PRINCIPALES SUJETOS AGENTES EN EL UNDERGROUND, SU DETERMINACIÓN E IDENTIFICACIÓN.

Autor: Jaime Araujo Ulco.
Procedencia: Perú

Al encontrarnos en el siglo XXI, el conocimiento se ha convertido en la única fuente de ventaja competitiva, pero solo este recurso humano se podrá emplear de una forma apropiada cuando existan condiciones debidamente calificadas.

Como es de suceder entre la información y el conocimiento existe una estrecha relación, presentándose como base de conocimiento la información, pero a su vez el conocimiento es fuente de información. Es por ello que no toda información se convierte automáticamente en conocimiento. Es decir el conocimiento requiere de cierto grado de razonamiento y enjuiciamiento que organiza la información mediante su comparación y clasificación, para ello es necesario un ejercicio interactivo sujeto-objeto del conocimiento, en el cual se debe asumir una posición crítica y creativa, con el propósito de generar nuevos conocimientos.

El conocimiento puede ser fuente creadora, así como también puede convertirse en un medio de destrucción. Esto nos plantea un reto de búsqueda de nuevos paradigmas, en los cuales el conocimiento se ponga al servicio de la sociedad. Hoy nos encontramos ante una verdadera revolución del conocimiento, a ello se suma que en la actualidad cada cinco años se duplica la información disponible y esta franja tiende a acortarse cada vez más, siendo el principal vehículo de propagación de la información, desafiando las nociones de tiempo y espacio las llamadas redes de información internacional, en especial la red de redes.

Como es visto el crecimiento de Internet ha sido impresionante, por ello de acuerdo con un informe del Departamento de comercio de Estados Unidos, donde nos da a conocer, que si la radio debió esperar 38 años para alcanzar 50 millones de oyentes, la televisión 13 años para lograr el mismo objetivo, mientras que Internet sólo necesitó 04 años.

Es por ello que desde la aparición de Internet en nuestras vidas, muchos cambios se han producido, para unos cambios importantes y trascendentales y para otros ínfimos o de poca importancia, con esto último debemos entender que poca importancia o casi nada han podido dar los detractores de las TIC (Tecnologías de la Información y Comunicación).

Hace buen tiempo se habla de una desmaterialización de la ley como tal, de una ciber-sociedad, sociedad virtual o aldea virtual, como producto de esta desvirtualización se ha creado nuevas formas delictivas de poder perpetrar delitos mediante la utilización de medios informáticos y tecnológicos, estos delitos han sobrepasado las fronteras de los estados. Ahora queda una tarea importante para poder comprender a las TIC, no regulando de una manera actividades imprecisas, sin saber y conocer de ellas.

Como vemos es una tarea importante en cuanto a regulación, puesto que tanto los juristas como los abogados, deben profundizar sus investigaciones enriqueciendo de una manera positiva su saber y por otro lado la praxis o práctica misma, ya que ello nos conlleva a poder conocer, y comprender de cierta manera las tecnologías con las cuales convivimos día a día.

Como es de entender, el Derecho Informático es tanto sapiens como praxis, mas no netamente un mero saber, por ende es inadmisible pensar que al estar sentado delante de una gran biblioteca, se pueda pensar regular de una forma adecuada al Derecho Informático, si fuera así, se desnaturalizaría como tal.

Queda claro entonces que los entes que vienen haciendo investigación en Derecho Informático, no pueden ser barreras de una manera errónea frente a las TIC, seria ir contra la naturaleza propia de las mismas, por ello es equiparable a ir contra el mismo cause natural de un río, como resultado, este obtendría, la búsqueda de su cause y se desbordaría; lo mismo pasará con las tecnologías si tratamos de ser barreras para ellas, puesto que como es visto las mismas tecnologías seguirán su propia naturaleza y se encausarán a seguir desarrollando nuevas formas para poder expandirse de tal manera que sería mas distante para los propios juristas, como para los estudiosos de esta materia que deben tratar de alcanzar a las TIC, saber de ellas, conocerlas y comprenderlas. De ello tomemos una idea muy contundente y trascendental a pesar que nos encontramos en el siglo XXI, Albert Einstein *"Miro a mi alrededor veo que la tecnología ha sobrepasado nuestra humanidad, espero que algún día nuestra humanidad sobrepase la tecnología".* Frase muy cierta y exorbitante para los que repelen la tecnología.

Teniendo claro la perspectiva de poder ver al Derecho Informático, no como meros espectadores, sino ser parte de ello, comenzare a determinar lo que es el llamado Underground.

Underground (Mundo subterráneo o Mundo Bajo Tierra), este mundo es concebido como una metáfora referida a la red de redes o a la gran telaraña mundial, en donde Underground, es un sub-mundo donde se infieren nuevas modalidades para poder cometer ilícitos penales, este un mundo desmaterializado, por el cual difiere mucho del mundo material, puesto que mientras que en el mundo material impera por lo general el temor ensañado a la brutalidad, en la red de redes los ilícitos cometidos por personas naturales, impera la astucia y conocimiento por encima de cualquier ente criminal que lo pueda cometer, sentados frente a un ordenador colgados en alguna red o a la red de redes o utilizando un medio tecnológico para poder cometer distintos ilícitos penales.

Dentro de este sub-mundo desmaterializado, en el cual encontramos a los Hacker tanto Hacker blancos como los Hacker negros, Cracker tanto de hardware como de software, Phreaker, Coders, Carder, Newbie, Lamer. De ellos sólo mencionaré de una forma generérica su perfil para poder comprender, ya que en un articulo anterior, se trato todo lo referente a estos sujetos agentes del Underground.[1]

De toda esta gama de sujetos, cada uno con cualidades y características distintas, lo agruparemos en dos categorías, uno conformado por entes que desarrollan técnicas y otro por entes que se valen de ellas.

Partimos de la premisa anterior y de esa manera poder hacer una diferencia del primer grupo entre el sujeto que comete el ilícito penal utilizando un medio informático-tecnológico y la acción propia, siendo determinante el ente y el grado de conocimiento, como es cierto, hoy por hoy vivimos la era del conocimiento o el poder por el conocimiento, ello es equiparable con la nueva economía por la cual todos circundamos a su alrededor, *esta, basada en el conocimiento como pilar principal con una intensa aplicación del Know-how del ser humano tanto a los bienes y servicios producidos como a los procesos involucrados en su elaboración, hasta tal punto que en la actualidad se produce el surgimiento de áreas destinadas exclusivamente al manejo de la información*.[2]

El propósito que persigue este artículo es la identificación entre el sujeto que comete el ilícito penal utilizando un medio informático-tecnológico y la acción propia siendo determinante el ente como tal y grado de conocimiento, dicho sea de paso que el grado de conocimiento se presenta como piedra angular para la determinación de la responsabilidad en cuanto a ilícito penal. Entre estas acciones podemos encontrar las siguiente: Hacking, Cracking y Phreaking. Como podemos observar la acción se puede determinar por la terminación “ING”, con respecto al sujeto.

Sin más preámbulo presentare una breve descripción de cada sujeto que interviene en el Underground, mas no haré una descripción detallada de los mismos, solo para poder tomar en cuenta y determinar así al sujeto y acción o a la acción y el sujeto.

Por Hacker, muchas conceptualizaciones se han podido recabar tanto on line como off line, por otro lado la prensa siendo un sector importante ha influenciado de cierta manera en la mal identificación y determinación de los Hacker´s, tanto es así, que la misma prensa ha podido hablar o especular desde hace mucho tiempo sin hacer una adecuada distinción. De ellos se puede decir mucho, es por eso que detrás de los Hacker´s se ha creado un cierto mito de Hakismo, historias y una serie de definiciones inciertas.

Entre tantas definiciones que se han dado de los Hacker´s, presentaré un perfil genérico, pero no único, de estos entes, por lo tanto, se pueden caracterizar a un Hacker como una persona ansiosa por conocer cada día sobre las TIC e interactuar con ellas, por otro lado tiene como premisa fundamental el poder del conocimiento. Un Hacker también es una persona inquieta, conocedor de sistemas avanzados o no avanzados, así como también de informática, telecomunicaciones y electrónica estos tienen como objetivo principal comprender los sistemas y su funcionamiento; además son personas inteligentes, astutas, introvertidas como extrovertidas, perseverantes, satisfaciendo su ego dando a conocer los bug´s[3] de los sistemas informáticos así también como sus hazañas, además brindan soluciones a una serie de problemas o dificultades a internautas que día a día se sumergen en la red de redes; en realidad son muchas y distintas las características del perfil del Hacker.

Es por ello y tomando como una definición concreta, se puede recoger una tesis en donde se realiza una definición de Hacker, donde está considerado

como una persona que está siempre en una continua búsqueda de información, vive para aprender y todo para el es un reto, no tiene barreras.[4]

Comprendido ello, estos entes desarrollan sus capacidades y cualidades cuyo resultado se puede reflejar en el ingreso mediante un método de cierto modo inadecuado, a redes no permitidas o ha ordenadores no permitidos, este método utilizado y desarrollado por ellos se conoce como Hacking.

Hack-er y Hack-ing, palabras similares pero distintas en su terminación en cuanto a escritura, estas dos palabras nos ayudaran a poder determinar e identificar tanto al sujeto-acción y a la acción-sujeto; la preposición hack significa corte, también es entendido como un golpe fuerte, hoy ese corte o golpe ya no es dado por la fuerza física de un ente al tratar de hacer funcionar uno de los grandes ordenadores, en ese entonces cuando se empezaba a utilizar dicha palabra, hoy ese golpe es traducido a un golpe inteligente y suspicaz, un golpe de conocimiento frente a la falta de desconocimiento y seguridad del que se encuentra en otro ordenador, desde cualquier punto de una red o red de redes.

Esas personas que en su génesis empezaron a tratar con los grandes ordenadores, tenían por denominación Hacker, luego con la aparición de los ordenadores de escritorio y la interconectividad abierta, se presentaron nuevos retos en cuanto a protección de información y por ende seguridad ya para los noventa, resuenan los primeros ingresos de personas no autorizadas a redes restringidas y privadas, estos con fines propios satisfaciendo su ego e inquietudes por saber que guardaba la red de redes frente a sus ordenadores o en otros casos para apoderarse de información, es así como en realidad nacen los primeros Hacker, nacen con Internet y la ruptura de barreras de información, de las fronteras de los estados, estos entes desarrollaron técnicas, entre una de muchas podemos citar, el escaneo de puertos explotando los

bug´s, surfing, sniffer, ingeniería social, etc. Hoy en día, no siendo Hacker´s, se valen muchas personas de estas técnicas y son mal llamados Hacker.

Si bien es cierto las técnicas explotadas, así como también los programas que ellos desarrollan, son puestos en distintos portales o páginas web, donde mas de un cibernauta accede. Como conclusión, entonces no siempre los Hacker son los que cometen los ilícitos penales, sino son en mayor número aquellos entes, los cuales causan estragos en la red de redes, estos lo podemos encontrar debajo de ellos en cuanto a poder por el conocimiento.

Por otro lado los Cracker, son entes cuyos conocimientos y técnicas se basan, en la descompilación y descifrado, este personaje tiene como cimiento la ingeniería inversa, donde dicha ingeniería consiste en remplazar líneas de código fuente, estas líneas son secuencia de ejecución de programas que son interrumpidas por parches o por pequeños programas denominados key Generador[5], Underground uno de tantos ejemplos un programa shareware[6] pasa a ser freedware. Esta ingeniería recoge: pasos, secuencias o procedimientos que sigue un software para ser utilizado en su magnitud y sin restricción alguna.

Crack-er y Crack-ing, una vez mas, hay que diferenciar tanto al ente que desarrolla el método como al que se vale del método desarrollado por el Craker, es por ello que no debemos confundir de una manera errónea al ente que se valga del Craking para cualquier fin que propugne. Como sabemos hoy en día es muy usual el poder valerse de este método, ya sea mediante los pequeños software denominado key Generador o en otro caso valiéndose de portales o páginas web en los cuales se puede encontrar serial o parches.

Por último los Phreaker, son personas con conocimiento en telefonía modular, debe entenderse como telefonía modular, a los llamados teléfonos fijos o teléfonos de casa y a las cabinas de teléfono público, estos personajes no sólo

conocen de telefonía modular sino también de telefonía móvil. Además de ello tienen bastos conocimientos en telecomunicaciones, electrónica y programación.

Ahora Phreak-er y Phreak-ing, no hay más que decir, es por ello que me evocaré a desarrollar el método. El método utilizado por estos personajes, es la reprogramación, desbloqueo, clonación, sustitución de líneas de código fuente, determinado por un algoritmo. En cuanto a celulares, estos desbloquean como reprograman o clonan sin contar con autorización alguna de la empresa prestadora de servicio de telefonía móvil. Sumado a ello, estos desencriptan las tarjetas GSM.

En lo que se refiere a telefonía modular, lo más usual es el pinchazo de líneas telefónicas, logrando de esa manera la interceptación de comunicaciones o en otro caso usar la línea para realizar llamadas libres (free call). Otra forma de poder lograr llamadas libres, es contando con líneas abiertas, pero con restricciones de marcado, por no contar con teclado de marcado o por que este se encuentre deshabilitado, acá es donde se realiza el Phreaking.

Este método también es utilizado mediante la identificación y modulación de la frecuencia en la cual trabaja la línea telefónica, a partir de ello se genera un número al cual se quiere llamar mediante un software determinado, logrando ello, se graba el sonido producido en la frecuencia determinada, guardando el sonido en una grabadora, para reproducir luego el sonido en el auricular del teléfono el cual identifica la frecuencia y nos da pase a la llamada que queremos.

Como es visto estos métodos tanto de Hacking, Cracking como de Phreaking, son desarrollados por los que en realidad se les puede denominar Hacker, Cracker o Phreaker. Ahora que estos métodos y técnicas sean distribuidos de una manera abierta y no soslayada en la red de redes, no implica por ninguna

razón la imprecisión y mal identificación e indeterminación a personajes que no se encuentran calificados como tales. Es por ello que se puede inferir de una manera segura y precisa que no se puede determinar a un simple ente como Hacker, Cracker o Phreaker, sin saber, conocer y comprender previamente quien es el sujeto y quien hace uso de las técnicas desarrolladas por un tercero.

Como resultado de este articulo se puede inferir entonces que tanto los periodistas, los profesionales de distintas áreas y los mismos ciudadanos que se sumergen a Internet convirtiéndose en cibernautas, desconocen hasta cierto punto la distinción entre un sujeto que desarrolla el método o técnica y aquel ente que se vale de ella, no siendo el mismo y mucho menos no sancionando de una manera correcta. Es así como se hizo mención al inicio del presente documento que el conocimiento se ha convertido en única fuente de ventaja competitiva, conocimiento por el cual, lo encontramos en gran magnitud en la red de redes y en la red invisible inmersa en ella.

Sólo para culminar, cabe recalcar que el conocimiento impera frente a la seguridad informática es por ello que cuando se quiebra dicha seguridad, esta se ha debido fundamentalmente a un descuido, que se ha producido siendo resultado de errores y desconciertos que ocurren a diario, y cuando ocurren estos incidentes, sólo quedará, reconfigurar el sistema y revisar las políticas de seguridad y leyes, por las cuales espero sean las adecuadas e idóneas.

Documento
Principales Sujetos Agentes en el Underground, su determinación e identificación.

Expuesto en el congreso:

- ✓ **V Congreso Andino de Derecho Informático,** realizado del 24 al 26 de Agosto del 2005. **PONENTE. La Paz - Bolivia.**

[1] ***"IV cuarto congreso mundial de Derecho Informático",*** Jaime Araujo Ulco***,*** 2004, Cusco-Perú. *"CLASIFICACIÓN DE LOS JURISTAS EN EL DERECHO INFORMÁTICO. E IDENTIFICACIÓN DE LOS SUJETOS AGENTES EN EL MUNDO UNDERGROUND"*

[2] ***"La Huella Digital".*** Daniel scheinsohn – Raúl Horacio Saroka, Argentina-Buenos Aires. Fundación OSDE. 2000. Pág. 212.

[3] Bug´s: Denominación de las puertas traseras de un ordenador.

[4] A.S.S BORGHELLO, Cristian Fabian. ***"Seguridad Informática sus implicancias e Implementación",*** Tesis en Licenciaturas de Sistemas, UTN, Argentina, Cap. 5, Pág 6.

[5] Programas creados por los Cracker, los cuales son capaces de generar las claves de registro de un programa Shareware. Este programa generador responde a un algoritmo específico.

[6] Software, los cuales son distribuidos en forma de prueba, con el propósito que una vez utilizado el software a un tiempo determinado o con algunas restricciones el usuario pague su precio al autor, para su uso completo. Dicha distribución se puede hacer tanto on line como off line.