LOS RIESGOS CIBERNETICOS

IGNACIO COSIDO GUTIERREZ
Jefe del Gabinete Técnico del Director General de la Guardia Civil

INTRODUCCION

La nueva revolución tecnológica de la informática y de las comunicaciones, con la aparición de los conceptos de red global, influirá de manera decisiva en la estructura social y política de nuestro mundo en el próximo siglo. Esa revolución condicionará también la concepción de la seguridad en las sociedades avanzadas y hará aparecer nuevos riesgos y amenazas asociadas a la utilización y a la creciente dependencia de estas tecnologías emergentes.

En la evolución del hombre desde sus lejanos antepasados de *Homo Habilis* hasta el *Homo Sapiens Sapiens* actual hay que considerar tres tipos de desarrollo que en cierto modo podemos suponer interconectados. El primero de ellos es la evolución puramente biológica desde nuestro antepasado con un cerebro de 600 gramos y un bipedismo incierto, hasta nuestro actual cerebro de 1.500 gramos y una posición erguida continua. El segundo desarrollo está ligado a una intensa evolución social que propició la aparición de estructuras que superaron las meras agrupaciones unidas por lazos familiares de nuestros antepasados. El tercero se refiere a la utilización extensiva de artefactos tecnológicos que potencian las habilidades puramente físicas del hombre para la consecución de objetivos que precisan de una planificación previa. Estos tres desarrollos interconectados han dado origen a la aparición del lenguaje humano, al complejo mundo técnico que nos rodea, a las estructuras sociopolíticas, y por encima de todo ello, a la conciencia.

Si pasamos a un examen más detallado de la dinámica que ha conducido a los desarrollos anteriores nos encontraremos con que las dos fuerzas más importantes en la evolución del

mundo biológico: la aparición de estructuras complejas como resultado de la evolución de sistemas lejos del equilibrio y la simbiosis entre entidades con funcionalidades diferentes, tienen también un protagonismo decisivo en los posteriores desarrollos tecnológicos, sociales y mentales del ser humano.

Este análisis nos lleva a identificar dos grupos de elementos evolutivos: procesos mentales y estructuras sociopolíticas. Para explicar los procesos mentales, una teoría reciente presenta a la conciencia como resultado de una simbiosis evolutiva entre diferentes razonamientos que en el caso de nuestros antepasados funcionaban desconectados y que en nuestros cerebros modernos han comenzado a comunicarse, lo que les ha permitido elevarse sobre los procesos individuales e inconexos mediante la conciencia, consiguiendo esa nueva cualidad de aprehensión del conocimiento.

Para entender la evolución en las estructuras sociopolíticas debiéramos considerar el cambio de la energía por la información como variable que nos permita considerar a dichas estructuras relacionadas con su entorno mediante intercambios de conocimiento. En ambos casos, la aproximación metodológica nos lleva a unos modelos que presentan unas características no lineales entre las causas y los efectos que inducen y, por tanto, a una sospecha de evolución caótica. Todo ello nos hace concluir en el principio de impredecibilidad que domina el futuro, tanto de las capacidades humanas como de las estructuras que las mismas crean. Principio que si no invalida cualquier ejercicio de prospectiva como el que pretendemos, sí debe al menos tenerse humildemente en consideración en cualquier análisis de futuro.

Este principio de incertidumbre nos permite además establecer un paralelismo entre los desarrollos tecnológicos y las estructuras sociopolíticas asociadas, desde las tribus de cazadores-recolectores con su modelo tecnológico de herramientas de caza y estructura social tribal, pasando por la introducción de las tecnologías de la agricultura y la ganadería y la aparición de las nuevas estructuras sociales de los poblados y las ciudades, hasta llegar a los primeros reinos e imperios. La posterior evolución de la tecnología ha dado origen a avances y retrocesos en las estructuras sociales hasta llegar con la revolución industrial al advenimiento de los modelos de las modernas democracias.

La nueva revolución tecnológica de la informática y las comunicaciones en curso, con la aparición del concepto de red global, no cabe duda que influirá en gran manera en la configuración que tome la estructura sociopolítica de la sociedad sobre la que se desarrollan dichas tecnologías. Esta nueva interrelación entre modelo tecnológico y el sociopolítico trae consigo amenazas y oportunidades que habrá que saber evitar y aprovechar respectivamente.

Estudiar esa conexión entre las nuevas tecnologías de la información y la comunicación con el mantenimiento de la estabilidad internacional, la convivencia pacífica de nuestras sociedades y la vigencia de nuestros principios democráticos, poniendo especial atención en identificar los nuevos riesgos y amenazas que emergen en este nuevo tipo de sociedades denominadas como sociedades de la información y del conocimiento, es el propósito de este análisis.

TIPOLOGIA DE LAS AGRESIONES TELEMATICAS

Cuando conectamos un ordenador a INTERNET, los intrusos pueden abrir agujeros de seguridad o puertas traseras por las que pueden acceder a los recursos de la red y modificar los archivos almacenados con información sensible. Los agresores pueden también interceptar el correo electrónico, introducir un virus, dañar el sistema o incluso destruir el sistema completamente.

Los tipos y estilos de ataques basados en INTERNET más habituales son relativamente conocidos. Entre ellos podemos destacar las agresiones basadas en la adquisición de contraseñas mediante las cuales acceden al interior de un sistema utilizando un programa generador de claves de acceso. En otros casos, se trata simplemente de curiosear en la red e interceptar paquetes de información valiosa mediante la utilización de "sniffers" o analizadores de red para interceptar las contraseñas de acceso a un sistema.

Existen también casos de falseamiento de identidades electrónicas, suplantaciones que se produce cuando alguien proporciona información falsa acerca de la identidad de su ordenador. Un ejemplo de este tipo de agresiones es el de una persona que envía un mensaje a un usuario de INTERNET, suplantando la personalidad del administrador del sistema, solicitándole la contraseña de acceso a la red y disponiendo por tanto de acceso a mucha información personal de ese ciudadano.

Finalmente, existen también ataques dirigidos a aprovechar los puntos vulnerables de la tecnología, realizando accesos ilegales a sistemas ajenos, utilizando para ello los fallos de seguridad que pueden existir en sus sistemas operativos.

Esta amplia variedad de tipos de ataques que pueden ejecutarse a través de estas nuevas tecnologías cibernéticas nos llevan a tener que establecer una relación de riesgos que sin ser exhaustiva mencione los principales casos conocidos. Entre ellos podemos destacar los siguientes:

Electronic mail bomb.

Existen determinados programas relacionados con la gestión de correo electrónico que permiten generar multitud de órdenes de correo desde un origen a un solo destinatario, de tal forma que es posible bloquear el ordenador del destinatario generando una gran multitud de estas órdenes o mensajes.

Caballos de Troya.

Es una forma de dañar datos de sistemas informáticos consistente en insertar determinadas instrucciones en la secuencia de ejecución de un programa de forma que realice una función no autorizada e incluso dañe otros datos mientras aparentemente realiza una función correcta.

Un caso especial dentro de los denominados Caballos de Troya son los denominados *Salamis*, que consisten en pequeñas modificaciones en programas utilizados en banca que realizan a su vez pequeñísimos asientos en multitud de cuentas bancarias, de forma que no sean detectados por su importancia, para realizar finalmente transferencias de esos asientos a otra cuenta bancaria.

Virus.

Tiene similitudes con un virus biológico, ya que un virus biológico necesita un cuerpo vivo para vivir, infecta células vivas de dicho cuerpo y se reproduce. En este sentido un virus informático que modifica a otro programa, dañándolo de tal forma que permite la nueva reproducción del programa o virus.

Worms (Tormentas).

Un "worm" o tormenta es un programa informático que no necesita otro para funcionar, a diferencia del virus. El worm simplemente se duplica el mismo tantas veces como está programado hasta que desborda por tamaño el ordenador o sistema informático donde está instalado.

Bombas lógicas.

Es un programa introducido en un sistema informático que se activa al coincidir una fecha y hora contenida en dicho programa con el reloj del ordenador donde se encuentra instalado, desencadenando a partir de ese momento una serie de órdenes (normalmente borrado físico de información) que dañan el sistema. Una bomba lógica puede ser introducida varios años antes de actuar.

Obtención de secretos teóricamente eliminados.

Este fue el caso del Teniente Coronel Oliver North en el que se revelaron secretos oficiales supuestamente destruidos relacionados con la operación Irán-contra.

Interceptación de líneas de datos y captura de emanaciones electrónicas.

La interceptación de líneas telefónicas o de transmisión de datos permite capturar toda la información que circule entre dos ordenadores interconectados.

Pero estas posibilidades de interceptación no sólo son posibles actuando sobre una línea

física de transmisión, sino también mediante la captación de las emanaciones electrónicas generadas por los sistemas.

Utilización de "Back Doors".

Esta técnica permite la modificación en un programa que permite traspasar la seguridad.

Utilización de SNIFFERS.

El "sniffer" o rastreador es un programa informático normalmente escrito en lenguaje de programación "C" que circula libremente en determinados foros de debate o "news" en INTERNET, por lo que puede ser copiado al ordenador personal de cualquier usuario.

Este programa está diseñado para ser ejecutado en una red informática y rastrear todas las transacciones que viajan por la red para volcarlas finalmente a un fichero de salida. Entre dichas transacciones pueden encontrarse palabras de paso de acceso a proveedores o números de tarjetas de crédito utilizadas para realizar operaciones bancarias que una vez contenidas en el fichero de salida pueden ser utilizadas de forma fraudulenta por el ejecutor del "sniffer".

Terrorismo informático.

Podemos considerar a los grupos terroristas como el ejemplo de delincuencia organizada más desarrollado y peligroso existente en nuestros días. No es extraño por tanto que también hayan utilizado los medios informáticos y concretamente INTERNET para desarrollar sus actividades.

En la actualidad los más importantes grupos terroristas existentes en Europa actúan como grupos organizados con diversos frentes de ataque o lucha. Así, encontramos un frente armado representado por un grupo terrorista específico, un frente político representado por un partido político legal o semiclandestino y un frente de masa representado por diferentes organizaciones legales que extienden las actividades terroristas en otros ámbitos (sindicatos, escuelas, fábricas). En la utilización que estos grupos hacen de las nuevas tecnologías podemos encontrar varios ejemplos:

Atentados a Sistemas Informáticos de centros neurálgicos como Aeropuertos, Empresas de Electricidad de ámbito estratégico, Sistema de impresión de billetes o Centrales Nucleares.

Este fue el caso de las Brigadas Rojas en Italia en los años setenta, que atentaron contra más de 25 centros considerados de interés neurálgico para el Estado. Hoy este tipo de ataques puede realizarse también, incluso con menor riesgo físico para los agresores, a través de las redes informáticas.

Utilización de correo electrónico asociado a cifrado de datos.

Otro ejemplo de utilización de estos medios para subvertir el orden social o político puede ubicarse en la red de comunicación de algunos de estos grupos.

Es fácil transmitir cualquier tipo de información de interés para un grupo terrorista (órdenes de ejecución de un atentado, documentos, planos, libros, fotografías de objetivos, vídeos) a través de correo electrónico entre dos usuarios conectados a INTERNET, uno por ejemplo en España y otro en Francia o Bélgica. La gran ventaja de este sistema es que pueden realizar esos enlaces sin moverse de su residencia habitual, lo que disminuye sustancialmente el riesgo de ser detectado y detenido.

Existen sin duda posibilidades técnicas de interceptar este tipo de mensajes e identificar origen y destino real de la información, sin embargo, las dificultades aumentan exponencialmente cuando el contenido del mensaje es cifrado mediante alguna clave.

La mayoría de los buenos sistemas de cifrado han sido durante años coto cerrado para las agencias o centros de inteligencia de determinados países. Sin embargo, hoy en día es sumamente fácil para cualquier usuario encontrar y disponer en INTERNET de un sistema de cifrado de datos de usuario, como PGP (Pretty Good Privacy), equiparable en cuanto a su eficacia a los grandes sistemas de cifrado conocidos.

Como ejemplo de la utilización de este tipo de cifrado en mensajes transmitidos por correo electrónico entre diversas células de un grupo terrorista, podemos destacar el uso de este

sistema por el grupo neonazi que realizó el atentado en los Juegos Olímpicos de Atlanta en 1996. La banda terrorista ETA viene utilizando también, cada vez con mayor asiduidad, este tipo de comunicación electrónica cifrada.

Presentación de información clandestina en INTERNET.

Es relativamente fácil encontrar información en INTERNET sobre el frente armado del IRA (Irish Republic Army) o del denominado frente de masas de ETA, conocido tradicionalmente como colectivo KAS (Koordinadora Abertzale Socialista) y posteriormente EKIN.

Hay también información abundante sobre grupos neonazis o sectas que dan publicidad a través de la red de sus actividades ilegales y animan a contactar con este tipo de organizaciones a través de correo electrónico. Todo ello supone una clara amenaza de expansión de ideologías racistas, destructivas y antidemocráticas.

Blanqueo de capitales.

Es posible encontrar en INTERNET determinados anuncios en páginas WEB, desde proveedores ubicados en paraísos fiscales como Gibraltar o la islas Caimán, donde se ofrece la compra de bienes de gran importancia como inmuebles, terrenos o empresas.

Estos anuncios, en algunos casos avalados por bancos existentes en dichos paraísos fiscales, permiten la compra de estos bienes simplemente mediante una transferencia bancaria a través de INTERNET, donde los datos introducidos en la página por el comprador pueden ser totalmente falsos, lo que no reviste importancia mientras la transferencia bancaria sea realizada correctamente. En este mismo sentido, tampoco importa el origen del dinero, que bien puede proceder de actividades ilegales como el tráfico de drogas o de armas.

El blanqueo de dinero procedente del narcotráfico o de otras actividades ilegales no es un delito nuevo, ni puede considerarse un "delito tecnológico" en sí mismo. Sin embargo, la utilización de un medio informático como INTERNET puede favorecer en gran medida este tipo de actividad ilícita, pues la operación detallada anteriormente se realizaría a través de ordenadores y manteniendo el anonimato de la persona que realiza la transferencia.

Pornografía infantil.

En este caso INTERNET es una vez más el medio informático utilizado para cometer un delito que se venía realizando a través de otros medios, como revistas especializadas que se venden en sex-shops o círculos cerrados. La cuestión esencial es cómo descubrir el mundo criminal existente detrás de la publicación de pornografía infantil en INTERNET.

En diversos foros de debate en INTERNET podemos encontrar numerosas fotografías y vídeos pornográficos que son difundidos o comercializados con medios de pago electrónicos al resto de los usuarios de la red desde proveedores existentes en España y otras partes del mundo.

El problema se plantea cuando las imágenes presentadas en esos foros son imágenes reales de menores de edad en las cuales puede detectarse prácticas sexuales abusivas e ilegales o cuando se llega incluso a ofrecer relaciones con esos menores, para lo cual es preciso abonar cierta cantidad de dinero y ponerse en contacto con el pederasta o pedófilo a través de una dirección de correo electrónico.

Este problema crece cuando dichas prácticas son realizadas en nuestro propio país. El presunto pedófilo difunde las imágenes pornográficas con menores de edad en un proveedor de Estados Unidos, donde para publicar cualquier tipo de información no se registra la identidad de la persona que origina la información. En este punto, podemos preguntarnos dónde realmente se comete el delito de pornografía infantil y cómo es posible detectar el origen si no existe un registro fidedigno de quién ha colocado la información en el proveedor. Las dificultades para reprimir este tipo de conducta en la red son obvias.

Fraude electrónico.

Existen determinadas páginas WEB que ofrecen la obtención de un servicio (un libro, una entrada de cine, la compra de un coche o hasta una casa) mediante la consignación de

datos específicos de medios de pago. A su vez, también circulan libremente por la red programas informáticos que generan números aleatorios de tarjetas de crédito y los van chequeando con estas páginas WEB, hasta que se produce la coincidencia con algún número real para así poder realizar un acto de disposición ilícito.

Extorsión a empresas.

Como ejemplo podemos mencionar la extorsión sufrida por la empresa IBM cuando un programador alemán introdujo un programa informático técnicamente denominado "Caballo de Troya" en el sistema de correo electrónico de la red informática mundial de IBM.

Copia ilegal de software.

La copia no autorizada de programas de ordenador (piratería) en la mayor parte de los casos a través de soporte CD-ROM constituye una agresión ilícita de los derechos de autor que causa muchos miles de millones de pérdidas a las empresas del sector en todo el mundo. España es además uno de los países que se encuentra a la cabeza del ranking de piratería informática en Europa.

La casuística en nuestro país con relación a este tipo de delitos es ya histórica, pues las Fuerzas de Seguridad han desarrollado a lo largo de la década de los ochenta y noventa numerosas aprehensiones de CD,s conteniendo copias ilegales de programas informáticos.

Sin embargo, el auge de INTERNET ha dado lugar a la proliferación de este tipo de piratería informática a niveles "industriales", causando graves perjuicios económicos a las compañías dedicadas a la producción y comercialización de software.

En definitiva, las nuevas tecnologías de la información y las comunicaciones ofrecen enormes posibilidades de desarrollo económico, social y cultural a las sociedades avanzadas. Sin embargo, el éxito de estas tecnologías pasa por comprender los riesgos y tomar las medidas de seguridad necesarias para proteger los datos y las redes.

Hay que ser conscientes que resulta imposible eliminar todos estos riesgos por completo. Así, dos principios fundamentales de la seguridad en estos nuevos entornos son que el único ordenador razonablemente seguro es aquel que no está conectado y que un ordenador realmente seguro es un ordenador muerto. Encontrar un nuevo punto de equilibrio entre libertad y seguridad, entre vulnerabilidad y protección, parece necesario en el nuevo mundo virtual.

CONCLUSION

La amenaza cibernética es el riesgo de destrucción total o parcial que planea sobre nuestros sistemas de información y comunicaciones como consecuencia de un ataque telemático por parte de un país enemigo, un grupo organizado de delincuentes o simplemente un individuo. La creciente dependencia de la sociedad actual y más en particular de nuestros sistemas de defensa de estas nuevas tecnologías hace que de tener éxito un ataque de este tipo pudiera tener efectos catastróficos sobre nuestra población, nuestro sistema productivo y nuestra propia capacidad de defensa.

Algunos han querido ver en esta nueva amenaza cibernética una sustitución de lo que la amenaza nuclear supuso en tiempos de la Guerra Fría. Sin embargo, esta comparación resulta exagerada. La amenaza nuclear fue durante todo ese período una amenaza cierta con una capacidad de destrucción total de bienes y personas. Por el contrario, la amenaza cibernética debe ser aún precisada tanto en su virtualidad como en su capacidad de destrucción real.

Pero tan erróneo puede resultar en este momento sobredimensionar esta amenaza emergente como negar de forma radical su existencia. En el nuevo mundo virtual hay factores que resultan inquietantes y a los que debemos dar respuesta adecuada si no queremos caer en riesgos inasumibles. Por un lado, no hay ya actividad humana en el que las nuevas tecnologías de la información y las comunicaciones no estén jugando un papel preponderante.

El trabajo, las relaciones sociales, el ocio, las infraestructuras básicas de transporte o de suministro de energía, los sistemas de defensa, los procesos industriales o de pro-

ducción, todo ello depende cada vez en mayor medida de equipos y sistemas electrónicos que presentan a su vez nuevas vulnerabilidades.

Por otro lado, todos estos sistemas tienden a relacionarse cada vez más a través de redes de comunicaciones complejas que tienden a converger a su vez en esa gran red de redes a la que denominamos INTERNET. Esa creciente capacidad de interconexión de sistemas cada vez más vitales para el funcionamiento normal y la seguridad de nuestra sociedad es lo que constituye un mayor riesgo, porque expone a todos esos equipos y sistemas al ataque, el sabotaje, el robo de información o cualquier otra acción de destrucción por parte de un tercero.

En tercer lugar, INTERNET permite una gran distancia y un mayor anonimato por parte del agresor. Las técnicas de furtivismo hacen difícil en ocasiones identificar a las personas u organizaciones que se encuentran detrás de una agresión. Alguien puede operar desde cualquier lugar del mundo y atacar cualquier sistema que esté conectado a la red sin importar donde se ubique físicamente ni donde vayan a tener efecto las consecuencias de su ataque. Las deficiencias de la legislación internacional hacen además que una posterior investigación, en especial si se cuenta con la complicidad de algún Estado, sea aún mayor.

Es un hecho que cada día se producen millones de intentos de incursiones fraudulentas por parte de personas ajenas a sistemas protegidos. Muchas de ellas logran su objetivo, cometiendo fraudes, robos y daños de distinta dimensión en muchas de las redes. La propagación de virus cada vez más destructivos es un hecho constatable por el creciente número de usuarios de la red o por los responsables de seguridad de los grandes sistemas informáticos. No estamos por tanto hablando de amenazas exclusivamente de futuro, sino de hechos reales que se producen cotidianamente.

La cuestión es que hasta ahora todas esas agresiones han tenido una escasa relevancia estratégica. Los ataques han sido protagonizados bien por personas que buscaban la diversión y la superación de retos, violando y penetrando determinados sistemas, bien por delincuentes que perseguían simplemente un beneficio económico. Pero no puede descartarse que estas mismas técnicas no estén siendo utilizadas por grupos terroristas o que en el futuro otros estados planeen este tipo de agresiones para atentar contra nuestra seguridad nacional. Es más, la dimensión de poder de determinados grupos organizados de delincuentes debe ponernos también en alerta sobre la posibilidad de que utilicen estas nuevas tecnologías como una forma no sólo de aumentar su capacidad para enriquecerse ilícitamente, sino de obtener nuevas posiciones de poder en nuestras sociedades.

La vulnerabilidad estratégica que supone este tipo de amenazas comprende dos tipos diferentes de amenazas. Por un lado, hemos de considerar los ataques contra aquellos sistemas que regulan infraestructuras básicas para el funcionamiento de un país. Poder dejar a una gran ciudad sin energía eléctrica como consecuencia de un ataque cibernético, paralizar la red de transporte ferroviario de un país, sabotear los servicios públicos de una administración son ejemplos de los riesgos que debemos considerar y que suponen un serio quebranto para la normalidad y la seguridad de una sociedad avanzada.

Todas estas infraestructuras básicas deben, cuando su funcionamiento depende de complejos sistemas informáticos y de comunicaciones, dotarse de elementos de protección suficientes como para poder neutralizar este tipo de agresiones.

Una segunda y más grave amenaza la constituye la penetración de sistemas que resultan críticos para nuestra seguridad nacional, como puedan ser la red de comunicación, mando y control de las Fuerzas Armadas, el sistema nacional de gestión de crisis o las bases de datos de nuestros servicios de inteligencia. Este tipo de agresiones puede suponer una amenaza directa a nuestra seguridad nacional y, por tanto, sus niveles de seguridad deben ser aún mucho mayores que en el caso anterior.

Esta amenaza cibernética cobra verdadera dimensión a la luz de las estrategias asimétricas que algunos países parecen estar pensando. Guerras como la del Golfo o la más reciente en Kosovo han demostrado la incapacidad de cualquier potencial enemigo para imponerse mediante una guerra convencional

a las potencias occidentales entre las que se encuentra España. Esa incapacidad les ha llevado a buscar nuevas formas de confrontación que pueden orientarse desde la acción terrorista en el territorio de nuestros países hasta la utilización de armas de destrucción masiva, preferentemente químicas y biológicas, con las que desequilibrar la abrumadora superioridad occidental en el campo convencional.

Todo ello obliga a incluir dentro de cualquier análisis de riesgos para las próximas décadas este tipo de amenazas. Algunos países, como China o Irán, tienen supuestamente avanzados programas de guerra cibernética que podrían utilizar en contra de nuestros intereses en caso de crisis. Por su parte, varios de nuestros aliados, en especial Estados Unidos, están a su vez desarrollando estrategias complejas y costosas de neutralización de esos riesgos tecnológicos emergentes. España debería, en el marco de una Revisión Estratégica a largo plazo como la que está desarrollando actualmente, contemplar estas nuevas vulnerabilidades y riesgos para así poder diseñar las estrategias adecuadas para una eficaz neutralización.