

Método
Grupo Transdisciplinario de
Investigación en Ciencias Sociales
www.grupometodo.org

Borradores de Método

Área de Metodología
ISSN: 1692-9667

**Transferencia de Tecnología y Crimen
Organizado**

Carlos A. Barrera C.

Documento 31
Enero 15 de 2005

BORRADORES DE MÉTODO es un medio de difusión de las investigaciones del Grupo Método. Estos documentos son de carácter provisional, de responsabilidad exclusiva de sus autores y sus contenidos no comprometen a la institución.

Borradores de Método. No 31. Enero 15 de 2005.
Editor Fundación Método
Colección Crimen y Conflicto.

© Carlos A. Barrera C.
Transferencia de Tecnología y Crimen Organizado

© Fundación Método. Carrera 8ª. No 37-10. Ofi: 501. Telefax: (571) 4005765
2005. Todos los derechos reservados.
Primera edición 2005.
Impreso en Bogotá, Colombia.

Transferencia de Tecnología y Crimen Organizado

Carlos A. Barrera C.

cbarrera@grupometodo.org

Resumen

El objetivo de este documento es mostrar la relación entre transferencia de tecnología y crimen organizado. Esta relación está entendida como el uso que hacen las organizaciones criminales de nuevos conocimientos e innovaciones para llevar a cabo actividades delictivas. En una primera parte se muestran los mecanismos actuales con los que se transfiere tecnología de un país a otro o de manera interna. En la segunda parte se establece la relación que existe entre el crimen y la tecnología dividiéndola en dos categorías: crímenes que usan la tecnología como una herramienta secundaria en la comisión de delitos y crímenes que requieren del uso directo de la tecnología en la consecución de una actividad ilícita. Además, se establece la conveniencia del uso de la tecnología por parte de las organizaciones criminales, así como posibles mecanismos en el control de este fenómeno. Por último, en la tercera parte se establecen algunas conclusiones.

Este documento es propiedad del autor y del Grupo Transdisciplinario de Investigación en Ciencias Sociales, MÉTODO. Agradecemos los comentarios.

Con el advenimiento de nuevas tecnologías e innovaciones que impulsan el progreso de un país, también se han desarrollado diferentes métodos criminales en los que el factor tecnológico ha tenido un papel definitivo. Los siguientes ejemplos muestran los nuevos procedimientos usados para la consecución de delitos por parte del crimen organizado:

- La droga denominada éxtasis, fabricada primordialmente en Holanda, la envían a Estados Unidos grupos del crimen organizado, algunos de los cuales son israelíes.
- Un virus de computadora, diseñado y enviado desde las Filipinas, hizo que se cerraran las computadoras en muchos organismos del gobierno estadounidense, algunas hasta por espacio de una semana.
- Un importante banco estadounidense descubrió que el crimen organizado ruso lo utilizaba para lavar dinero.
- Se ha informado que grupos colombianos del crimen organizado verifican por computadora la cuenta bancaria de los conductores que se detienen al encontrar que la carretera por la que circulan ha sido bloqueada; de ese modo pueden seleccionar a las personas adineradas para secuestrarlas.¹

Lo que nos muestra estos ejemplos es que a la par con los adelantos científicos y tecnológicos que ayudan a erradicar enfermedades y mejorar el bienestar general de la población, también existen innovaciones y métodos novedosos que utilizan tecnologías de punta para la comisión de delitos y la realización de actividades criminales. En este contexto, el tema de la transferencia de tecnología adquiere relevancia, y más en un mundo globalizado como el actual, en el que los procesos de traslado de conocimiento de un sitio geográfico a otro son cada vez más vertiginosos y dinámicos. En este caso, los conocimientos de los que se habla, son todos aquellos que las diferentes redes criminales están interesadas en obtener, en aras de realizar una labor criminal más eficiente.

El objetivo de este documento es mostrar los mecanismos de transferencia de tecnología que existen, bien sea en un país o de manera transnacional, y ubicar cuáles de esos mecanismos pueden ser usados por las empresas criminales para acceder al conocimiento necesario en el desarrollo de sus actividades ilícitas. El documento empezará en un primera parte por mostrar los diferentes medios de transferencia de tecnología, teniendo en cuenta la evolución de los paradigmas a

¹ DOBRIANSKY, Paula. *El Crecimiento explosivo del crimen mundializado*. Cuestiones Mundiales. Periódico Electrónico del Departamento de Estado de Estados Unidos. Volumen 6, Número 2. Agosto 2001.

este respecto. En una segunda parte se mostrará cómo la tecnología ha influido en las redes criminales en sus actividades y la importancia que adquieren los conocimientos innovadores en la comisión de delitos, así como algunos mecanismos que pueden ser implementados para controlar este fenómeno. Por último se concluye mostrando que el entender el funcionamiento e importancia de la transferencia de tecnología en las redes criminales, es un primer paso para contrarrestar sus efectos y desarrollar políticas de defensa contra sus actividades.

Aunque el término “crimen organizado”, como lo muestran Beltrán y Silva presenta problemas en su definición,² para el desarrollo de este documento se utilizarán dos definiciones. La primera es extractada de la legislación de California, Estados Unidos:

Crimen Organizado consiste en dos o más personas que, con un propósito de continuidad, se involucran en una o más de las siguientes actividades: (a) la oferta de bienes ilegales y servicios, por ejemplo, el vicio, la usura, etcétera, y (b) delitos de predación, por ejemplo, el robo, el atraco, etcétera. Diversos tipos específicos de actividad criminal se sitúan dentro de la definición de crimen organizado. Estos tipos pueden ser agrupados en cinco categorías generales: (1) Mafia: actividades criminales organizadas. (2) Operaciones viciosas: negocio continuado de suministrar bienes y servicios ilegales, por ejemplo, drogas, prostitución, usura, juego. (3) Bandas de asaltantes-vendedores de artículos robados: grupos que se organizan y se involucran continuamente en un tipo concreto de robo como proyectos de fraude, documentos fraudulentos, robos con allanamiento de morada, robo de coches y secuestros de camiones y adquisición de bienes robados. (4) Pandillas: grupos que hacen causa común para involucrarse en actos ilegales. (5) Terroristas: grupos de individuos que se combinan para cometer actos criminales espectaculares como el asesinato o el secuestro de personas prominentes para erosionar la confianza del público en el gobierno establecido por razones políticas o para vengar por algún agravio.

La otra definición es la que promulga la ONU, y que define al crimen organizado como:

Las actividades colectivas de tres o más personas, unidas por vínculos jerárquicos o de relación personal, que permitan a sus dirigentes obtener beneficios o controlar territorios o mercados, nacionales o extranjeros, mediante la violencia, la intimidación o la corrupción, tanto al servicio de la actividad delictiva como con fines de infiltrarse en la economía legítima, en particular por medio de: (a) el tráfico ilícito de estupefacientes o sustancias sicotrópicas y el blanqueo de dinero, tal como se definen en la Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Sicotrópicas de 1998; (b) la trata de personas, tal como se define en el Convenio para la represión de la trata de personas y de la explotación de la prostitución ajena de 1949; (c) la falsificación de dinero, tal como se define en el Convenio internacional para la represión de la falsificación de moneda de 1929; (d) El tráfico ilícito o el robo de objetos culturales, tal como se definen en la Convención sobre medidas que deben adoptarse para prohibir e

² DE LEÓN BELTRÁN, Isaac; SILVA, Germán. *Problemas sociológicos y de tipificación penal relacionados con el crimen organizado*. Borradores de Método Área de Crimen y Conflicto. Documento 25. junio 15 de 2004.

impedir la importación, la exportación y la transferencia e [sic] propiedad ilícita de bienes culturales de 1970 y la Convención sobre bienes culturales robados o ilegalmente exportados de 1995 del Instituto Internacional para la Unificación del Derecho Privado de las Naciones Unidas para la Educación, la Ciencia y la Cultura; (e) el robo de material nuclear, su uso indebido o la amenaza de uso indebido en perjuicio de la población, tal como se define en la Convención sobre la protección física de los materiales nucleares de 1980; (f) los actos terroristas; (g) el tráfico ilícito o el robo de armas y materiales o dispositivos explosivos; (h) el tráfico ilícito o el robo de vehículos automotores; e (i) la corrupción de funcionarios públicos

De la misma manera, es necesario establecer que el crimen organizado tiene particularidades frente a otro tipo de delitos (ver tabla).

Diferencias entre los delitos del crimen organizado y otros tipos de delitos

	CRIMEN ORGANIZADO	OTROS TIPOS DE DELITO
Transacción	Producción y distribución de nuevos bienes y servicios	Redistribución de la riqueza existente
Relaciones	Intercambio multilateral	Transferencia bilateral
Intercambio	Consensual	Involuntario
Víctimas	¿Sociedad?	Individuos o empresas
Moralidad	Ambigua	No ambigua
Política pública	¿Criminalizar la asociación? ¿Interceptar los activos?	Castigar al criminal Restaurar la propiedad

FUENTE: R. Thomas Naylor, "Mafias, myths, and markets: on the theory of enterprise crime", *Transnational Organized Crime*, vol. 3, núm. 3 (Otoño de 1997), pág. 4.

Aunque las definiciones y la tabla abarcan un amplio espectro de lo que se puede considerar *crimen organizado*, y actualmente no hay consenso entre los académicos y formuladores de política acerca de lo que éste es e implica, para el desarrollo de

este documento, las definiciones son útiles para mostrar cómo la tecnología y el conocimiento influyen en los métodos criminales para la comisión de delitos.

1. Transferencia de Tecnología

En los diferentes indicadores de desarrollo de un país, la Ciencia, la Tecnología y la Innovación (C+T+I), ocupan un lugar predominante, ya que se asume que hay una estrecha relación entre generación de nuevo conocimiento, crecimiento económico y bienestar general de la población³.

En ese orden de ideas, la transferencia de tecnología se incorpora en los procesos de adquisición de conocimiento por parte de aquellos que los requieren para sus procesos productivos. Según Maskus, la transferencia de tecnología es “cualquier proceso por medio del cual una parte obtiene acceso a información técnica de otra, y logra de manera exitosa aprenderla y absorberla para su incorporación en procesos de producción. La tecnología puede estar codificada (e.g. en planos) o no codificada (e.g. el know-how de los ingenieros). Puede estar incorporada en productos o desincorporada en ideas; abarca desde la selección de combinaciones de insumos y la calidad de los resultados, hasta las etapas de producción, la gerencia y los medios de financiación, entre otros elementos⁴”.

Maskus también muestra que los procesos de transferencia de tecnología se dan bajo mecanismos de mercado y en mecanismos fuera de éste. Los primeros, que incluyen al comercio de bienes y servicios, la inversión extranjera directa, el licenciamiento, los joint-ventures y la movilidad de personal a través de fronteras son las principales vías de este conocimiento. Sin embargo, también existen mecanismos fuera de mercado tales como la imitación, la movilidad de empleados poseedores de conocimientos, el estudio de datos de prueba e información disponible en diferentes fuentes (p.e. los bancos de patentes), así como la migración temporal de estudiantes, científicos y personal técnico o administrativo hacia diferentes entidades y actividades (universidades, laboratorios o congresos), llevando consigo conocimiento desarrollado en su lugar de origen y que puede ser aplicado al sitio donde se llega.

³ No es casualidad que los países que se consideran más desarrollados sean los mayores generadores de conocimiento. Contrastando los datos del índice de competitividad elaborado por el Foro Económico Mundial con el gasto en I & D de los países, se encuentra que Estados Unidos, que ocupa el segundo puesto en el *ranking* de competitividad, gasta el 2.6% de su PIB en I & D. En el otro lado del espectro se encuentra Paraguay, que ocupa el puesto 100 y gasta el 0.10% de su PIB en I & D.

⁴ MASKUS, Keith E; *Transfer of Technology and Technological Capacity Building*. University of Colorado ICTSD-UNCTAD Dialogue, 2. Bellagio Series on Development and Intellectual Property, 18-21 Sept. 03

1.1. Nuevos Paradigmas de Transferencia de Tecnología

En su artículo *International technology transfer in small business: a new paradigm*, Balachandra⁵, reformula las tendencias tradicionales de transferencia de tecnología, proponiendo nuevos postulados que indican un mayor dinamismo en lo que se refiere al traslado de conocimiento de una persona o sitio a otro. La comparación entre los viejos paradigmas y el nuevo se encuentran resumidos en la siguiente tabla.

Tema	Viejo Paradigma	Nuevo Paradigma
Tamaño de las empresas que ofrecen la tecnología	Grandes empresas	Pequeñas y medianas empresas
Forma de negociación de la tecnología.	Extensiva, intervención gubernamental y aprobación requerida.	Poca intervención gubernamental. Se maneja bajo mecanismos de mercado
Tecnología	Se debe adquirir un conjunto de conocimientos (no es tan fácil adquirir una tecnología específica).	Se puede adquirir la tecnología que se desee.
Proceso de transferencia	Largo, involucra a muchas personas, departamentos y vendedores.	Rápido, pocas personas y pocos vendedores.
Proceso de comunicación	Formal	Informal.

Fuente: Balachandra.

A partir de este cuadro se puede afirmar que el dinamismo dado en los procesos de transferencia de tecnología, permite que sea más fácil para una red criminal acceder a los conocimientos que requiere para posteriormente ejecutarlos en sus actividades, ya que los procesos de transferencia son más informales, dinámicos y, en la misma medida, con menores costos de transacción.

⁵ BALACHANDRA. R. (1996). *International Technology Transfer in Small Business: a New Paradigm*. Int J. Technology Management, Vol 12, Nos 5/6. Special Issue. Pp. 625-638.

1.2. Mecanismos de Transferencia de Tecnología

Los mecanismos actuales que se usan en los procesos de transferencia de tecnología son:

- Patentes y acuerdos de patentes
- Acuerdo de Asistencia Técnica
- Acuerdo de Know How
- Acuerdo de servicios de ingeniería
- Acuerdo sobre marcas comerciales
- Acuerdo de concesión

Todos estos acuerdos requieren unos procesos jurídicos para que la transferencia de tecnología se lleve a cabo. Sin embargo, en el acuerdo de asistencia técnica que básicamente abarca la transmisión de un conocimiento específico por parte de un experto en el tema, se puede dar de manera informal, permitiendo por ejemplo que una red criminal, contrate a alguien para que los entrene específicamente en el conocimiento que necesitan. Por ejemplo, el 6 de septiembre de 2000, la Fiscalía General de la Nación encontró un submarino en Facatativa, Cundinamarca, con el que el narcotráfico pretendía llevar drogas ilícitas a los Estados Unidos sin ser detectado. En este caso en particular, se requirió de la aplicación de varias áreas del conocimiento y de la asesoría de expertos en el tema, para llevar a cabo esta actividad sin precedentes en el país⁷.

2. Transferencia de Tecnología y Crimen Organizado

El uso de tecnología en procesos criminales se puede dividir en dos categorías:

- Crímenes que usan la tecnología como una herramienta secundaria en la comisión de delitos.
- Crímenes que requieren del uso directo de la tecnología en la consecución de una actividad ilícita.

En el primer grupo se encuentran aquellos crímenes que se han llevado a cabo sin que la tecnología existente sea relevante, pero han sabido aprovechar las

⁶ Sistema madri+d. <http://www.madrimasd.org/iberoamerica/servicios/asesoramiento/faq/faq.asp#14>
Consulta (Diciembre 2, 2004)

⁷ CASTILLO, Fabio. *Cocaina.com.co*. En: El Espectador. Agosto 18. 2002.

innovaciones desarrolladas para ser más eficientes en la ejecución del delito. Un ejemplo de esto es lo que se conoce como el timo del prisionero español. En la década de los años 20 éste se hizo muy popular:

En él, las víctimas eran contactadas por alguien pidiendo ayuda para sacar de prisión al hijo de una acaudalada familia. Por supuesto, la recompensa cubriría con creces el dinero adelantado para el soborno de policías y carceleros. Pero imprevistos de última hora hacían fracasar siempre la operación⁸.

Este crimen siguió desarrollándose e incluso trascendió fronteras, ya que otros países empezaron a utilizarlo. Tal es así que

En los años ochenta, y valiéndose de cartas escritas a máquina y enviadas por correo regular, timadores profesionales con base probablemente en Nigeria inundaron el mundo con propuestas "falsas" sobre lavado de dinero fruto de supuesta corrupción gubernamental. Básicamente ofrecían un porcentaje del 25 % sobre el total del dinero "lavado" para lo cual uno debía prestar su nombre y datos como "proveedor" de grandes obras que habrían tenido lugar en Nigeria. Siendo que manejan cifras muy importantes: 25 millones de dólares o más, la supuesta comisión de US\$ 6,25 millones hizo caer a más de uno en dicha trampa. (...) Básicamente la estafa consiste en que para poder recibir dicho dinero había que abrir una cuenta corriente en el Banco Central de Nigeria, la cual posee un mínimo de US\$ 5.000. Aparentemente, este banco estaría controlado por estas personas, y luego de recibido el dinero, uno no sabe más de ellos y en el banco no dan explicaciones por lo que técnicamente se quedan con esos US\$ 5.000. Y ellos ya saben que por US\$ 5.000 no da para viajar a Nigeria a reclamar nada, además de que allí no existen demasiadas seguridades jurídicas como para reclamarle nada a nadie y menos a funcionarios gubernamentales⁹.

Se calcula que en esta época los estafadores lograron que más de 50.000 personas enviaran sus cinco mil dólares, por lo que se quedaron con 250 millones de dólares. Teniendo en cuenta que esto se hizo con cartas a hechas a máquina, el potencial que tiene este crimen con uso de nuevas tecnologías es bastante alto.

Actualmente, se cuentan con millones de bases de datos y la rapidez del correo electrónico, lo que brinda a los estafadores la capacidad de llegar a millones de personas que usan el correo electrónico, con lo que las cifras prometidas llegan a los US\$ 5 millones.¹⁰ La modalidad más reciente de este tipo de estafa es la que se denomina como 'phising'.

El *modus operandi* de estos delincuentes cibernautas, comienza con un correo diciendo que necesitan con urgencia actualizar la información financiera de su cuenta. Ocasionalmente se hacen pasar incluso por el banco (usualmente el Citibank) aduciendo que necesitan hacer una actualización de la información de la cuenta. Si uno sigue las instrucciones de estos correos, será llevado a sitios web fraudulentos, con aspecto de banco, en donde le solicitarán información financiera y datos personales. Las estadísticas señalan que de Mayo a Junio, los ataques denominados "Phishing" crecieron casi un 50%. Inicialmente utilizan un correo de retorno fraguado, por lo que aparentan resultar creíbles. De acuerdo a un reporte de Gartner Research, sólo el año pasado el 57% de los

⁸ CRIADO, Miguel Angel. *¡Cuidado con los timos!*. En: ARIADNA, El mundo. Enero 18, 2004.

⁹ CALANDRA, Gianni. *Estafa por Internet*. En: Guía de la computación. Edición 84. Octubre. 2001.

¹⁰ CASTILLO, Fabio. *Travesía para ser millonario*. En: El Espectador. Junio, 2004.

norteamericanos recibieron un correo de algún phisher. Más preocupante aún, es el hecho de que casi el 19% hizo clic en la URL contenida en el mismo. De acuerdo a un estudio de Webroot (compañía de software que está por lanzar un programa gratuito anti-phisher), la estafa promedio es de US\$ 1.200 y usualmente caen con más facilidad usuarios mayores (entre 50 y 70 años), que tienden a confiar con más facilidad que otros en este tipo de mensaje, y además son generalmente más solventes¹¹.

Como lo establece este ejemplo, esta primera categoría que relaciona crimen con tecnología demuestra que aunque el crimen es en esencia el mismo, son los mecanismos para llegar a las potenciales víctimas, los que varían de acuerdo al desarrollo tecnológico.

En la segunda categoría, la de los crímenes en los que el uso de la tecnología es indispensable para llevarse a cabo, se encuentran principalmente aquellos delitos en los que el computador y las redes de comunicación electrónicas como Internet tienen directa participación en la ejecución de los crímenes. Actualmente este tipo de delitos se denomina 'cibercrimen'. Dentro de los principales delitos de esta categoría se encuentran¹²:

- **Diseminación de material ofensivo:** Este incluye la publicación y distribución de material sexual explícito, propaganda racista e instrucciones para la fabricación de material explosivo e incendiario, entre otros. Aunque anteriormente se desarrollaban actividades criminales similares, lo cierto es que con el auge de Internet, los que publican y distribuyen este material a través de la red, tienen resultados antes impensados y con consecuencias que tienen preocupadas a las autoridades encargadas de controlar este tipo de delitos.
- **Lavado electrónico de dinero:** Actualmente las instituciones financieras multinacionales no son las únicas con la capacidad de realizar transferencias de dinero de diferentes jurisdicciones en cuestión de segundos. Esto es aprovechado por las organizaciones criminales para lavar su dinero, ya que pueden soslayar la supervisión de un banco central.
- **Vandalismo electrónico:** De este crimen se puede decir que nació con la invención de Internet, ya que antes era muy aislado el caso de personas que ingresaran a empresas a realizar actos vandálicos con el fin de perjudicarlas. Actualmente, la sociedad industrial depende tanto de los sistemas de telecomunicaciones y de complejos procesadores de datos, que un sabotaje contra estas herramientas puede causar daños catastróficos, no solo a las empresas sino incluso a gobiernos.

¹¹ CALANDRA, Gianni. *Phishing: El último alarido de la moda en delitos de Internet*. En: Guía de la computación. Edición 110. septiembre, 2004.

¹² WRIGHT, Paul; SMITH, Russell; GRABOSKY, P.N. *Crime and Telecommunications*. Australian Institute of Criminology. Trends and Issues. Agosto, 1996.

Aunque existen otros delitos que aprovechan las tecnologías para su ejecución como el fraude electrónico, el fraude en la transferencia electrónica de fondos y el robo de propiedad intelectual, los tres primeros enunciados son los más representativos e ilustran el potencial que tienen las nuevas tecnologías para cometer crímenes si son usadas por las personas u organizaciones equivocadas.

Las principales razones por las que el crimen organizado ha sabido hacer uso de las herramientas tecnológicas en el desarrollo de sus actividades son¹³:

- Ha permitido flexibilizar las estructuras de las organizaciones permitiendo una actuación en redes que tiende a maximizar los beneficios y evitar la eventual actuación de las agencias de seguridad.
- Por otro, ha evitado la acumulación de papeleo eliminando así muchas de las pruebas incriminatorias que podrían allanar las actuaciones policiales de represión.
- Se ha producido una transformación en la naturaleza de las amenazas a la seguridad, que si antes estaban asociadas a grandes acumulaciones de poder, recursos y territorio, en la actualidad pasan por el control y generación de información.

Formas de combatir la tecnología en el crimen organizado

Las características excepcionales de los delitos ejecutados por organizaciones criminales usando como herramientas las nuevas tecnologías, hacen que su control sea en la actualidad insuficiente. Además es necesario decir que “existe una tendencia global hacia la interdependencia y cooperación entre todas las organizaciones delictivas, circunstancia que hace imposible contrarrestar el accionar de éstas con el esfuerzo aislado de los estados”¹⁴. Por esta razón, es necesaria la cooperación de los países así como el actuar de las organizaciones internacionales para controlar de manera global y conjunta las actividades ilegales desarrolladas por las organizaciones criminales.

¹³ NESTARES, Carlos. *Crimen Organizado Transnacional: Definición, Causas y Consecuencias*. Universidad Autónoma de Madrid. En www.uam.es/personal_pdj/economicas/cresa/text11.html Consulta (Noviembre 15 de 2004).

¹⁴ DUARTE, Roberto. *La Globalización y el Riesgo del Crimen Organizado Transnacional*. En: VII Encuentro Nacional de Estudios Estratégicos. Noviembre 2 al 4 de 2004.

Actualmente, diversos organismos como las Naciones Unidas, la OEA y la Unión Europea, promueven actividades y proyectos para estudiar y tratar de controlar este fenómeno. Sin embargo los resultados son aún incipientes.

Dentro de las recomendaciones hechas por Duarte en su ponencia “*La Globalización y el Riesgo del Crimen Organizado Transnacional*”, el autor expone que es necesario armonizar los procedimientos de extradición sobre la base de acuerdos multilaterales para incrementar la eficacia policial y jurídica, en la prevención y represión de esta modalidad criminal. Otra medida propuesta por el autor, es la de considerar la tipificación internacional del delito, mediante acuerdos bilaterales o multilaterales, para que un delito que involucre dos o más países por parte de organizaciones criminales y que además tenga un componente tecnológico, pueda ser castigado con rapidez y eficiencia.

3. Conclusiones

El objetivo de este documento fue mostrar la relación entre la transferencia de tecnología y las actividades criminales, en este caso, las desempeñadas por el crimen organizado. Esta relación está entendida como el uso que hacen las organizaciones criminales de nuevos conocimientos e innovaciones para llevar a cabo actividades delictivas.

En primera instancia se puede concluir que los nuevos mecanismos de transferencia de tecnología, caracterizados por ser más dinámicos, informales y de bajo costo, son ideales para que las organizaciones criminales puedan hacer uso de nuevo conocimiento que sea útil en sus actividades delictivas. Por esta razón, aunque cualquier individuo puede aprovechar los adelantos tecnológicos para usarlo con fines ilegales, las organizaciones criminales brindan un escenario ideal al contar con una infraestructura sólida, que le brinda economías de escala y por ende, permite un mayor flujo de conocimiento para usar inventos e innovaciones en actividades criminales.

También es importante establecer que el uso de la tecnología por parte de las organizaciones criminales puede ser dividido en dos categorías: crímenes que usan la tecnología como una herramienta secundaria en la comisión de delitos y crímenes que requieren del uso directo de la tecnología en la consecución de los mismos. Estas dos categorías muestran que la tecnología no es mala *per se*, sino que todo depende del uso que se le de, en este caso el uso que le dan las organizaciones criminales para su propio beneficio, obviamente perjudica a individuos, empresas, gobiernos y a la sociedad en general.

Finalmente, es necesario que los gobiernos y los organismos internacionales realicen proyectos de cooperación y actividades conjuntas para reprimir y desincentivar a las organizaciones criminales a usar desarrollos tecnológicos en sus actividades, ya que es claro que un país actuando individualmente, no tiene la infraestructura ni la institucionalidad necesaria para contrarrestar este fenómeno.

Referencias Bibliográficas

- BALACHANDRA, R. (1996). *International Technology Transfer in Small Business: a New Paradigm* Int J. Technology Management, Vol 12, Nos 5/6. Special Issue. Pp. 625-638.
- CALANDRA, Gianni. *Estafa por Internet*. En: Guía de la computación. Edición 84. Octubre. 2001.
- CALANDRA, Gianni. *Phishing: El último alarido de la moda en delitos de Internet*. En: Guía de la computación. Edición 110. Septiembre, 2004.
- CASTILLO, Fabio. *Cocaina.com.co*. En: El Espectador. Agosto 18. 2002.
- CASTILLO, Fabio. *Travesía para ser millonario*. En: El Espectador. Junio, 2004.
- CRIADO, Miguel Angel. *¡Cuidado con los timos!*. En: ARIADNA, El mundo. Enero 18, 2004.
- DE LEÓN BELTRÁN, Isaac; SILVA, Germán. *Problemas sociológicos y de tipificación penal relacionados con el crimen organizado*. Borradores de Método Área de Crimen y Conflicto. Documento 25. junio 15 de 2004.
- DOBRIANSKY, Paula. *El Crecimiento explosivo del crimen mundializado*. Cuestiones Mundiales. Periódico Electrónico del Departamento de Estado de Estados Unidos. Volumen 6, Número 2. Agosto 2001.
- DUARTE, Roberto. *La Globalización y el Riesgo del Crimen Organizado Transnacional*. En: VII Encuentro Nacional de Estudios Estratégicos. Noviembre 2 al 4 de 2004.
- MASKUS, Keith E; *Transfer of Technology and Technological Capacity Building*. University of Colorado ICTSD-UNCTAD Dialogue, 2. Bellagio Series on Development and Intellectual Property, 18-21 Sept. 03
- NESTARES, Carlos. *Crimen Organizado Transnacional: Definición, Causas y Consecuencias*. Universidad Autónoma de Madrid. En www.uam.es/personal_pdj/economicas/cresa/text11.html
- SISTEMA MADRI+D. <http://www.madrimasd.org/iberoamerica/servicios/asesoramiento/faq/faq.asp#14>
- WRIGHT, Paul; SMITH, Russell; GRABOSKY, P.N. *Crime and Telecommunications*. Australian Institute of Criminology. Trends and Issues. Agosto, 1996.