DERECHO PENAL

Ciberterrorismo. Una aproximación a su tipificación como conducta delictiva

Informática y delito de lavado de activos

Riesgo, daño y responsabilidad jurídica en la era digital

El delito informático en Colombia: Insuficiencias regulativas

Manipulaciones de tarjetas magnéticas en el Derecho penal colombiano

Amenazas informáticas y seguridad de la información

CIBERTERRORISMO. UNA APROXIMACIÓN A SU TIPIFICACIÓN COMO CONDUCTA DELICTIVA

*Iván González Amado**

"Los ciberataques de Al Qaeda asustan. Los terroristas están a las puertas de usar la Internet como un arma para el derramamiento de sangre, dicen los expertos".[1]

1. INTRODUCCIÓN

La humanidad se había acostumbrado a señalar con sucesos históricos fijados en el tiempo y en el espacio sus momentos más notables o los hitos de la evolución de sus culturas. Así, la revolución industrial la hemos asociado siempre con THOMAS NEWCOMEN que en 1705 inventó en Inglaterra la máquina de vapor, posteriormente perfeccionada por JAMES WATT en 1769, y con JAMES HARGREAVES que inventó en 1767 la "Spinnny Jenny" que permitía el entramado de varios hilos a la vez. El origen de los computadores lo hemos asociado con BLAISE PASCAL que en 1642 inventó la calculadora mecánica que permitía realizar, automáticamente, sumas y restas; y con GOTTFRIED WILHEM VON LEIBNIZ inventor del sistema binario y, en 1672, de la máquina de calcular con la que se podían hacer las cuatro operaciones matemáticas básicas.

---

* Profesor de Derecho Penal y Ciencias Criminológicas en la Universidad Externado de Colombia.

1 Titular del Washington Post, 27 de junio de 2002.

De la misma forma, "La caída de Constantinopla en manos de los turcos otomano el martes 29 de mayo de 1453 fue un suceso histórico que, en la periodización clásica y según algunos historiadores, marcó el fin de la Edad Media en Europa y el fin del último vestigio del Imperio Bizantino y de la cultura clásica".[2]

A su turno, la toma de La Bastilla el 14 de Julio de 1789 se considera el símbolo del inicio de la Revolución Francesa y el comienzo del estado liberal moderno.

El 28 de junio de 1914 cuando el heredero del trono austro-húngaro, el archiduque FRANCISCO FERNANDO cayó víctima de un terrorista servio, se ha fijado como el hecho fundamental del inicio de la primera guerra mundial y la modernización de Europa. El 6 de agosto de 1945, cuando el bombardero Enola Gay, lanzó la bomba atómica "Little Boy" sobre Hiroshima, y el 9 de agosto, cuando el avión Bockscar lanzó la segunda bomba atómica, apodada Fat Man, sobre Nagasaki, son los referentes históricos del fin de la segunda guerra mundial.

A partir de lo que algunos denominan la época nuclear, y más precisamente, con el comienzo de la llamada revolución digital, y contemporáneamente, suceden las cosas tan rápidamente que es imposible fijar en hechos históricos aislados el progreso de la humanidad. Además, la reducción del espacio y del tiempo, así como los gigantescos avances que se han presentado en las comunicaciones, hacen imposible que consideremos un solo acontecimiento como el origen de una nueva era o el único factor desencadenante de un evento.

A esta nueva visión del mundo han contribuido enormemente los computadores, aparatos responsables del avance vertiginoso de las comunicaciones, del rápido progreso de la industria, de la revolución educativa y de mucha parte de nuestro bienestar, así como la nueva tecnología de las comunicaciones que mantiene conectadas estas máquinas y les permite respuestas múltiples en instantes y simultáneamente, con una gran cantidad de información y diversos enlaces coordinados. Uno y otro recursos, empero, también son responsables de la mayor parte de las modernas intromisiones a nuestra intimidad, de muchas de las actuales angustias, de múltiples fuentes de riesgo en la sociedad e, incluso de la globalización actual.

Los computadores, en efecto, se desarrollaron a partir de gigantescas máquinas que nos permitían realizar una gran cantidad de operaciones en pocos minutos y fueron evolucionando muy rápidamente hasta el actual computador personal que, además de haber reducido el tiempo del procesamiento de datos, se ha ocupado del manejo de muchos de los procesos técnicos contemporáneos y de muchos de los servicios que utilizamos, gracias, a su vez, a la creación de lo que se ha llamado la autopista informá-

2 Wikipedia, La enciclopedia libre, Internet.

tica, o la red de redes: la Internet, que se estableció como medio de telecomunicación entre las máquinas.

Los computadores y las telecomunicaciones, entonces, han permitido un amplio desarrollo de la humanidad y cada vez más de los primeros se conectan a la autopista de la información con el objeto de alcanzar el procesamiento de datos en tiempo real, brindar respuestas inmediatas a los problemas que se presentan a una distancia a la que el hombre no alcanzaría a llegar de usar los métodos tradicionales de desplazamiento, y potenciar el control de los procesos y el conocimiento, a partir de la acumulación de datos e información que reposan en cualquier parte del mundo.

> *"La tecnología militar en la actualidad depende en gran parte de la informática, así como los mecanismos de preservación y análisis de información de seguridad. Internet, la Red de redes nació de la idea y de la necesidad de establecer múltiples canales de telecomunicación entre computadores. En caso de un ataque nuclear que eliminara líneas de conexión existentes, se utilizarían medios alternos de conexión informática sin importar la ruptura de otras líneas o canales de conexión. Entonces la idea de este tipo de redes fue la de garantizar las telecomunicaciones militares con fines de seguridad y defensa en los Estados Unidos en Norteamérica. Esta red conocida como Arpanet fue desarrollándose de tal forma que evolucionó paralelamente una red pública para uso de universidades bajo este mismo concepto de múltiples conexiones telemáticas."*[3]

Los computadores y la Internet sin embargo, son, ante todo, un instrumento del hombre, en manos del hombre, al servicio del hombre y por lo tanto dependen de él y actúan para él. En este sentido, no son más que recursos que pueden ser usados en bien de la humanidad, o como armas para atacarla o destruirla. Armas poderosas como jamás ninguna otra lo haya sido, porque le permiten al ser humano estar en donde no está, mirar lo que no puede ver, conocer lo que no sabe que existe, utilizar las herramientas que no están a su alcance, y todo ello con la garantía del anonimato, la posibilidad de producir resultados sin necesidad de una acción física que los desencadene, el secreto de sus actos y la garantía de éxito de sus propósitos.

Por esta razón, el mal uso de los computadores nos ha puesto, en la época actual, "al borde de un ataque de nervios" ante la comprobada probabilidad de que sean asaltadas nuestras cuentas bancarias; la expectativa angustiosa de que se cometan errores en el manejo de las centrales nucleares; la proliferación de mensajes apocalípticos que anuncian los más catastróficos resultados; la real posibilidad de que se acumule información sobre nuestra identidad y preferencias sin que lo advirtamos siquiera, y otra serie de situaciones que pueden generar efectos nocivos en la tranquilidad de los ciudadanos.

---

3 Raymond Orta Martínez, en *Alfa-redi*. Revista de derecho informático, N.º 082, mayo de 2005.

Frente a estas condiciones, también cabe preguntamos: ¿Pueden utilizarse los computadores para la creación y conducción de actos terroristas? ¿Existe algún comportamiento que pueda ser calificado como terrorismo digital, o terrorismo computarizado, o como generalmente se le conoce, ciberterrorismo? ¿Es el ciberterrorismo una amenaza real en la sociedad actual?

Las siguientes páginas apuntan a brindar algunas reflexiones sobre la existencia de este tipo de comportamientos, de los elementos que pueden ser tomados en cuenta para la construcción de un concepto específico de ciberterrorismo, y a plantear algunas inquietudes sobre la necesidad o posibilidad de que el derecho penal entre a regular la libertad de acceso de los ciudadanos a una fuente de información que, hasta el momento, ha sido pública, libre y con pretensiones de igualdad.

2. PRESUPUESTOS CONCEPTUALES

2.1. La nueva sociedad de la información y el conflicto de derechos

Considero necesario comenzar por inscribir el problema del ciberterrorismo en el ámbito de una nueva sociedad, porque es a ella a la que pertenece. La sociedad del pasado era una comunidad atómica, es decir, que sus relaciones se fundamentaban en la existencia de un mundo real caracterizado por la materia conformada por átomos, en la que todo tenía una configuración real, perceptible por los sentidos o por los instrumentos que extendían el alcance de las percepciones pero que, en todo caso, dependía de la materia para su conocimiento, intercambio de información y progreso.

Sin perjuicio de que sigan influyendo en nosotros esta modelo de sociedad, la actual es, por el contrario, una sociedad digital, una sociedad virtual que no depende de la materia para el intercambio de sus conocimientos o el desarrollo de sus tecnologías, sino que construye su saber a partir de mundos virtuales, inexistentes materialmente pero posibles como representaciones numéricas, que permiten la manipulación del "futuro" antes de que éste suceda[4] y la creación de un presente más allá de lo que los átomos permiten, tal como puede comprobarse con un paseo virtual por cualquiera de los museos del mundo, sin contar para ello más que con un computador debidamente equipado.

En la actual sociedad digital se establecen nuevas relaciones entre los hombres, caracterizadas por la eliminación de las distancias físicas; la igualdad virtual; las posibilidades ilimitadas del conocimiento en cualquier área del saber humano; el acceso a la información en "tiempo real", es decir, dentro de "un sistema de tiempo capaz de procesar

4 No me refiero aquí a la ingenua idea de que con la cibernética se puedan modificar los acontecimientos futuros, sino a la efectiva posibilidad de crear escenarios virtuales que anticipen los resultados por venir.

una muestra de señal antes de que ingrese al sistema la siguiente muestra"[5]; la libertad informática, y el anonimato, que es uno de los derechos del usuario de Internet, expresión del derecho fundamental a la intimidad y al secreto de las comunicaciones[6] y que permite que ninguno otro de los usuarios de la red pueda conocer los sitios visitados por cualquiera de ellos, los conocimientos buscados o los propósitos de tales accesos.

La Internet ha permitido esta sociedad virtual en donde la igualdad, la libertad y el anonimato son los valores prevalecientes, que han impulsado, además, a la negación de la intervención estatal en la red. Internet es de la sociedad, no la controla ningún gobierno ni depende de normas jurídicas; es ante todo un recurso en el cual se asegura la igualdad de sus usuarios en el "ciberespacio" y, por lo tanto, los límites de su acceso están dados solamente por sus capacidades de conocimiento de la red, de conocimiento de los programas informáticos que circulan por ella y de su máquina.

Gracias a Internet se pueden realizar muchas cosas. Las compras diarias; el pago de servicios públicos; el desarrollo de nuevo software; el manejo de las máquinas y demás sistemas que requieren los servicios públicos; el control de las armas nucleares; la recopilación de datos que quedan en el ciberespacio; la vigilancia de nuestras propiedades; el control de la asistencia y puntualidad de los servidores públicos; las clases virtuales; la participación en foros de discusión que se desarrollan en cualquier parte del planeta; la simulación de desastres naturales y la forma como se puede reaccionar ante ellos; la creación de escenarios virtuales para el manejo de cualquier situación inesperada, en fin, cuanto se le ocurra a la imaginación humana en la perspectiva de este nuevo avance digital.

Obviamente, en esta nueva situación se presenta una serie de conflictos que en la sociedad atómica no podían ser planteados: ¿Cómo conciliar el derecho de acceso a las redes de información y el consiguiente derecho al anonimato con las necesidades de protección de bienes jurídicos de la sociedad (quienes son y no son usuarios de Internet), de los demás cibernautas, de los programadores y propietarios de los programas digitales desarrollados (software)? ¿Cómo conciliar el principio de libertad de acceso a la red con la posibilidad de control que se deba o pueda reconocer a las autoridades públicas? ¿Cómo conciliar el principio de igualdad de los usuarios en el ciberespacio con la restricción de acceso a algunos datos o bancos de datos?

En esta nueva sociedad, en consecuencia, se relacionan, cuando menos, el derecho a la intimidad con el derecho a la propiedad; el derecho a la intimidad con el derecho a la seguridad; el derecho a la intimidad con el derecho al libre acceso a la red; el derecho a la intimidad con el derecho al desarrollo del conocimiento y el derecho a la libertad con lo que pudiéramos llamar el derecho al control (publico –de intervención

---

5 Wikipedia, La enciclopedia libre.

6 Moron Lerma, Esther, Internet y derecho penal: hacking y otras conductas ilícitas en la red.

estatal– o privado –que ejercen los usuarios de la red sobre otros incluso sin que estos sepan–), así como el derecho a la igualdad con el derecho a la intervención estatal (si de él pudiera hablarse).

Según se vean unos y otros, se podrá propender por diversas posiciones teóricas que van desde la libertad absoluta del usuario, hasta la mayor restricción al acceso a una red pública, ampliamente desarrollada y cuya razón de ser es, precisamente, la posibilidad de acceso a la información sin discriminación ni control.

La razón de estos conflictos radica en el hecho de que a medida que se van ampliando las redes de la información, van apareciendo dentro de ella comportamientos que se consideran peligrosos para el sistema, atentados contra la libre circulación de datos, riesgos para el comercio electrónico, y un gran número de conductas que causan alarma entre los usuarios.

No se trata aquí de analizar estos enfrentamientos ni de plantear una tesis jurídica acerca de cómo resolverlos. Simplemente se dejan propuestos como un problema a resolver en otros espacios académicos, pues lo cierto es que, en la actualidad, el principio general es el de que el acceso a las redes de información no puede ser controlado más que por los sistemas de protección que desarrollan quienes crean los programas que por ella circulan.

La actual configuración de conductas relevantes para el derecho penal, en efecto, no tiene que ver con el control de acceso a las redes de información, sino con la violación de algunos derechos que pueden verse implicados en el manejo de la información –así, la pornografía infantil, por ejemplo–, o en el acceso no autorizado a ella –lo que se denomina el intrusismo informático–, pero, por lo demás, cualquiera de nosotros puede informarse sobre cómo construir una bomba, o adquirir armas, o violar los sistemas de seguridad de los programas, o controlar bases de datos, o, en fin, desencadenar fuerzas peligrosas controladas por los computadores conectados a la red.

2.2. Algunos comportamientos generadores de riesgos o daños en las redes de información. Las herramientas del ciberterrorismo.

Indudablemente, la Internet es una magnifica herramienta para la comunicación y la investigación, pero también genera muchos riesgos de seguridad tanto relacionados con los datos que circulan por la denominada autopista de la información, como referidos a la integridad física de las máquinas que se utilizan para acceder a este moderno recurso e, incluso, a los procesos que se manejan en el ciberespacio y consiguientemente, para la seguridad de la comunidad que puede verse afectada con la alteración de un procedimiento específico.

Junto con los programas de aplicación creados para permitir el uso adecuado de los computadores y la Internet, han aparecido de tiempo atrás otros programas destinados

a atacar los sistemas de computadores conectados a la red, con el fin de capturar información sin que el usuario lo detecte, controlar máquinas o servidores específicos, dañar los recursos técnicos de los aparatos o hacer que éstos realicen operaciones no queridas por el usuario y, en la mayoría de los casos, ni siquiera advertidas por él.

Los ataques a los computadores personales no siempre se hacen con el fin único de perjudicar al usuario del mismo o acceder a su información personal con el fin de defraudarlo, sino que, en no pocas ocasiones, persiguen el aprovechamiento de los recursos técnicos tales como el espacio de su disco duro, la conexión a Internet o el procesador de alta velocidad, con el fin de atacar otros computadores en la red y evitar que se descubra el paradero y la acción del intruso, quien asegura la impunidad de su conducta al utilizar un mayor número de enlaces. Los computadores personales, en este sentido, son mejores victimas que las máquinas institucionales y servidores, en razón de que son más fáciles de atacar al tener menos controles y programas de seguridad[7].

No podré, dada la magnitud del tema, referirme a todas las formas como pueden afectarse datos, programas, computadores o derechos en el uso de la red pública de información. Sin embargo, considero necesario hacer referencia a las más conocidas formas de afectación del sistema, que son necesarias para reconocer que, así como es posible alterar la información, también es una posibilidad real la comisión de actos terroristas a través del empleo de la red digital, pues cada una de tales maneras de violar las seguridades, constituye una puerta más a través de la cual se pueden lograr resultados que infundan temor en la ciudadanía, en diversos grado, modalidad y consecuencias.

Todas las formas de programas y códigos de ellos que se citan a continuación constituyen lo que algunos técnicos denominan en términos generales *malware* o *programas maliciosos*, expresiones que designan un software diseñado o desarrollado por "enemigos" del sistema de comunicación global, con intenciones dañinas como parte de las formas de conseguir un determinado objetivo. Comúnmente el propósito del *malware* es tener acceso a los recursos de información sin el consentimiento ni conocimiento del usuario final, y es utilizado como instrumento de una intención dolosa, lo mismo que el delincuente callejero usa armas de fuego, ganzúas o palancas[8].

2.2.1. Hacking

Quizás la palabra más familiar a nosotros en términos de utilización de los computadores y la red de información, sea la de *hacker*, con la que identificamos a aquella persona que logra penetrar al sistema para obtener datos que luego utilizará en su propio beneficio o en provecho de terceros, bien para modificar los programas que habitualmente utiliza-

---

7 Cfr. Cómo permanecer seguro en el espacio cibernético, Lawrence R. Rogers.

8 Cfr. The Use of Malware Analysis in Support of Law Enforcement, Nicholas Ianelli.

mos, con propósitos no definidos o incompatibles con la libertad que rige la utilización del medio informático, o ya, simplemente, para probar su habilidad.

En un sentido técnico, el *hacking* identifica una cultura propia de algunos usuarios de computadores, que tiene una jerga particular, que reclama para sí legitimidad en el ejercicio de sus actividades, encaminadas a la difusión masiva de los programas que circulan por la red, haciéndolos accesibles a todos los usuarios sin costo alguno. El *hacker* es el nuevo Robin Hood informático, que defiende uno de los derechos fundamentales de las redes de información, cual es el derecho a la igualdad en la utilización de los recursos y a la propiedad pública de los programas que se utilizan para el desarrollo cibernético.

En este sentido un *hacker* es quien rompe las seguridades de un computador o de una red informática con espíritu altruista o chocarrero, particularmente ingenioso, con profunda inclinación hacia la programación de las máquinas cibernéticas, y que desafía permanentemente los límites del software o el hardware al que accede. Los *hackers* buscan fama y renombre perforando estas barreras, cuestionan a la autoridad y demuestran ser poseedores de conocimiento y tecnología, y para destacar sus logros tienen varias direcciones donde se cruzan mensajes (www.260.com ó www.antionline.com)[9]. Se dice que los creadores de Microsoft y Linux, los más ampliamente difundidos programas operativos, fueron *hackers* en su momento.

En la mayoría de las legislaciones y buena parte de la doctrina se identifica la conducta del *hacker* con la expresión de "*acceso no autorizado*" a las redes de información, que reduce los términos de la imputación a aquellas situaciones en las que el autor de la conducta, una vez ingresa al sistema o a la máquina, no produce daños ni hace mal uso, en sí, de la información obtenida mediante el acceso no autorizado, y por lo tanto la infracción se queda en el campo de la mera violación del derecho a la intimidad, o bien un atentado contra el derecho a la propiedad intelectual de quienes crearon los programas que deben circular en una autopista pública.

2.2.2. Cracker

El *cracker*, a diferencia del anterior, es una persona malintencionada que penetra a un computador o una red de ellos, con el fin de obtener información o modificar maliciosamente las aplicaciones, a fin de causar perjuicios a los usuarios del sistema o al autor del software que ha logrado penetrar.

Esta conducta puede ser definida, en términos sencillos, como la modificación de un programa con la intención de hacer que éste se comporte de una forma particular, diferente a aquella que estaba destinado a operar cuando fue diseñado, sin validación

---

9 Luciano Salellas.

de las palabras secretas de acceso (password) ni la observancia de otras restricciones de acceso.

De acuerdo con su metodología habitual, el *cracker* inicialmente observa cuidadosamente el programa objeto de su conducta; luego lo traslada a un "desensamblador" o herramienta que es usada para revelar los códigos del programa, en especial los relacionados con las palabras secretas de acceso, la fecha y condiciones de expiración, etc.; luego se aprenden las rutinas de protección, después de lo cual el programa es abierto con otra herramienta llamada HIEW (Hacker's view), que hace cambios en el desensamblador del código del programa, los que luego se introducen en él y así son deshabilitados los rasgos o rutinas restrictivas de su uso o protectoras de su contenido.

No obstante lo dicho, alguna autora identifica la conducta del *cracker* con la del *hacker*, desconociendo la diferencia que en temas de seguridad informática se hace respecto de ellos, así como las finalidades de cada uno. La profesora MORÓN LERMA, en efecto, dice que:

> *"La conducta de cracking, con arreglo a su significación originaria, se caracteriza por eliminar o neutralizar los sistemas de protección de un sistema informático, ya sea de un programa o del propio sistema operativo de la máquina. Habitualmente, se rompe la protección de un programa que impide su copia no autorizada o la de una aplicación shareware que impide su uso, pasada una determinada fecha. Este comportamiento se cifra, pues, en la copia inconsentida y, en su caso, posterior distribución ilegal, de programas informáticos (denominados warez, esto es, programas comerciales que han sido sometidos a la acción de un crack), con vulneración de los derechos de autor".*[10]

2.2.3. Pishing

Los ataques de *pishing* usan ingeniería social y subterfugios técnicos para robar los datos de identidad y de cuentas financieras de los consumidores. Los esquemas de ingeniería social utilizan correos electrónicos llamados *"spoofed*" (mistificados) para conducir a los consumidores a sitios falsos de la red informática designados para engañar a los receptores divulgando datos financieros tales como números de tarjetas de crédito, nombres de los propietarios de las cuentas bancarias, palabras secretas de acceso y demás datos de identidad.

Mediante el robo de nombres registrados de los bancos, de vendedores al detal en la red, o de compañías de tarjetas de crédito, los *pishers* a menudo convencen a los receptores de sus mensajes a responderlos y mediante los esquemas del engaño técnico, implantan códigos o programas "criminales" en los computadores personales,

---

10 Internet y derecho penal: hacking y otras conductas ilícitas en la red, ESTHER MORÓN LERMA.

para robar directamente las credenciales adecuadas, a menudo usando un sistema de espionaje troyano.

La conducta de *pishing* implica, por regla general, el robo de la información encontrada o de los programas afectados y la defraudación del patrimonio de una o varias personas, razón por la cual se puede adecuar a un delito contra el patrimonio económico (estafa informática, por ejemplo).

2.2.4. Sniffing

Se conoce como *sniffing* el hecho de lanzar programas de rastreo a la red informática, con el propósito de que capten, en el ciberespacio, los datos y mensajes que circulan por él, con la finalidad de leer su contenido y obtener información acerca tanto del remitente como del destinatario.

Posteriormente, esta información es utilizada por el intruso para propósitos de difusión de algunos mensajes, o bien para trasladarlos, sin consentimiento del usuario, a otros bancos de datos que utilizarán la información sin consentimiento del usuario inicial. Esta es una forma de obtener datos que luego serán utilizados, por ejemplo, para la difusión masiva de mensajes y, en esa medida, son invasión de la intimidad de los usuarios.

A través del *sniffing* también se puede hacer espionaje electrónico, de forma que el programa adecuado puede captar los datos del ciberespacio para identificar los contenidos y preferencias de un determinado usuario de la red y construir con ellos verdaderos "archivos de inteligencia" que pueden poner en peligro los derechos del afectado.

2.2.5. Spaming

La conducta de *spaming*, en términos generales, consiste en enviar multiplicidad de mensajes no solicitados por la red, a muchos destinatarios, generalmente con propósitos comerciales a fin de difundir un producto, una determinada oferta o, incluso, de diseminar información –cierta o falsa– relacionada con una específica situación.

La conducta de *spaming*, por sí misma, no implica un determinado daño a las máquinas o a la red de información, pero se convierte en uno de los medios preferidos de los criminales informáticos para obtener sus fines, toda vez que permiten sobrecargar un determinado servidor o una específica terminal, de forma que pueden vulnerar, con mayor facilidad, las seguridades que los protegen.

De hecho, a través del *spaming* se han logrado producir caos informáticos que han impedido a algunas empresas la utilización de sus recursos o la prestación adecuada de los servicios que ofrecen, inmovilizando o dificultando las respuestas al ataque. Es pues, una modalidad para impedir el dominio de los procesos computarizados.

2.2.6. La instalación de bombas lógicas

En un programa de computador una bomba lógica, también llamada código escoria, es un código programado que se inserta subrepticia o intencionalmente para que se ejecute (o explote) bajo circunstancias tales como cierto período de tiempo o ante la respuesta del usuario a un específico comando del programa intervenido. La bomba lógica habitualmente está programada para que muestre o imprima un determinado mensaje, borre o corrompa los datos del computador, o tenga efectos indeseados por el usuario. En este sentido, son utilizadas por muchos programadores que venden software mediante crédito, con el fin de que si no se pagan las cuotas correspondientes, el programa se borre de la memoria de quien ha querido utilizarlo sin pagar su costo.

Algunas bombas lógicas pueden ser detectadas y eliminadas antes de que exploten con el periódico "escaneo" de todos los programas, incluyendo los archivos comprimidos, con un adecuado programa antivirus que debe ser corrido siempre que el usuario conecte su máquina a la Internet.

Las bombas lógicas son muy fáciles de programar pero, su debilidad es que no se replican a sí mismas, razón por la cual no pueden esparcirse hacia víctimas no deseadas y, en esta medida, son menos dañinas para el sistema que otros tipos de ataques.

Un ejemplo de esta bomba lógica lo encontramos en el ataque que uno de sus exempleados hizo a un banco norteamericano. Antes de ser retirado del servicio, programó una bomba lógica que semanalmente debitaba diez centavos de cada una de las cuentas del banco y los acreditaba en la última cuenta que aparecía en los registros de la entidad. Luego, el exempleado abrió una cuenta bajo el apellido Ziegler y comenzó a aumentar su saldo con los traslados que hacía el sistema, sin que los clientes o los empleados del banco notaran la defraudación que, en últimas, se descubrió cuando otra persona, de apellido Zyegler, abrió otra cuenta y notó con sorpresa que todos los sábados se acreditaba a ella una enorme cantidad de dinero, producto de las acciones que estaba programada para hacer la bomba lógica puesta por el exempleado del banco.

Las bombas lógicas, si bien se han utilizado en la mayoría de los casos para defraudar el patrimonio económico, también han sido utilizadas para atacar los aparatos de control informático de servicios públicos, generando procesos no deseados y actividades cibernéticas no contempladas en los programas afectados, con el consiguiente peligro para la comunidad.

2.2.7. La introducción de virus, gusanos informáticos y caballos de Troya

Un virus es un programa o parte del código de un programa que se introduce en un computador sin consentimiento del usuario, ejecuta operaciones contra los deseos de éste y se reproduce a sí mismo. Puede atacar a otros programas y crear copias de sí

mismo para corromper o dañar los datos, cambiarlos, degradar el rendimiento del sistema afectando la memoria de la máquina o el espacio del disco.

Los virus pueden ser clasificados según afecten el sector principal del computador, sólo la grabación maestra (MBR viruses), un archivo o programa, o cierto tipo de archivos.

Los virus del sector principal infectan el *boot record* del disco duro y de los periféricos y permanece en la memoria para infectar otros medios periféricos cuando el usuario grabe en ellos alguna información.

Los virus que afectan la grabación maestra son muy similares a los anteriores, excepto porque estos infectan la "Master boot record" en lugar de otros sectores.

Los virus infectantes contiene códigos ejecutables del tipo .EXE y .COM; algunos son diseñados para residir en la memoria del computador para que continúen infectando otros programas, bien sin necesidad de acción alguna, ya cuando éstos sean ejecutados.

Los macrovirus infectan cierto tipo de archivos de datos, tales como los contenidos en Microsoft Office, como documentos de Word, hojas de cálculo de Excel y presentaciones de PowerPoint y habitualmente utilizan el macro lenguaje de *Visual Basic* de las aplicaciones de Microsoft Office y algunos han sido diseñados como gusanos para que se repliquen en otras máquinas a través de la red.

Los gusanos informáticos son programas que se copian a sí mismos a través de la red de información y difieren de los virus en el hecho de que los gusanos pueden correr o ejecutarse por sí mismos, en tanto que los virus necesitan un programa que los aloje.

El *caballo de Troya* es un programa destructor que se hace pasar por un programa de aplicación benigno y se expande vía correo electrónico o salas de conversación (chat), habitualmente ligado a mensajes muy sugestivos que el destinatario, aunque no conozca a su remitente, abre por curiosidad e infecta su sistema, o bien presentado como un programa destructor de virus que, en realidad, los esparce. A diferencia de los virus, los caballos de Troya normalmente no se esparcen por sí mismos y deben utilizar, para hacerlo, otros mecanismos.

Así, un virus caballo de Troya es un virus que se esparce engañando a un usuario confiado que lo ejecuta. Un virus caballo de Troya puede ser aquél que necesita un usuario de la red para que abra un mensaje adjunto en un correo electrónico, para activarse. Una vez activado, el virus envía copias de sí mismo a todos quienes se encuentren en el directorio electrónico del usuario infectado, propagándose de esta forma a múltiples computadores. En estos casos se afirma que el virus caballo de Troya infecta como un caballo de Troya, pero se esparce como un virus.

La víctima de los caballos de Troya usualmente da al atacante algún grado de control sobre su máquina, que puede permitir el manejo remoto de la misma con todos los privilegios que tiene el usuario afectado y, por lo mismo, el atacante puede vincular dicho computador con una red de negación distribuida de servicios (DDoS), la que es usada para atacar a otras víctimas, o puede solamente enviar datos al atacante.

En la actualidad los programas antivirus detectan los caballos de Troya conocidos; sin embargo, como éstos son más fáciles de crear que los virus, cada día aparecen nuevos programas que no son detectados por las herramientas de seguridad del sistema, de forma que la mejor manera de protegerse contra ellos es negándose a abrir los programas que son enviados por el correo electrónico o en las salas de conversación.

2.2.8. El ataque para producir la negación de servicio

En estos eventos el atacante informático inunda un recurso computarizado con más peticiones de las que puede manejar, lo que causa un colapso en el sistema que produce la negación del servicio a los usuarios autorizados de dicho recurso informático. Este tipo de conductas pueden realizarse, incluso, por muchos atacantes geográficamente dispersos (lo que se conoce como Distributed Denial of Service, o DDoS) lo que hace más difícil de controlar los efectos nocivos del ataque.

Este tipo de ataques, en especial los de negación distribuida de servicios, se han practicado para lograr el colapso de algunas empresas –por ejemplo, *ebay*, el conocido sitio de remates por Internet– así como para impedir que las máquinas que controlan algunos procesos de prestación de servicios públicos, respondan adecuadamente a otros ataques simultáneos que modifican la programación de tales recursos informáticos y hacen que el servicio público presente deficiencias en su funcionamiento.

Como se ve, toda esta serie de posibles ataques a través de la red brindan al intruso un amplia gama de posibilidades de actuar criminalmente, bien sea obteniendo información a la cual no tiene derecho; afectando la propiedad intelectual de quienes diseñan programas informáticos; dañando físicamente las máquinas de los usuarios de la red; manipulando la información que circula por la red, o bien accediendo a una máquina para manejarla o manipular los procesos que ésta puede controlar.

3. HACIA UNA CONSTRUCCIÓN DEL CONCEPTO JURÍDICO DE CIBERTERRORISMO

3.1. Introducción

Antes de examinar qué se puede entender por ciberterrorismo, creo necesario establecer algunas premisas que permiten considerar este tipo de conductas como una real posibilidad en el mundo de hoy.

La primera de ellas, enseña que todos los sistemas informáticos dependen del hombre y, por consiguiente, en la medida en la que el usuario u operador quiera desencadenar el terror a través de las máquinas que opera, lo podrá lograr si tiene suficiente conocimiento para ello y para violar las seguridades informáticas de los programas y computadores a los que quiere acceder.

La segunda premisa está relacionada con una de las leyes de la seguridad informática, según la cual la tecnología no es la solución de todos los males, de forma que ni siquiera el desarrollo más avanzado de sistemas de seguridad, o los más sofisticados programas, pueden por sí mismos evitar la posibilidad de que algunas personas acudan al terrorismo a través de las computadoras, es decir, que todos los mecanismos de seguridad desarrollados pueden ser violados. Ningún sistema informático es ciento por ciento seguro.

Una tercera premisa se fundamenta en el desarrollo de la tecnología. En la moderna sociedad de la información los ciudadanos, cada vez más, dependen en su vida diaria de los procesos que se realizan con la ayuda de los computadores, y tales procesos, a su turno, día a día deben "colgarse" en la Internet, es decir, deben garantizar que las distintas máquinas que los han de operar estén interconectadas. Muchas de nuestras actividades cotidianas dependen casi en su totalidad de la informática y de la comunicación entre las distintas máquinas y, por consiguiente, existen muchas puertas de entrada al manejo de fuerzas peligrosas, de armas ampliamente desarrolladas y de sistemas que pueden desencadenar alarma y zozobra en la sociedad.

Como cuarto presupuesto, se puede asegurar que la seguridad informática no depende solamente de los programas (software) que la desarrollan, sino, y en gran medida, de la propia seguridad de las máquinas que se utilizan para los diferentes procesos y de la confiabilidad de los operadores. Por esta razón, a fin de minimizar los riesgos del mal manejo de la informática, quizás sea necesario limitar el uso de las computadoras oficiales o encargadas de manejar los procesos más peligrosos para la sociedad, o bien diseñar computadores que solamente puedan correr determinado tipo de programas que estén a disposición del público en general, pero que no se encuentren habilitados para otra serie de operaciones más complejas que se reservarían a funcionarios gubernamentales o al sector privado encargado de la prestación de los servicios públicos. Esta idea, no obstante, resulta poco realizable, en la medida en la que, entonces, se cortaría la relación entre la ciudadanía usuaria de los servicios, y la entidad encargada de prestarlos.

En quinto lugar debemos tener en cuenta que según los reportes consultados, la seguridad informática es violada, primordialmente, por personas que se encuentran en el entorno en donde ella misma ha sido desarrollada. Así, son rutinarios ya los casos en los que son los exempleados de las empresas atacadas los que han logrado penetrar a sus sistemas para causar graves perjuicios a sus finanzas o a sus datos, la mayoría de las veces como venganza por antiguas diferencias laborales. No obstante, es preciso

también tener en cuenta que cada día se reportan más incidentes de seguridad informática en los que se reputa la intervención de personas que no han tenido relación alguna con el sistema atacado, sino que han logrado penetrar a él con la simple utilización de los recursos que hallan dispersos en la red pública de información.

De acuerdo con estas premisas, encontramos dos áreas diferentes sobre las cuales deben caer las reflexiones para configurar una definición de ciberterrorismo: el campo de lo que pudiéramos denominar el "intrusismo informático", y el campo de la utilización de la cibernética para causar terror en la población o generar daños físicos en ella.

En este segundo aspecto, podemos afirmar que las redes de información y su infraestructura son débiles y, tal debilidad puede ser aprovechada por los enemigos del sistema informático, pero también puede ser usada por los enemigos de un gobierno, de un sistema político, o de un grupo enfrentado por el control del poder en la sociedad, como medio para obtener una determinada posición o ventaja, o procurar el respaldo de la comunidad a sus propósitos, o simplemente para mantener el control de un determinado territorio o sector de la población con fundamento en el terror.

Como la red de información facilita las misiones de las organizaciones estatales y privadas y, por ello, no resulta muy fácil intervenirla sin poner en riesgo muchos de los servicios que tales instituciones prestan a la comunidad, los terroristas cibernéticos pueden aprovechar esta circunstancia para utilizar un recurso que no será inhabilitado mientras planean sus operaciones, desarrollan sus actos o alcanzan sus propósitos.

No obstante, parecería ser que ante la posibilidad de un ataque a la población a través de los medios cibernéticos, resulta aconsejable que éstos sean utilizados también como un medio para reducir la efectividad del enemigo, lo que justificaría que los gobiernos pudieran degradar la capacidad de las redes, sus niveles de servicio o la calidad de los datos que circulan por ella, lo que, sin embargo, afectaría a los ciudadanos en su libertad de acceso, en la satisfacción de algunas de sus necesidades, y en la dinámica misma de la vida social.

La posibilidad de que la infraestructura informática sea manipulada como un arma de ataque, a fin de que se destruya o afecte ella misma –vía la implantación de múltiples piezas de software malicioso, o bien vía acciones deliberadas que exploten sus debilidades–, puede ser también un arma de doble filo para el ciberterrorista, en la medida en la que los programas de seguridad pueden desarrollar esquemas y procedimientos que retrasen la preparación de quien usa el sistema para atacar a la sociedad, mientras se logra descubrirlo y planear una intervención en su contra.

Lo que se espera, como predicción normal de quienes se ocupan del fenómeno del ciberterrorismo, es que en una guerra cibernética los ataques se dirijan inicialmente contra blancos críticos de la infraestructura de una nación: energía, transporte, finanzas, agua, comunicaciones, servicios de emergencia y la misma infraestructura de información,

con lo cual se estima que un ciberataque puede producir significantes pérdidas de vidas humanas (por ejemplo, al desbordar una presa o suspender el suministro de energía) así como degradación social y económica (v.gr. al afectar la seguridad de las operaciones financieras y comerciales).

> "Una pérdida crónica de las capacidades de generación y transmisión de energía, por ejemplo, pueden tener un mayor impacto en los sistemas médicos y de emergencia, en las capacidades de comunicación y en la capacidades de manejo. Un falla en los sistemas de emergencia de las mayores ciudades puede producir no sólo la muerte de quienes utilizan estos servicios, sino también en la pérdida de confianza en el gobierno y en sus capacidades de proveer los servicios básicos o la protección a la ciudadanía. Como puede ser que el ataque se vea con capacidad suficiente para impactar otras infraestructuras tales como el transporte y el agua, los niveles de miedo y de pérdida de confianza en el gobierno, pueden tener impacto serio en el tejido social. Los ataques contra la infraestructura financiera pueden erosionar la capacidad de los negocios para funcionar normalmente e incrementan las dudas entre el público acerca de sus finanzas personales, incluyendo sus cuentas bancarias, inversiones y cuentas de ahorro. Las redes militares, como todas aquellas que utilizan patrones de comunicaciones comerciales, pueden ser obstaculizadas socavando su comando y su control, la logística, y las operaciones logísticas o de reacción inmediata. En una ilimitada ciberguerra los ataques virtuales pueden tener consecuencias reales. La ironía es que estas naciones, como USA y sus aliados de la OTAN, que tienen la capacidad de sobresalir en la ciberguerra, también son las más vulnerables. Hay, por consiguiente, medidas que deben ser tomadas para reducir esas vulnerabilidades".[11]

De esta forma, el concepto de ciberterrorismo debe contemplar fundamentalmente las modalidades de los ataques que pueden realizarse a través de la autopista de información, así como las consecuencias que los mismos pueden producir en el manejo de los procesos, y los efectos que puedan tener en la comunidad.

3.2. Las diferentes nociones de ciberterrorismo

No hay acuerdo entre los doctrinantes –la mayoría de ellos expertos en seguridad informática o en política, no en derecho) acerca de una definición única de ciberterrorismo. Muchos centran la noción en el elemento cibernético –con lo cual se amplían peligrosamente sus términos para incluir como autor de la conducta a cualquiera que penetra en la red informática–; otros dan especial relevancia al elemento terror, con lo cual se quedan en el campo de la realidad material (la sociedad del átomo), desconociendo la posibilidad de que la realidad virtual desencadene efectos similares.

---

11 CYBERSECURITY - The truth about Cyberterrorism Comments By SCOTT BERINATO.

La más simple, y quizás por ello mismo la que más presenta objeciones, es la definición de *ciberterrorismo* del argentino Luciano Salellas. Para él,

> "El ciberterrorismo es la acción violenta que infunde terror realizada por una o más personas en Internet o a través del uso indebido de tecnologías de comunicaciones.
> Estos grupos preparan sus acciones por medio de mensajes encriptados a través del correo electrónico, impidiendo la penetración de los organismos de seguridad de los Estados.
> A esto hay que sumar los sitios web donde estos grupos terroristas dan a conocer su historia, postulados, objetivos.
> Algunos de estos grupos son: KKK en Estados Unidos, ETA en España, grupos neonazis de Bélgica y Holanda y Verdad Suprema en Japón."[12]

Como se ve, poco aporta esta concepción para delimitar lo que es el delito de terrorismo cibernético. Parte de la exigencia de una acción violenta que infunde terror, quizás aludiendo no a las acciones que tienen curso en la red de la información, sino pensando en los resultados de éstas que se puedan producir en el mundo material externo al ciberespacio.

Esta alusión puede deducirse de los párrafos previos al transcrito, en lo que el autor ha hecho específica referencia a los atentados terroristas de Madrid en los que se emplearon algunas tarjetas electrónicas y telecomunicaciones avanzadas, así como de las frases subsiguientes a la transcrita, una de las cuales, por ejemplo, dice que "*Un ciberterrorista podría cambiar remotamente la presión de los gasoductos causando fallas en las válvulas, y desencadenando una serie de explosiones e incendios"*.

La noción de Salellas, en efecto, apunta a no diferenciar el terrorismo del ciberterrorismo, pues, en últimas, éste no tiene más requisito que el de haber usado la Internet o, indebidamente, la tecnología de las comunicaciones, es decir, que en esta primera aproximación no encontramos elementos diferenciadores precisos entre el terrorismo tradicional y el ciberterrorismo.

El Centro de Protección de la Infraestructura Nacional (NIPC, por sus siglas en inglés) de los Estados Unidos, bajo la dirección de Ron Dick, define el ciberterrorismo como:

> "Un acto criminal perpetrado a través de computadores que resulta en violencia, muerte y/o destrucción y crea terror con el propósito de coaccionar a un gobierno a cambiar sus políticas."[13]

---

12 SALELLAS LUCIANO, *Delitos Informáticos* –ciberterrorismo

13 BERINATO, SCOTT Cybersecurity - The truth about Cyberterrorism

Elementos del ciberterrorismo de acuerdo con esta tesis son, pues:

a. El uso de computadores.
b. Un resultado de violencia, muerte o destrucción.
c. La creación de un estado de terror (en la población).
d. Una motivación política concretada en la coacción a un gobierno determinado.

De ellos, para BERINATO son especialmente importantes los criterios de la motivación política y los resultados destructivos, de los cuales, afirma, los ataques a través de computadores generalmente satisfacen solamente el primero, ya que los efectos destructivos, de violencia o muerte son muy difíciles de obtener por medio de las máquinas, que si bien pueden producir consecuencias molestas, costosas y peligrosas, éstas no son, por sí mismas, destructivas.

No obstante lo anterior, el autor sostiene, también, que la definición de ciberterrorismo incluye dos clases de subcategorías de amenazas terroristas:

a. Las amenazas a la infraestructura física de una nación que compromete las áreas críticas de servicio, tales como el suministro de energía, agua y alcantarillado, el manejo de presas, servicios hospitalarios, oleoductos, comunicaciones, satélites de posicionamiento global, sistemas de tráfico aéreo y otros sistemas conectados a la red de información, y pueden producir muerte o destrucción.
b. Las amenazas contra bancos de datos críticos, que pueden afectar los sistemas de computadores a través del robo de información o daños irreversibles a datos vitales para los servicios que presta el estado, tales como secretos militares, registro de seguridad social e información financiera, que eventualmente pueden acarrear la muerte de algunas personas, destrucción, o pánico económico.

De estos dos tipos de amenazas, en realidad, respondería a los criterios que BERINATO ha señalado para el concepto de ciberterrorismo, solamente la primera, en tanto que es ciertamente muy difícil obtener la muerte de una persona, o la destrucción de bienes físicos de una comunidad, a través de la simple alteración de los registros almacenados en un sistema informático. En estos casos, la muerte o la aniquilación solamente podrían reputarse como consecuencias indirectas de tal manipulación de información, de forma que no es en sí el manejo de los computadores lo que la produce.

En lo que respecta al pánico económico, evidentemente posible como un efecto inmediato de la manipulación de los bancos de datos –especialmente los que soportan el sistema financiero– no podría afirmarse que éste constituye, en nuestro criterio, un caso de ciberterrorismo, en razón de que el terror que asociamos a él se refiere a las amenazas contra la seguridad personal –vida e integridad– de una población, y no a todo tipo de zozobra o temor que, como resultado, puede constituir otro tipo de conducta criminal, como sucede en nuestro caso con el pánico económico, protector del bien jurídico colectivo del orden económico social.

Una segunda acepción del concepto de ciberterrorismo la proporciona la Oficina Federal de Investigaciones de los Estados Unidos, que, según lo afirma SARAH GORDON, consultora de la firma Symantec, para el año 2002 definía la conducta como:

> "El uso ilegal de la fuerza o la violencia contra las personas o su propiedad, por un grupo de dos o más individuos, con el fin de intimidar o coaccionar a un gobierno, a la población civil o a cualquier segmento de ella, para alcanzar objetivos políticos o sociales."

Llama la atención, de este concepto, que no se hace referencia de forma alguna a la utilización de computadores o sistemas informáticos para la obtención del propósito político y se finca el centro de atención de la conducta en otros aspectos fundamentales:

a. El ejercicio ilegal de la fuerza o la violencia.
b. La necesaria conjunción de dos o más autores.
c. El objetivo de intimidar o coaccionar a un gobierno o a la población civil o a parte de ella.
d. El propósito de alcanzar objetivos políticos o sociales.

No debe olvidarse que la definición mencionada corresponde a una agencia de cumplimiento de la ley norteamericana y, como tal, está influida por las necesidades que ese específico órgano tiene de amparar sus acciones de investigación y seguimiento bajo nociones más o menos amplias que le permitan la intervención en esferas de la actividad privada que pueden estar más allá de los límites constitucionales.

Esta noción puede cuestionarse no sólo por la ausencia de una referencia específica al uso de la tecnología, de la cibernética o de las redes de información para el ejercicio de la violencia –elemento que considero indispensable para configurar el concepto de ciberterrorismo–, sino también porque incluye, dentro de los propósitos del terrorista informático, el logro de objetivos sociales, de forma que permite incluir dentro de la categoría criminal a grupos de personas –no necesariamente aparatos organizados de poder– que buscan alcanzar reivindicaciones sociales, generando de esta forma una reacción negativa en contra de quienes, por ejemplo, luchan en contra de un régimen opresor, o buscan condiciones suficientes para satisfacer sus necesidades mínimas de subsistencia.

A este propósito, obsérvese que el ejercicio ilegal de la fuerza o la violencia que configura la noción comentada, no requiere que ésta se concrete en daño alguno ni en un resultado específico, de forma que una simple amenaza –uso ilegal de la fuerza moral– puede calificar como suficiente para la tipicidad del hecho.

Al contrario, es positivamente destacable de esta definición, que se exija la actuación simultánea de dos o más sujetos, pues este elemento abre la puerta para que el delito se repute de un grupo de personas y, por esta vía, se pueda doctrinariamente señalar

que el ciberterrorismo es, ante todo, conducta de un aparato organizado de poder, tenga éste reconocimiento de personería internacional –un estado– o no –un grupo armado al margen de la ley, por ejemplo–.

De la misma manera, considero que la inclusión de la población civil como objetivo del ataque es una afortunada opción, ya que en el mundo actual las amenazas pueden diseminarse por los medios electrónicos en contra de una infinidad de personas que están al margen de los conflictos fundamentales que se plantean entre los grupos terroristas y los estados, de forma que la presión en contra de éstos puede ser incluso más efectiva si se realiza en contra de los civiles inocentes, que si se dirigiera contra los responsables del gobierno.

Los dos últimos señalados, como se aprecia, apuntan a inscribir el ciberterrorismo dentro de la categoría de los antiguamente llamados "delitos de estado" y que, hoy por hoy, podrían denominarse "delitos de aparatos organizados de poder", que en el ámbito internacional designan aquellas conductas cometidas por grupos institucionalizados o no que, mediante una organización jerárquica, desarrollan comportamientos que habitualmente involucran, como sus víctimas, a los miembros de la población que no toman parte en un conflicto determinado, sea éste armado o no, sea el mismo internacional o sin tal carácter.

Un tercer intento de definición de ciberterrorismo lo hallamos en el Departamento de Defensa de los Estados Unidos, que fija menos los límites de la conducta. En ella, se entiende por ciberterrorismo:

> "El uso ilegal o la amenaza del uso ilegal de la fuerza o la violencia contra individuos o propiedad, para coaccionar o intimidar gobiernos o sociedades, a menudo para conseguir objetivos políticos, religiosos o ideológicos."[14]

Valgan, aquí, las mismas críticas que hice a la noción anterior. Su amplitud, empero, se denota con la falta de restricción en cada uno de sus elementos. En efecto, de acuerdo con esta tesis no se incluye tampoco el uso de los computadores, las redes informáticas o la tecnología cibernética como instrumento indispensable para la configuración del delito, lo que podría significar que el Departamento de Defensa de los Estados Unidos, al igual que lo hace su Oficina Federal de Investigaciones, considera que puede llegarse al ciberterrorismo no solamente con la utilización de las redes de información, sino atacando la infraestructura de las mismas, es decir, que podría reputarse como ciberterrorista un ataque que afectaran físicamente los cables dedicados a la transmisión de información, con lo cual parece perderse la esencia de la conducta que se analiza, caracterizada, justamente, por la utilización del "mundo virtual" para el logro de los

---

14 Citado en *Cyberterrorism?* por Sarah Gordon.

objetivos terroristas, dejando al campo del terrorismo tradicional los ataques y efectos ocurridos en el mundo material.

Valga aclarar, adicionalmente, que tanto en la definición que comento, como en la anterior del FBI, se hace alusión al ejercicio de la violencia contra "la propiedad", pero que este término no es entendido en el estrecho marco que tal concepto puede tener en el ámbito de los que en Colombia denominamos el patrimonio económico, sino que se refiere, en términos generales, a los bienes de una persona, una comunidad, un gobierno o un grupo, independientemente de que sobre ellos se ejerzan los atributos propios del dominio.

Adicionalmente, destaco que en este nuevo concepto de ciberterrorismo se excluyen acertadamente los objetivos sociales –a los que me referí con anterioridad–, pero a cambio de ellos se incluyen los propósitos religiosos o ideológicos, con lo cual se logra un doble efecto: ampliar la noción a las conductas realizadas para la defensa de una ideología determinada o de unas reglas religiosas específicas, obviamente ligando el concepto a la realidad material de los ataques terroristas conducidos dentro de una *yihad*, pero también, reducir su ámbito de acción, eliminando del concepto los hechos que estén encaminados a la defensa de reivindicaciones sociales.

Lo que considero que está en el sustrato de esta última precisión, es, sin embargo, que se deben considerar como parte constitutiva del ciberterrorismo, los motivos de discriminación injustificada, o de intolerancia a la diversidad, en los tres campos señalados: político, religioso, ideológico. Es decir, que la característica de la conducta sería la de ser una manifestación de intolerancia y ataque en contra de la libertad de las personas o grupos de personas.

A este elemento, podría añadirse el ya insinuado en la definición de la Oficina Federal de Investigaciones, también incorporado por el Departamento de Estado de los Estados Unidos a su concepto de terrorismo, cual es el hecho de que la violencia o la amenaza que implican todas las formas de terrorismo, sea perpetrada en contra de un gobierno o de una población civil o parte de ella –o de los denominados "no combatientes"–, de forma que la conducta se fijaría dentro del específico marco de una confrontación –armada o no– entre aparatos organizados de poder, y realizada por lo que se han llamado grupos "subnacionales" o "agentes clandestinos".[15]

Paralelamente este ingrediente, así como la referencia explícita a dos o más personas, o a un grupo, ayuda a mantener en el ámbito de los conflictos grupales el concepto de ciberterrorismo, pues es evidente que este tipo de conductas no pueden ser realizadas con efectividad y alcances generales en la población, más que por un colectivo de personas que actúan bajo unos propósitos comunes y con finalidades específicas, pues a

15 Ídem, la noción de terrorismo que proporciona el Departamento de Defensa de los Estados Unidos.

pesar de todas las debilidades que presentan las redes de información, un solo intruso no es capaz de manipular todas las exigencias técnicas que requiere un ataque cibernético con efectos generales.

De todas formas, de las definiciones transcritas surgen más preguntas que precisiones. Si hablamos del uso de la violencia como uno de los factores para calificar la conducta como ciberterrorista, ¿a qué tipo de violencia nos estamos refiriendo? Obviamente el problema se plantea cuando abandonamos el mundo atómico para considerar la cuestión en el mundo digital. ¿Puede considerarse violencia, en este último, la emisión de un mensaje electrónico en el que se incite a una parte importante de la población a dar muerte a sus enemigos políticos? ¿Acaso el término violencia debe entenderse en el sentido de violación de las seguridades cibernéticas? O quizás, ¿para calificar el ciberterrorismo se debe exigir, mejor, un resultado materialmente considerado que se manifieste en muerte de personas, lesiones físicas a ellas, o destrucción de bienes?

Tal vez para permitir la configuración de la conducta, es más preciso hablar de la utilización de medios electrónicos con los cuales se puedan crear estados de alarma en la comunidad, bien mediante la difusión de mensajes, programas, códigos de programas o software malicioso que amenacen la seguridad o la tranquilidad públicas, ya a través del acceso a las redes, a los programas o a las máquinas que controlen fuerzas peligrosas o servicios cuya perturbación o manipulación cause, aun cuando sea potencialmente, daños a las personas o a los bienes.

Obviamente también existen dificultades para identificar, en el ciberespacio, un grupo subnacional, incluso un grupo nacional (cuando se refiere a los sujetos activos de la conducta), pero también la población objeto de amenaza y la extensión de ésta. Dada la eliminación de las barreras físicas en la red, y teniendo en cuenta la posibilidad de los múltiples enlaces entre ubicaciones dispersas por todo el globo, la precisión de estos conglomerados podría ser imposible, al punto de que, eventualmente, el terror se podría cernir sobre todos los habitantes del planeta (piénsese, por ejemplo, en la amenaza de producir un grave accidente nuclear) o bien podría extenderse la calidad de autor a un número indefinido de personas ubicadas en los más remotos lugares de la tierra que solamente podrían tener en común el hecho de tener acceso o ser propietarios de un computador[16].

Esta situación pone de presente que, aun cuando comparto el concepto de que el ciberterrorismo debe ser un delito de aparatos organizados de poder, la exigencia de grupos –ya en la parte activa, ora en la pasiva de la descripción típica– no debe hacerse bajo el concepto de la época digital, sino mediante la identidad de propósitos –que excluye a los usuarios cuyos computadores son intervenidos y manejados por terceros– y la

16 Recuérdese que las máquinas pueden ser controladas remotamente sin conocimiento ni consentimiento del usuario.

igual posibilidad de sufrir las consecuencias de la violencia con la que se amenaza –de forma que se identifican los blancos del ciberterrorista con los efectos materiales de su comportamiento.

No puede dejarse de enunciar el concepto de ciberterrorismo que trae DAN VERTON, para quien

> "El ciberterrorismo quizás sea uno de los términos más malentendidos y malempleados de la era de la información. En términos generales, el ciberterrorismo es la ejecución de un ataque sorpresa por parte de un grupo (o persona) terrorista extranjero subnacional con objetivo político utilizando tecnología informática e Internet para paralizar o desactivar las infraestructuras electrónicas y físicas de una nación, provocando de este modo la pérdida de servicios críticos, como energía eléctrica, sistemas de emergencia telefónica, servicio telefónico, sistemas bancarios, Internet y otros muchos. El objetivo de un ataque ciberterrorista no es sólo impactar sobre la economía de una región o país, sino amplificar los efectos de un ataque terrorista físico tradicional provocando confusión y pánico adicionales en la población en general.
> Sin embargo, el ciberterrorismo también puede tomar la forma del terrorismo tradicional, mediante el cual son destruidos físicamente nodos de energía eléctrica, comunicaciones e Internet, provocando fallos generales en cascada de sistemas electrónicos que pueden amenazar tanto la salud de la economía como la seguridad del público… Un ataque ciberterrorista, por tanto, debe analizarse en términos del objetivo que persigue y de su impacto, y no solamente por el modo de ataque."[17]

En esta noción observo un afán de ampliar los términos de su configuración hacia espacios que generan confusión e impiden precisar qué entendemos por ciberterrorismo. Lo primero que se advierte, es que VERTON no se define claramente si la conducta de ciberterrorismo ha de ser cometido por un grupo de personas o puede obedecer a la actuación de un solo individuo, de forma que parece entender que el terrorismo tiene tanto manifestación personal como de grupo, olvidando de esta forma el contexto internacional en el que se liga el concepto de acciones terroristas con la existencia de un grupo de personas unidas por una ideología, una religión o una causa política común.

Adolece la definición que comento, además, de una tautología que resulta al parecer de su autor, inevitable, al definir el ciberterrorismo a través de los actos cometidos por una persona o grupo "terrorista extranjero subnacional", haciendo depender la calificación del hecho de la condición –previa– de la persona que lo ejecuta y abre así la puerta para que cualquier acto de intrusismo informático pueda ser calificado como

---

17 VERTON DAN, *La amenaza invisible del ciberterrorismo*. Black ice.

ciberterrorismo, lo que resulta contrario a la naturaleza misma de la conducta, al menos en la forma como la entiendo.

De otra parte, resulta cuando menos curioso que VERTON omita en el inicio de su texto la mención al estado de temor que se procura lograr con los actos de ciberterrorismo, y que éste solamente sea mencionado como un efecto directamente ligado a los actos de terrorismo común, olvidando que desde el mundo digital se puede crear una situación que genere zozobra o terror, sin que sea necesario que efectivamente se produzcan en el mundo físico consecuencias nocivas o peligrosas.

Por su parte JEFFREY F. ADDICOTT, más precisamente que VERTON, sostiene que: "Ciberterrorismo es el empleo de varios recursos de computación para intimidar o coaccionar a otro (usualmente un gobierno) en procura de específicos objetivos" y luego de recordar la definición que del término hiciera MARK POLLIT, agrega que el terrorismo envuelve actividades de irrupción, corrupción, denegación o destrucción de información contenida en computadores o en una red de computadores, aclarando, empero, que no todos los actos de cibercrimen pueden constituir actos de ciberterrorismo[18].

El profesor ADDICOTT critica así mismo a quienes consideran que el término ciberterrorismo se refiere a cualquier ataque sobre las redes de información, y sostiene que en muchas ocasiones un ataque cibernético puede ser utilizado para destruir no sólo los elementos electrónicos, sino también la infraestructura que mantiene integrada a una nación, refiriendo en este punto específico los sistemas de aprovisionamiento de agua y energía, transporte y sistema financiero así como los servicios de emergencia que están electrónicamente controlados por una red centralizada de computadores denominada Supervisory Control and Data Acquisition (SCADA) que provee el "poder cerebral" para manejar dicha infraestructura y cuya afectación puede desencadenar masivos daños económicos o físicos a lo largo y ancho de un país.

DOROTHY E. DENNING, de la Universidad de Georgetown, proporciona otro concepto de ciberterrorismo:

> "Ciberterrorismo es la convergencia del terrorismo y el ciberespacio. El término es generalmente utilizado para significar ataques ilegales y amenazas de ataques contra computadores, redes de información, y la información almacenada en ellos, que pretenden intimidar o coaccionar a un gobierno o a su población, en persecución de objetivos políticos o sociales. Adicionalmente, para calificar como ciberterrorismo un ataque, éste debe producir violencia contra las personas o la cosas, o al menos causar suficiente daño para generar temor. Los ataques que conducen a la muerte, lesiones corporales, explosiones, colisiones de aviones, contaminación de aguas o severas pérdidas económicas, pueden ser ejemplo

18 ADDICOTT, JEFFREY F., Cases and material on terrorism law.

> de ello. Serios ataques contra la infraestructura crítica (de un país) pueden ser actos de ciberterrorismo, dependiendo de su impacto. Ataques que perturban los servicios no esenciales o que son principalmente molestias económicas, pueden no serlo".[19]

En esta noción hallamos un recurso a la enunciación de actos de ciberterrorismo para tratar de precisar el concepto, que está construido, fundamentalmente, a partir de los siguientes elementos:

a. La utilización del ciberespacio.
b. Ataques ilegales y amenazas de ataques contra computadores, redes digitales y la información almacenada en ellos o que corren por la red.
c. La finalidad de intimidar a un gobierno o a una población.
d. La persecución de objetivos políticos o sociales.
e. La generación de violencia contra las personas o las cosas mediante el ataque a los recursos informáticos, o al menos su capacidad de infundir temor.

Muy importante resulta que en esta definición –que es muy frecuentemente citada en los artículos científicos sobre ciberterrorismo– se haga expresa mención de la utilización del ciberespacio como elemento integrador del concepto, pues de esta forma se excluyen los actos que ocurren en el mundo material y solamente se pueden incorporar a la noción aquellos actos que tienen lugar en el mundo digital.

Además, obsérvese que la profesora Denning también precisa que para el cabal entendimiento del término, los blancos que han de recibir los ataques ciberterroristas han de ser los computadores, las redes de información o los datos almacenados en ellos o que circulan por ellas, con lo cual se gana en precisión al excluir a la población como objeto mismo del ataque.

En efecto, considero que una comprensión adecuada de ciberterrorismo debe referirse a aquellas conductas que tienen lugar en el "espacio virtual" y que, por lo tanto, no requieren de una concreción en el mundo material, razón por la que, además, solo puede ejecutarse sobre los elementos propios de ese mundo digital, es decir, de los computadores (entendidos como instrumentos de almacenamiento de información, no como máquinas en sí mismas), las redes o autopistas de información, y la misma información que circula por el ciberespacio.

Por lógica, la descripción de la conducta no se puede detener en la mención del ciberespacio y de los objetivos del ataque. Para que exista ciberterrorismo, como lo anota Denning, es preciso que confluya la finalidad del autor del hecho para intimidar a una población o a un gobierno, la persecución de finalidades políticas (mas no sociales,

---

19 Traducción libre de Cyberterrorism. de Dorothy E. Denning.

como se incluye en la definición) y la generación de violencia contra las personas o las cosas o, cuando menos, la capacidad del ataque para infundir temor en la población o el gobierno.

De esta forma se gana en precisión para distanciar el concepto de ciberterrorismo de aquello que pueda entenderse como comportamiento terrorista en el sentido tradicional, ya que es la cibernética la que gobierna la definición del hecho, y las personas o las cosas se incluyen no como quienes reciben directamente la conducta (el ataque digital) –objeto material, en términos más técnicos–, sino como los perjudicados con la conducta, es decir, los sujetos pasivos del acto, en tanto que son ellas quienes sufren el temor, o las consecuencias materialmente apreciables del acto criminal específico.

En conclusión, como elementos integradores de un posible tipo penal de ciberterrorismo, se deberían tener en cuenta los siguientes elementos:

a. La concepción del delito como una forma de criminalidad de aparatos organizados de poder.
b. La afectación o posibilidad de afectación de la población civil.
c. La necesaria utilización del ciberespacio, los computadores, las redes de información y la tecnología informática para la realización de las acciones que lo constituyan.
d. La mención de personas y bienes como los destinatarios finales de las consecuencias desplegadas con el ataque informático.
e. Una motivación de discriminación injustificada o intolerancia y, por consiguiente, la persecución de objetivos políticos, ideológicos o religiosos.
f. La finalidad de intimidar o coaccionar a un gobierno o a una población.
g. La utilización de violencia o la amenaza de uso de la misma.

3.3. El ciberterrorismo y el terrorismo tradicional

Parecería ser que todas las anteriores consideraciones no son más que expresiones de un diletante que busca problemas en donde no existen, y crea polémicas en donde no las hay. De hecho, muchos profesionales del derecho, de la política, de la seguridad y de la informática minimizan o niegan el problema del ciberterrorismo, asumiendo que sus manifestaciones pueden controlarse adecuadamente, en el caso del derecho, con las normas jurídicas existentes que protegen el acceso a las redes de información, los derechos de propiedad intelectual sobre los programas informáticos, o el patrimonio económico o la integridad moral de los usuarios de la autopista de la información.

En el plano político, se niega la necesidad de un concepto de ciberterrorismo, sobre una doble base: la aseveración de que esta nueva categoría no hace más que presentar un problema ficticio con el objetivo de distraer fondos públicos hacia unos técnicos iniciados que exageran la amenaza cibernética, y la consideración de que el concepto de ciberterrorismo se está instrumentalizando para ampliar las esferas de intervención

del estado en la vida privada de los ciudadanos, con el consecuente recorte de sus derechos civiles.

Los técnicos, por su parte, aducen que los sistemas de seguridad que hoy amparan la información digital y los programas que la manejan, son prácticamente inviolables, o necesitan de una amplia y difundida acción de ataque para que finalmente se puedan producir consecuencias desastrosas para la humanidad.

No me aparto, que algunas de estas objeciones tengan algo de razón, analizadas desde las particulares perspectivas de quienes las proponen. Sin embargo, considero infundadas la mayoría de ellas, en razón de los siguientes argumentos que pretenden desvirtuarlas.

3.3.1. La imprecisión del concepto de terrorismo y la insuficiencia de su definición legal para cobijar las hipótesis de terrorismo cibernético

Lo primero que considero necesario destacar es que el concepto de terrorismo tradicional en nuestro derecho penal, presenta una serie de deficiencias que hacen prácticamente inasible su contenido, o bien dejan al arbitrio del juez la delimitación de las conductas que constituyen esta específica modalidad de conducta típica.

Así, por ejemplo y como lo anotara en un trabajo anterior, la legislación colombiana utiliza una doble definición legal para el terrorismo: la primera, contenida en el artículo 144 de la Ley 599 que tipifica los "Actos de terrorismo" e inscribe en el marco de un conflicto armado, y la segunda, prevista en el artículo 344 del mismo Código Penal, bajo la denominación de "Terrorismo", regulando, por lo tanto, el fenómeno en los estados de paz interna.

Esta doble incriminación utiliza, además, diferentes expresiones para referirse a una conducta que es similar, en la medida en la que las dos descripciones hacen referencia al efecto de producir terror en la población, pero contradictoriamente sanciona con mayor pena el delito de actos de terrorismo que el terrorismo, como si la perturbación de la seguridad y la tranquilidad públicas fuera menos trascendente en los estados de paz que en las épocas de conflicto armado.

Más allá de este cuestionamiento, se tiene que de acuerdo con la regulación legal del fenómeno en Colombia y a la interpretación de las normas con apoyo en algunas disposiciones de derecho penal internacional, se pueden considerar como elementos estructurantes del delito de terrorismo:

a. Unos actos particularmente ligados al terrorismo, que implican, por regla general, la muerte de las personas, la producción de lesiones físicas a ellas, o la destrucción o daño en bienes materiales.

b. Unos instrumentos a los que se les exige la capacidad de causar estragos, con lo cual se ligan las consecuencias del terrorismo a lo que hemos denominado anteriormente el mundo atómico.
c. Unas víctimas, identificadas con el término preciso de población civil.
d. Unos procedimientos específicamente referidos a acciones propias del mundo material, tales como chantaje, extorsión, secuestro, destrucción de bienes, ataques excesivos, etc.
e. Unos lugares determinados que protegen, primordialmente, aquellos sitios de especial concentración de personas, o en donde se focaliza la infraestructura de un país.
f. Unos efectos que exigen la creación de un estado de zozobra o terror, o bien la afectación de la paz internacional.

El desarrollo que la doctrina ha hecho de estos elementos poco ayuda a la precisión de los conceptos y deja muy pocas posibilidades de que los actos a los que he hecho alusión como manifestaciones específicas del ciberterrorismo, puedan ser incluidos como parte del tipo penal de terrorismo o actos de terrorismo.

Es verdad que las definiciones legales son muy amplias y usan expresiones tales como "actos o amenazas de violencia" (art. 144 C.P.) o "actos que pongan en peligro" (art. 343 C.P.), con lo que parecería ser que caben todo tipo de expresiones humanas. No obstante, esta generalidad debe interpretarse dentro del contexto general del tipo y, en este esfuerzo interpretativo, se puede concluir que no quedan cobijados los actos propios del ciberterrorismo.

Obsérvese, por ejemplo, lo que ocurre con esta última conducta frente a la definición del art. 344 del Código Penal colombiano. Esta disposición prevé:

> Artículo 343. Terrorismo. El que provoque o mantenga en estado de zozobra o terror a la población o a un sector de ella, mediante actos que pongan en peligro la vida, la integridad física o la libertad de las personas o las edificaciones o medios de comunicación, transporte, procesamiento o conducción de fluidos o fuerzas motrices, valiéndose de medios capaces de causar estragos, incurrirá en prisión....
> Si el estado de zozobra o terror es provocado mediante llamada telefónica, cinta magnetofónica, video, casete o escrito anónimo, la pena será..."

De los elementos que integran el tipo penal mencionado se destaca la coincidencia del estado de zozobra o terror que también es exigible del ciberterrorismo; de la misma forma, el hecho de que la protección a la comunidad debe prestarse no solamente ante efectivos resultados, sino que basta la simple amenaza del daño para que el estado deba reaccionar punitivamente.

No obstante estas coincidencias, existen otros elementos del ciberterrorismo que están incluidos en el tipo penal. Así, la descripción del art. 343 del C.P. está prevista como un

delito individual, es decir, que su comisión puede ser realizada a título personal por un sujeto que actúe aisladamente, en tanto que, de acuerdo con lo visto, el ciberterrorismo es, ante todo, un delito de aparatos organizados de poder, con capacidad de coacción por la fuerza misma de su organización y que generalmente aglutina a sus miembros mediante el poder de una ideología, una religión o una posición política determinada.

Por otra parte, obsérvese que la norma hace referencia a actos que pongan en peligro, todos ellos y alternativamente, a la vida de las personas; la integridad física de ellas; la libertad de las mismas; las edificaciones; los medios de comunicación; los medios de transporte, y el procesamiento o conducción de fluidos o fuerzas motrices y que estos actos deben producirse "valiéndose de medios capaces de causar estragos".

En los eventos de ciberterrorismo, en realidad, este peligro no se cierne originariamente sobre los elementos descritos en el tipo penal citado, sino sobre los sistemas de información, los datos incluidos en ellos o las máquinas que los administran, de forma que la amenaza se concreta en la posibilidad de crear el peligro al que se refiere el art. 343 del C.P., no a la generación del riesgo mismo.

Por lo demás, los ataques digitales no son, por sí mismos, un medio con potencialidad para producir estragos, esto es, "ruina, daño o asolamiento", sino que estos efectos deberán producirse como consecuencia de la afectación de los sistemas informáticos y programas que regulan y controlan algunos medios materiales con los que, ahora sí, podría producirse daños generales a la población o a las condiciones materiales en las que ella desarrolla su vida ordinaria.

La manipulación de los sistemas digitales, propia del ciberterrorismo, ciertamente puede generar un peligro para la seguridad, la libertad y la tranquilidad de las personas, así como para la integridad de los medios materiales que soportan las comunicaciones, el transporte y el suministro de fluidos o fuerzas motrices, pero la conducta no necesariamente se agota en la amenaza, sino que debe trascender a la real posibilidad de penetración al mundo virtual y de afectación de los datos que circulan por el mundo virtual.

Estas últimas exigencias para la incriminación de la conducta como delito, las considero indispensables en razón de la necesidad de protección de los derechos que surgen a las personas en la moderna sociedad de la información. De hecho, si se estimara suficiente la previsión legal actual para castigar los actos de ciberterrorismo, se tendría que aceptar como legítima la intromisión del Estado en esferas de la libertad individual que hasta este momento no se han tocado, y se ampliarían las funciones de control y vigilancia de la conducta privada de las personas.

Como lo anotara desde el comienzo, la Internet se caracteriza por ser un sistema en el que domina una perspectiva "pública", no en el sentido de "lo público" como propio de las organizaciones políticas estatales, sino en el preciso entendimiento de que las redes de información están a disposición de todos los habitantes del planeta, sin restricciones

originadas en las condiciones mismas de la autopista de la información ni en su funcionamiento, y como tal, no es de nadie pero es de todos, sin admitir ingerencias de los gobiernos para controlar el acceso, la información que circula por ella, los contenidos de la información, las relaciones que se establecen entre los distintos cibernautas o los programas que se utilizan para el manejo o circulación de la información.

De considerar el cibeterrorismo como un fenómeno del mundo de los átomos, a mi juicio el estado se hallaría legitimado para anticipar la protección de los bienes jurídicos como lo hace en el mundo material y, absurdamente, podría incriminar como delito, de similar forma a como lo hace con las armas, el porte de computadores o de software o la utilización de una conexión a Internet. Lo que frente a la realidad tecnológica se podría admitir no sería la intervención estatal en estos campos, sino la necesidad de que se construyera un espacio virtual en el que no se permitiera el acceso al público como sucede con el manejo de las armas nucleares, es decir, en lugar de restricciones a los ciudadanos, se deberían generar obligaciones para quienes manejan y controlan los servicios públicos y las fuerzas peligrosas de constituir una red privada inviolable a la que no se admitiera a los usuarios de las redes públicas de información.

4. CONCLUSIONES

De todo lo dicho, podríamos llegar a las siguientes conclusiones:

4.1. La nueva tecnología cibernética propone al hombre un nuevo mundo virtual que no desplaza al mundo material, pero requiere soluciones diversas a las tradicionales, en tanto que en el ciberespacio aparecen fenómenos que no son posibles en el mundo real y formas de interrelación diversas.

4.2. Las redes públicas de información están abiertas a todo el mundo y son indispensables para el progreso de la humanidad, generando, por lo tanto, nuevas concepciones de los derechos de libertad, igualdad, intimidad y propiedad, que deben ser considerados tanto a la hora de regular el acceso a Internet, como al momento de tipificar conductas penalmente relevantes o intervenir en tales derechos, o que, como se ha reclamado en el ámbito de la Comunidad Europea, "Las medidas restrictivas de derechos que deban ser adoptadas, en la prevención y represión de los ilícitos perpetrados en Internet, resulten debidamente justificadas, necesarias y proporcionales"[20].

4.3. Ningún programa ni aplicación, en la era cibernética, es ciento por ciento seguro, de modo que los usuarios de las redes pueden acceder a ellos sin necesidad de mayores desarrollos. Este hecho impone la necesidad de diversificar el avance informático para mantener abierta la red pública a todos los usuarios del mundo, y desarrollar una red

---

20 Moron Lerma, Esther, *Internet y derecho penal: hacking y otras conductas ilícitas en la red.*

privada en aquellos aspectos en los que el acceso a los programas y aplicaciones y su manipulación malintencionada, pueda generar graves riesgos a la comunidad.

4.4. El ciberterrorismo es una amenaza real para la población mundial y se intensifica a medida que una nación desarrolla o adopta nuevas tecnologías e implementa éstas con apoyo en las redes públicas de información. Por ello, antes de que se produzcan resultados realmente catastróficos, es preciso comenzar a ocuparnos del problema en el campo del derecho, para buscar una respuesta adecuada a las nuevas amenazas, sin sacrificar los novísimos contenidos de los derechos que se crearon a los usuarios de las redes públicas de información.

4.5. Las nuevas tecnologías brindan al hombre, además de múltiples ventajas, un mayor riesgo y lo exponen a nuevas formas de lesión de sus derechos penalmente protegidos. Por ello, al parecer no es suficiente, frente al terrorismo –como ha sucedido en relación con la propiedad, por ejemplo– el tipo penal que fue construido para sancionar los actos cometidos en el mundo real, y en donde no caben, en principio, las acciones lesivas que se realizan en el mundo virtual.

4.6. En el mundo virtual, las manos del autor de un delito son reemplazadas por los recursos tecnológicos que son, en realidad, los que pueden desencadenar los estragos en el momento de producirse un ataque ciberterrorista. Por ello, quizás es necesario considerar, para efectos del derecho penal, un nuevo de acción típicamente relevante.

4.7. En los ataques a los sistemas de información se puede retrasar los resultados, en tanto que el desencadenamiento de un proceso puede programarse para una fecha futura o para la realización de un determinado proceso –que incluso, puede ocurrir o no– y ello impone que, de llegarse a la configuración de un tipo penal de ciberterrorismo, se tengan en cuenta estas posibilidades de producción del daño, para que no queden impunes conductas que no fueron detectadas a tiempo.

4.8. En la nueva sociedad de la información puede generarse estado de temor en la población mediante actos que aún no pongan en peligro la vida o la integridad de las personas o de los bienes, sino con la simple amenaza de utilizar recursos informáticos, y esta posibilidad real debe ser tenida en cuenta al momento de abordar, eventualmente, la tipificación del ciberterrorismo. Por lo demás, el temor que se deriva de los ciberataques puede ser, también, un resultado tardío de la conducta, en la medida en que solamente se desatará al momento de conocer un incidente de seguridad en los sistemas, y es necesario, entonces, contemplar también esta situación al momento de tipificar la conducta.

4.9. La tipificación y castigo del mero intrusismo informático no parece ser suficiente para prevenir las conductas terroristas que pueden ser cometidas a través de las redes de información, de manera que se requiere un nuevo tipo penal, porque resultaría

antitécnico e insuficiente punitivamente, regular el ciberterrorismo como una simple circunstancia agravante del intrusismo informático.

5. BIBLIOGRAFÍA

ADDICOTT, JEFFREY F., Cases and materials on terrorism law, 3ª Ed. Lawyers and Judges Publishing Inc., Tucson, 2004.

ALCAIDE FERNÁNDEZ, JOAQUÍN, Las actividades terroristas ante el derecho internacional contemporáneo, Tecnos, Madrid, 2000.

ANÓNIMO, Yo cacé terroristas, Ediciones El Bronce, Barcelona, 2003, Trad.: P. J. GORDON.

BERINATO SCOTT, Cybersecurity –The truth about Cyberterrorism–, en www.cio.com/article/30933/, consultado el 17 de febrero de 2007.

BOVARD, JAMES, Terrorismo y tiranía, Editorial El Ateneo, 1ª Ed., Buenos Aires, 2004, Trad.: JORGE SALVETI.

CONDORELLI, LUIGI, et. al., Terrorismo internacional y principio de distinción entre combatientes y civiles, Ediciones jurídicas Gustavo Ibáñez, Bogotá, 2004, Trad.: RAFAEL PRIETO S.

CORTE IBAÑEZ, LUIS, DE LA, La lógica del terrorismo, Alianza Editorial, Madrid, 2006.

COUNCIL OF EUROPE, Convention on cybercrime, Budapest, 23.XI.2001 Additional Protocol Explanatory Report Français Non-official translations, en http://conventions.coe.int/Treaty/EN/Treaties/HTML/185.htm, consultado el 15 de abril de 2007.

DENNING, DOROTHY E., Cyberterorism, Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, Georgetown University, May 23, 2000, en www.cs.georgetown.edu/~denning/infosec/cyberterror.html, consultado el 23 de enero de 2007.

EN LA CONFERENCIA MUNDIAL SOBRE SEGURIDAD Advierten por un ataque ciberterrorista, PERFIL.COM, 21 de febrero de 2007, consultado el 30 de junio de 2007.

GELLMAN, BARTON, Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say, Washington Post Staff Writer, Thursday, June 27, 2002; Page A01, en www.washingtonpost.com/wp-dyn/contest/article, consultado el 27 de junio de 2007.

GORDON, SARAH, Cyberterrorism? en www.symantec.com/avcenter/reference/cyberterrorism.pdf, consultado el 1 de julio de 2007.

GRABOSKY, PETER, et. al., Cyberterrorism, Australian National University, University of California, Santa Barbara, Published in *Reform* Issue 82, Autumn 2003 - National and international security, en http://www.alrc.gov.au/reform/summaries/82.htm, consultado el 18 de abril de 2007.

HORGAN, JOHN, Psicología del terrorismo, Gedisa, Barcelona, 2006, Trad.: JOAN TRUJILLO PARRA.

IANELLI, NICHOLAS, et. al., The Use of Malware. Analysis in Support of Law Enforcement, CERT Coordination Center, en www.cert/cc, USSS July 11, 2007, consultado 20 de julio de 2007.

LAWRENCE R. ROGERS, Cómo permanecer seguro en el espacio cibernético, Instituto de Ingeniería de Programas de Computadora, Universidad Carnegie Mellon, en www.usinfo.state.gov/journals/itgic/1103/ijgs/gj7.htm, consultado el 3 de marzo de 2007.

Ley 599 de 2000.

MORON LERMA, ESTHER, Internet y derecho penal: hacking y otras conductas ilícitas en la red, Aranzadi, 2ª. Edición, Elcano, 2002.

NASIRI, OMAR, Mi vida en Al Qaeda, El Andén, Barcelona, junio 2007, Trad.: DIANA HERNÁNDEZ.

ORTA MARTÍNEZ, RAYMOND, Ciberterrorismo, ALFA-REDI, Revista de derecho informático, Edición electrónica, N.º 082 - Mayo del 2005, consultada 2 de mayo 2007.

POLLITT, MARK M., Cyberterrorism -Fact or Fancy?, FBI Laboratory 935 Pennsylvania Ave. NW Washington, D. C. 20535, en www.cs.georgetown.edu/~denning/infosec/pollitt.html, consultado el 27 de mayo de 2007.

REPORT TO THE PRESIDENT, February 2005, Cyber security: a crisis of prioritization, en www.nitrd.gov/pitac/reports/, consultado el 10 de abril de 2007.

SALELLAS, LUCIANO, Delitos informáticos –Ciberterrorismo, en http://www.astrolabio.net/datafiles/1160518424.html, consultado el 25 de febrero de 2007.

SHIMEALL, TIMOTHY, et. al., Countering cyber war, NATO REVUE, On line library, Edición electrónica, Volúmen 49, N.º 4, Winter 2001, en www.nato.int/docu/review/2001/0104-04.htm, consultada 1º de junio de 2007.

VERTON, DAN, BLACK ICE: la amenaza invisible del ciberterrorismo, Mc Graw Hill, Madrid, 2004, Trad.: SUSANA NIETO MOYA.

WEIMANN, GABRIEL, Cyberterrorism How Real Is the Threat?, SPECIAL REPORT 119, December 2004, en http://www.usip.org/pubs/specialreports/sr119.html, consultado el 23 de julio de 2007.

WIKIPEDIA, La enciclopedia libre, Internet, consultada el 1 de mayo de 2007.