Conferencia sobre "Cyber Money Laundering" variante "Cyber Gambling"

(transcripción de la exposición realizada el 08-08-2013 en el CARI)

Prof. Dr. Roberto Uzal (*)
Director del Doctorado en Ingeniería Informática
Universidad Nacional de San Luis
Miembro del Grupo de Trabajo sobre Criminalidad Organizada Transnacional
Consejo Argentino para las Relaciones Internacionales

Introducción

Este trabajo constituye un nuevo aporte de conceptos y aspectos instrumentales del Grupo Criminalidad Organizada Transnacional del CARI y del Laboratorio de Calidad e Ingeniería de Software de la Universidad Nacional de San Luis en el ámbito de la Ciberdefensa y de la Ciberseguridad [1]. No se trata de una contribución aislada. Está sustentada en trabajos previos y está orientada a constituirse en el origen de importantes trabajos de I+D.

En este caso se propone la utilización del enfoque y de las herramientas de "Análisis de Flujo de Datos" [2][3] como medios idóneos para encarar la prevención y la lucha contra el denominado Cyber Money Laundering - Ciber Lavado de Dinero [4][5]. Se muestra que el "seguimiento de la ruta del dinero", en el caso de Cyber Money Laundering es inconducente e ineficaz. Se propone un desplazamiento del foco de las acciones "anti lavado" desde "lo jurídico financiero" a "lo tecnológico informático".

En el caso del Cyber Money Laundering, los "Patrones de Comportamiento" de los "Flujos de Datos" en las redes teleinformáticas ofrecen mayores oportunidades de éxito a quienes investigan Lavado de Activos que el "seguimiento de la ruta del dinero". En este trabajo se detalla el funcionamiento de un esquema en particular del Cyber Money Laundering para demostrar las dificultades de investigar usando los enfoques "canónicos" recomendados por organismos de control nacionales e internacionales. Se detalla la variante de Cyber Money Laundering denominada Cyber Gambling - Apuestas utilizando Internet [6][7][8] que es la más efectiva, según lo relevado por el autor, de estas modalidades delictivas.

Como contribución sustantiva se propone que, ante evidencia forense no rebatible de Cyber Money Laundering, organismos internacionales tales como Interpol, sean facultados para "neutralizar" los "Command & Control Servers" y "Master Botnet" correspondientes a una infraestructura tecnológica de Cyber Money Laundering.

La tendencia al reemplazo de los métodos "tradicionales" de Lavado de Activos hacia lo que internacionalmente se conoce como Cyber Money Laundering es cada día que pasa más notoria.

En el ejemplo citado en la lámina siguiente se distingue: a) la existencia de empresas cuyo negocio es proporcionar servicios de lavado y b) el uso en expansión de dinero "virtual" / "digital" el que facilita aún más la operatoria de los esquemas de Cyber Money Laundering.

***Nota importante**: El presente es un trabajo de reflexiones académicas. No deben considerarse como comprobadas las referencias a estados naciones, instituciones financieras o personas físicas. Simplemente se suministran ejemplos que no guardan relación con circunstancias específicas. Sólo se busca otorgar características tangibles a los planteos y propuestas formulados.*

1. La Agenda

    a. Motivación
    b. ¿Qué es Cyber Money Laundering?
    c. Entornos propicios para el Cyber Money Laundering
    d. "Ventajas" del Cyber Money Laundering
    e. Efectos sinérgicos: El "Cyber Gambling"

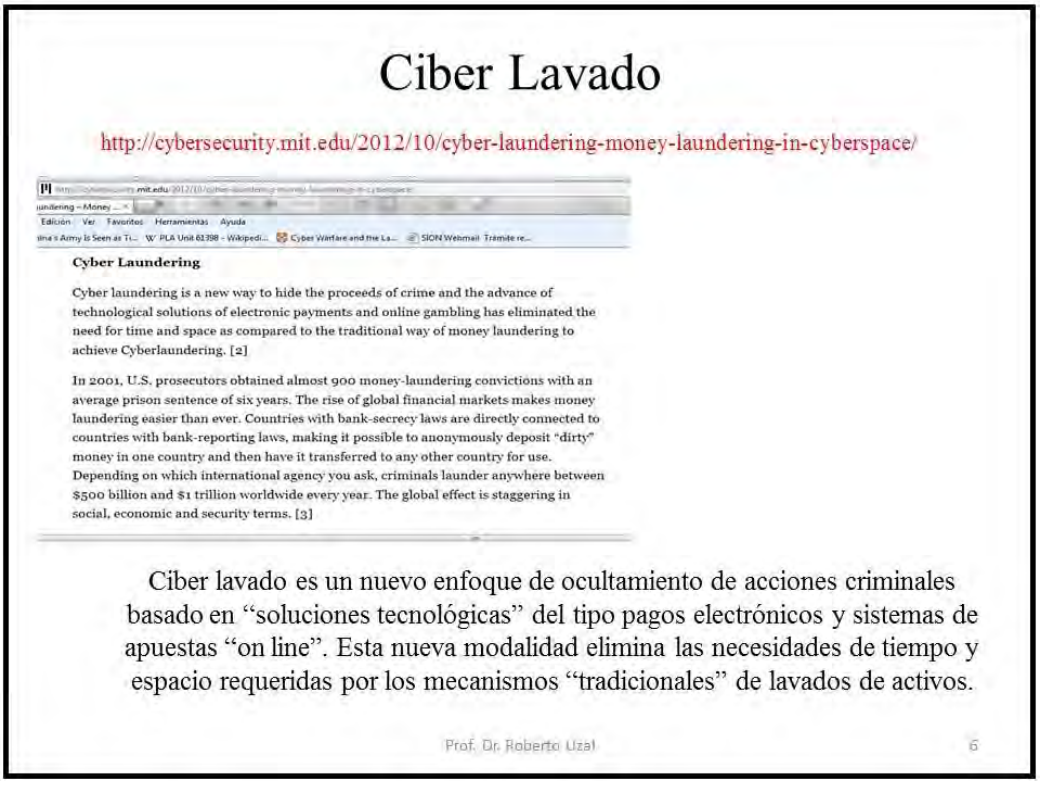
f. El caso "Second Life": La tendencia
g. Capacidad de Lobby (del "Cyber Gambling")
h. Aporte de la Universidad de Hamburgo
i. "Cadena de Valor" del Ciber Juego ("Cyber Gambling")
j. Los orígenes de estas "empresas de servicios"
k. Conceptos de Master botnet y C & C Server (su uso en Ciber Juego – Cyber Gambling)
l. Analogías conceptuales y tecnológicas con el enfoque utilizado en la guerra entre Rusia y Estonia
m. Efecto del Cyber Laundering / Cyber Gambling: smartphones, PC y tablets realizando apuestas sin que sus usuarios lo sepan
n. "Arquitectura Conceptual del Negocio": Una Unidad de Negocios "Cyber Gambling" en una isla estado – nación imaginaria
o. La ruta del dinero (Proceso de Lavado)
p. Gerenciamiento del tiempo y del cash flow en el proceso de lavado
q. ¿Cómo enfrentar con eficacia el uso de Internet para el Lavado de Activos? Conclusiones
r. Aspectos pendientes a ser discutidos

2. Motivación

a. El "volumen" del "negocio" Lavado de Activos, con tendencia a adoptar mayormente la forma de Cyber Money Laundering
b. La "prioridad" que Cyber Money Laundering está adquiriendo en la Criminalidad Organizada Transnacional: como se mostrará en la exposición, Cyber Money Laundering posee una "Rentabilidad Esperada" tal que supera a la de los "delitos precedentes" (narcotráfico, corrupción gubernamental o tráfico ilegal de armas)
c. El golpe más serio que podrían recibir el narcotráfico, la corrupción gubernamental y el tráfico ilegal de armas sería la imposibilidad del Lavado de Activos adquiridos fraudulentamente. En dicho contexto no caben dudas, según lo relevado por el autor, que el núcleo del Lavado de Activos, en la actualidad, lo es el denominado Cyber Money Laundering.

3. ¿Qué es Cyber Money Laundering?

"Ciber Lavado" es un nuevo enfoque de ocultamiento de acciones criminales basado en "soluciones tecnológicas" del tipo "pagos electrónicos" y "sistemas de apuestas *on line*". Esta nueva modalidad elimina las necesidades de tiempo y espacio requeridas por los mecanismos "tradicionales" de Lavado de Activos. Se sugiere estudiar, por ejemplo, posturas como las del área Cyber security del Massachusetts Institute of Technology [9].



4. Entornos propicios para el Cyber Money Laundering

   Entre otros, se mencionan:

   a. Sistemas de apuestas “on line” mediante Internet
   b. Sistemas de “pagos electrónicos” mediante Internet
   c. Sistemas de compras “on line”
   d. Sistemas de prestación de servicios de Licitaciones Electrónicas
   e. Sistemas de prestación de servicios de “dinero plástico”
   f. Tarjetas de compras pre pagas
   g. Servicios de pornografía y de películas para adultos
   h. Servicios de agencias matrimoniales mediante Internet
   i. Servicios de sexo o de citas mediante Internet
   j. Servicios de consultoría “on line”
   k. Servicios educativos mediante Internet

5. “Ventajas” del Cyber Money Laundering

   Se entiende que se trata de “ventajas” para los delicuentes:

   a. Dinero sucio “lavado” en plazos muchísimos más breves
   b. Operación muchísimo más discreta. Difícilmente se dará el caso de secretarias despechadas o empleados resentidos revelando detalles de la operatoria.
   c. “Seguridad” o sea impunidad para el lavador
   d. Enfoque global: la operación de lavado queda diluida en el mundo lo que dificulta la labor de policías, fiscales y jueces
   e. Caída significativa de “costos operativos”: Los montos de las erogaciones correspondientes a los sobornos que están asociados al “lavado tradicional”, caen muy significativamente.
   f. No hay necesidad de testaferros; la experiencia indica que, con el transcurso del tiempo, terminan desnaturalizando su rol de tales auto promocionándose a socios (en el “mejor” de los casos)

6. Efectos sinérgicos: El “Cyber Gambling”

   Está globalmente asumido que el juego, las apuestas, constituyen ambientes “extremadamente amigables” para el Lavado de Activos desde siempre.

   Cuando interactúan el juego / las apuestas con redes de alcance mundial (Internet y redes “asociadas”, se produce un efecto sinérgico que, con el correspondiente know how en

Administración Financiera y en Tecnología Informática, facilitan el Lavado de Activos y minimizan los riesgos de los delincuentes.

7. El caso “Second Life”: Un ejemplo de “la tendencia”

Second Life inicia sus actividades a mediados del año 2003. Es un “Mundo Virtual” que posibilita, a sus usuarios, tener una Segunda Vida en paralelo, en el Ciberespacio. Los que adhieran a la propuesta tendrán una vida afectiva / social, una carrera profesional y un desarrollo económico al margen del “mundo tradicional”.

Second Life tiene su propia "vida" económica y su propia moneda: dólares Linden (L$). Los "residentes" en el mundo virtual de Second Life pueden comprar y vender bienes y/o servicios; por supuesto bienes y/o servicios asociados a dicho mundo virtual.
Lo asombroso: Existe una tasa de conversión entre los dólares EEUU y los dólares Linden.

Antecedentes para ser estudiados en profundidad:

- El éxito de Second Life provocó que corporaciones como Dell, Coca Cola, Peugeot, Citroën, Nissan, Sony, Wells Fargo Bank, Reebok, General Motors, Intel, Microsoft, y muchas otras están desarrollando negocios en el mencionado "mundo virtual" y, sobre todo, han encarado agresivas campañas publicitarias en esta suerte de economía virtual paralela.
- Existen, en el contexto de Second Life, garantías respecto de los derechos de autor de los "residentes" y han logrado legalizar y hacer habitual el intercambio de la divisa virtual, el Linden Dólar, con dinero real, por ejemplo, Dólares de EEUU.

No se desea dejar la menor sombra de sospecha sobre los seguramente legítimos negocios de Linden Lab (creadores de Second Life). Eso sí, tampoco puede dejar de mencionarse que este tipo de contextos virtuales constituyen un verdadero paraíso para los especialistas en Ciber Lavado de Activos.

8. Capacidad de Lobby (del "Cyber Gambling")

La capacidad de lobby de las corporaciones empresariales orientadas al negocio del juego en general y del Cyber Gambling en particular es muy grande.

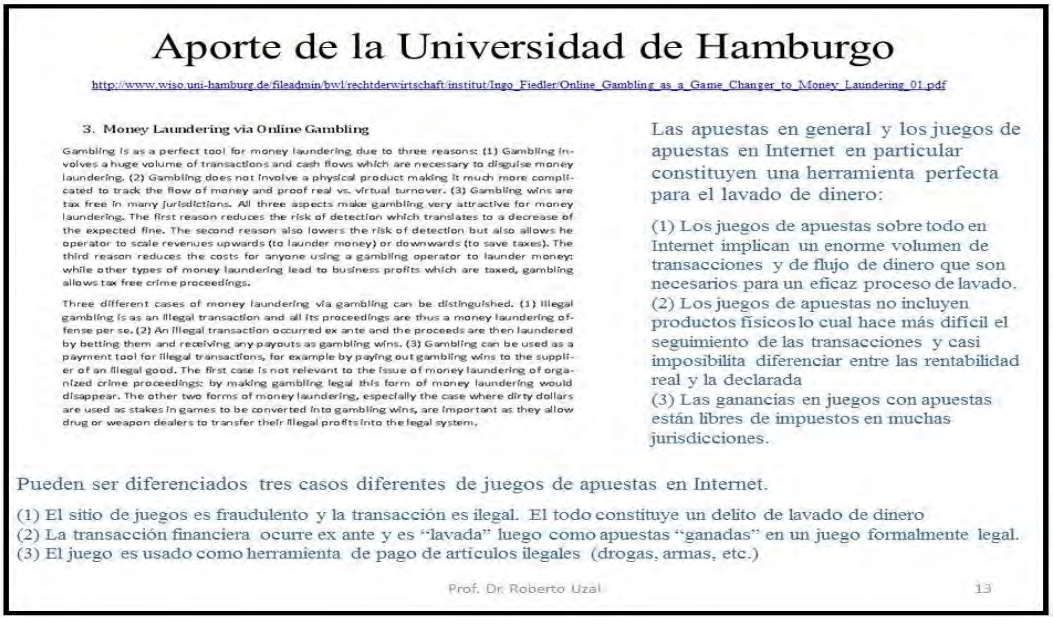
9. Aporte de la Universidad de Hamburgo

Las apuestas en general y los juegos de apuestas en Internet en particular constituyen una herramienta perfecta para el lavado de dinero [10]:

a. Los juegos de apuestas sobre todo en Internet implican un enorme volumen de transacciones y de flujo de dinero que son necesarios para un eficaz proceso de lavado.
b. Los juegos de apuestas no incluyen productos físicos lo cual hace más difícil el seguimiento de las transacciones y casi imposibilita diferenciar entre las rentabilidad real y la declarada
c. Las ganancias en juegos con apuestas están libres de impuestos en muchas jurisdicciones.

Pueden ser diferenciados tres casos diferentes de juegos de apuestas en Internet.

I. El sitio de juegos es fraudulento y la transacción es ilegal. El todo constituye un delito de lavado de dinero.
II. La transacción financiera ocurre “ex ante” y es “lavada” luego como apuestas “ganadas” en un juego formalmente legal.
III. Las “ganancias” del juego son utilizadas como medio de pago de artículos ilegales (drogas, armas, etc.)



Aporte de la Universidad de Hamburgo

http://www.wiso.uni-hamburg.de/fileadmin/bwl/rechtderwirtschaft/institut/Ingo_Fiedler/Online_Gambling_as_a_Game_Changer_to_Money_Laundering_01.pdf

3. Money Laundering via Online Gambling

Gambling is as a perfect tool for money laundering due to three reasons: (1) Gambling involves a huge volume of transactions and cash flows which are necessary to disguise money laundering. (2) Gambling does not involve a physical product making it much more complicated to track the flow of money and proof real vs. virtual turnover. (3) Gambling wins are tax free in many jurisdictions. All three aspects make gambling very attractive for money laundering. The first reason reduces the risk of detection which translates to a decrease of the expected fine. The second reason also lowers the risk of detection but also allows he operator to scale revenues upwards (to launder money) or downwards (to save taxes). The third reason reduces the costs for anyone using a gambling operator to launder money: while other types of money laundering lead to business profits which are taxed, gambling allows tax free crime proceedings.

Three different cases of money laundering via gambling can be distinguished. (1) Illegal gambling is as an illegal transaction and all its proceedings are thus a money laundering offense per se. (2) An illegal transaction occurred ex ante and the proceeds are then laundered by betting them and receiving any payouts as gambling wins. (3) Gambling can be used as a payment tool for illegal transactions, for example by paying out gambling wins to the supplier of an illegal good. The first case is not relevant to the issue of money laundering of organized crime proceedings: by making gambling legal this form of money laundering would disappear. The other two forms of money laundering, especially the case where dirty dollars are used as stakes in games to be converted into gambling wins, are important as they allow drug or weapon dealers to transfer their illegal profits into the legal system.

Las apuestas en general y los juegos de apuestas en Internet en particular constituyen una herramienta perfecta para el lavado de dinero:

(1) Los juegos de apuestas sobre todo en Internet implican un enorme volumen de transacciones y de flujo de dinero que son necesarios para un eficaz proceso de lavado.
(2) Los juegos de apuestas no incluyen productos físicos lo cual hace más difícil el seguimiento de las transacciones y casi imposibilita diferenciar entre las rentabilidad real y la declarada
(3) Las ganancias en juegos con apuestas están libres de impuestos en muchas jurisdicciones.

Pueden ser diferenciados tres casos diferentes de juegos de apuestas en Internet.

(1) El sitio de juegos es fraudulento y la transacción es ilegal. El todo constituye un delito de lavado de dinero
(2) La transacción financiera ocurre ex ante y es “lavada” luego como apuestas “ganadas” en un juego formalmente legal.
(3) El juego es usado como herramienta de pago de artículos ilegales (drogas, armas, etc.)

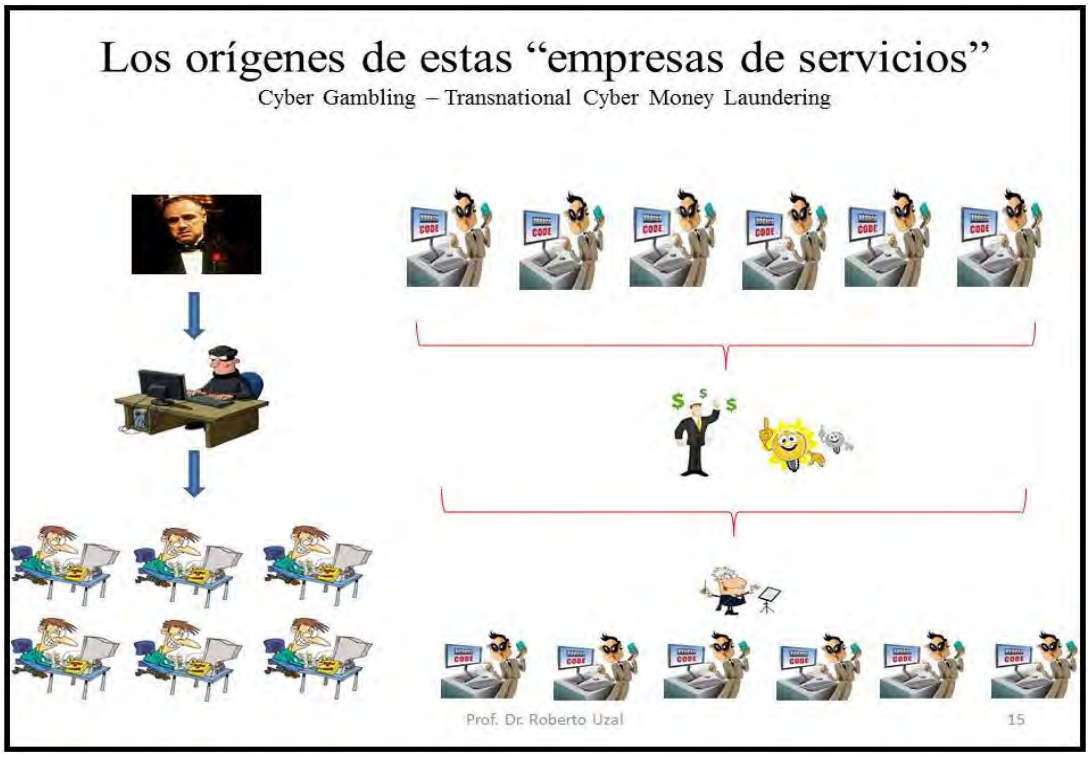
Prof. Dr. Roberto Uzal 13

10. “Cadena de Valor” del Ciber Juego (“Cyber Gambling”)

Niveles y roles

a. Nivel de la Inversión en nuevos tipos de Juegos: Comprende las inversiones para el desarrollo de nuevos módulos de software de juegos de apuestas, la publicidad acerca de estos módulos y su comercialización. Los beneficios en este nivel provienen del licenciamiento de los módulos para juegos de apuestas. Los clientes de este nivel son los administradores integrales de sitios de juegos de apuestas por Internet.
b. Nivel del Diseño y Desarrollo de los Productos (juegos): Incluye a los desarrollistas, diseñadores, artistas. Trabajan mediante esquemas de contratos individuales con los Inversores (nivel anterior).
c. Nivel del Hardware o Máquinas Virtuales o Plataforma de Software del Usuario Final: Consolas, módulos para smartphones, máquinas virtuales, interfaces con ambientes de redes sociales, etc. Sus clientes también lo son los administradores integrales de sitios de juegos de apuestas por Internet.
d. Nivel de las herramientas integradas y de la producción: Comprende la implementación de los contenidos integrales de los sitios de Ciber Juego, las herramientas para la gestión integral de sitios de “Ciber Juegos”, las interfaces con instituciones financieras, tarjetas de crédito, etc. Comprende esencialmente la Administración, la Producción y el Mantenimiento integral del sitio. Este es el nivel de las Unidades de Negocio de Cyber Gambling (de Apuestas *on line*).
e. Nivel del “holding” al que pertenece la Unidad de Negocio de Cyber Gambling (de Apuestas *on line*). En el “holding” hay unidades de negocio de ventas de libros por Internet, CD de música, artículos de belleza, de correos postales, etc. El “holding” debe estar en otro país y los estados contables consolidados se elaboran en el país en el que está radicado el “holding” (distinto estado nación en el que está basada la Unidad de Negocios de Juegos / Apuestas mediante Internet – Cyber Gambling). En caso de actividades fraudulentas (lavado) en Unidades de Negocio de Cyber Gambling, la no pertenencia a un “holding”, las coloca en situación de extrema vulnerabilidad ante investigadores “anti Lavado de Activos”).
f. Nivel del Marketing / Publicidad de las Unidades de Cyber Gambling orientado al Usuario Final (Apostador): Catálogos, difusión de información, …, destinados al Apostador. Sus clientes son las Unidades de Negocio de Cyber Gambling
g. Nivel del Usuario Final: Apostadores (reales y/o “fantasmas” con identidades robadas en el caso Lavado de Activos)

11. Los orígenes de las “empresas de servicios” de Cyber Money Gambling - Cyber Gambling



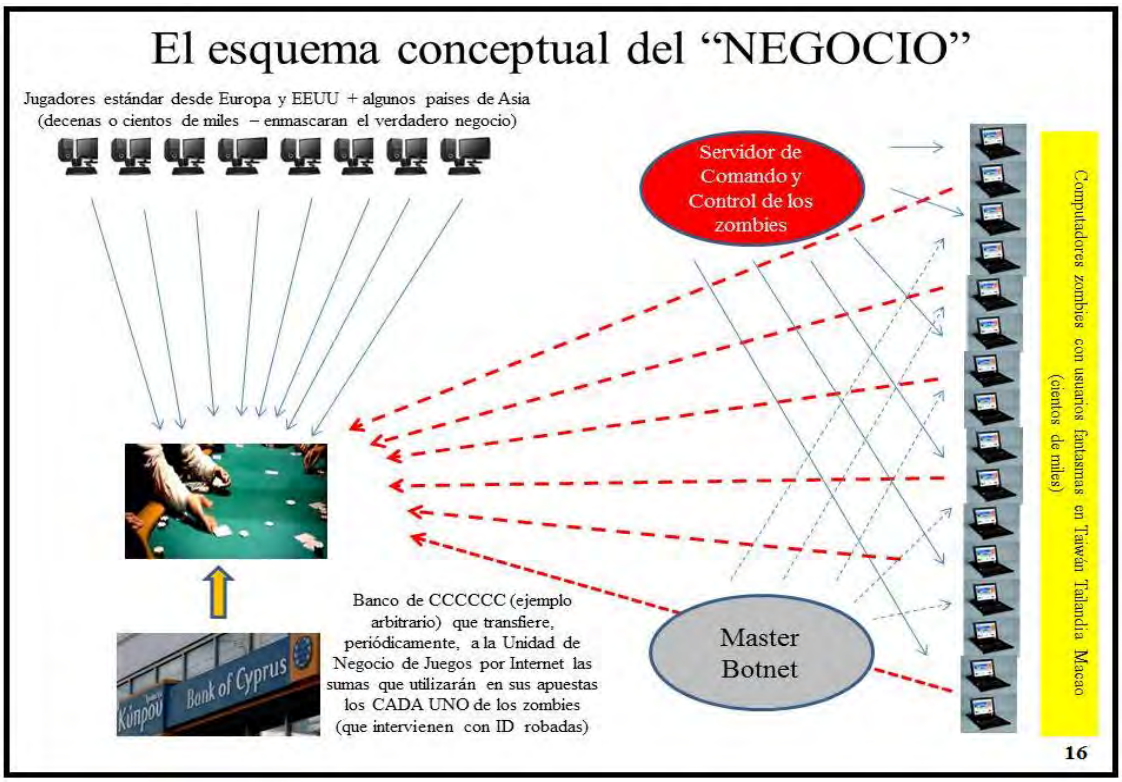
I. Una organización criminal transnacional que decide organizar una nueva “Unidad de Negocios”. Lidera el proceso un “experto” contratado “ad hoc” (hacker individual, ex empleado de una empresa de Seguridad Informática, ex agente de agencias estatales expertos en Seguridad Informática o Guerra Cibernética, delincuente con gran experiencia y gran solvencia en el tema)

II. Delincuentes (hacker) individuales que detectan las ventajas de estos esquemas asociativos. Seleccionan al líder de la nueva “Unidad de Negocios” y el “holding” del que formarán parte.

12. Conceptos de Master botnet y C & C Server (su uso en Cyber Gambling - Ciber Juego)

La ubicación geográfica de la Unidad de Negocios de Cyber Gambling es esencial [11][12][13][14]. Contar con el soporte de instituciones financieras “adecuadas” es otro “factor crítico de éxito”. La ubicación geográfica del “holding” al cual pertenece la Unidad de Negocios de Cyber Gambling, en otro estado nación, es otro aspecto muy importante. Acciones de marketing de alta eficacia deben provocar que exista una

importante "cartera de clientes reales" residentes, por ejemplo, en EEUU, Europa, Australia. Estos son clientes "estándar" y deben estar sometidos a reglas de juego muy claras, transparentes y fácilmente auditables.



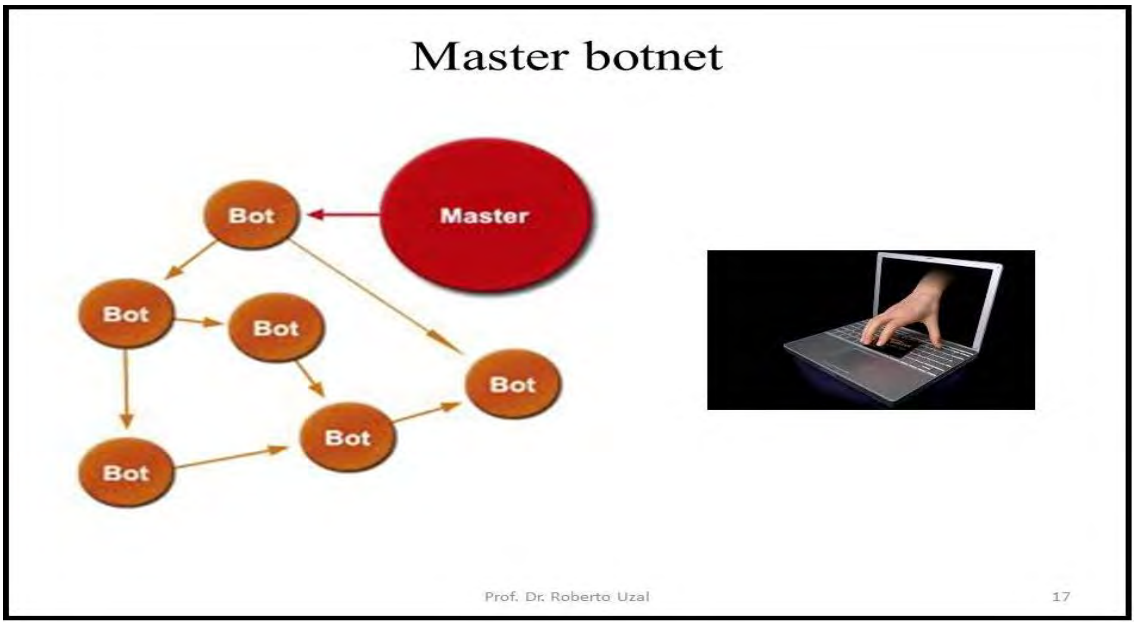
Las identidades de estos clientes reales deben poder ser fácilmente verificadas. Por otro lado, en estados naciones que, por razones de idioma, ubicación geográfica y barreras culturales, los mecanismos de control sean complicados de ser ejercidos, serán "reclutados", robo de identidad mediante, "apostadores zombies" o "fantasmas".

Centenares de miles de dispositivos del tipo computadores personales y smartphones, sin que los legítimos propietarios lo noten, operarán según pautas establecidas por los "Master Botnet" y de acuerdo a la "ordenes específicas / de detalle" impartidas por el correspondiente Command & Control Server.

Las identidades de los "apostadores zombies" o "fantasmas" serán utilizadas para abrir cuentas en el banco que opera en apoyo de la Unidad de Negocios de Cyber Gambling.

En dichas cuentas se depositará, distribuido convenientemente, el dinero del soborno.

Volviendo a la “red” de usuarios “zombies” o “fantasmas”: Se suele denominar "bot" a un tipo de malware (software malicioso) que posibilita a un agresor tomar el control de un dispositivo infectado. Casi siempre los bots ("robots en la web") conforman una red de máquinas infectadas que se denominan “botnet”. Los dispositivos infectados sin conocimiento de sus propietarios pueden estar distribuidos en áreas geográficas muy amplias. En el límite, pueden tener características globales. Dado que un dispositivo infectado por bots cumple las órdenes “externas”, es común referirse a estos “equipos víctima” como “zombies”.



El artífice y coordinador de una botnet o Master Botnet puede controlar todos los dispositivos infectados de forma remota y normalmente lo hace a través del IRC (Internet Relay Chat) el cual es un protocolo de comunicación en tiempo real basado en texto, que permite conversaciones entre dos o más usuarios. Recientemente se encuentran nuevas versiones de botnets enfocados hacia entornos de control mediante HTTP (Hyper Text Transfer Protocol - protocolo de transferencia de hipertexto). En este contexto, mantener el control de los dispositivos infectados es más sencillo.

Los dispositivos incluidos en una botnet reciben instrucciones para actuar ante situaciones específicas desde los Command-and-Control (C&C) Server (Servidores de Comando y Control). En el caso de Cyber Money Laundering – Cyber Gambling estas instrucciones serían:

- Inscribirse, con los datos robados al propietario del dispositivo, como apostador en la Unidad de Negocios de Cyber Gambling.

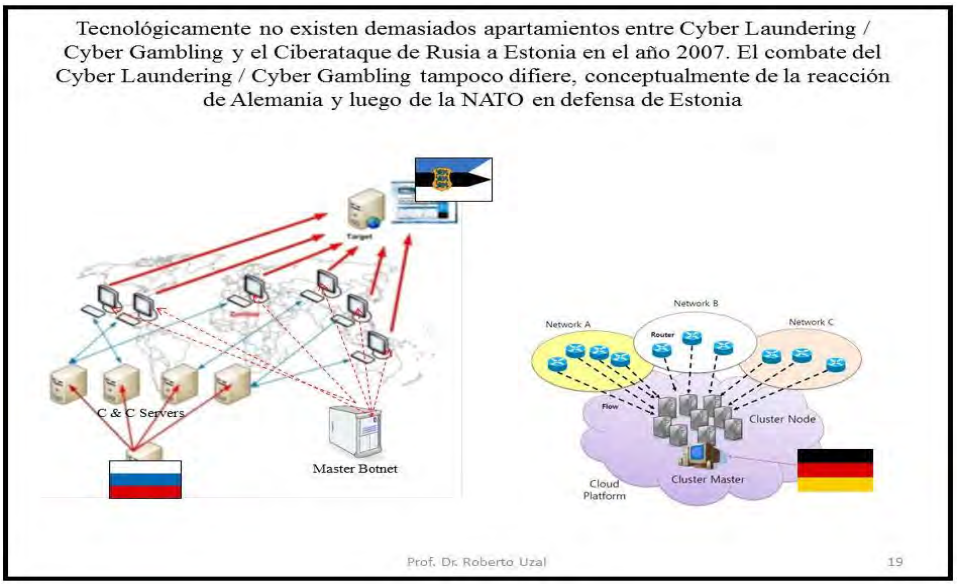
- Abrir una cuenta (obviamente fraudulenta) en el banco que da soporte a la Unidad de Negocios de Cyber Gambling.
- Realizar distintos tipos de apuestas
- Cerrar la cuenta.

El manejo del "timing" con el que actúa cada "zombie" es esencial en Cyber Money Laundering - Cyber Gambling. Administrar dicho "timing" es una función muy sensitiva de los Command-and-Control Servers.

13. Analogías con la guerra de Rusia y Estonia

Cuando Rusia comenzó su ataque a Estonia, el 27 de abril de 2007 [15][16][17], decenas de botnet (redes de zombies), en diversos territorios, habían sido conformadas. Cada botnet estaba regulada por su Master Bonet y estaba orientada a un blanco específico en Estonia. Dichos blancos lo fueron:

- Servidores del sistema de control de tráfico aéreo en Estonia.
- Servidores del sistema ferroviario de Estonia.
- Servidores del sistema de salud de Estonia.
- Servidores de distintas dependencias gubernamentales de Estonia
- Servidores correspondientes a la distribución energética de Estonia.
- Servidores de periódicos de Estonia



En la figura se modelan unos pocos "zombies", pertenecientes a un solo botnet, orientado a un único blanco (un servidor específico en Estonia).

Alemania, mediante un enfoque de Análisis de Flujo de Datos, logró reunir evidencia tal que le permitió a la NATO (Organización del Tratado del Atlántico Norte) intimar a Rusia para que interrumpiera sus ataques de Denegación de Servicios (DoS), es decir, saturación de los "servidores blanco" mediante requerimientos de alta prioridad (según los protocolos vigentes), provenientes de cientos de miles de "zombies" y efectuados una gran cantidad de veces por unidad de tiempo (segundo). La inutilización de "servidores blanco" mediante saturación de requerimientos es la esencia de los ataques DoS.

Existe una importante analogía entre lo ocurrido en el conflicto Rusia – Estonia con un esquema orientado al Cyber Money Laundering – Cyber Gambling:

- En Cyber Money Laundering – Cyber Gambling tambien se "reclutan" cientos de miles de "zombies" pero para interactuar fraudulentamente con la Unidad de Negocios de Cyber Gambling.
- Para detectar esquemas de Cyber Money Laundering – Cyber Gambling, en este trabajo se propone el uso de un enfoque de Análisis de Flujo de Datos que guarda una importante correspondencia con el usado en 2007 por Alemania.

14. Efecto del Cyber Money Laundering / Cyber Gambling: smartphones, PC y tablets realizando apuestas sin que sus usuarios lo sepan

En una estructura del tipo Cyber Money Laundering - Cyber Gambling se tiene a cientos de miles de smartphones, PC y tablets realizando apuestas sin que sus usuarios / propietarios lo sepan. Es muy importante insistir en que, en paralelo, otros miles de usuarios "reales", realizan apuestas no fraudulentas.

Las citadas apuestas no fraudulentas, administradas en un adecuado balance con las fraudulentas, efectuadas por dispositivos "zombies", constituyen una efectiva cobertura de una estructura del tipo Cyber Money Laundering - Cyber Gambling.

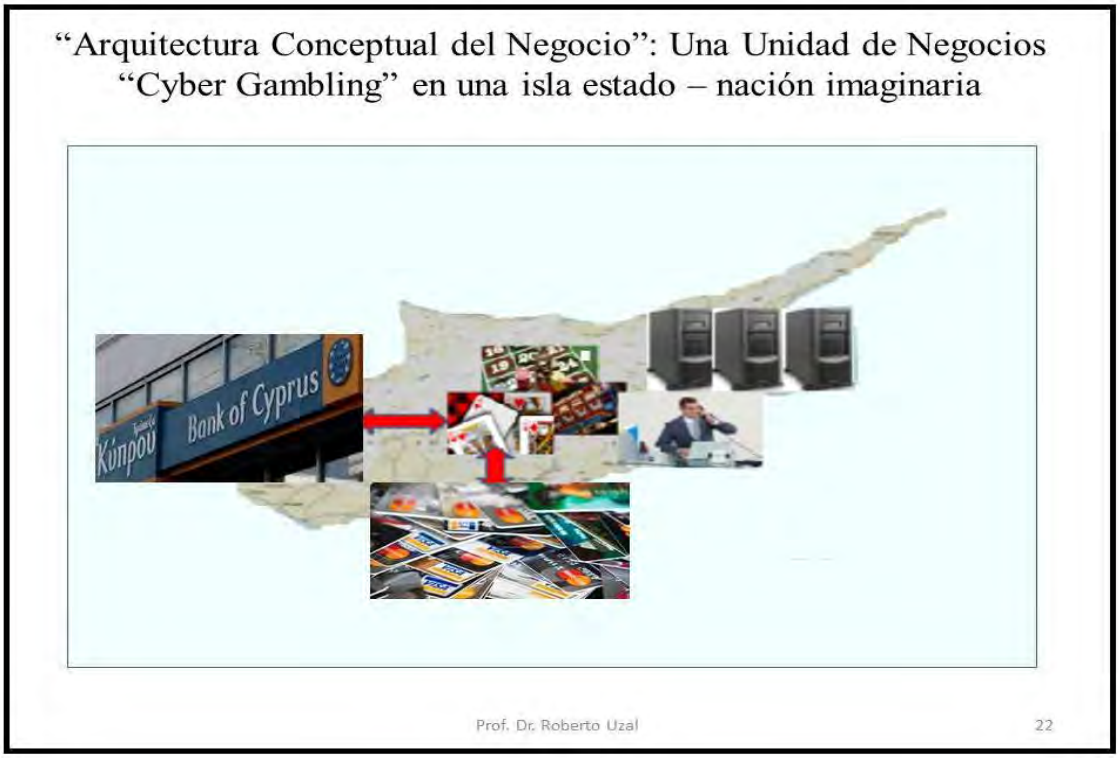
Conviene recordar que la Unidad de Negocios del Cyber Gambling está integrada a un "holding" que posee Unidades de Negocios de Arbitraje Financiero, de Servicios Portales, de Servicios de E-Learning, etc.

Los enfoques contables forenses tradicionales normalmente resultarán ineficaces para demostrar la existencia de una organización orientada al Cyber Money Laundering - Cyber Gambling.

15. “Arquitectura Conceptual del Negocio”: Una Unidad de Negocios “Cyber Gambling” en una isla estado – nación imaginaria

    Influyen en la elección del estado nación en el que estará instalada la Unidad de Negocios de Cyber Gambling:

    - La localización geográfica [18][19][20]
    - El tipo de gobierno [21]
    - La legislación vigente en lo tributario y en el ámbito bancario [18][19][20] [21]
    - Enfoque de lo relacionado con el “secreto bancario” [18][19][20] [21]



En este caso imaginario se ha pensado en un sector de una isla estado nación, cercana al continente, con un régimen jurídico singular y con normas de funcionamiento del sistema financiero sumamente adecuadas. Allí suponemos instalada una Unidad de Cyber Gambling, al banco que le da el correspondiente soporte, al gerenciamiento local de la Unidad de Cyber Gambling y a la infraestructura de Tecnología Informática (la que se encuentra “discretamente” replicada en otro estado nación).

Conviene insistir: El “holding” debe estar en otro país. Es necesario que los estados contables consolidados se elaboren casualmente en el país en el que está radicado el mencionado “holding” (distinto al estado nación en el que está basada la Unidad de

Negocios de Juegos / Apuestas mediante Internet – Cyber Gambling). El "holding", en este ejemplo, posee Unidades de Negocios de Arbitraje Financiero, de Servicios Postales, de Servicios de E-Learning, de Encuentros Personales mediante Internet, de venta de e-Books, etc. En el diseño de estos esquemas debe cuidarse que:

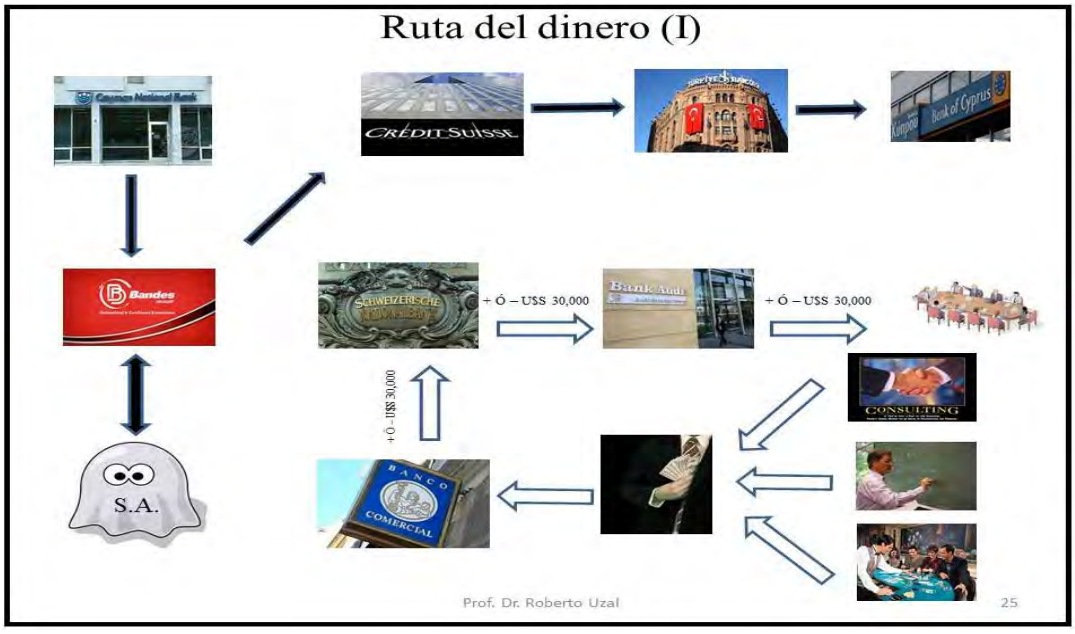
- En el "holding", fuera de la Unidad de Negocios de Cyber Gambling, todas las otras actividades deben tener características irreprochables.
- Todas las Unidades de Negocios del "holding" se deben corresponder con negocios que impliquen un enorme número de transacciones con montos asociados pequeños para cada una de ellas.
- El "holding" debe ser auditado, regularmente, por la filial local de una muy respetable firma de auditoría externa cuya casa central se encuentre en un tercer país.

El banco en el continente, que interactúa con el banco que, en la isla, apoya la Unidad de Negocios de Cyber Gambling, debe ser distinto al o a los bancos con los que actúa el "holding" como un todo.

16. La ruta del dinero (Proceso de Lavado)

a. Las “empresas de servicios” Cyber Money Laundering – Cyber Gambling desarrollan sus actividades con un enfoque general que debe ser “instanciado” cuidadosamente a cada caso de lavado en particular. El enfoque y herramientas utilizados son los mismos; los parámetros con los que se las usa, tanto al enfoque como a las herramientas, dependen del origen del dinero negro (corrupción / narcotráfico / tráfico ilegal de armamento) y del lugar de residencia del “cliente”.
    I. Para facilitar la comprensión del funcionamiento del esquema Cyber Money Laundering – Cyber Gambling se trabajará con un caso particular imaginario pero concreto y tangible, no con el enfoque general que tiene características algo más abstractas.
    II. Dicha ”instanciación” o caso particular de lavado se caracteriza por:
        1. El ”cliente” (persona física con dinero a ser lavado) es un funcionario público (imaginario) que reside en Argentina.
        2. El origen del dinero a ser lavado lo es un soborno, ”ex ante”, por adjudicar una gran obra pública a una gran corporación empresarial transnacional.

b. Aclaraciones adicionales
    I. Se resalta: Si el ”cliente” fuera un ”narco”, los flujos transnacionales de dinero y los flujos de información serían distintos al del ejemplo a ser expuesto
    II. Se destaca: El país de residencia del ”cliente” influye en la determinación de los países que quedarán comprendidos en los flujos transnacionales de dinero y los flujos de información



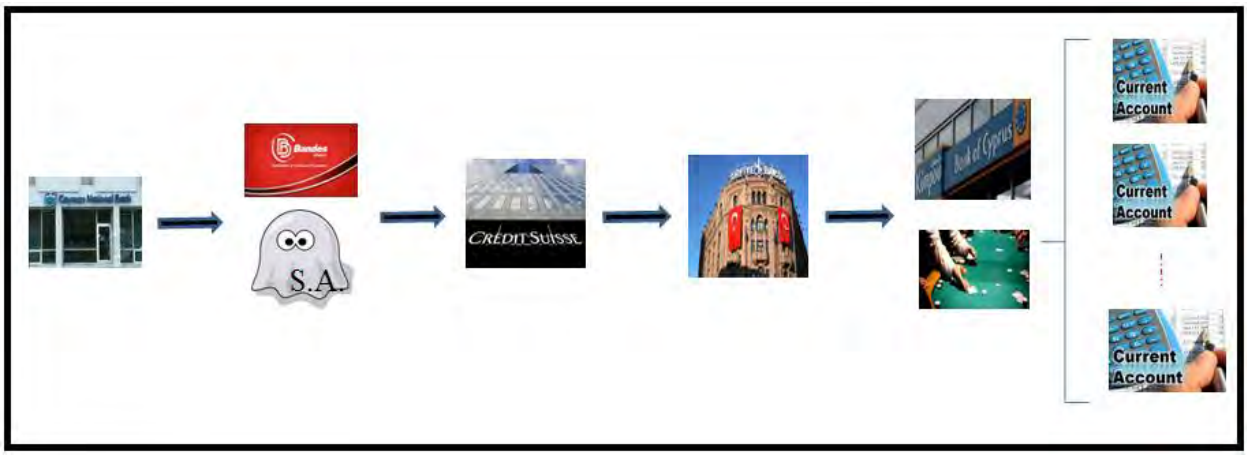
Es necesario distinguir en la figura precedente:

- El flujo del dinero correspondiente al soborno (flechas con relleno negro)
- El flujo del dinero que simulará inversiones en el "holding" - compra de acciones / obligaciones negociables (flechas con relleno blanco)

El dinero del soborno (no debería superar los 3 ó 4 M de U$S en cada operación) se origina en un banco ubicado en un país en el cual el "secreto bancario" es "valor supremo" y que está encuadrado en lo que comúnmente se denomina "paraíso fiscal". La regla es: Todo "empresario sobornador" **debe** tener al menos una cuenta de este tipo. Al respecto se sugiere un análisis comparativo "empresario sobornador" versus "testaferro" en cuanto al origen del dinero del soborno.

También según un "timing" a ser acordado, el dinero del soborno es transferido a una cuenta bancaria de una Sociedad Anónima "fantasma" en un país cercano al de residencia del "cliente", en el cual este tipo de operaciones contribuya significativamente a su PBI.

Siguiendo el itinerario que se muestra en la siguiente figura, este dinero finaliza su recorrido en las cuentas de los apostadores "zombies", abiertas en el banco ubicado en la isla estado nación que se ha venido mencionando.



Respecto del flujo del dinero destinado a simular inversiones en el "holding" (del orden de decenas de miles de U$S), el mismo tendrá las siguientes características:

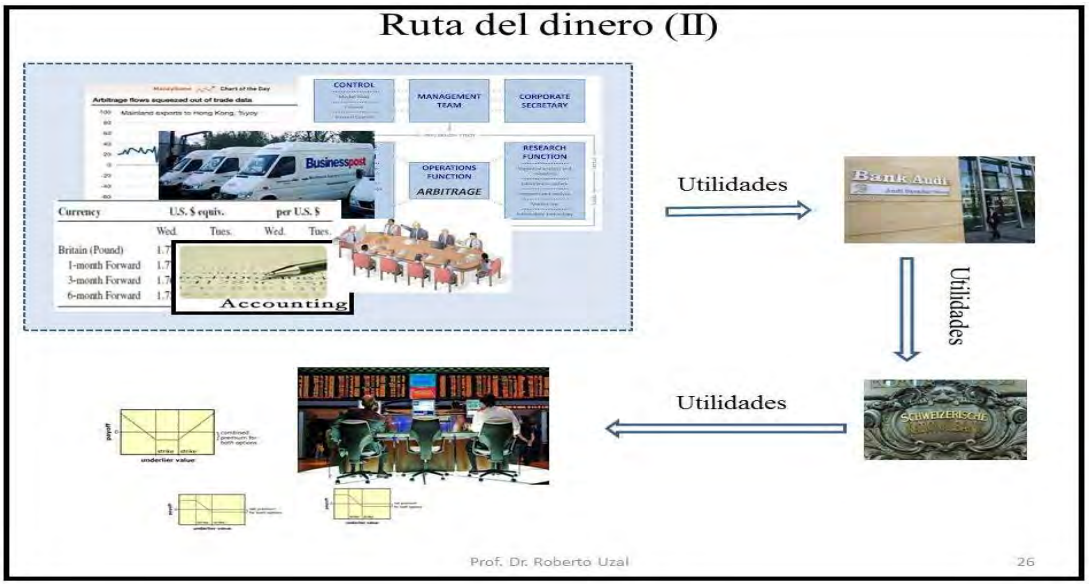
- El "cliente" (la persona a la que se le está brindando el servicio de lavado) deberá trasladarse al mismo país vecino en el que se había conformado la S.A. "fantasma".

Una vez en dicho país, en una o varias estadías (a ser establecido por la "empresa de servicios" de lavado) realizará actividades del tipo:

- Concurrirá a un casino en el obtendrá ganancias por un monto del orden de algunos miles de U$S.
- Será convocado para asesorar a una organización u empresa por lo que recibirá honorarios, también por un monto del orden de algunos miles de U$S.
- Será invitado a desarrollar exposiciones en foros diversos, las que serán retribuidas, de la misma manera, por un monto del orden de algunos miles de U$S.

- El "cliente" depositará las ganancias en el casino y sus honorarios por consultoría y como expositor en un banco de ese país vecino, distinto al banco en el que se había abierto la cuenta de la S.A. "fantasma".
- Según indicaciones de la "empresa de servicios" de lavado regularizará, utilizando documentación de respaldo inobjetable, el depósito en U$S en el mencionado país cercano ante la AFIP.
- Según un "timing" determinado por la "empresa de servicios" de lavado, transferirá el dinero declarado ante la AFIP a un banco de Europa ubicado en un país de reputación impecable.
- Desde allí, en determinado momento, dicho dinero será invertido en acciones u obligaciones negociables del "holding".

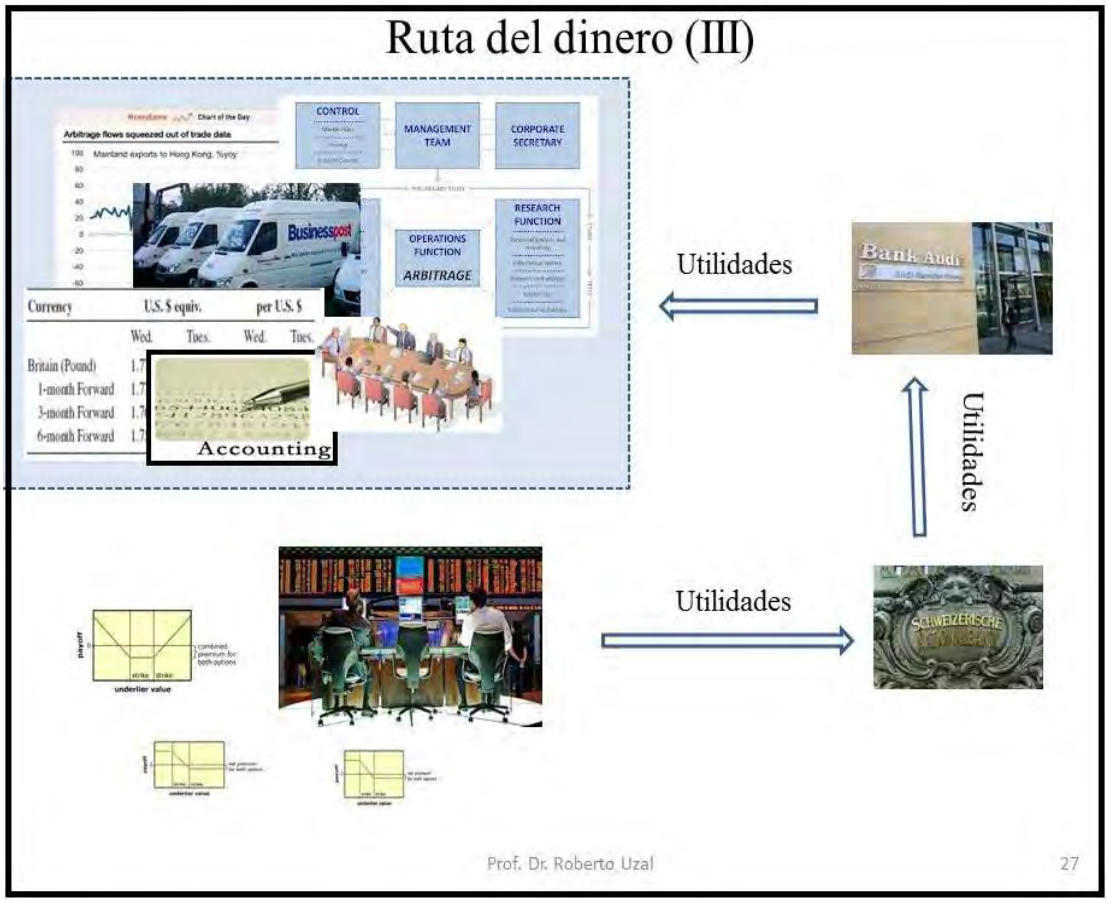
La "utilidades blanqueadas": Siempre siguiendo el "timing" determinado, se le transfiere "al cliente" el "producido" por las utilidades de las acciones y/o compra de las obligaciones negociables. Ver el "itinerario" en la siguiente figura:



Características del "itinerario" de las utilidades:

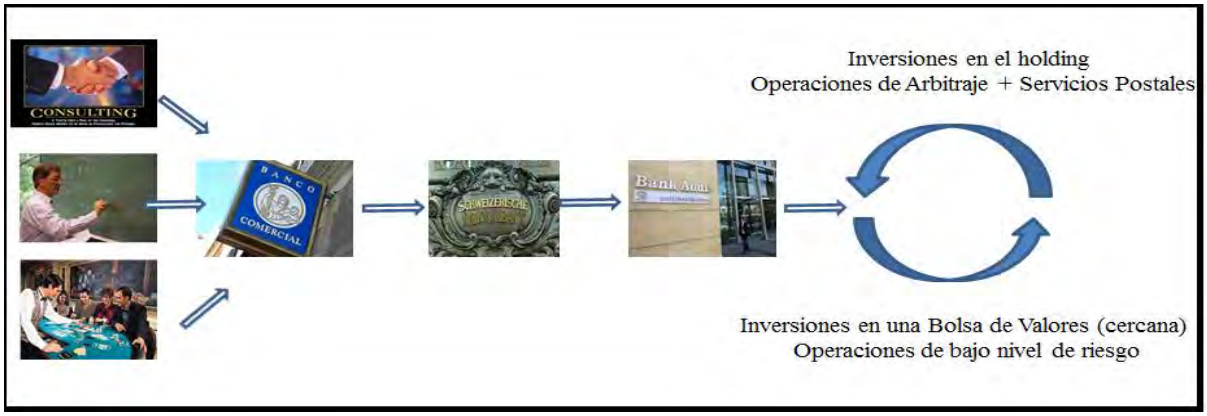
- Desde el banco (o los bancos) con el/los que trabaja el "holding", en el continente, se transfieren las utilidades "logradas por el cliente" al banco de Europa ubicado en un país de reputación impecable.
- Desde el banco de Europa, ubicado en un país de reputación impecable, se transfieren las utilidades a un prestigioso "broker / agente" de bolsa que opera en la quizás más importante bolsa de Latinoamérica. Allí las utilidades se invierten en derivados financieros que minimizan riesgos.

Pasado cierto tiempo se produce el siguiente "itinerario" inverso:



Es importante destacar que esta primera re inversión es unas diez veces mayor que la inversión inicial.

El ciclo "retiro de utilidades / re inversión" se repite tantas veces como para cada caso especial lo determine la "empresa de servicios" de lavado.



17. Gerenciamiento del tiempo y del cash flow en el proceso de lavado

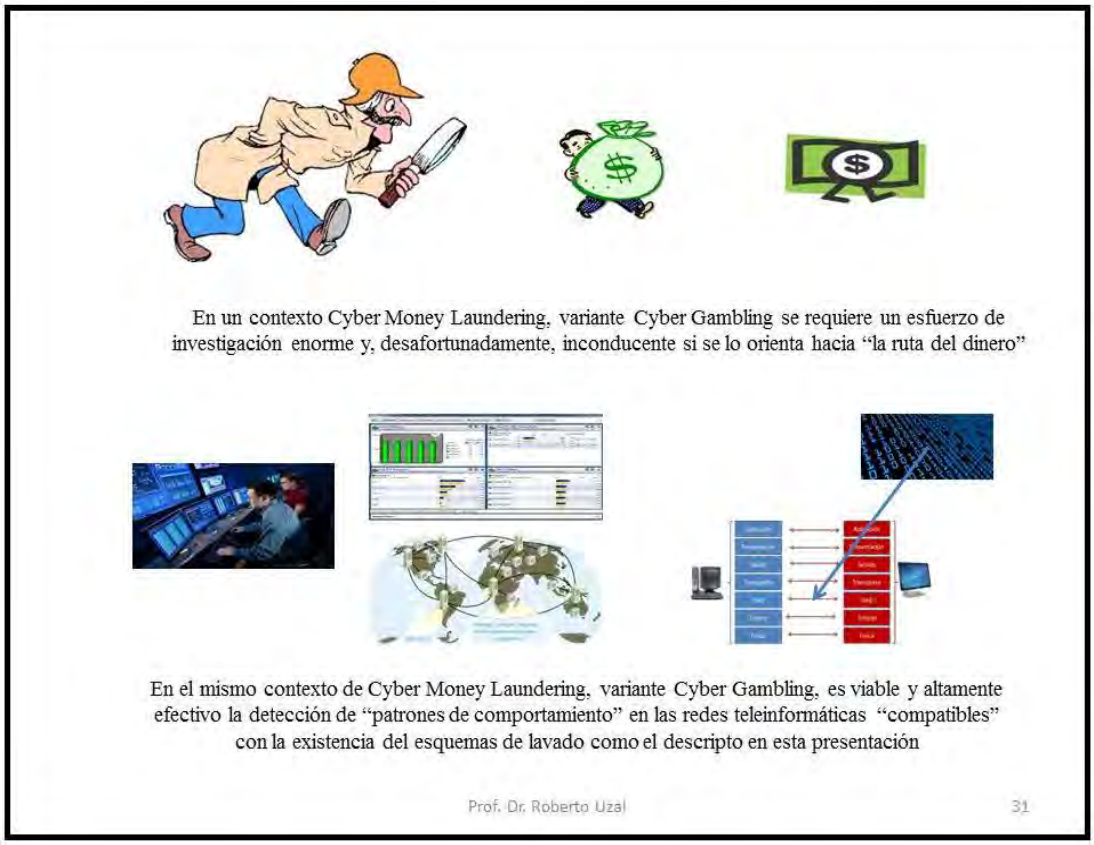
La "excelencia" del mencionado gerenciamiento es lo que impedirá, no sólo que el "cliente" pueda a llegar a ser inculpado de lavado; difícilmente llame la atención de los organismos de control si se utilizan los enfoques "tradicionales". Lo sintetizado en la siguiente figura es claramente viable:

El dinero del soborno, que desde un "paraíso fiscal caribeño" (imaginario), luego de etapas intermedias que limitan / impiden su detección, llega a las cuentas corrientes de los apostadores "fantasmas".

A través del proceso mostrado, termina siendo controlado por el "cliente", con documentación que acredita plenamente su "legitimidad".

Obviamente, durante el proceso, se deducen los "honorarios" de la "empresa" de servicios de Cyber Money Laundering / Cyber Gambling.

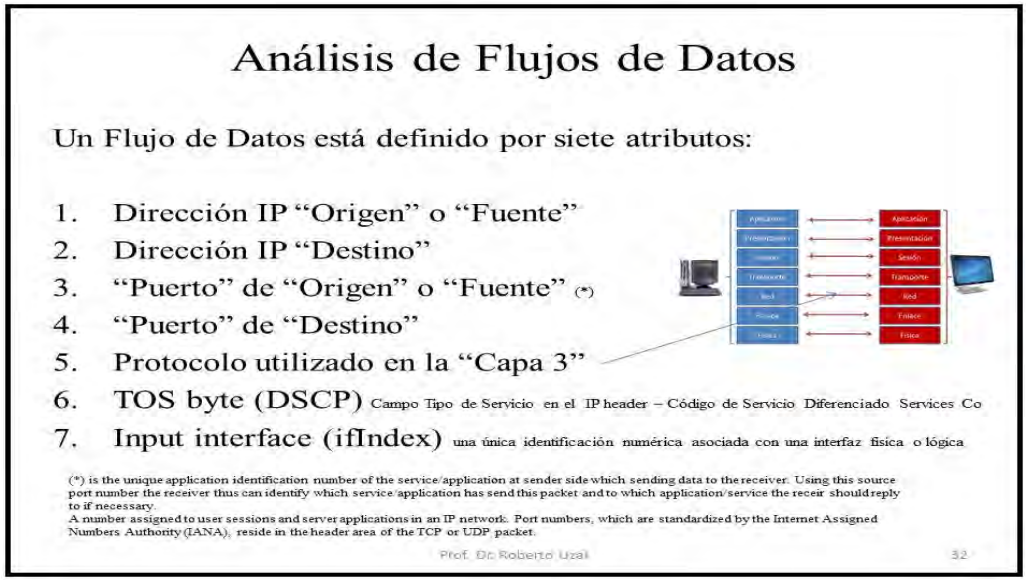
18. ¿Cómo debemos enfrentar efectivamente el uso de Internet para el Lavado de Activos?



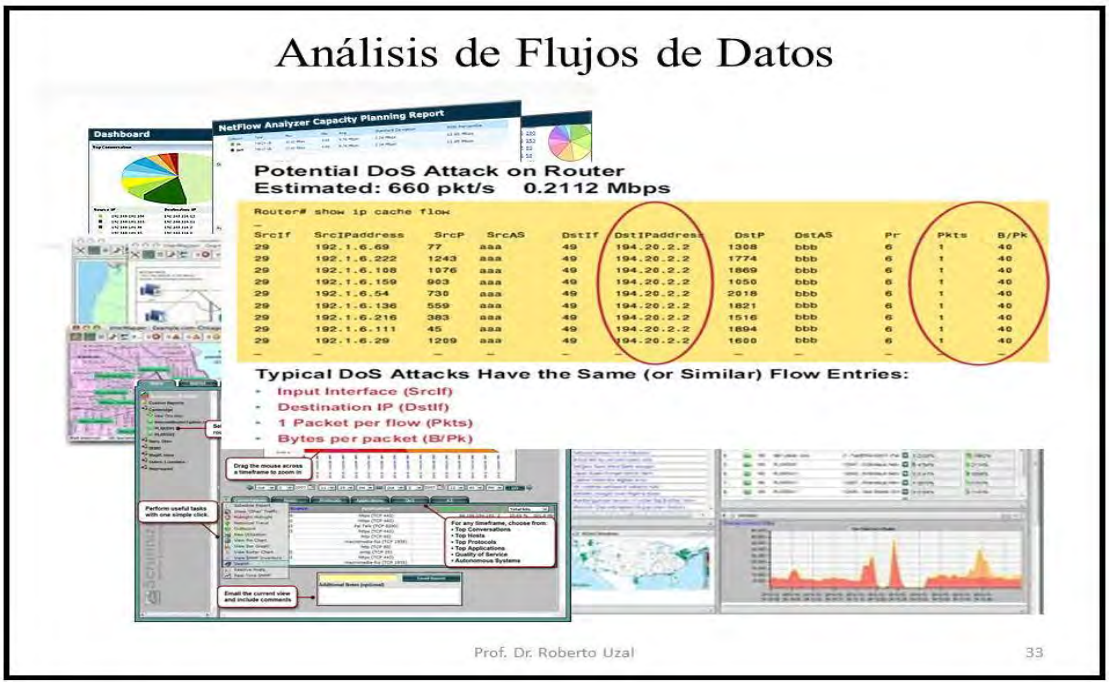
La esencia de esta presentación es la de proponer poner el énfasis en el Análisis de Flujo de Datos y no tanto en el Flujo del Dinero para enfrentar el Lavado Internacional de Activos. Se está migrando masivamente hacia un esquema del tipo Cyber Money Laundering [22] y, en dicho contexto, el llamado Cyber Gambling demuestra ser una efectiva cobertura en operaciones de Lavado Internacional de Activos,

Análisis de Flujo de Datos no necesariamente implica violaciones a la privacidad. Lo importante es identificar y vigilar "patrones de comportamiento" de los Flujos de Datos en las Redes Teleinformáticas.

En la siguiente figura se mencionan los atributos que caracterizan a un Flujo de Datos. También se modela el modelo de referencia ISO-OSI [23][24][25] de comunicación entre computadoras. La Capa 3 de dicho modelo de siete Capas es la Capa de Red. Este nivel es particularmente importante en el Análisis de Flujos de Datos.



En la siguiente ilustración se muestran las modelos estadísticos de "patrones de comportamiento" de Flujos de Datos en Redes Teleinformáticas.



Patrones de comportamiento de Flujos de Datos correspondientes a apuestas fraudulentas

- El análisis estadístico de los Flujos de Datos correspondientes a los flujos de dinero por apuestas y cobranzas permiten distinguir a los apostadores reales de los apostadores "zombies".
- En Ciber Defensa teníamos que los DoS (ataque por Denegación de Servicios), cientos de miles de "zombies" emitían una enorme cantidad de Flujos de Datos idénticos, con requerimientos triviales pero de alta prioridad según los protocolos vigentes, a un mismo servidor o unos pocos servidores (blancos del ataque). Dichos servidores quedaban fuera de servicio por saturación (lo ocurrido, por ejemplo, en la guerra Rusia / Estonia).
- En Cyber Gambling se tiene a un o unos pocos Command & Control Servers, enviando Flujos de Datos similares, con notable "monotonía, a cientos de miles de "zombies". Dicho Flujos de Datos guardan fuerte correlación con el comportamiento de los "zombies" realizando "apuestas". Este es el patrón de comportamiento que más caracteriza a las apuestas fraudulentas provenientes de "zombies".
- Los apostadores reales suelen estar radicados (geográficamente) en países de Europa o América; los apostadores "zombies" suelen residir en países asiáticos tales como Tailandia, Macao, India, etc. en los cuales, por razones de idioma, legislación o inexistencia de tratados, es más difícil caracterizar el "robo de identidad" de propietarios de computadoras y smartphones.

- El análisis estadístico de estos patrones, con un rigor tal que llegue a configurar evidencia forense ante organismos internacionales, es posible y además estrictamente necesario.

¿Cómo debemos enfrentar efectivamente el uso de Internet para el Lavado de Activos?
Kilian Strauss http://academia.edu/1369342/Cyber-laundering_-_How_can_we_combat_money_laundering_over_the_internet

- Conocimientos de Tecnología de la Información más profundos a nivel de académico, a nivel profesionales y, fundamentalmente, a nivel de los usuarios
- Mejores y más creativos sistemas de verificación de identidades cuando se accede a dispositivos conectados a Internet
- Más profundos conocimientos y herramientas más efectivas de Análisis de Flujo de Redes fundamentalmente en lo que hace a IP "tracking"
- Una mejor, honesta y efectiva cooperación internacional

19. Conclusiones

- Es posible definir con precisión los patrones de comportamiento de flujos de datos correspondientes a cada uno de las variantes de Cyber Money Laundering. Estos patrones se manifiestan estadísticamente como histogramas o curvas de distribución.
- Es posible desarrollar herramientas para el análisis automatizado de los flujos de datos especialmente orientadas a detectar patrones de comportamiento de flujos de datos correspondientes a cada uno de las variantes de Cyber Money Laundering.
- También es posible detectar los "Master botnet" y los "Command & Control Servers" correspondientes a varios de los esquemas Cyber Money Laundering.
- El desarrollo de herramientas para "discontinuar" el funcionamiento de Master botnet" y "Command & Control Servers" específicos es viable. Claro que sólo sería legítima su utilización por alguna organización internacional con atribuciones específicas en dicho contexto.

20. Aspectos a ser discutidos

- ¿Debe Interpol u otra organización análoga poseer las capacidades detalladas en "Conclusiones"?

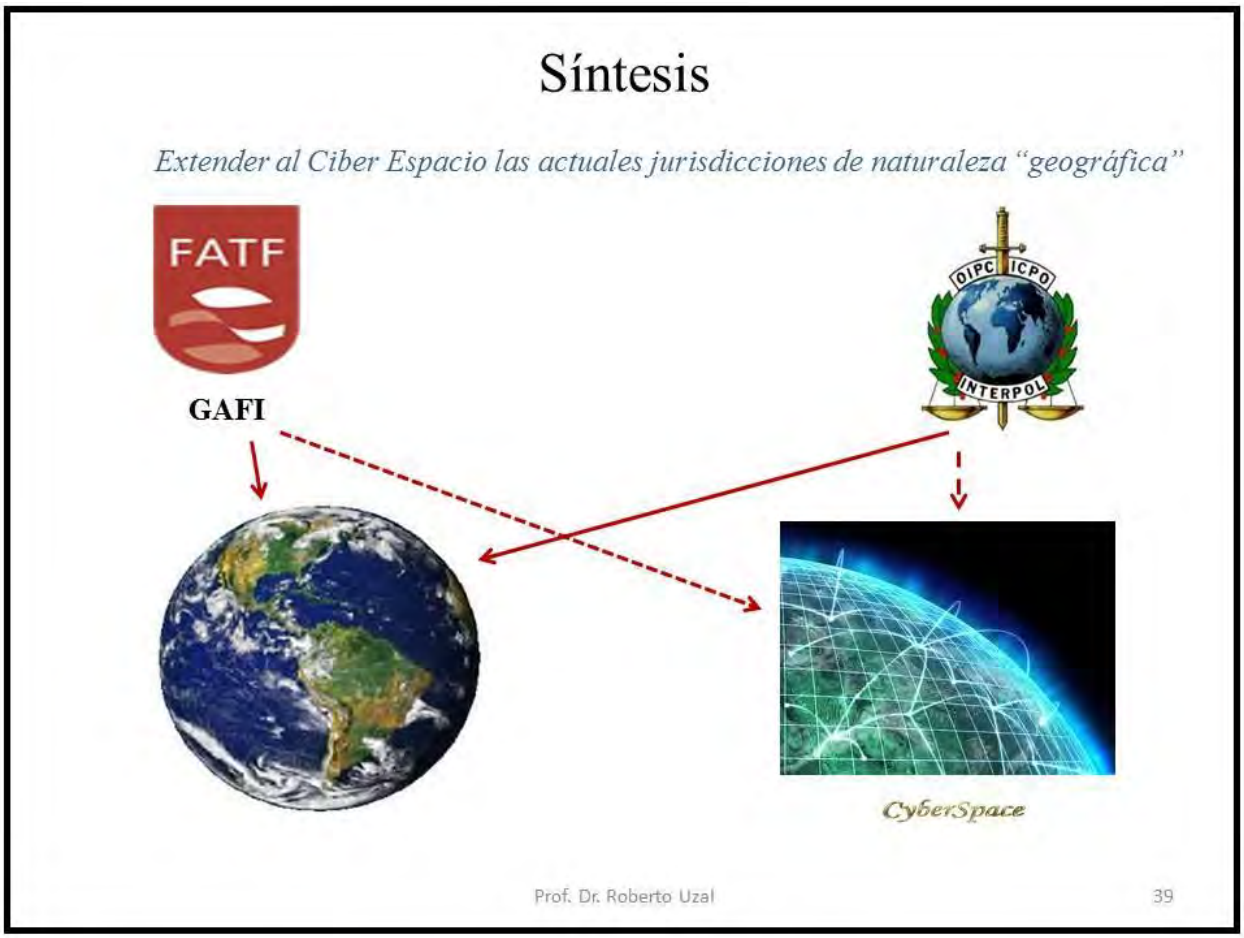
- ¿Es posible que la Asamblea General y el Comité Ejecutivo de Interpol puedan llegar a tratar los aspectos mencionados en "Conclusiones"?

- ¿En un esquema de Cyber Gambling como el tratado como ejemplo, qué jueces podrían declararse competentes?

- Considerando que "lavar el dinero" proveniente del narcotráfico es un "negocio" posiblemente más rentable que las distintas variantes del narcotráfico, tratar los aspectos mencionados en "Conclusiones" y desarrollar las correspondientes capacidades, ¿Es actualmente asumido como incumbencia de Interpol? ¿Debería ser asumido?

- El Grupo de Acción Financiera Internacional sobre el blanqueo de capitales ¿Debería contar con información objetiva respecto de organizaciones de lavado como las descriptas en esta presentación (estructura y funcionamiento)?

- ¿Debería dotarse al GAFI con herramientas para poder acceder a dicha información objetiva?



Referencias

[1] Aportes anteriores del autor anteriores en Ciberdefensa y en Ciberseguridad:

I. Conferencia de difusión sobre Ciberguerra realizada, en marzo de 2012, en el Club de Oficiales de las Fuerzas Armadas (C,A.B.A.)
II. Entrevista en el Canal C5N en agosto de 2012 a investigadores del LaCIS;
III. Reportaje a investigadores del LaCIS. Revista DEF (especializada en temas de Defensa) también en agosto de 2012
IV. Seminario desarrollado en el COPITEC (Consejo Profesional de Ingeniería de Telecomunicaciones, Electrónica y Computación – CABA) sobre Guerra Cibernética en agosto de 2012;
V. Seminario sobre Ciberdefensa en la Escuela Superior de Guerra Conjunta (Ministerio de Defensa), desarrollado en octubre de 2012

VI. Elaboración de un artículo sobre Ciberdefensa para la Revista "Visión Conjunta" de la Superior de Guerra Conjunta (Ministerio de Defensa) Número 7, Año 4

VII. Desarrollo de un Seminario en el Consejo Argentino de relaciones Internacionales sobre Ciberamenazas (Ciberdelito + Ciberterrorismo + Ciberdefensa) el 12 de noviembre de 2012;

VIII. Desarrollo del LaCIS junto con Cancillería, de las Jornadas por un Ciberespacio Seguro y Confiable el 18 de diciembre de 2012

IX. Desarrollo de una conferencia sobre Defensa Cibernética organizada por "The Armed Forces Communications and Electronics Association" en la Facultad de Ingeniería del Ejército – Escuela Superior Técnica, Av. Cabildo 15 – C.A.B.A., el 27 de junio de 2013

X. Colaboración con el Estado Mayor Conjunto – Ministerio de Defensa en la elaboración del Plan Estratégico de Ciberdefensa durante el primer semestre de 2013.

XI. Trabajo de Investigación: "Planeamiento Estratégico Informático: Planeamiento Basado en Capacidades aplicado al Planeamiento Estratégico de la Ciberdefensa" presentado y aceptado para las 42 JAIIO (Jornadas Argentinas de Informática e Investigación Operativa) – FAMAF – UNCba – 16 al 20 de Septiembre, Córdoba

XII. Trabajo de Investigación: "Aportes a la Ciberseguridad: Bases e instrumentos para el uso de Análisis de Flujos de Datos para evitar el Ciber Lavado de Dinero" presentado para ser expuesto en el CoNaIISI, organizado por la red de carreras de Ingeniería Informática / Sistemas de Información (RIISIC) perteneciente al CONFEDI (Consejo Federal de Decanos de Ingeniería), fecha 21 y 22 de Noviembre de 2013, Córdoba

[2] http://www.syssec-project.eu/media/page-media/3/bilge-acsac12.pdf

[3]http://www.acsac.org/2012/openconf/modules/request.php?module=oc_program&action=summary.php&id=73

[4] http://www.academia.edu/1369342/Cyber-laundering_-_How_can_we_combat_money_laundering_over_the_internet

[5] http://money.cnn.com/2013/05/28/news/companies/money-laundering-arrests/index.html

[6] http://techcrunch.com/2013/04/30/first-legal-online-gambling-site-launches-in-the-u-s-but-only-for-nevada-residents-for-now/

[7] http://igamingandmarketing.wordpress.com/2013/02/20/online-gambling-blocked-from-cyprus/

[8] http://calvinayre.com/2013/02/20/business/cyprus-orders-isps-to-block-270-online-gambling-domains-or-face-e30k-fines/

[9] http://cybersecurity.mit.edu/2012/10/cyber-laundering-money-laundering-in-cyberspace/
[10]http://www.wiso.unihamburg.de/fileadmin/bwl/rechtderwirtschaft/institut/Ingo_Fiedler/Online_Gambling_as_a_Game_Changer_to_Money_Laundering_01.pdf
[11] http://www.oecd.org/countries/monaco/listofunco-operativetaxhavens.htm
[12] http://www.offshorecompany.co.uk/taxhavens/locations.htm
[13] http://www.huffingtonpost.com/2011/10/04/top-ten-tax-havens_n_994273.html
[14] http://www.pwc.pt/en/guia-fiscal-2011/paraisos-fiscais.jhtml
[15]http://infouniversidades.siu.edu.ar/noticia.php?titulo=guerra_cibernetica:_el_nuevo_paradigma_en_seguridad_informatica&id=1645
[16]http://sedici.unlp.edu.ar/bitstream/handle/10915/27537/Documento_completo.pdf?sequence=1
[17] http://news.bbc.co.uk/2/hi/europe/6665145.stm
[18] http://www.ft.com/intl/cms/s/0/f8ec22c6-c852-11e2-acc6-00144feab7de.html
[19] http://www.reuters.com/article/2013/03/25/us-eurozone-cyprus-austria-idUSBRE92O0L920130325
[20] http://www.isla-offshore.com/services/banking-cyprus/
[21] http://www.cypnet.co.uk/ncyprus/main/polsyst/
[22] http://www.world-check.com/insights-expert-talk/cyber-crime-financial-fraud-and-money-laundering-understanding-new-threat-landscape
[23]http://www.iso.org/iso/products/standards/catalogue_ics_browse.htm?ICS1=35&ICS2=100&
[24] http://es.wikibooks.org/wiki/Redes_inform%C3%A1ticas/Modelo_OSI_de_ISO
[25] http://www.exa.unicen.edu.ar/catedras/comdat1/material/ElmodeloOSI.pdf

(*) Prof. Dr. Roberto Uzal

Director del Doctorado en Ingeniería Informática de la Universidad Nacional de San Luis
Director de la Maestría en Ingeniería de Software de la Universidad Nacional de San Luis
Director de la Maestría en Calidad del Software de la Universidad Nacional de San Luis

Categorizado como Investigador Superior – Categoría I en el Programa de Incentivo a la Investigación en Universidades Nacionales
Coordina, por Argentina el Programa CAPG-BA de integración de la enseñanza de IV nivel con Brasil.
Acredita treinta y cinco años de enseñanza a nivel grado y post grado en la Universidad de Buenos Aires
Supera las 150 publicaciones internacionales sobre temas de Tecnología Informática arbitraje mediante

Posee experiencia internacionalmente reconocida, de más de treinta años, en el desarrollo e implantación de productos de software de alta complejidad.
Miembro del Grupo de Trabajo sobre Criminalidad Organizada Transnacional del Consejo Argentino de Relaciones Internacionales

Formación:

Doctor en Administración - Facultad de Ciencias Económicas - Universidad de Belgrano
Especialista en Administración Financiera - Facultad de Ciencias Económicas – Universidad de Buenos Aires
Certificado en Estudios Avanzados en Management - California State University - Los Angeles
Licenciado en Sistemas - Facultad de Ingeniería – Universidad de Buenos Aires
Ingeniero Químico – Ingeniero Militar - Facultad de Ingeniería del Ejército – Escuela Superior Técnica
Teniente Coronel de Infantería (Retirado) – Paracaidista Militar - Promoción 95 del Colegio Militar de la Nación
Bachiller – Subteniente de Reserva – Liceo Militar General San Martín – Promoción 19

(**) El presente texto sólo es representativo de la postura del autor / expositor en su condición de profesor – investigador universitario; no compromete la opinión oficial de institución alguna
.