ser ético el *hacking*?

- El nombre *hacker* es un neologismo utilizado para referirse a un experto (Gurú) en varias o alguna rama técnica relacionada con las tecnologías de la información y las telecomunicaciones: programación, redes, sistemas operativos.

- El nombre *cracker* (criminal *hacker*, 1985) es alguien que viola la seguridad de un sistema informático de forma similar a como lo haría un *hacker*, sólo que a diferencia de este último, el *cracker* realiza la intrusión con fines de beneficio personal o para hacer daño a su objetivo.

- El nombre *Hacker* ético hace referencia a profesionales de la seguridad que aplican sus conocimientos de *hacking* con fines defensivos (y legales).

– Diremos *hacker* siempre, pero hay que fijarse en el contexto.

45 MALAGÓN, Constantino. *Hacking ético*. Universidad Nebrija. Madrid.

8.2. Elementos de seguridad

Elementos esenciales de la seguridad:

- *Confidencialidad:* tiene que ver con la ocultación de información o recursos.

- *Autenticidad:* es la identificación y garantía del origen de la información.

- *Integridad*: se refiere a cambios no autorizados en los datos.

- *Disponibilidad*: posibilidad de hacer uso de la información y recursos deseados.

8.3. ¿Qué puede hacer un *hacker*?

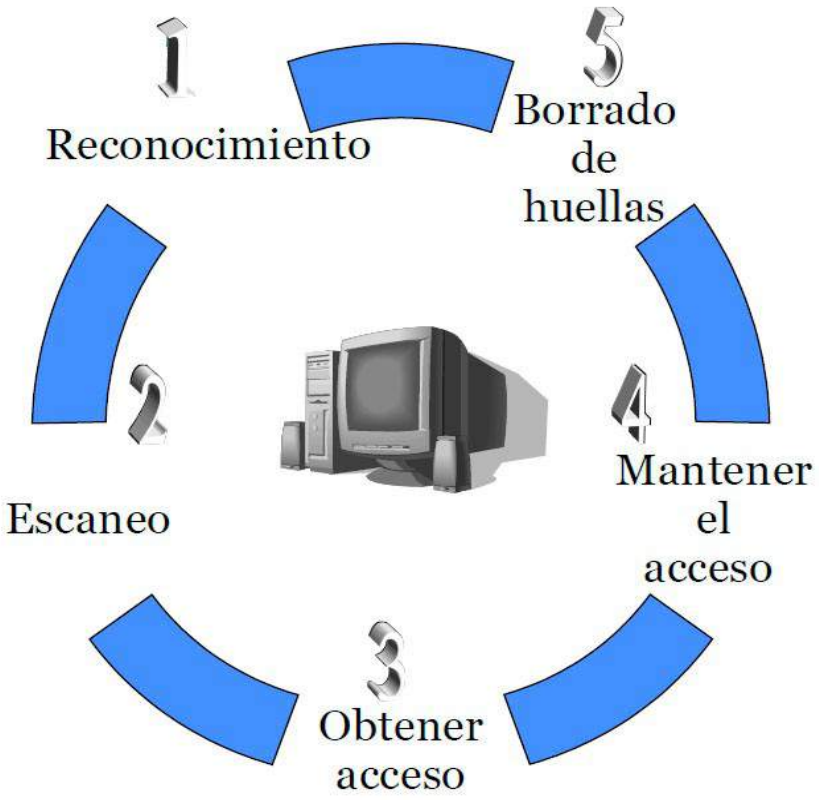
- Reconocimiento
    · Pasivo

- Rastreo (escaneo)
    · Activo

- Acceso
    · Sistema operativo / aplicación
    · Redes
    · Denegación de servicio

- Mantener el acceso

    – Borrado de huellas



8.3.1. Fase 1. Reconocimiento

Previo a cualquier ataque.

- Información sobre el objetivo

- Reconocimiento pasivo:
  - Google *Hacking*
  - Ingeniería social
  - Monitorización de redes de datos. Por ejemplo, sniffing, etc.

8.3.2. Fase 2. Escaneo

Escaneo es una fase de pre-ataque.

- Se escanea la red pero ya con información de la fase previa.

- Detección de vulnerabilidades y puntos de entrada.

- El escaneo puede incluir el uso de escaneadores de puertos y de vulnerabilidades.

- Reconocimiento activo: Probar la red para detectar.
  · Hosts accesibles
  · Puertos abiertos
  · Localización de routers
  · Detalles de sistemas operativos y servicios

8.3.3. Fase 3. Ataque. Obtener acceso

Obtención de acceso: Se refiere al ataque propiamente dicho.

- Por ejemplo, hacer uso de un exploit o bug.
  · Obtener una password, ataques man-inthe_ middle (spoofing), exploits (buffer overflows), DoS (denial of service).

8.3.4. Fase 4. Ataque. Mantener acceso

Mantenimiento del acceso: Se trata de retener los privilegios obtenidos.

- A veces un *hacker* blinda el sistema contra otros posibles *hacker*, protegiendo sus puertas traseras, rootKits y Troyanos.

8.3.5. Fase 5. Borrado de huellas

Borrado de huellas: Se intenta no ser descubierto.

- Hay que tener claro que hay técnicas más intrusivas (y por lo tanto delatoras) que otras.

  – Análisis forense

8.4. Tipos de *hacker*

- Black Hats:

Son individuos con habilidades extraordinarias en computación. Recurren a actividades maliciosas o destructivas. También se les conoce como *Crackers*.

- White Hats:

Son individuos con habilidades de *Hacker*. Utilizan sus habilidades con fines defensivos. También se les conoce como *Analistas de Seguridad.*

- Gray Hats:

Son individuos que trabajan tanto ofensivamente como defensivamente.

8.5. *Hacktivismo*

El concepto de *hacktivismo* lo hemos analizado profundamente en el punto 2.5. Aquí solamente nos limitamos a recordarlo pues es importante hacerle una reseña si hablamos de *hacking* ético.

- Se refiere a '*hacking* por una causa'.

- Es el compromiso político o social del *hacking*.

- Por ejemplo, atacar y alterar sitios web por razones políticas, tales como ataques a sitios web del gobierno o de grupos que se oponen a su ideología.

- Pero hay acciones que son delito (tengan o no una justificación idelológica).

8.6. ¿Qué puede hacer un *hacker* ético?

"If you know the enemy and know yourself, you need not fear the result of a hundred battles."
Sun Tzu, Art of War

- Un *hacker* ético intenta responder a las siguientes preguntas:

- ¿Qué puede saber un intruso de su objetivo? **Fases 1 y 2**
- ¿Qué puede hacer un intruso con esa información? **Fases 3 y 4**
- ¿Se podría detectar un intento de ataque? **Fases 5 y 6**

- ¿Para que querría una empresa contratar a un *hacker* ético?

8.7. Perfil de habilidades de un *hacker* ético

- Experto en algún campo de la informática.

- Conocimientos profundos de diversas plataformas (Windows, Unix, Linux).

- Conocimientos de redes.

- Conocimientos de hardware y software.

8.8. ¿Qué debe hacer un *hacker* ético?

Fases de un proceso de evaluación de la seguridad:

- Preparación: Se debe tener un contato firmado por escrito donde se exonere al *hacker* ético de toda responsabilidad como consecuencia de las pruebas que realice (siempre que sea dentro del marco acordado).

- Gestión: Preparación de un informe donde se detallen las pruebas y posibles vulnerabilidades detectadas.

- Conclusión: Comunicación a la empresa del informe y de las posibles soluciones.

8.9. Modos de *hacking* ético

- Redes remotas: Simulación de un ataque desde Internet.

- Redes locales: Simulación de un ataque desde dentro (empleados, *hacker* que ha obtenido privilegios en un sistema,...)

- Ingeniería social: Probar la confianza de los empleados.

- Seguridad física: Accesos físicos (equipos, cintas de backup,...)

8.10. Evaluando la seguridad

Tipos de tests de seguridad:

- Black-box: Sin conocimiento de la infraestructura que se está evaluando.

- White-box: Con un conocimiento completo de la infraestructura que se está evaluando.

- Gray-box: Se examina la red desde dentro.

8.11. ¿Qué se debe entregar?

- Ethical *Hacking* Report

- Detalles de los resultados de las actividades y pruebas de *hacking* realizadas. Comparación con lo acordado previamente en el contrato.

- Se detallarán las vulnerabilidades y se sugiere cómo evitar que hagan uso de ellas.

¡Ojo, que esto debe ser absolutamente confidencial!

- Deben quedar registradas en el contrato dichas cláusulas de confidencialidad.

9. Consecuencias jurídicas del *hacking*[46]

La Ley Orgánica 5/2010, de 22 de junio, introduce en el art. 197.3 el acceso sin autorización y vulnerando las medidas de seguridad establecidas a datos o programas informáticos contenidos en un sistema o en parte del mismo, dentro del descubrimiento y revelación de secretos, lo que comúnmente viene a ser *hacking*, pese a toda la discusión sobre el concepto. La literatura y el cine han rodeado a los *hackers* de cierto romanticismo, la propia entrada de la Wikipedia exalta el compromiso social y bondades de estas conductas frente a los malvados *crackers*, que hacen lo mismo pero en beneficio propio o para causar un perjuicio. En todo caso, aún considerando esa ética del *hacker*, si en vez de hablar de SGAE y el Ministerio de Cultura habláramos de ANESVAD o la web del Defensor del Menor, por poner un par de ejemplos de estas conductas, las cosas se verían de otro modo. (El autor hace referencia a los ataques de denegación de servicio a los sitios web de SGAE y el Ministerio de Cultura y las manifestaciones sobre la supuesta licitud que tuvieron lugar en 2010.) De cualquier forma, esta reforma tenía que llegar, pues la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005 obligaba a incluirlas antes del 16 de marzo de 2007.

46 PRENAFETA Rodríguez, Javier. *Consecuencias jurídicas de los ataques a sistemas informáticos*. Identificador: 1010087527283. 08-oct-2010 1:07 UTC. Tipo de obra: Literaria, Artículo

La ley anterior también cambia la redacción del art. 264 del Código Penal, relativo a los daños (aquí entrarían específicamente las conductas del *cracker*), básicamente para añadir la obstaculización o interrupción de un sistema informático ajeno, ya sea introduciendo, transmitiendo, dañando, alterando, suprimiendo o haciendo inaccesibles datos informáticos. Se repite algún concepto, y aunque se exija que dichas conductas sean graves y el recorrido de la pena se reduzca para el tipo básico (para conductas agravadas se llega hasta los cuatro años y medio de prisión), ya no se exige la constatación de un daño, como sucedía hasta ahora. En ambos casos, tanto en el 197.3 como en el 264 se prevé responsabilidad para las personas jurídicas.

Pese a la reforma, entiendo que el *hacking* es perseguible actualmente con la regulación vigente si consideramos que el simple descubrimiento de una clave ya supone la vulneración de un secreto. El informe del Consejo General del Poder Judicial a propósito de la reforma del 197.3 indicaba al respecto que no se tutela la intimidad y la privacidad con esta incorporación, sino el mero intrusismo informático, aunque lleva implícito el ánimo de descubrir secretos, pues la inclusión de barreras a un sistema informático demuestra la voluntad de que no sean accesibles a los demás.

Por otro lado, en cuanto a la consideración de los daños, hay que tener en cuenta todas las conductas realizadas en un intrusismo informático y sus consecuencias. Esto es, por un lado, que existe un daño evaluable económicamente en la medida en que la restauración del sistema informático tiene un coste, y además siendo que el autor tiende a borrar sus huellas, alterará o eliminará los registros del sistema. Todo ello sin perjuicio de que la privación a terceros del acceso a los servicios de la víctima puede conllevar pérdidas económicas, si bien esto más que daño sería perjuicio patrimonial, lo que difícilmente estaría cubierto en el ámbito penal. Con todo, junto a lo anterior habría que valorar la culpa de la víctima, pues hoy en día deben exigirse medidas de protección adecuadas para salvaguardar todo sistema informático, y especialmente si éste aloja datos de carácter personal.

Sin embargo, la reforma de estos delitos no va a quedar ahí. España ratificó el 20 de mayo de 2010 el Convenio del Consejo de Europa sobre Ciberdelincuencia de 2001 (Convenio de Budapest) , que precisamente obliga a llevar a cabo las reformas anteriores, pero también a tipificar como delito la producción, venta, obtención para su utilización, importación, difusión u otra

forma de puesta a disposición de: (a) dispositivos, incluidos los programas informáticos, diseñados o adaptados principalmente para la comisión de cualquiera de los delitos anteriores, y (b) una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático. Sin duda es un cambio importante, con la clara finalidad de abarcar todos los actos previos, con la salvedad de que deben estar encaminados a la comisión de dichos delitos, excluyéndose usos lícitos como la realización de pruebas autorizadas o la protección de un sistema informático. Pero también introduce la indeterminación de cuándo un dispositivo está diseñado o adaptado principalmente para llevar a cabo un acto de interceptación ilícita, de intrusismo informático o de daños en los sistemas.

Y, a pesar de todo, que una conducta no sea delito no significa que sea lícita. En todo caso existe un daño o un perjuicio en estos actos perseguible civilmente, pudiendo exigirse responsabilidad con menos limitaciones que en la legislación penal.

9.1. Delito de *hacking*[47]

El miedo a la amenaza de la delincuencia organizada y a los ataques terroristas, conocido argumento para llevar a cabo medidas drásticas, muchas veces pisoteando los derechos civiles, es lo que, aparentemente, ha motivado la Decisión Marco 2005/222/JAI , del Consejo de la Unión Europea, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, que impone a los Estados Miembros la obligación de modificar su legislación penal (antes del 16 de marzo de 2007) para dar cabida a una serie de conductas.

Las infracciones que contempla la Decisión Marco son las siguientes:

1) Acceso ilegal a los sistemas de información, definido como el acceso intencionado sin autorización al conjunto o a una parte de un sistema de información, es decir, el *hacking*, actualmente conducta atípica según el Código Penal español. Se deja al margen de los Estados regular si será perseguible sólo cuando se transgredan medidas de seguridad. Veremos por qué opta el legislador español. No se trata ya sólo de que el término *hacker* se esté prostituyendo,

47 PRENAFETA Rodríguez, Javier. *Consecuencias jurídicas de los ataques a sistemas informáticos*. 19-mar-2005. Tipo de obra: Literaria, Artículo

como se señalaba hace pocos días en Barrapunto, perdiendo su sentido original, sino que ahora se les considerará, directamente, delincuentes.

2) Intromisión ilegal en los datos, consistente en todo acto intencionado, cometido sin autorización, de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información. Actualmente podría entenderse regulado en el artículo 264.2 del Código Penal español como delito de daños. Nuestra regulación incluso va más allá, contemplando la comisión por imprudencia en los términos del artículo 267.

3) Intromisión ilegal en los sistemas de la información, que consiste en todo acto intencionado y sin autorización para obstaculizar o interrumpir, de manera significativa (he aquí un margen de discrecionalidad) el funcionamiento de un sistema de la información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos. La Decisión Marco regula esta conducta previamente a la anterior, aunque yo entiendo que en realidad constituye una figura agravada de aquélla en tanto que incluye un elemento volitivo (la intencionalidad del autor de obstaculizar o interrumpir el funcionamiento del sistema de la información). Como tal, tampoco está regulada en nuestro Código Penal.

La Decisión Marco prevé además, sin perjuicio de la responsabilidad penal de los infractores, la responsabilidad de las personas jurídicas que hayan resultado beneficiadas por dichas conductas, a las que se les impone un deber de vigilancia y control, que no se concreta. Las sanciones previstas para las personas jurídicas contemplan incluso la posibilidad de prohibición definitiva del ejercicio de actividades comerciales.

Se exceptúa de esta resposabilidad a los Estados, organismos públicos que ejerzan prerrogativas estatales y organizaciones internacionales de derecho público. Según esto, si un funcionario cometiera estas infracciones no sería responsable la entidad en la que presta sus servicios aún cuando ésta resultara beneficiada, que tampoco tendría por qué controlar lo que hace su personal.

10. Ámbito legal, normativas y disposiciones[48]

10.1. Objetivos

El objetivo principal del capítulo es la presentación del marco legal específico que regula las actividades informáticas en general. Estas leyes son las de Propiedad Intelectual, la de Protección de Programas de Ordenador y la de Protección de Datos.

También vamos a ver algunos conceptos sobre el delito informático: sus características, su tipología, el perfil del delincuente informático y la problemática de su investigación.

10.2. Introducción

Vamos a tratar las tres leyes que constituyen una base en nuestro ordenamiento jurídico, para la salvaguarda de aspectos relacionados con la información y los medios de tratamiento de la misma.

48 BERNAL Rafael, Lorente David, *Auditoría de Sistemas de Información*. Apuntes

En primer lugar estudiaremos la **Ley de Propiedad Intelectual**, con un espectro de aplicación más amplio, pero que engloba también la función informática. A continuación, trataremos la **Ley Orgánica de Protección de Datos de Carácter Personal** (L.O.P.D), y en tercer lugar, estudiaremos la **Ley sobre la Protección Jurídica de Programas de Ordenador,** que es la más específica en relación a la función Informática. Dentro de esta sección caracterizaremos la "piratería informática".

Finalmente, estudiaremos y caracterizaremos el **delito informático** y sus variedades.

10.3. Legislación sobre la Propiedad Intelectual

Esta ley se aprobó el 11 de Noviembre de 1987.
Mediante ésta ley se defiende el derecho de autor.
Esta ley regula:

Los derechos morales.
Los derechos de explotación.

La propiedad intelectual de una obra literaria corresponde al autor por el sólo hecho de su creación, y no es obligatorio inscribirse en el registro.

10.3.1. Ley de la Propiedad Intelectual

Autores y Modos de Creación
El autor es el que crea la obra literaria, artística ó científica, aunque también pueden ser titulares personas jurídicas cuando lo admita la ley.

Independiente: Una persona crea una obra y él es el autor.

En colaboración: Resultado unitario de la creación de varios autores, y queda clara cual ha sido la colaboración de cada uno, así, todos tienen derecho sobre la obra.

Colectiva: Participan varias personas, pero con iniciativa y bajo la dirección de una de ellas. Los derechos son de la persona que dirige la obra.

Compuesta: Alguien crea una obra incorporando otra obra creada con anterioridad. Hay que pedir permiso y pagar derechos por la obra.

Objeto de la Ley de Propiedad Intelectual

Son objeto de propiedad intelectual todas las creaciones originales literarias, artísticas ó científicas expresadas en cualquier medio o soporte.

Los Derechos Morales

El autor ostenta una serie de derechos morales, irrenunciables e intransmisibles:

Decidir si la obra ha de ser divulgada y de qué forma.
Si se ha de hacer con su nombre o con seudónimo.
Exigir el respeto a la integridad de la obra, a modificarla, a retirarla del comercio.
Acceder al ejemplar único de la obra si se halla en poder de otro.

Los Derechos de Explotación

1) Derecho de reproducción: Cualquier fijación de la obra sobre cualquier medio que permita la comunicación de la obra a otras personas y la copia de la obra.

2) Derecho de distribución: Poner a disposición del público la obra mediante alquiler, etc.

3) Derecho de comunicación pública: Realización de actos por los cuales muchas personas puedan tener acceso a la obra.

4) Derecho de transformación: Derecho a modificar la forma de la obra y de ésta saldría otra obra diferente.

Los derechos de explotación duran toda la vida del autor y 60 años después de su muerte.

Otros Derechos de Propiedad Intelectual

Derechos afines: Derechos de personas que no son los autores de la obra.

Ejemplo: director de orquesta.

Protección de los Programas de Ordenador mediante el Derecho Intelectual

La protección jurídica, no sólo protege al programa, sino el manual de uso, las sucesivas

versiones del programa, los programas derivados, y la documentación técnica.

La duración de los derechos de explotación de un programa será de 50 años. En el caso de la transmisión de los derechos de explotación, sólo se cede el uso del programa, no todo el programa. En éste caso, no se tiene derecho a nada, solamente a la copia de seguridad y a la introducción del programa en la memoria del ordenador.

10.4. Legislación sobre la Protección de Datos Personales

LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

10.4.1. Introducción

La Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD), tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar.

Su objetivo principal es regular el tratamiento de los datos y ficheros, de carácter personal, independientemente del soporte en el cual sean tratados, los derechos de los ciudadanos sobre ellos y las obligaciones de aquellos que los crean o tratan.

“La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.” (Cap. II Art. 18.4 Constitución Española)
2007 – RD1720 (Desarrolla LOPD)
1999 – LOPD, LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
RD994(Medidas Seguridad LORTAD), de 11 de junio, por el que se aprueba el reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.
1995 – Directiva 95/46/CE del Parlamento y el Consejo Europeo, de 24 de octubre de 1995, sobre protección de las personas en relación con el procesamiento de sus datos personales y el libre movimiento de dichos datos.
1992 – LORTAD LEY ORGÁNICA 5/1992, de 29 de octubre, de regulación del tratamiento

automatizado de los datos de carácter personal
1985 – Acuerdo de Schengen
1981 – Convenio nº 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal

Directiva 95/46/CE de la Unión Europea

Artículo 1. Objeto de la Directiva

1. Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.

Convenio 108 del Consejo de Europa

Articulo 1. Objeto y fin

El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona.

Acuerdo de Schengen

Artículo 94.1

.....

3. Respecto a las personas, los elementos introducidos serán como máximo los siguientes:
   a) El nombre y los apellidos; en su caso, los alias registrados
   b) Los rasgos físicos particulares, objetivos e inalterables
   c) La primera letra del segundo nombre
   d) La fecha y lugar de nacimiento
   e) El sexo
   f) La nacionalidad
   g) .....

10.4.2. LOPD

Qué supone la ley

Un RESPALDO para los ciudadanos contra la posible utilización indebida de sus datos personales.

Supone una GARANTIA de que los datos personales serán tratados con el RESPETO necesario.

Otorga un mecanismo de CONTROL al titular sobre sus propios datos.

Nacimiento de una Obligación:

Quien trata datos de carácter personal ha de cumplir con una serie de Obligaciones.

Protección frente a la indefensión:

Confiere una serie de derechos y garantías a los ciudadanos.

¿Por qué cumplir con la ley?

Desde un punto de vista legal: por la necesidad de garantizar un Derecho Fundamental a la Protección de datos.

Desde un punto de vista práctico: porque se establece un Régimen sancionador muy severo: Sanciones que van desde los 601,01 € hasta los 601.012,10 €.

Desde el punto de vista del empresario: Es una ocasión para realizar una auditoria y establecer un control de su sistema organizativo y técnico.

Objeto de la ley

“Datos de carácter personal que estén registrados en un fichero y a los que se les de un determinado tratamiento”.

Datos de Carácter Personal: Cualquier información relativa a personas física identificadas o

identificables.

Fichero: Cualquier conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permita la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

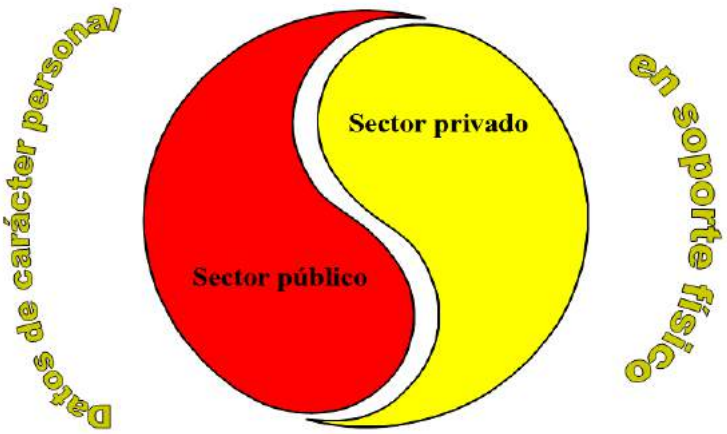
A quién afecta la ley

Responsable del fichero o tratamiento:
Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

Encargado del tratamiento:
Persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

Afectado o interesado:
Persona física titular de los datos que sean objeto del tratamiento.

Ámbito de aplicación



Normativa sobre seguridad

Real Decreto 1720/2007, de 21 de diciembre

Entró en vigor el 19 de abril de 2008

Deroga el anterior Real Decreto 994/1999 de 11 de junio de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

Dos objetivos:

Dotar de seguridad jurídica el ordenamiento en materia de protección de datos de carácter personal.

Contribuir al logro de una mayor claridad en la aplicación práctica.

Real Decreto 1720/2007, de 21 de diciembre

Se amplían y modifican las medidas y niveles de seguridad aplicables a cada tipo de fichero

Se regulan medidas de seguridad específicas en el tratamiento de datos en soporte papel

Se modelan y aseguran las medidas a adoptar en materia de información y obtención del consentimiento a la hora de la recogida de datos personales

Se dota de norma a la subcontratación del tratamiento de los datos de personas a terceros

Real Decreto 1720/2007, de 21 de diciembre

Se fijan los requisitos necesarios para las transferencias internacionales de datos de personas, dependiendo del país y receptor de los datos, así como establecer los niveles de seguridad

No se aplicará a:

Datos de personas jurídicas

Datos de personas físicas que presten sus servicios en personas jurídicas (datos exclusivos profesionales)

Datos de empresarios individuales que hagan referencia a su actividad (sin perjuicio de la aplicación de la Ley34/2002 Servicios Sociedad Información)

Objeto

El presente reglamento tiene por objeto el desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal (LOPD)

Real Decreto 1720/2007, de 21 de diciembre

Título VIII, establece las medidas de índole técnico y organizativo que los responsables de los tratamiento o los ficheros y los encargados de tratamiento han de implantar para garantizar la seguridad en los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de datos de carácter personal.

Entre estas medidas, se encuentra la elaboración de un documento que recogerá las medidas de índole técnica y organizativa acorde a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los datos de carácter personal.

Título VIII. Medidas de seguridad

Capítulo I. Disposiciones generales (arts. 79 - 87)

Capítulo II. Del documento de seguridad (art. 88)

Capítulo III. Medidas de seguridad aplicables a ficheros y tratamientos automatizados

Sección Primera. Medidas de seguridad de nivel básico (arts. 89 - 94)

Sección Segunda. Medidas de seguridad de nivel medio (arts. 95 - 100)

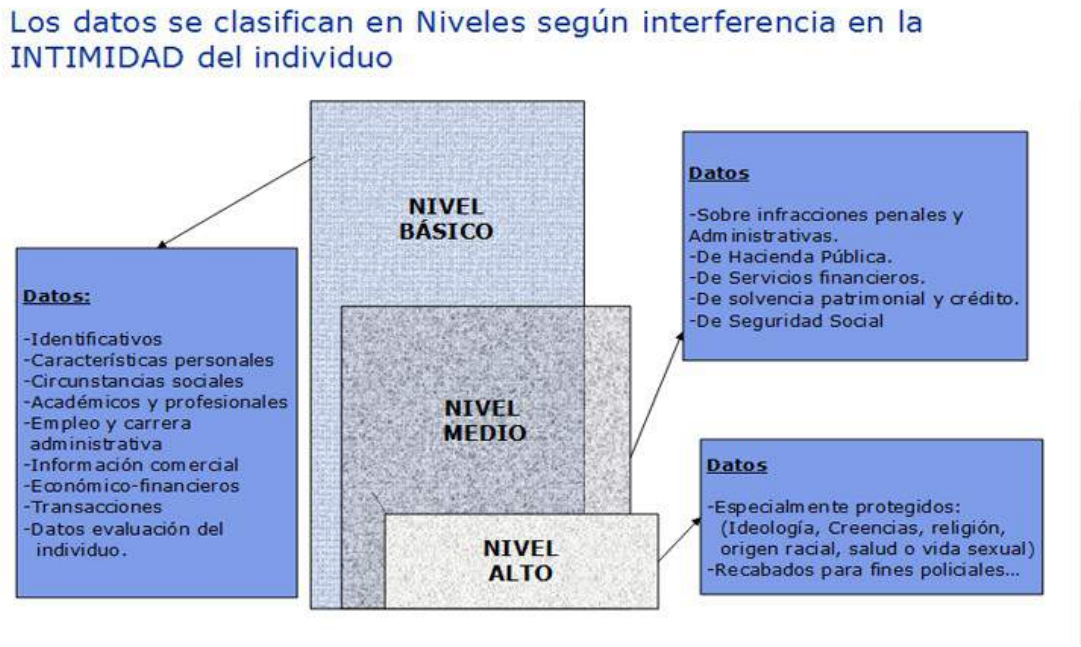
Sección Tercera. Medidas de seguridad de nivel alto (arts. 101 – 104)

Capítulo IV. Medidas de seguridad aplicables a ficheros y tratamientos no automatizados

Sección Primera. Medidas de seguridad de nivel básico (arts. 105 - 108)

Sección Segunda. Medidas de seguridad de nivel medio (arts. 109 - 110)

Sección Tercera. Medidas de seguridad de nivel alto (arts. 111 – 114)



10.5. Legislación sobre la Protección de Programas de Ordenador

10.5.1. Introducción

En Diciembre de 1993, el Parlamento español aprobó la transposición, al ordenamiento jurídico español, de la Directiva del Consejo de la CE del 14 de Mayo de 1991 sobre la protección jurídica de programas de ordenador.

La protección del programa informático, contaba ya en nuestro país con la cobertura legal de las disposiciones contenidas en la Ley de Protección Intelectual de 1987. Pero con ésta nueva ley, se incrementan y se hacen más eficaces las medidas para evitar la piratería informática.

10.5.2. Ley sobre la Protección Jurídica de Programas de Ordenador

Objeto de la Protección

Los programas y su documentación preparatoria recibirán la misma protección que las obras literarias, que se consideran creaciones intelectuales de su autor.

Titularidad de los Derechos

Será considerado autor del programa de ordenador, la persona o grupo de personas físicas que los hayan creado, o la persona jurídica que sea contemplada como titular de los derechos de autor en los casos expresamente previstos por la Ley de Propiedad Intelectual.

Cuando un trabajador asalariado cree un programa de ordenador, en el ejercicio de las funciones que le han sido confiadas o siguiendo las instrucciones de su empresario, la titularidad de los derechos económicos correspondientes al programa de ordenador así creado corresponderán exclusivamente al empresario salvo en pacto contrario.

Beneficiarios de la Protección

La protección se concederá a todas las personas físicas y jurídicas que cumplan los requisitos establecidos en la Ley de Propiedad Intelectual para la protección de los derechos de autor.

Duración de la Protección

Si el autor es una persona jurídica, la protección será durante toda la vida del autor y 50 años después de su muerte.

Si el programa de ordenador es una obra anónima o bajo seudónimo, el plazo de protección será de 50 años desde el momento en que se puso legalmente por primera vez a disposición del público.

Infracción de los Derechos

1) Los que pongan en circulación una o más copias de un programa de ordenador conociendo o pudiendo presumir su naturaleza ilegítima.

2) Quienes tengan con fines comerciales una o más copias de un programa de ordenador, conociendo o pudiendo presumir su naturaleza ilegítima. La adquisición de un programa de ordenador permite al comprador hacer una sola copia de seguridad.

3) Quienes pongan en circulación o tengan, con fines comerciales, cualquier medio, cuyo único uso sea facilitar la supresión o neutralización no autorizadas de cualquier dispositivo técnico utilizado para proteger un programa de ordenador.

10.5.3. Ventajas e inconvenientes de usar software original

VENTAJAS	INCONVENIENTES
✓ Aplicaciones fiables. ✓ Sistemas con soporte técnico. ✓ Completa y correcta formación. ✓ Protección contra virus. ✓ Seguridad y fiabilidad. ✓ Mayor eficiencia en su actividad.	✓ Virus. ✓ Falta de servicio. ✓ Falta de documentación de soportes técnicos. ✓ Falta de seguridad.

10.6. El delito informático

10.6.1. Introducción

Antes de empezar, quisiera recordar qué es un delito.
Según el Código Penal, en su art. 10, Son delitos o faltas las acciones y omisiones dolosas o imprudentes penadas por la Ley. De modo que hablaremos de delito siempre y cuando esté regulado por el Código Penal. (Es importante señalar que el Código Penal de 1995 y sus sucesivas reformas efectúan un fuerte avance en cuanto a la persecución de delitos informáticos se refiere. De hecho incluso hace alusiones a Internet. Destacar también que con la informática no aparecen delitos nuevos, pero sí nuevas formas de cometerlos). El delito informático es un tipo de delito nuevo y diferente muy complejo de prevenir y detectar.

La inexistencia generalizada de controles en los sistemas informáticos y en la información que procesan, es lo que permite que se produzcan los delitos informáticos.

Cuando un sistema se mecaniza, los usuarios asumen que el ordenador efectuará todos los controles necesarios para hacer el sistema seguro, así, disminuyen o desaparecen los controles

sobre las tareas previas y posteriores al proceso mecanizado, y es cuando se produce el fraude.

Ejemplo

En 1986, el Ministerio de Trabajo detectó por medio de un nuevo procedimiento de control de bajas, que desde hacía dieciocho meses se estaban pagando pensiones a 54.464 pensionistas fallecidos, cuya defunción no había sido comunicada por sus familiares, con lo cual, la ineficacia del control interno en los sistemas informáticos de la Seguridad Social nos costó a los contribuyentes la increíble cifra de TREINTA MIL MILLONES DE PESETAS. (180.303.631,31 Euros)

10.6.2. Características del delito informático

1. Concentración de la información. La tendencia a centralizar y consolidar toda la información corporativa en grandes bases de datos, sobre las que interaccionan multitud de usuarios, posibilita considerablemente el acceso a cualquier tipo de información, una vez se han penetrado las medidas de control de accesos que estén establecidas.

2. Ausencia de registros visibles. La posibilidad de descubrir un hecho fraudulento por simple inspección visual está completamente eliminada, al estar la información grabada en forma de impulsos eléctricos sobre soportes magnéticos, que no son directamente legibles por el ser humano.

3. Los programas y los datos pueden alterarse sin dejar rastro. En tanto que la manipulación de registros escritos es bastante difícil y suele dejar evidencias, la alteración de programas o datos grabados en soportes magnéticos puede hacerse sin dejar rastro, salvo que se hayan adoptado las adecuadas medidas de control.

4. Fácil eliminación de pruebas. Es extremadamente fácil, en caso de peligro, hacer desaparecer programas manipulados o ficheros completos de datos alterados, desde la consola del ordenador o desde un terminal tan sólo pulsando una tecla o emitiendo una instrucción de borrado, lo cual, posteriormente, puede hacerse pasar como un error fortuito.

5. Complejidad del entorno técnico. Incluso los sistemas más sencillos presentan una gran complejidad en términos de capacitación técnica. El usuario debe emplear el tiempo necesario para entender en detalle qué hace el sistema y cómo lo hace. Generalmente, y después de un corto tiempo, los usuarios comienzan a aceptar la integridad del sistema sin cuestionárselo,

especialmente si está diseñado para que la intervención humana sea mínima.

6. Dificultad para proteger los ficheros mecanizados. A diferencia de lo sencillo que resulta proteger físicamente archivos tradicionales, de tal forma que sólo sean utilizables por el personal autorizado, la protección de la información almacenada en soportes magnéticos es mucho más compleja.

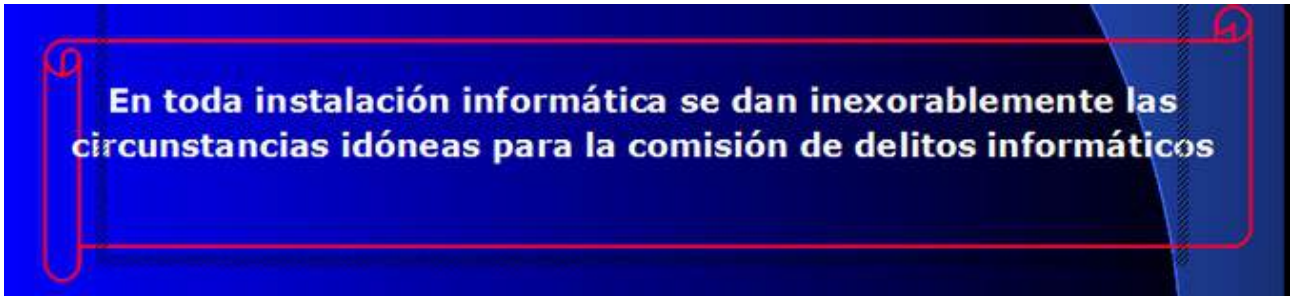
7. Concentración de funciones. El concepto de segregación de funciones incompatibles suele ser inexistente en los centros de proceso de datos, especialmente en los de tamaño medio y pequeño en los que priman los conceptos de funcionalidad y versatilidad del personal sobre el concepto de seguridad.

8. Carencia de controles internos en las aplicaciones. La inexistencia generalizada en los departamentos de análisis y programación, de metodologías de desarrollo de software que incluyan de forma estándar medidas de control interno y pistas de auditoría, en las nuevas aplicaciones, explica la extremada debilidad de éstas ante intentos de manipulaciones fraudulentas.

9. Controles ineficaces para el personal técnico. En general, puede afirmarse que la mayoría de los controles establecidos en las aplicaciones, o sobre los ficheros mecanizados, pueden ser fácilmente soslayados por técnicos informáticos de una cierta cualificación.

10. Dispersión territorial de los puntos de entrada al sistema. La mayor parte de los sistemas complejos, están diseñados sobre la filosofía de una fuerte descentralización, para acercar la informática al lugar donde está el usuario o donde se producen los datos de entrada, y curiosamente, mientras se establecen medidas de control de forma centralizada, éstas suelen ser inexistentes en la práctica en los puntos remotos de entrada al sistema.

11. Dependencia de redes públicas de transmisión de datos. Dado que todavía no existen líneas privadas, la previsión a medio plazo es que la totalidad de las comunicaciones se harán por redes públicas, es necesario considerar que dichas redes son compartidas por una multitud de usuarios, y no es posible establecer medidas de control sobre ellas.



10.6.3. Tipos de delitos

Básicamente el Código Penal español regula los siguientes tipos de delito relacionados con la informática:

- DELITOS **CONTRA LA PROPIEDAD INTELECTUAL** (CP arts. 270-272) O LA PROPIEDAD INDUSTRIAL (CP arts. 273-277 y CP arts. 298-304).

- DELITOS **CONTRA EL DERECHO A LA INTIMIDAD** (CP. arts. 197-201). INTERCEPTACIÓN DE COMUNICACIONES.

- DELITOS **CONTRA EL PATRIMONIO**: ESTAFAS, APROPIACIÓN INDEBIDA (CP arts. 252-254) Y FRAUDES (CP arts. 255,256).

- DELITOS DE **SABOTAJE INFORMÁTICO** (CP arts. 263-269, 346, 347, 351 y siguientes, 263, 264).

- DELITOS **CONVENCIONALES**. ESPIONAJE, ESPIONAJE INDUSTRIAL Y TERRORISMO INFORMÁTICO.

- DELITOS **DE MAL USO DE LA RED** (CYBERTORTS). USOS COMERCIALES NO ÉTICOS, ACTOS PARASITARIOS Y OBSCENIDADES.

- DELITOS **CONTRA LA LIBERTAD Y AMENAZAS** (CP arts. 169 y siguientes).

- DELITOS **CONTRA EL HONOR** (CP arts. 205-210). CALUMNIAS (CP art. 205) E INJURIAS (CP art. 208).

- DELITOS **CONTRA EL MERCADO Y LOS CONSUMIDORES**. REVELACIÓN DE SECRETOS (CP art. 278), PUBLICIDAD ENGAÑOSA (CP art. 282) Y FALSEDADES DOCUMENTALES (CP arts. 390 y siguientes, 395, 396 y 400).

- DELITOS **CONTRA LA LIBERTAD SEXUAL** (CP arts. 187, 189). PROVOCACIÓN SEXUAL Y PROSTITUCIÓN.

- DELITOS TRADICIONALMENTE DENOMINADOS "**INFORMÁTICOS**". ACCESO NO AUTORIZADO, DESTRUCCIÓN DE DATOS, CIBERTERRORISMO, INFRACCIÓN DE LOS DERECHOS DE AUTOR, INFRACCIÓN DEL COPYRIGHT DE BASES DE DATOS, INTERCEPTACIÓN DE E-MAIL, ESTAFAS ELECTRÓNICAS. TRANSFERENCIAS DE FONDOS, PHISING.

Quiero señalar, llegados a este punto, que además de los delitos mencionados, también pueden producirse infracciones de la Ley de Protección de Datos y de la Ley de Propiedad Intelectual. Siendo infracciones y no delitos, se castigan con sanciones generalmente económicas, y no con privación de la libertad, como puede ocurrir en los delitos.

10.6.4. Tipología del fraude informático

El fraude informático puede adoptar diversidad de formas, y el único límite viene dado por tres factores:

La imaginación del autor.

Su capacidad técnica.

Las deficiencias de control existentes en la instalación.

10.6.5. Ejemplos de fraudes informáticos (Parker)

10.6.5.1. Introducción de datos falsos

Es el método más sencillo y más utilizado habitualmente, consistente en manipular los datos antes ó durante su entrada al ordenador.

Un caso públicamente conocido de fraude cometido por este procedimiento ocurrió en Baltimore, Maryland, en Mayo de 1980, y fue cometido por Janet Blair, empleada de oficinas de la Seguridad Social. La Srta. Blair introducía desde su terminal inteligente, conectado con el potente ordenador central, transacciones falsas para producir la emisión de cheques fraudulentos, consiguiendo por este procedimiento defraudar un total de 102.000 dólares. La Srta. Blair fue acusada y condenada a 8 años de prisión federal y al pago de una multa de 500 dólares.

10.6.5.2. El Caballo de Troya

Consiste en introducir dentro de un programa de uso habitual una rutina o conjunto de instrucciones, por supuesto no autorizadas, para que dicho programa actúe en ciertos casos de una forma distinta a como estaba previsto.

A finales de 1984 en nuestro país, un ex-empleado del centro de proceso de datos de una entidad financiera, introdujo una rutina dentro del programa de tratamiento de cuentas corrientes para que un determinado día, aproximadamente seis meses después de haber cesado el empleado en su trabajo, y a una hora determinada, autorizase el pago de un talón de una cuenta concreta sin consultar el saldo. Posteriormente, la rutina borraba parte del programa modificado con lo cual se eliminaba el rastro de la comisión del delito. El fraude fue de unos 10 millones y no se pudo probar la autoría del mismo y por lo tanto no se pudo denunciar.

10.6.5.3. La técnica del Salami

Consiste en introducir o modificar unas pocas instrucciones en los programas para reducir sistemáticamente en unos pequeños céntimos las cuentas corrientes, los saldos con acreedores, etc. transfiriéndolos a una cuenta corriente, proveedor ficticio, etc., que se abre con un nombre supuesto y que obviamente controla el defraudador.

En una importante compañía norteamericana, un programador que tenía bajo su responsabilidad el sistema mecanizado de personal, introdujo en el mismo unas pequeñas modificaciones, que afectaban a los cálculos del plan de inversiones para los empleados que la dirección de la empresa tenía establecido. La compañía había acordado con sus empleados que cada mes se les retendría una pequeña cantidad de sus salarios para invertirlos en valores mobiliarios. Lo único que tuvo que hacer el programador fue quitar un pequeño porcentaje de las fracciones de acciones propiedad de cada empleado y transferirlo a su propia cuenta. De esta forma antes de ser descubierto, el programador defraudó 400.000 dólares.

10.6.5.4. Superzapping

Normalmente, los sistemas informáticos complejos poseen unos programas de acceso universal que permiten entrar en cualquier punto del sistema en caso de emergencia. El *superzapping*

consiste en usar estos programas sin autorización.

Un conocido caso de fraude por éste método ocurrió en un banco de New Jersey, con el resultado de una pérdida económica de 128.000 dólares. El autor del fraude fue el jefe de explotación del CPD del banco, quien, en virtud de la facilidad que tenía para utilizar un programa de acceso universal, comenzó a desviar fondos desde las cuentas de diferentes clientes a las de unos amigos, sin que quedara en el ordenador ninguna evidencia de las modificaciones efectuadas en los saldos de las cuentas y por tanto sin que nadie en el bando se apercibiera de lo que estaba sucediendo. El fraude se descubrió merced a la reclamación que hizo uno de los clientes afectados, lo cual motivó una investigación que acabó con la detención y el procesamiento del autor.

10.6.5.5. Puertas falsas

Utilización de las "interrupciones" en la lógica de un programa, durante la fase de desarrollo para su depuración, y uso posterior para fines delictivos.

Tal es el caso de unos ingenieros de una fábrica de automóviles de Detroit, que descubrieron una puerta falsa en una red de servicio público de time-sharing de Florida. Después de una serie de intentonas, consiguieron hacerse con una clave de acceso de alto nivel, según parece la del propio presidente ejecutivo de la compañía de time-sharing, y utilizándola pudieron apoderarse de diferentes programas clasificados como reservados y archivados en el ordenador bajo la denominación de "secretos comerciales", al tiempo que utilizaban el servicio de la red sin cargos económicos. Como suele ser tradicional en los fraudes informáticos fueron circunstancias accidentales las que originaron el descubrimiento de los hechos, sin que nunca se llegara a saber cuántas personas y en cuántas ocasiones pudieron hacer lo mismo.

10.6.5.6. Bombas lógicas

Programas que se ejecutan en un momento específico, o periódicamente, cuando se cumplan determinadas condiciones. Se suelen utilizar cómo venganza, sin otro beneficio que el placer de perjudicar.

Una forma bastante extendida de utilizar ésta técnica es la que realizan muchos fabricantes de paquetes de software para asegurarse el cobro de los mismos. Consiste en programar unas instrucciones que comprueban la fecha del día, lo que permite que los productos tengan una fecha de caducidad oculta que ha introducido el fabricante del producto al instalarlo en el ordenador del cliente y que no será eliminada o prorrogada hasta que el cliente pague lo que el vendedor le reclama.

10.6.5.7. Ataques asíncronos

Consiste en aprovechar el funcionamiento asíncrono del sistema operativo.

Uno de los típicos fraudes de este tipo es el que puede producirse en los puntos de recuperación del

sistema. Si entre dos puntos de recuperación del sistema (cada 5 o 10 minutos graban en soporte magnético el estado del programa) se provoca voluntariamente una caída del sistema, y se manipulan los parámetros en que se va a apoyar el sistema operativo para volver a arrancar, es obvio que las condiciones en que se ejecutará el programa serán distintas de las que deberían ser, por lo que sus resultados serán fraudulentos o cuando menos erróneos.

10.6.5.8. Recogida de información residual

Consiste en aprovechar los descuidos de los usuarios o los técnicos informáticos, para obtener información que ha sido abandonada sin ninguna protección como residuo de un trabajo real efectuado con autorización.

Una de las formas más estúpidamente simples de que se produzca este delito es cuando se preparan ficheros spool para impresora diferida, ya que en ellos queda preparada la información que posteriormente se imprimirá sin ningún tipo de protección, siendo fácilmente recuperable sin necesidad de utilizar ningún identificador, clave de acceso o cualquier otro procedimiento se seguridad, a pesar de que en muchos casos se trata de información altamente confidencial.

10.6.5.9. Filtración de datos

Sustracción de información confidencial de un sistema.

Un empleado ejemplar había sido durante años aquel hombre, honrado a carta cabal que, después de media vida trabajando en una entidad bancaria sita en Barcelona se vio obligado, por circunstancias ajenas a su voluntad, a sustraer información confidencial sobre los clientes de la entidad para venderla y así poder sufragar los gastos que le originaba su hijo drogadicto, el cual había llevado a la familia a la ruina.

10.6.5.10. Trasiego de personas

Conseguir acceder a áreas controladas por medios electrónicos y mecánicos.

Unos estudiantes de una universidad de U.S.A. mandaron una comunicación en papel oficial a todos los usuarios del ordenador de la universidad, advirtiéndoles que el número de conexión al ordenador había sido cambiado y facilitando el nuevo número, el cual correspondía en realidad al ordenador personal de los estudiantes, que estaba programado para responder exactamente igual que lo hacía el equipo de la universidad. En consecuencia, y dado que lo primero que pedía el sistema al conectarse eran las claves de identificación, el equipo de los estudiantes recogía la clave y respondía que hasta nueva orden volvieran a llamar al número antiguo. Esto les permitió hacerse con las claves de todos los usuarios, las cuales utilizaron para divertirse descubriendo todos los secretos de la universidad, hasta que, descubierta la situación, todas las claves fueron cambiadas.

10.6.5.11. Simulación y modelado de delitos

Utilizar el ordenador cómo instrumento para planificar y controlar un delito, utilizando técnicas de simulación y modelo.

Un contable que antes de efectuar el fraude que tenía pensado, contrató los servicios de una oficina de servicios con el fin de montar una copia de la contabilidad de la empresa para la que trabajaba, lo que le permitió estudiar detenidamente las repercusiones de los asientos fraudulentos que pensaba realizar para embolsarse una sustancial cantidad de dinero.

10.6.5.12. Pinchado de líneas

Intervención de las líneas de comunicación para acceder o manipular los datos que son transmitidos.

10.6.5.13. Hoax

Son bulos e historias inventadas, que no son más que eso, mentiras solapadas en narraciones cuyo fin último es destapar el interés del lector o destinatario. Dichas comunicaciones pueden tener como finalidad última: Conseguir dinero o propagar un virus.

"Salvad a Willy:

Willy sigue vivo, la última fotografía que se le hizo data de una semana. Los veterinarios y especialistas en animales en extinción han confirmado que, o se actúa rápido o Willy morirá. Si Usted desea ver a Willy volviendo a surcar los mares del mundo, no dude en aportar su imprescindible ayuda, bien con mensajes de apoyo, bien mediante su aportación económica al número de cuenta que se adjunta.
Pásalo a todos sus amigos."

10.6.5.14. Pirámides de valor

El objetivo es captar a usuarios, con la única finalidad de que lean el cuerpo del mensaje y se crean que pueden conseguir grandes comisiones por no hacer nada.

"Consiga aumentar su beneficio en poco tiempo"

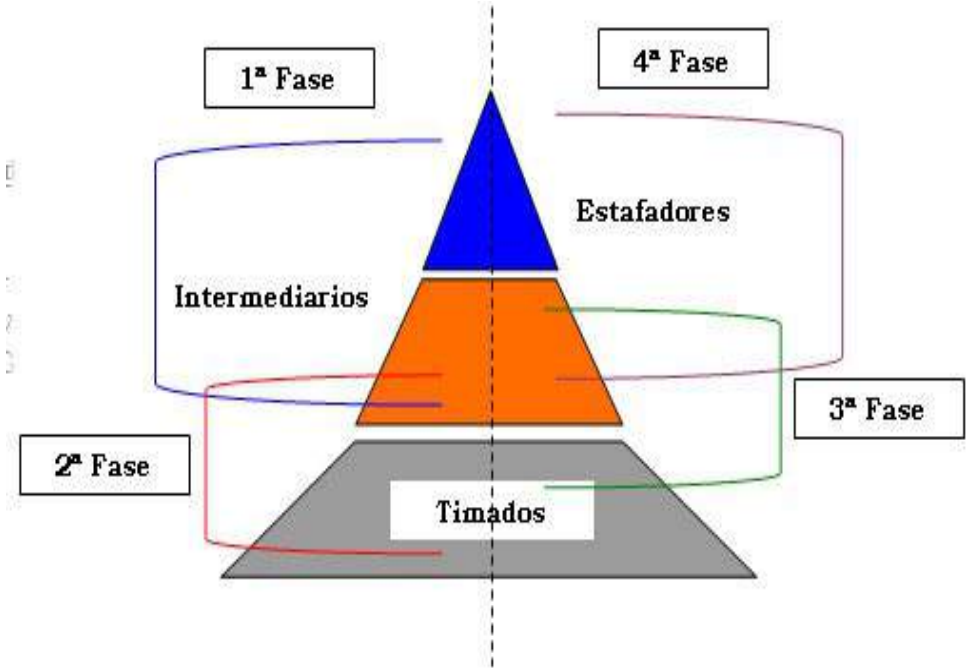
10.6.5.15. Phising

El phishing es una técnica de captación ilícita de datos personales (principalmente relacionados con claves para el acceso a servicios bancarios y financieros) a través de correos electrónicos o páginas web que imitan/copian la imagen o apariencia de una entidad bancaria/financiera (o cualquier otro tipo de empresa de reconocido prestigio).


https://boveda.banamex.com.mx/serban
Banamex
BancaNet
Con sólo un
click...
Advertencia
Esta PC NO cuenta con la herramienta Anti-intruses instalada
Contáctanos
Banamex siempre a la vanguardia en tecnología de seguridad,
pone a tu disposición, sin costo adicional, una herramienta para proteger tu computadora
del Vandalismo y Espionaje Cibernético, servicio proporcionado por la
empresa internacional Hauri, líder en el ramo.
Más Información
Compromiso de Seguridad


http://boveda.bbanamex.com
Banamex
BancaNet
Con sólo un
click...
Advertencia
Esta PC NO cuenta con la herramienta Anti-intruses instalada
Contáctanos
Por tu Seguridad
Nuevas Operaciones en BancaNet

10.6.5.16. Scam



10.6.6. El delincuente informático

Los delincuentes informáticos suelen ser empleados de confianza de la empresa, que tienen acceso al sistema informático y conocen suficientemente sus debilidades como para permitirle realizar el hecho delictivo.

Según las estadísticas, más del 90% de los delitos son cometidos por los usuarios del sistema, y los otros pocos por técnicos informáticos. Pero se cree que esto es debido a que los fraudes cometidos por informáticos nunca llegaron a descubrirse, por su sofisticación técnica y a que una vez realizados, los rastros fueros adecuadamente borrados.

Como norma general, todos los autores de delitos informáticos carecen de antecedentes penales.

10.6.7. La investigación del delito informático

El primer problema consiste en determinar, si cuando se descubren irregularidades en el sistema, si realmente se ha cometido un delito y luego es cuando realmente comienzan los problemas al

tratar de establecer el tipo de delito, cómo, cuando y dónde se realizó, sus consecuencias previsibles, la identidad del posible autor, y las posibles pruebas que pudieran encontrarse como consecuencia de la investigación.

Otro problema con que se encuentra el investigador informático es conseguir reproducir las circunstancias existentes cuando se produjo el delito, lo que en algunos casos puede ser totalmente determinante para establecer las responsabilidades.

Las técnicas de Auditoria de sistemas y los conocimientos de control interno son una herramienta de excepcional valor para la investigación, ya que permiten analizar con extrema rapidez las debilidades de control interno que presentan los sistemas, investigar en los registros de transacciones cualquier anormalidad que exista, e identificar las evidencias que puedan utilizarse como pruebas de la acusación.

10.6.8. Un futuro preocupante

Se considera que en la situación actual, la posibilidad de que el autor de un delito informático resulte condenado es de una entre veintisiete mil, y ello es debido a tres circunstancias clave:

1. La casi total ausencia de medidas de seguridad.
2. La falta de una legislación adecuada.
3. La gran inexperiencia existente para investigar los fraudes informáticos y reunir pruebas que puedan inculpar a sus autores.

Existen tres factores esenciales que pueden condicionar de forma absoluta el futuro de los delitos informáticos:

1. La incorporación de nuevos avances tecnológicos al trabajo diario sin haber medido previamente sus repercusiones sobre las condiciones de seguridad.
2. La paulatina constatación, por parte de las personas que trabajan en contacto con los sistemas informáticos, de lo fácil que es defraudar utilizando las deficiencias de los sistemas y la escasa probabilidad de ser descubierto y castigado.
3. La entrada de organizaciones criminales profesionales en un campo delictivo tan prometedor como el de los delitos informáticos.

11. Resumen[49]

Investigar el delito desde cualquier perspectiva es una tarea compleja; de eso no hay duda. Las dificultades que surgen al tratar de aplicar el método científico a la Delincuencia Transnacional y al Crimen Organizado en buena parte ya fueron establecidas en estudios anteriores, pero enfrentar este tipo de delincuencia a todo nivel es la tarea a la que se ve avocada le Ministerio Público por mandato constitucional y por disposición legal. Ahora bien el fenómeno descrito en los últimos tiempos ha tenido un avance significativo tomando en cuenta la manifestación de la globalización, la cual no solo ha tenido beneficios, sino también ha contribuido a la masificación de esta clase de delitos y tecnificado a otra clase de cómo son los llamados Delitos Informáticos.

Como escribe Albanese, citado por Carlos Resa, "el crimen organizado no existe como tipo ideal, sino como un "grado" de actividad criminal o como un punto del 'espectro de legitimidad". En este contexto es el crimen organizado que a través de los años se ha ido transnacionalizando su actividad y por ello se habla de Delincuencia Transnacional.

Dentro de esta definición de crimen organizado, la gama de actividades que puede ejecutar un determinado grupo de crimen organizado puede ser extensa, variando en cada caso según diversas variables internas y externas a la organización, y combinar uno o más mercados, expandiéndose asimismo por un número más o menos limitado de países, aunque en tiempos

49 ACURIO del Pino, Santiago. *Delitos Informáticos: Generalidades*. Apuntes

recientes existe una fuerte tendencia a la concentración empresarial en cada vez menos grupos de un mayor número de campos de la ilegalidad. Su repertorio de actividades incluye el delito de cuello blanco y el económico (en donde se encontrarían los Delitos Informàticos), pero supera a éste último en organización y control, aunque los nexos de unión entre ambos modelos de delincuencia tienden a fusionarse y el terrorismo y el ciberterrorismo pueden llegar a formar parte de sus acciones violentas en ciertas etapas o momentos. En un inventario amplio, las actividades principales de las organizaciones criminales, en suma, abarcan la provisión de bienes y servicios ilegales, ya sea la producción y el tráfico de drogas, armas, niños, órganos, inmigrantes ilegales, materiales nucleares, el juego, la usura, la falsificación, el asesinato a sueldo o la prostitución; la comercialización de bienes lícitos obtenidos por medio del hurto, el robo o el fraude, en especial vehículos de lujo, animales u obras de arte, el robo de identidad, clonación de tarjetas de crédito; la ayuda a las empresas legítimas en materias ilegales, como la vulneración de las normativas medioambientales o laborales; o la utilización de redes legales para actividades ilícitas, como la gestión de empresas de transporte para el tráfico de drogas o las inversiones inmobiliarias para el blanqueo de dinero. Entre aquellas organizaciones que pueden considerarse como típicamente propias del crimen organizado, practicando algunas de estas actividades, se encuentran, dentro de un listado más o menos extenso, las organizaciones dedicadas casi exclusivamente al tráfico de drogas a gran escala, ya sean propias de los países europeas o se generen en países latinoamericanos, del sudeste y el sudoeste asiático, la Mafia italiana en su proceso de expansión mundial que ya se inició hace décadas, las YAKUZA japonesas, las TRIADAS chinas y, en última instancia, ese magma que constituye el crimen organizado en Rusia y en otros países del Este europeo, y ahora existo otro grupo que a entrado a la escena del crimen organizado transnacional son los llamados CRAKERS, los verdaderos piratas informáticos, que a través del cometimiento de infracciones informáticas, han causado la perdida de varios millones de dólares, a empresas, personas y también a algunos estados.

Ahora en bien en el tema que nos interesa, en la actualidad las computadoras se utilizan no solo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio eficaz para obtener y conseguir información, lo que las ubica también como un nuevo medio de comunicación. Según el diccionario de la Real Academia de la Lengua Española, informática es el "conjunto de técnicas empleadas para el tratamiento automático de la información por medio de sistemas computacionales".

La informática está hoy presente en casi todos los campos de la vida moderna. Con mayor o menor rapidez todas las ramas del saber humano se rinden ante los progresos tecnológicos, y comienzan a utilizar los sistemas de información, para ejecutar tareas que en otros tiempos realizaban manualmente. Vivimos en un mundo que cambia rápidamente. Antes, podíamos tener

la certeza de que nadie podía acceder a información sobre nuestras vidas privadas. La información era solo una forma de llevar registros. Ese tiempo ha pasado, y con él, lo que podemos llamar intimidad. La información sobre nuestra vida personal se está volviendo un bien muy cotizado por las compañías del mercado actual. La explosión de las industrias computacionales y de comunicaciones ha permitido la creación de un sistema, que puede guardar grandes cantidades de información de una persona y transmitirla en muy poco tiempo. Cada vez más y más personas tienen acceso a esta información, sin que las legislaciones sean capaces de regularlos.

Los progresos mundiales de las computadoras, el creciente aumento de la capacidad de almacenamiento y procesamiento, la miniaturización de los chips de las computadoras instalados en productos industriales, la fusión del proceso de la información con las nuevas tecnologías de comunicación, así como la investigación en el campo de la inteligencia artificial, ejemplifican el desarrollo actual definido a menudo como la "era de la información", a lo que con más propiedad, podríamos decir que más bien estamos frente a la "ERA DE LA INFORMÁTICA".

Por tanto, abordar el estudio de las implicaciones de la informática en el fenómeno delictivo resulta una cuestión apasionante para quien observa el impacto de las nuevas tecnologías en el ámbito social. Efectivamente, el desarrollo y masificación de las nuevas tecnologías de la información han dado lugar a cuestiones tales como el análisis de la suficiencia del sistema jurídico actual para regular las nuevas posiciones, los nuevos escenarios, en donde se debaten los problemas del uso y abuso de la actividad informática y su repercusión en el mundo contemporáneo.

Es por esta razón, que paralelamente al avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, han surgido una serie de comportamientos disvaliosos antes impensables y en algunos casos de difícil tipificación en las normas penales tradicionales, sin recurrir a aplicaciones analógicas prohibidas por el principio de legalidad.

La doctrina ha denominado a este grupo de comportamientos, de manera genérica, «delitos informáticos, criminalidad mediante computadoras, delincuencia informática, criminalidad informática».

En efecto, tratándose del sistema punitivo, se ha suscitado una ingente discusión en cuanto a la vocación de los tipos existentes para regir las nuevas situaciones, que el uso y abuso de los sistemas computacionales han logrado con los llamados delitos informáticos o también llamada criminalidad informática. Lo anterior tiene especial relevancia si consideramos los principios

informadores del derecho penal, los que habrán de tenerse a la vista en todo momento. En efecto, no basta en este caso la "intuición" en cuanto a que se estima que una determinada conducta podría ser punible, el derecho penal exige una subsunción exacta de la conducta en la norma penal para que recién se esté en presencia de un "hecho que reviste carácter de delito", que autoriza su investigación.

En nuestro país nos encontramos con que el ordenamiento jurídico en materia penal, no ha avanzado en estos últimos tiempos a diferencia de otras legislaciones, para darnos cuenta de esto simplemente debemos recordar que nuestro actual código penal es del año de 1938 y que de esa fecha a la actualidad han pasado más de 65 años, por tanto es necesario para enfrentar a la llamada criminalidad informática que los tipos penales tradicionales sean remozados, sean actualizados para así consolidar la seguridad jurídica en el Ecuador, ya que el avance de la informática y su uso en casi todas las áreas de la vida social, posibilita, cada vez más, el uso de la computación como medio para cometer delitos. Esta clase de conductas reprochables resultan en la mayoría de los casos impunes, debido a la falta de conocimiento y preparación de los organismos de administración de justicia y los cuerpos policiales que no poseen las herramientas adecuadas para investigar y perseguir esta clase de infracciones.

En este orden de ideas, y al verse la posibilidad, que por medio del uso indebido de los sistemas informáticos o telemáticos se dé paso a la manipulación de sistemas de hospitales, aeropuertos, parlamentos, sistemas de seguridad, sistemas de administración de justicia, etc. Nos permiten imaginar incontables posibilidades de comisión de conductas delictivas de distintas características, por eso es necesario que el Ministerio Público en cumplimiento de su deber constitucional y legal instruya y facilite las herramientas necesarias a los Ministros Fiscales, Agentes Fiscales y personal de Apoyo a fin de combatir esta clase de comportamientos delictivos que afectan directamente a la sociedad ecuatoriana en su conjunto.

Esta dependencia de la Sociedad de la Información a las nuevas tecnologías de la información y de las comunicaciones (TIC), hace patente el grave daño que los llamados delitos informáticos o la delincuencia informática pueden causar a nuestro nuevo estilo de vida, la importancia que cobra la seguridad con la que han de contar los equipos informáticos y las redes telemáticas con el fin de poner obstáculos y luchar con dichas conductas delictivas, y la necesidad de tipificar y reformar determinadas conductas, a fin de que esta sean efectiva y positivamente perseguidas y castigadas en el ámbito penal.

Es en este orden de cosas que Augusto Bequai, en su intervención Computer Related Crimes en el Consejo de Europa señala que: "Si prosigue el desorden político mundial, las redes de cómputo

globales y los sistemas de telecomunicaciones atraerán seguramente la ira de terroristas y facinerosos. …

Las guerras del mañana serán ganadas o perdidas en nuestros centros de cómputo, más que en los campos de batalla. ¡La destrucción del sistema central de una nación desarrollada podría conducir a la edad del oscurantismo!. … En 1984, de Orwell, los ciudadanos de Oceanía vivían bajo la mirada vigilante del Hermano Grande y su policía secreta. En el mundo moderno, todos nos encontramos bajo el ojo inquisidor de nuestros gigantes sistemas computacionales. En occidente, la diferencia entre el Hermano Grande y nuestra realidad es la delicada fibra política llamada democracia; de colapsarse ésta, el edificio electrónico para una implantación dictatorial ya existe. … La revolución de la electrónica y la computación ha dado a un pequeño grupo de tecnócratas un monopolio sobre el flujo de información mundial. En la sociedad informatizada, el poder y la riqueza están convirtiéndose cada vez más en sinónimos de control sobre los bancos de datos. Somos ahora testigos del surgimiento de una elite informática".

La reseña casi profética hecha por Bequai, es una visión aterradora que de lo que podría suceder y de hecho está sucediendo en estos momentos, por lo tanto si los países y las naciones no se preparan adecuadamente para contrarrestar a la criminalidad informática, podrían sucumbir ante el avance incontrolable de este fenómeno.

A este respecto el Profesor español Miguel Ángel Davara señala que: "La intangibilidad de la información como valor fundamental de la nueva sociedad y bien jurídico a proteger; el desvanecimiento de teorías jurídicas tradicionales como la relación entre acción, tiempo y espacio; el anonimato que protege al delincuente informático; la dificultad de recolectar pruebas de los hechos delictivos de carácter universal del delito informático; las dificultades físicas, lógicas, y jurídicas del seguimiento, procesamiento y enjuiciamiento en estos hechos delictivos; la doble cara de la seguridad, como arma de prevención de la delincuencia informática y, a su vez, como posible barrera en la colaboración con la justicia. Todas ellas son cuestiones que caracterizan a este nuevo tipo de delitos y que requieren –entre otras- respuestas jurídicas. Firmes primeros pasos ya que se están dando a niveles nacionales, quedando pendiente una solución universal que, como todo producto farmacológico que se precie, se encuentra en su fase embrionaria de investigación y desarrollo".

Nuestro país en este sentido no puede quedar a la saga de los otros países y debe empezar a tomar todas las acciones y todas las medidas necesarias, y prepararse para el futuro y así no quedar al margen de situaciones que podrían en forma definitiva terminar con la sociedad de la información ecuatoriana, en este sentido el presente trabajo pretende ser un aporte a la escasa o

inexistente doctrina, que en el campo del Derecho Penal existe en nuestro país con respecto a los llamados Delitos Informáticos.

12. Conclusiones

Tras el estudio detenido y la investigación, así como búsqueda y filtraje de información de la temática que nos ocupa, las conclusiones que se desprenden son bastante obvias. El mundo avanza, las tecnologías avanzan, la informática avanza. Y todo esto se hace a una relativa gran velocidad. La informática avanza de forma positiva, pero también de forma negativa. He ahí los *crackers*, o los piratas de software, por ejemplo.

Por otra parte, el mundo está regulado por leyes. El mundo de las leyes siempre ha sido conflictivo y, en muchas ocasiones, ambiguo. Hablamos de la legislación en general. Estos dos factores se extienden al mundo de la informática de una manera incremental. Este incremento se produce por la diferencia de velocidad a la que progresan las tecnologías de la información, y la lentitud y en ocasiones poca eficacia con que cambian, se reestructuran, o se crean nuevas leyes que atañen a estas tecnologías. De hecho, casos judiciales semejantes en ocasiones dan lugar a sentencias distintas, cuando hablamos de juicios de carácter informático. Nos encontramos con un tema peliagudo, dos mundos que deben ser conectados poco a poco, de manera que todo el avance en tecnologías de información sea regulado por las leyes que hemos tratado en este proyecto.

13. Palabras clave

Hacking, *cracker*, *ciberdelito*, legislación, deontología.

14. Anexos

Se encuentran adjuntos los siguientes documentos:

1. **Web de *Hacking y Repercusiones Legales de la Informática*** *(realizada por el mismo autor que este proyecto). Incluye, además de un subconjunto de la información presentada en estas memorias: vídeos, libros, noticias, artículos, autos, sentencias y bibliografía por secciones.*

2. GIMENEZ Solano, Vicente Miguel; Iranzo Martínez, Manuel; et. Alt. ***Los Virus Informáticos.*** Asignatura: Auditoría de Sistemas de Información. ETSINF 2011

3. Diversas **prácticas** de la asignatura: Deontología y Aspectos Legales de la Informática.

15. Bibliografía

Libros y artículos

DE MIGUEL, María del Rosario y Juan Vicente Oltra. *Deontología y aspectos legales de la informática: cuestiones éticas, jurídicas y técnicas básicas*. Valencia : Ed. UPV, 2007. ISBN 978-84-8363-112-6.

GREGORY, Peter. *Computer Viruses for Dummies*. Indianapolis, Indiana: Wiley Publishing, Inc.ISBN: 0-7645-7418-3.

HERNÁNDEZ, Claudio. *Hackers: Los piratas del Chip y de Internet*. 1999

LEVY, Steven. *Hackers*. Capítulo: *La ética del hacker. Ed. Penguin, 2001*

MALAGÓN, Constantino. *Hacking ético*. Universidad Nebrija. Madrid.

PRENAFETA Rodríguez, Javier. *Consecuencias jurídicas de los ataques a sistemas informáticos.* Identificador: 1010087527283. 08-oct-2010 1:07 UTC. Tipo de obra: Literaria, Artículo.

PRENAFETA Rodríguez, Javier. *Consecuencias jurídicas de los ataques a sistemas informáticos.* 19-mar-2005. Tipo de obra: Literaria, Artículo.

Apuntes

ACURIO del Pino, Santiago. *Delitos Informáticos: Generalidades*. Apuntes.

BERNAL Rafael, Lorente David, *Auditoría de Sistemas de Información*. Apuntes.

PFC's

GIJÓN, Jesús. *Hackers, crackers y sus implicaciones sociales y mediáticas.* Valencia UPV.

Recursos de Internet (se encuentran descargados todos en la web anexada)

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Richard_Stallman, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Dennis_Ritchie, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Ken_Thompson, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Brian_Kernighan, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/John_Draper, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Paul_Baran, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://en.wikipedia.org/wiki/Gene_Spafford, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://en.wikipedia.org/wiki/Mark_Abene, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://en.wikipedia.org/wiki/Penet_remailer, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Wietse_Venema, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Kevin_Mitnick, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Kevin_Poulsen, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://en.wikipedia.org/wiki/Justin_Tanner_Petersen, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Vladimir_Levin, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Hacker, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Ingenieria_Social, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Top_Manta, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Virus, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Troyanos, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Spam, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Irc, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Unix, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Antivirus, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Mit, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Tech_Model_Railroad_Club, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/TX-0, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/PDP-10, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Laboratorios_Bell, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Plan_9_from_Bell_Labs, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Bluebox, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/Dan_Farmer, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/COPS, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://es.wikipedia.org/wiki/TCP_Wrapper, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://en.wikipedia.org/wiki/DEF_CON, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://en.wikipedia.org/wiki/Tsutomu_Shimomura, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://en.wikipedia.org/wiki/ILoveYou, Agosto/2011

http://www.wikipedia.org, Wikipedia, http://en.wikipedia.org/wiki/Pacific_Bell, Agosto/2011

Vídeos (se encuentran descargados todos en la web anexada)

Historia Secreta de los Piratas Informáticos
Duración: 40'

Hackers del Espacio
Duración: 52'

Hackers: Heroes o Delincuentes
Duración: 45'

Ciberguerrilla: Hackers, Piratas y Guerras Secretas
Duración: 52'

En Busca de Hackers
Duración: 60'

Hacktivistas: Los Agitadores de la Red
Duración: 105'

The History of Hacking
Duración: 50'