Lavado Transnacional de Activos en el Ciberespacio. Presentación del contexto, planteo del problema y formulación de propuestas

Roberto Uzal [1] Daniel Riesco [1] German Montejano [1] Walter Agüero [1] Claudio Baieli [1]

[1] Universidad Nacional de San Luis – Argentina
ruzal@unsl.edu.ar

Keywords: "transnational cyber money laundering"; "lavado transnacional de activos en el ciberespacio"; "transnational money laundering"; "lavado transnacional de activos; "money laundering"; "lavado de activos"

Resumen

En este trabajo se desarrolla un tema de especial sensibilidad, tanto para los gobiernos de estados naciones como para organismos internacionales: El Lavado Transnacional de Activos. Año a año se incrementa la proporción de Lavado de Activos que se realiza mediante mecanismos cuyos aspectos esenciales utilizan la naturaleza, características y las posibilidades del Ciberespacio. Se expone en esta contribución el relevamiento de un esquema para el Lavado Transnacional de Activos en el Ciberespacio basado en la modalidad o variante "apuestas en línea". Se describe la ruta del dinero a ser lavado y se presenta una variante del esquema tecnológico que soporta al Lavado Transnacional de Activos en el Ciberespacio. En el trabajo se proponen conceptos y herramientas destinados a mitigar significativamente el impacto producido por los resultados de los "servicios de Ciber Lavado" ofrecidos por organizaciones criminales transnacionales. Dichos conceptos y herramientas han sido discutidos, en forma previa a la elaboración de este reporte, con expertos de primer nivel internacional; fueron objeto de experiencias a nivel laboratorio y también se realizaron trabajos de campo. Estos últimos se ejecutaron utilizando prototipos desarrollados en el contextos de grupos de investigación universitarios. Se espera que esta presentación trascienda el ámbito académico y se constituya en una referencia de valor en los entornos social, político y de gobierno.

1. Introducción general

De acuerdo con las estimaciones de "The United Nations Office on Drugs and Crime" (UNODC)[1], el "negocio" del Lavado de Activos tiene asociado ingresos anuales equivalentes a entre el 3 y el 5 % del Producto Bruto Global. Utilizando el léxico anglo sajón, estaríamos en el orden de "trillones" de U$D por año, es decir, trece dígitos significativos a la izquierda del punto (o coma) decimal.[2] [3] Al estudiar las investigaciones de UNODC se verifica que el monto total del Lavado de Activos (MADINGER, J. -2011) se incrementa anualmente; esto lisa y llanamente indica que los "clásicos" tres delitos precedentes [1] [2] al Lavado de Activos (corrupción gubernamental, tráfico ilegal de armas y narcotráfico) también han venido incrementando su "volumen de negocios" año a año.

Existen abundantes evidencias respecto de que la tendencia del Lavado de Activos lo es hacia el Lavado Transnacional de Activos en el Ciberespacio[4] [5]

> Por otro lado, es ampliamente conocido, desde hace mucho tiempo, que el juego ha sido y es uno de los "contextos estrella" del Lavado de Activos [6] [7]. El juego, como casi sinónimo de Lavado de

[1] http://www.unodc.org/
[2] http://www.unodc.org/unodc/en/money-laundering/introduction.html
[3] http://www.unodc.org/unodc/en/frontpage/2011/October/illicit-money_-how-much-is-out-there.html
[4] http://cybersecurity.mit.edu/2012/10/cyber-laundering-money-laundering-in-cyberspace/
[5] http://money.cnn.com/2013/05/28/news/companies/money-laundering-arrests/
[6] http://www.theguardian.com/uk-news/2013/nov/08/gambling-machines-drug-money-laundering-bookies
[7] http://www.gamblingcommission.gov.uk/Gambling-sectors/Casinos/Operating-licence-holders/Key-information/Prevention-of-money-laundering.aspx

Activos cuando es administrado por el Crimen Organizado, es algo que ya lleva alrededor de casi tres cuartos de siglo de vigencia[8].

Casualmente el Crimen Organizado Transnacional ha venido implementando verdaderas "empresas de servicios" de Lavado Transnacional de Activos en el Ciberespacio [9] [10]. Estas "empresas de servicio" posibilitan que narcos, funcionarios corruptos y traficantes ilegales de armas se concentren en su "negocio" evitando que incursionen en Lavado de Activos, actividad en la que suelen incurrir en ineficiencias por des-especialización.

Apuestas en línea[11], específicamente, es la variante preferida por el Crimen Organizado para implementar las citadas "empresas de servicios" de Lavado Transnacional de Activos en el Ciberespacio. El juego, como contexto casi ideal para el Lavado de Activos, llevado al entorno virtual del Ciberespacio, constituye un ámbito pleno de oportunidades para el Crimen Organizado Transnacional.

Este trabajo se inicia con una descripción de la naturaleza y características del Ciberespacio. Se incluyó este punto pues se espera que este reporte sea examinado y evaluado por profesionales de formación diversa y que impacte en el entorno social, político y de gobierno.

Se propone a continuación, en este reporte, una catalogación de las Ciber Agresiones en una suerte de complementación / perfeccionamiento de la clasificación que habitualmente menciona Richard Clarke [12]. A los efectos de esta presentación se considera útil la división de las Ciber Agresiones en Activismo Hacker, Ciber Crimen Organizado Transnacional, Ciber Espionaje, Ciber Terrorismo y Ciber Guerra. Es muy importante tener presente que dichos criterios clasificatorios no dan por resultado subconjuntos mutuamente excluyentes.

A continuación, en este trabajo, se describe el esquema general del Lavado Transnacional de Activos en el Ciberespacio: La ruta del dinero y el funcionamiento general de las "empresas de servicios" de Lavado Transnacional de Activos en el Ciberespacio en la modalidad apuestas en línea.

Los fundamentos tecnológicos (BILGE, l., et al, 2012), aplicables en la detección y "neutralización" de sistemas de Lavado Transnacional de Activos en el Ciberespacio, son presentados de una manera accesible a profesionales de distintas disciplinas que se espera analicen y evalúen esta presentación

Un aspecto de este trabajo que se considera de especial importancia: Desencadenar un intercambio de opiniones respecto de la potencial intervención de la Unión Internacional de Telecomunicaciones en el ámbito del Lavado Transnacional de Activos en el Ciberespacio. La Unión Internacional de Telecomunicaciones registra antecedentes de exitosas intervenciones en el ámbito de las Ciber Agresiones en general [3][4].

Como es de estilo, este trabajo finaliza con las conclusiones y propuestas del aporte. Esta presentación contiene numerosas llamadas y referencias que serán útiles a quienes deseen profundizar en los temas abordados.

2. El Ciberespacio

La búsqueda de una definición adecuada de "Ciberespacio" podría desencadenar controversias prolongadas e inconducentes. Por otro lado, no se verifican demasiadas objeciones cuando se hace mención, como Ciberespacio, al dominio, ámbito no tangible o realidad virtual que están sustentados

[8] http://www.lasvegasnevada.gov/factsstatistics/history.htm
[9] http://www.crime-research.org/library/Cybercrime.htm
[10] http://www.state.gov/j/inl/rls/nrcrpt/1999/928.htm
[11] http://www.fbi.gov/news/stories/2007/june/gambling_060607
[12] https://www.youtube.com/watch?v=6_ek8mugOUc

por los diversos servicios o prestaciones que suministran tanto Internet como otras redes que, directa o indirectamente, se encuentran vinculadas a la citada Red de Redes.
El Diccionario de la Real Academia Española, en este caso, no agrega demasiado valor, podemos leer: "Ciberespacio, ámbito artificial creado por medios informáticos" [5].
Se acepta que el término "Ciberespacio" nació en el mundo de la Ciencia Ficción[13]; sin embargo hoy se lo utiliza para identificar al mundo virtual generado como consecuencia de la interconectividad global de redes teleinformáticas.

Se asume como existente la imprecisión asociada al uso generalizado de la no del todo definida palabra "Ciberespacio" pero se estima que la esencia del presente reporte no se verá afectada por ello. La carencia de una definición precisa de "Ciberespacio", no provocará dificultad alguna en el desarrollo de las ideas presentadas en este aporte.

Para finalizar este punto, se destaca que, la motivación para la elaboración de esta presentación, la integran las siguientes aseveraciones:

- En el Ciberespacio están hoy sustentados importantes aspectos de la administración gubernamental en general de un estado nación, de la gestión de la defensa, de la economía y de las finanzas, de la gestión de la salud, de la obtención y distribución de alimentos y del agua potable, de la generación y distribución de energía, de las comunicaciones, del transporte, de la educación, de la cultura, del mundo de los negocios y hasta del mundo del entretenimiento. En la mayoría de los estados naciones existe una muy fuerte interrelación entre Ciberespacio y la infraestructura crítica de cada país.
- Gravísimas modalidades delictivas han encontrado en el Ciberespacio un ámbito o dominio extremadamente propicio para su aparición, su expansión y/o perfeccionamiento (HOLT, T., BOSSLER, A. - 2015). El ejemplo quizás más contundente, por lo pernicioso y por su "rentabilidad" para el crimen organizado, es el Lavado Transnacional de Activos en el Ciberespacio. Su muy alta "tasa interna de retorno" efectúa un efecto de "tracción"[14] o "incentivo" sobre los delitos precedentes tales como corrupción gubernamental, tráfico ilegal de armas y narcotráfico.
- La existencia de eficaces y altamente especializadas "empresas de servicios" de Lavado Transnacional de Activos en el Ciberespacio que eliminan una parte importante del riesgo del "negocio integrado". Al concretarse los delitos precedentes se evita que sus ejecutores (funcionarios corruptos, traficantes ilegales de armas y narcos) incurran en ineficiencias por des-especialización al intentar ingresar a los mercados financieros legales el producto de sus actividades fuera de la ley. El Ciberespacio es un dominio o contexto que posibilita que el Lavado Transnacional de Activos alcance "niveles de excelencia" si este "sub negocio" es administrado por especialistas de "primer nivel".

3. Las agresiones en el Ciberespacio

A fin de facilitar la transmisión de las ideas contenidas en este punto, se propone, en principio, la siguiente catalogación de las Ciber Agresiones que no es mutuamente excluyente:

- Activismo Hacker
- Ciber Crimen Organizado Transnacional
- Ciber Espionaje
- Ciber Terrorismo
- Ciber Guerra

3.1. Se entiende como Activismo Hacker (GOMEZ VIEITES, A. - 2011), en el contexto de esta presentación, al conjunto de acciones de personas o de grupos de personas que, mediante una

[13] Utilizado por primera vez por William Ford Gibson en su obra "Neuromante" en 1984
[14] Entrevistas a expertos internacionales con aquilatada experiencia

aparentemente no-violenta utilización de habilidades y herramientas, actúan en el Ciberespacio encarando, entre otras, acciones tales como la toma del control de sitios web de diversas personas y organizaciones cambiando su apariencia y contenidos, vulnerando las medidas de seguridad de redes teleinformáticas gubernamentales o empresariales de alta sensibilidad y de difícil acceso, realizando ataques de denegación de servicios dirigidos a instalaciones críticas, saboteando instalaciones de gran importancia y sustrayendo y distribuyendo información secreta de gobiernos y corporaciones empresariales.

Algunos grupos y personas incluidas en el activismo hacker sostienen "cuasi ideológicamente" que no debe existir barrera de acceso alguna respecto de contenidos almacenados y/o procesados en el Ciberespacio, sean cuales fueren dichos contenidos; otras organizaciones catalogables en Activismo Hacker se comportan como una suerte de abanderados o líderes de un "neo anarquismo virtual".

En los hechos el Activismo Hacker constituye un criterio de clasificación con contenidos muy heterogéneos. Al mencionarse al Activismo Hacker resulta casi inevitable mencionar a personas tales como Julian Assange[15] y Aaron Swartz[16], al polifacético conglomerado Anonymous[17] y a la organización mediática internacional WikiLeaks[18].

3.2. En cuanto al Ciber Crimen Organizado Transnacional se destaca que constituye un nuevo e importante desafío para los gobiernos y las Fuerzas de Seguridad de todos los países del mundo y para instituciones como Interpol y la Unión Internacional de Telecomunicaciones. También constituye gran desafío para los especialistas en Derecho Internacional. Por su gran efectividad y altísima rentabilidad, el Ciber Lavado Transnacional de Activos constituye un capítulo relevante en el contexto del Ciber Crimen Organizado Transnacional y del Ciber Crimen en general. El aditamento "Organizado Transnacional" constituye una calificación que excluye de alcance de este trabajo a lo que podríamos denominar "ladrones de gallinas del Ciber Espacio". El foco está puesto en Ciber Crímenes que comprenden una utilización creativa y sofisticada de redes teleinformáticas complejas. Sólo aspectos del "Ciber Crimen Organizado Transnacional" serán analizados en este reporte.

3.3. Se asume que Ciber Espionaje (GOMEZ VIEITES, A. - 2011) comprende a aquellas acciones que llevan a obtener información secreta, en distintos formatos, sin la autorización de quien ejerce legítimamente la propiedad de dicha información. Los afectados por el Ciber Espionaje pueden ser individuos, corporaciones empresariales competidoras, grupos políticos y gobiernos. Las motivaciones del Ciber Espionaje pueden ser personales, sociales, políticas, económicas o del ámbito de la defensa.

3.4. En este trabajo se entiende como Ciber Terrorismo (GOMEZ VIEITES, A. - 2011) a las Ciber Agresiones cuyas motivaciones sean de tipo religioso, social, racial o político. Estudiosos del tema estiman que el Ciber Terrorismo constituirá un muy grave problema en el futuro próximo[19].

3.5. Respecto de Ciber Guerra (CLARKE, R., KNAKE, R. - 2010) se remarca que, hasta nuestros días, se entendía que las beligerancias entre estados naciones se libraban en los "clásicos" dominios: tierra, mar, aire y espacio exterior. Desde el año 2005 hasta la actualidad, muchos países han venido reconociendo al Ciberespacio como un nuevo ámbito o dominio de las confrontaciones entre estados naciones.

[15] http://www.biography.com/people/julian-assange-20688499
[16] http://www.biography.com/people/aaron-swartz
[17] http://resources.infosecinstitute.com/a-history-of-anonymous/
[18] http://actualidad.rt.com/themes/view/44187-wikileaks
[19] Entrevistas a expertos de primer nivel global

En la Figura 1 se modelan los distintos tipos de Ciber Agresiones y se muestra la interrelación de las incumbencias de la Ciber Defensa y la Ciber Seguridad. Dada la naturaleza y características de ciertas Ciber Agresiones, no resulta sencillo asignarlas, con carácter excluyente, o a la Defensa o a la Seguridad. Constituye un ejemplo de ello el Ciber Lavado Transnacional de Activos. Considerando que puede afectar la estructura económica de un estado nación por los montos afectados y, teniendo en cuenta la complejidad y distribución geográfica de las "empresas de servicios" de Lavado Transnacional de Activos, no resulta trivial definirlo como incumbencia específica del área Defensa o del área Seguridad de los estados naciones.

Figura 1

4. Ciber Crimen: Lavado Transnacional de Activos mediante apuestas en línea

4.1. Síntesis de la "ruta del dinero" a ser lavado (dinero "en negro")

4.1.1. El itinerario a ser descripto es una suerte de "promedio" de los casos estudiados por el equipo que realizó el relevamiento[20]. Por otro lado el caso está instanciado a un caso de corrupción gubernamental. El "cliente" de los servicios de lavado espera recibir su "participación" por haber facilitado el trámite de adjudicación de una licitación de una obra pública muy importante. Quien fuera el "beneficiario" (empresario a quien se le adjudicó amañadamente la licitación) es el origen del "flujo de fondos" a ser lavados al pagar el soborno acordado.

4.1.2. En un país vecino, donde continúan las facilidades para crear sociedades anónimas de vida efímera y de características "cuasi virtuales", se crea una de estas "figuras jurídicas"; sus "directivos" (reclutados ad hoc y sin conocimiento de la naturaleza del "negocio") abren una cuenta corriente a nombre de la nueva sociedad en un banco especialmente apto para este tipo de operaciones. Desde una isla del Caribe, paradigma del paraíso fiscal[21], el "beneficiario" efectúa una transferencia a dicha cuenta corriente en el "país cercano".

4.1.3. El "cliente" verifica que el "beneficiario" cumplió con lo anteriormente pactado (crédito en la correspondiente cuenta). En otras palabras, verifica que pagó el soborno.

[20] Docentes investigadores, doctorandos y alumnos de maestría de la UNSL asistidos por expertos de primer nivel global

[21] http://www.taxhavens.biz/caribbean_tax_havens/

4.1.4. El banco en el país vecino transfiere los fondos a un banco de Europa Central con una consolidada tradición de eficiencia en este tipo de menesteres (luego de que costos y honorarios fueran descontados).

4.1.5. El banco de Europa Central, como se expresó, con una consolidada fama de eficiencia en este tipo de trámites, transfiere los fondos a un banco de un país de Este de Europa en el cual está basado el holding muy diversificado al que pertenece la "unidad de negocios específica" de apuestas online.

4.1.6. Desde el banco del país de Este de Europa mencionado, se transfieren los fondos a un banco basado en una isla (imaginaria a los efectos de este reporte) cercana a la costa del continente europeo. Dicho banco opera con la "unidad de negocios específica" de apuestas online. Este banco, paulatinamente, acredita los fondos en miles de cuentas corrientes, abiertas con identidades robadas, en correspondencia con un verdadero ejército de computadores zombis, tal como se detalla en el punto siguiente.

En la Figura 2 se modela un itinerario similar / análogo a los itinerarios reales relevados por los investigadores de la UNSL[22].

Figura 2

4.2. Síntesis de la "ruta específica de lavado" (dinero "en blanco").

4.2.1. Siguiendo las indicaciones de ejecutivos de la "empresa de servicios de lavado" el "cliente" (funcionario corrupto) se traslada a un país vecino en el cual desarrolla las siguientes actividades "exitosas": I) Concurre a un casino en el cual gana muchísimo dinero. Retira sus ganancias obteniendo la correspondiente documentación respaldatoria. II) Es contratado por importantes corporaciones empresariales de ese país para desarrollar actividades de capacitación. Sus importantes honorarios están documentalmente respaldados. III) Desarrolla actividades de consultoría, también en importantes corporaciones empresariales. Su retribución también está debidamente documentada.

4.2.2. Los ingresos mencionados en el párrafo anterior son depositados en un banco del citado país vecino.

4.2.3. Contadores de la "empresa de servicios de lavado" armonizan lo expresado con las regulaciones impositivas vigentes en el país de origen del "cliente".

[22] No se hace referencia a institución o país alguno. El itinerario es el relevado. Se han cambiado nombres de empresas y las referencias a estados naciones sólo tienen como motivo darle tangibilidad a la descripción.

4.2.4. Transcurrido un plazo conveniente, los fondos depositados por el "cliente" son transferidos a otro banco, este último basado en un país de Europa Central adecuadamente seleccionado. Desde allí son posteriormente transferidos a un banco basado en un país de Europa del Este. Dicho país es en el que se encuentra el "holding" al que reporta la "unidad de negocios específica" de apuestas en línea que, como ya se señaló, está instalada en una isla (imaginaria) cercana a la costa (de Europa del Este).

4.2.5. Los pasos anteriores, para cada monto a ser lavado, se repiten tantas veces como lo consideren conveniente los ejecutivos de la "empresa de servicios de lavado" (ver Figura 3).

Itinerario del dinero "formalmente legal" desde el "país vecino" hasta la adquisición de acciones en el "holding" supuestamente basado en el Este de Europa

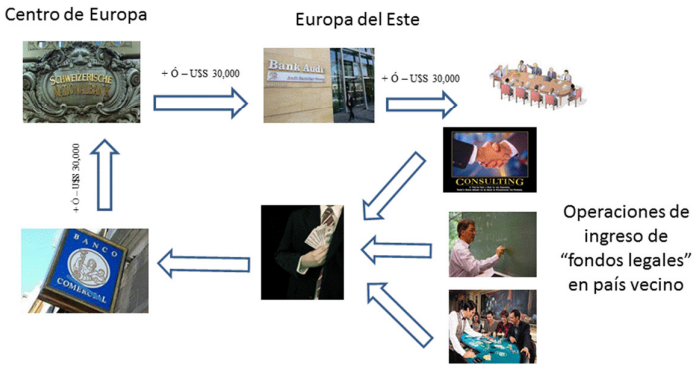

Figura 3

4.2.6. El "cliente", con el dinero "semi lavado" depositado en el banco basado en el citado país de Europa del Este, compra acciones del "holding" al que reporta la "unidad de negocios específica" de apuestas en línea. Dicho holding constituye una corporación sumamente diversificada: Empresas de correo y de transporte, centros de entretenimiento del tipo multi cines, algunas empresas de construcción, etc. Los estados contables consolidados del "holding" están auditados por la quizás más importante firma de auditoría externa de Europa.

4.2.7. El "cliente" recibe paulatinamente su dinero lavado en la forma de utilidades de sus inversiones en el holding.

4.2.8. Dichos activos son invertidos en una bolsa de valores muy importante de Sudamérica (en la forma de derivados financieros de bajo nivel de riesgo).

Observar una síntesis gráfica de este itinerario en la Figura 4

Figura 4

4.2.9. En algunos casos se desinvierte en la citada bolsa de valores y se vuelve a invertir en acciones del anteriormente mencionado “holding”.

4.2.10. Ejecutado el número de ciclos holding -> bolsa -> holding convenientes, el “cliente” logra la disponibilidad plena del monto involucrado (descontados los importantes márgenes de la “empresa de servicios” de Lavado de Activos”).

Durante todo el proceso, contadores de la “empresa de servicios de lavado” han estado “armonizando” la situación patrimonial del “cliente” ante las autoridades fiscales de su país de origen.

5. El núcleo del Lavado Transnacional de Activos en el Ciberespacio

5.1. En esta modelización se muestran los aspectos esenciales del núcleo de un esquema de un esquema de Ciber Lavado basado en apuestas en línea. La unidad específica de “cyber gambling” y el banco que trabaja en forma asociada con ella se encuentran en una isla (imaginaria como se remarcó) cercana a la costa del continente europeo (Europa del Este).

5.2. Dicha isla, por su situación política y su ubicación geográfica. es particularmente adecuada a los fines del “negocio” que se está describiendo. En la isla, las políticas impositivas son de escasa o nula tributación. No existen normas restrictivas en materia de transacciones financieras y se favorece la opacidad de las sociedades que allí se asientan; es muy difícil la identificación de los titulares y es casi imposible detectar el origen de los fondos que se administran en el territorio insular. Ver la relación “unidad de negocios” de apuestas en línea instalada en la isla con el “holding” diversificado basado en el continente en la Figura 5.

Modelado de la relación "unidad de ciber lavado" con el "holding"

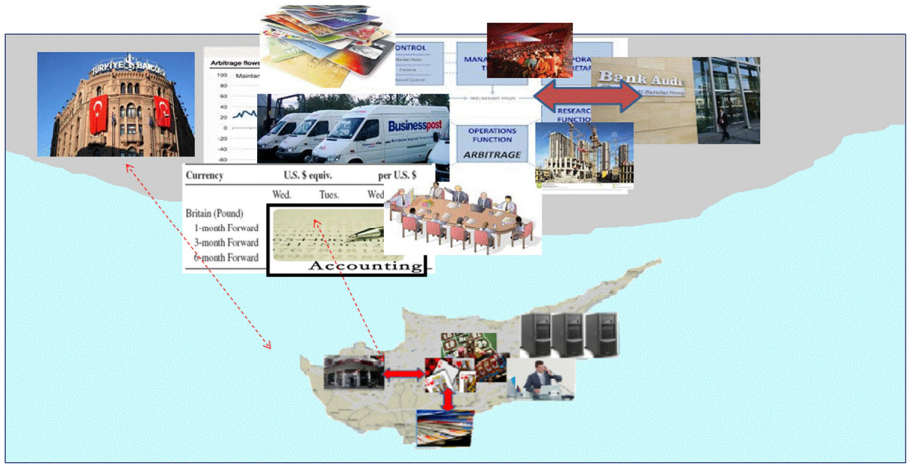

Figura 5

5.3. En el esquema que se está describiendo, decenas o cientos de miles de apostadores reales realizan sus apuestas desde países del Oeste de Europa, América del Norte y algunos pocos países de Asia, Japón por ejemplo. La actividad de estos apostadores enmascara al verdadero "negocio".

5.4. Por otro lado, existe un verdadero ejército de computadores zombis o botnet. Mediante el término Botnet hacemos referencia a un conjunto o red de robots informáticos o bots; éstos ejecutan sus tareas (fingir la presencia de apostadores) de manera cuasi autónoma y automática sin que los propietarios de los computadores infectados sepan que un programa malicioso está operando en su equipo. Denominaremos en este caso Master Botnet al artífice de la botnet que también puede controlar todos los computadores infectados de forma remota y que, en este caso en estudio, se utilizan para simular la existencia de cientos de miles de jugadores falsos.

5.5. Un servidor o "cluster" de servidores de comando y control permiten la gestión integrada del sistema y también brinda servicios análogos a los de un tablero de comando integrado o cuadro de mando integral.

5.6. Los computadores infectados o falsos jugadores se localizan físicamente en países asiáticos tales que, por razones geográficas, culturales, económicas y legales resulta imposible encarar en ellos investigaciones o acciones judiciales con los enfoques "tradicionales".

En la Figura 6 se puede observar la arquitectura conceptual de la "unidad de Ciber Lavado" que se ha venido describiendo.

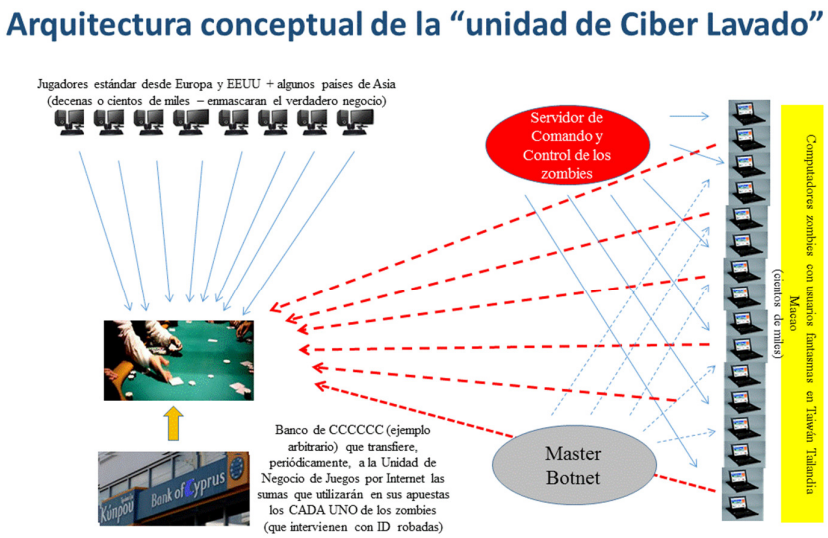

Figura 6

6. Fundamentos tecnológicos aplicables en la detección y "neutralización" del Lavado Transnacional de Activos en el Ciberespacio

Para abordar los aspectos centrales de este punto se recurrirá al modelo de referencia de interconexión ISO - International Organization for Standardization / OSI - Open System Interconection el que fue presentado originalmente en el año 1984[23] [24]. El desarrollo de este punto está limitado al mínimo necesario para dar sustento a los otros aspectos tratados en este trabajo.

El modelo ISO / OSI proporcionó a los proveedores de equipos y servicios en el ámbito de la teleinformática una referencia que permitió una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red ofrecidos por una enorme cantidad de empresas.

La referencia ISO / OSI posibilitó el desarrollo de numerosos protocolos que, por mucho tiempo, han venido desempeñando un rol fundamental en la tecnología de redes teleinformáticas.

El modelo de referencia ISO / OSI propone siete capas o niveles:

Nivel físico
Nivel de enlace de datos
Nivel de red
Nivel de transporte
Nivel de sesión
Nivel de presentación
Nivel de aplicación

6.1. Sólo a los efectos del propósito de este artículo se remarca que, en el nivel físico, las ramificaciones correspondientes a la topología de una red se concretan mediante los concentradores o hubs, dispositivos que reciben una señal y la repiten, simultáneamente y sin cambios u omisiones, tantas veces como puertos de salida posea este dispositivo (hub).

[23] http://www.iso.org/iso/home.html
[24] http://www.iso.org/iso/catalogue_detail.htm?csnumber=20269

6.2. Por otro lado, en el nivel del enlace de datos, se utilizan conmutadores o switches. A diferencia de los hubs, los switches pueden definir cuáles puertos de salida retransmitirán la señal y cuáles no. Esta selección de puertos de salida se realiza mediante la dirección MAC (Media Access Control) la cual es un identificador de 48 bits (6 bloques hexadecimales) que se corresponde en forma única con cada placa o dispositivo de red. La dirección MAC se conoce también como dirección física, y es una identificación única para cada dispositivo integrante de una red.

6.3. En el nivel 3 o nivel de red actúan los enrutadores españolizado como rúter (routers). La función esencial de un router consiste en enviar o encaminar paquetes de datos desde una red a otra. Los routers, que son usados para manejar los datos que circulan en forma de datagramas, posibilitan el pasaje de un tipo de red a otra de otro tipo. No todas las redes administran el mismo tamaño de paquetes; los routers deben entonces subdividir los paquetes de datos para que puedan navegar entre redes heterogéneas. Los routers trabajan con direcciones IP; (IP de Internet Protocol) las que se identifican con un número único e irrepetible con el cual se señala, lógicamente, a los dispositivos conectados a una red.
Por otro lado conviene, a esta altura, aclarar que en este trabajo se identifica como Flujo de Red (Netflow) a una suerte de "arreglo de variables" del tipo: dirección IP de origen, dirección IP de destino, etc. En otras palabras, en este trabajo, se toma como referencia a lo que la Unión Internacional de Comunicaciones denomina Flujo de Red.

Cuando se recomienda la utilización de Análisis de Flujo de Red en Gran Escala (Bilge, 2012) (Baieli, Cunha, Uzal, 2014) en el ámbito de la Seguridad Cibernética o de la Defensa Cibernética, se menciona la utilización de estadísticas del comportamiento de los routers (nivel 3); estadísticas elaboradas con alguno o varios de los componentes de los Flujos de Red.

Se remarca que, en Análisis de Flujo de Red en Gran Escala, se trabaja fundamentalmente en el nivel 3, lejos del "nivel de aplicación" (nivel 7) que es el más sensitivo respecto del derecho a la confidencialidad de los usuarios. En otras palabras, acciones preventivas y de detección de Ciber Agresiones pueden ser encaradas sin violar el derecho a la privacidad de persona alguna. Una Internet segura y en la que tengan vigencia los derechos humanos básicos es posible y, además, estrictamente necesaria.

6.4. El nivel 4 o de transporte se corresponde, casualmente, con el transporte de los datos (que se encuentran dentro del paquete) del dispositivo de red de origen al de destino, independizándolo del tipo de red física que esté utilizando.

6.5. En el nivel 5 o de sesión se mantiene y controla el enlace establecido entre dos dispositivos.

6.6. El nivel 6 o de presentación se encarga de la representación de la información de manera que, aunque existan entre los equipos de la red diferentes representaciones internas de caracteres los datos, lleguen de manera reconocible a los dispositivos de la red que operen como destino.

6.7. En el nivel 7 o de aplicación se ofrecen a las aplicaciones las facilidades para acceder a los servicios de los demás niveles y se define los protocolos que utilizan las aplicaciones para intercambiar datos.

El nivel 7 es el más sensitivo a los efectos de preservar la confidencialidad y otros derechos humanos básicos de los usuarios. Las recomendaciones de carácter preventivo contenidas en este trabajo, en general, constituyen estudios estadísticos realizados en general en el nivel 3 o de red. La detección de acciones maliciosas e la red está fundamentada en estudios estadísticos del comportamiento de los routers o enrutadores, expresado como línea general de trabajo. Este aspecto ha venido siendo expuesto, por el equipo

de la UNSL que desarrolló este trabajo, en diversos foros[25] [26] (UZAL, R., MONTEJANO, G., RIESCO, D., 2014 – 1 - 2).

7. Introducción al Análisis de Flujo de Redes

El Análisis de Flujo de Red[27] en general y específicamente el Análisis de Flujo de Redes en Gran Escala c en particular constituyen ítems de gran relevancia en el contexto de este trabajo. Mediante la secuencia de pasos incluidos en el Análisis de Flujos de Redes es posible obtener registros que pueden ser asociados o a actividades sospechosas en una red monitoreada. En otras palabras, en una "etapa de aprendizaje", los citados registros, muchas veces en forma de histogramas, son asociados a distintos tipos de agresiones. La analogía con la correspondencia "impresiones digitales / identidad de las personas" es realmente muy importante. Estas asociaciones histograma / agresión deben ser almacenadas en una sofisticada data warehouse (gran reservorio de datos). También son necesarios mecanismos de data mining ("minería" de datos) de alta eficacia para recuperar oportunamente los contenidos de la data warehouse.

Agresiones como ataques distribuidos masivos para obtener "denegaciones o bloqueos de servicios", acciones destinadas a la detección de vulnerabilidades y muchas otras actividades vinculables a Ciber Ataques (GOMEZ, 2011 pp 195-231), pueden ser detectadas con tasas de efectividad muy altas y también con tasas de falsos positivos realmente bajas.

En un trabajo cooperativo entre la Universidad Federal de Minas Gerais (Brasil) y la Universidad Nacional de San Luis (Argentina) se construyó, a nivel prototipo (BAIELI, C., CUNHA, I., UZAL, R. - 2014), una herramienta basada, casualmente, en "Análisis de Flujo de Redes a Gran Escala".

Esta herramienta genera flujos de datos de red a partir de paquetes capturados; luego se los exporta a un colector de flujos donde son analizados para determinar su compatibilidad o no con comportamientos sospechosos en la Red tales como Ciber Ataques, Ciber Espionaje, ejecución de Análisis de Vulnerabilidades, etc.

Esta capacidad de generación de flujos, a partir de paquetes de datos, la disponen routers de distintas marcas y tipo. Una adecuada selección de routers, ubicados estratégicamente en distintos segmentos de la Red a ser monitoreada, posibilita el mencionado "Análisis a Gran Escala".

La citada herramienta prototipo fue desarrollada en un contexto de programación multiparadigma. Además se desarrollaron e hicieron funcionar exitosamente rutinas de prueba y pequeños script en lenguaje PYTHON para comparar registros de Flujos de Red con los contenidos de una base de datos (data warehouse) MYSQL. Alrededor de catorce millones de registros fueron obtenidos de trabajos análogos realizados en otras universidades.

La herramienta fue testeada en un servidor de 6 Gb de memoria RAM y un disco 1 Terabyte y un procesador INTEL de dos núcleos.

Se realizaron pruebas "de campo" en espacios geográficos importantes las que permitieron validar los "perfiles" de histogramas correspondientes a actividades ilícitas o sospechosas en la Red tales como "scanning" de redes, "scanning" de puertos, ataques a diccionarios, denegación de servicios, etc.

Se obtuvieron series numéricas, tomando repetitivamente muestras en distintos intervalos, las que dieron lugar a histogramas, tomando como base para cada intervalo, por ejemplo:

[25] http://content.netmundial.br/contribution/internet-roadmap-topics-freedom-and-security-in-cyberspace-a-cyber-defense-perspective/61
[26] http://www.sbseg2014.dcc.ufmg.br/programacao/
[27] https://www.manageengine.com/products/netflow/cisco-netflow.html

Cantidad de flujos por IP de origen
Cantidad de flujos por IP de destino
Cantidad de flujos por puerto de origen
Cantidad de flujos por puerto de destino
Tamaño de flujos en un dado intervalo: 1, 2, 3, 4 y 5 minutos
Cantidad de flujos por protocolo de red (TCP, ICMP o UDP)
Otros
Combinaciones de los anteriores

En la Figura 7 se observa el tráfico en la Red (paquetes), los atributos de un Flujo de Red y el modelado del comportamiento estadístico de un router caracterizando el tráfico en la Red en forma análoga a "impresiones digitales"

La idea es que la herramienta correspondiente "aprenda" asociando histogramas u otros elementos estadísticos a distintos tipos de malware. Posteriormente, en base al aprendizaje, la herramienta deberá "detectar" la presencia de dichos diversos tipos malware en el tráfico de red.

Tráfico en la Red, atributos de un Flujo de Red y comportamiento estadístico de un router caracterizando el tráfico en la Red

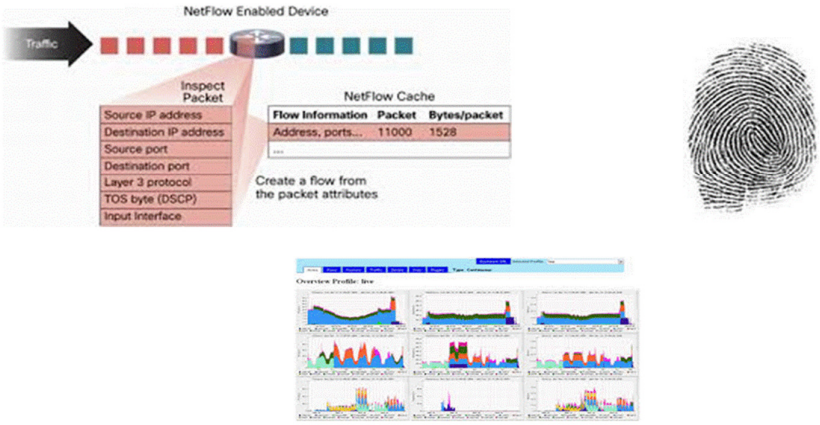

Figura 7

Como se adelantó, algunos de los módulos del prototipo desarrollado se comportan en forma análoga a un AFIS - Sistemas de Identificación mediante huella dactilar. Los histogramas que modelan el comportamiento de los routers, en los "puntos de toma", se comparan con los histogramas contenidos en una data warehouse. Experimentalmente se probó que dicha comparación es eficaz para detectar Flujos de Red compatibles con los de Ciber Agresiones.

7.1. Ejemplos de patrones a ser utilizados en el Análisis de Flujos de Red

En la Figura 8 se adelanta un ejemplo de utilización de reconocimiento de patrones para identificar la presencia de software malicioso

Ejemplo de utilización de reconocimiento de patrones para identificar la presencia de software malicioso

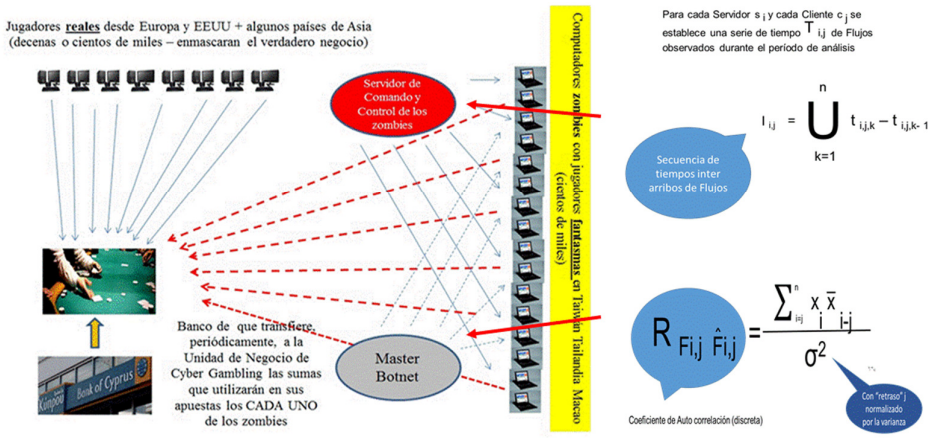

Figura 8

7.1.1. Patrones basados en Autocorrelación

La Autocorrelación es utilizada para comparar una señal consigo misma en un contexto de procesamiento de señales. La Autocorrelación es muy útil para identificar patrones repetitivos en los datos de series temporales. Una serie series de tamaños de flujo Fi,j puede ser mostrada como una serie temporal considerando los tamaños de Flujo de Red en el tiempo. Dado que la función de Autocorrelación también requiere un muestreo periódico como entrada, segmentamos las series de tiempo en intervalos fijos calculando el valor medio en cada uno de dichos intervalos. Empíricamente se encontró que son apropiados intervalos de muestreo de 1, 2, 3, 4 y 5 minutos, coincidiendo con resultados de otros grupos de investigación citados en este trabajo. Dado que las series temporales con muestreo periódico i,j han sido derivadas de Fi,j , se procesan dichas series utilizando una función de Autocorrelación; aspectos importantes se extraen del resultado de aplicación de dicha función. En este caso utilizamos un coeficiente de Autocorrelación discreta.

$$R_{Fi,j\,\hat{}\,Fi,j} = \frac{\sum_{i=j}^{n} X_i \bar{X}_{i-j}}{\sigma^2}$$

La salida de la función de autocorrelación se verifica para cada uno de los períodos incluidos en la serie temporal. Dicha salida es a su vez procesada para obtener la media y la desviación típica de estos valores para llegar a los resultados finales constituidos por los patrones que identifican la naturaleza de distintos tipos de tráficos en la red.

7.2. Patrones de acceso de clientes a sus respectivos servidores de comando y control.

Una característica o propiedad típica de los botnets o redes de computadores zombis es que cada uno de dichos zombis establece, con una determinada e identificatoria frecuencia, la conexión con los servidores de comando y control y/o master botnet.

Esas conexiones tienden a ser efímeras, dado que conexiones de larga duración pueden llamar atención en demasía respecto de la presencia de redes de zombis.

El fundamento para seleccionar los aspectos a ser extraídos de manera de distinguir entre patrones de acceso maliciosos y patrones de acceso benignos es, en general, el estudio y comparación de las frecuencias de acceso; los clientes tipo zombis muestran patrones de comportamiento que los diferencian de tráfico benigno en la Red.

Los clientes que solo brindan servicios benignos no exhiben, en general, patrones de comportamiento en común, entre otras cosas, por las diversas interacciones con operadores reales (seres humanos) que suelen tener conductas no repetitivas. Dado que todos los zombis comparten el mismo o muy similar patrón de acceso (por ello se los llama bot), es posible plantear:

$$I_{i,j} = \bigcup_{k=1}^{n} t_{i,j,k} - t_{i,j,k-1}$$

Para una serie de flujos Ti,j bajo observación en el período de análisis, consideramos una secuencia de tiempos inter arribos de los flujos **I** i,j la que es derivada de la serie de tiempo tomando la diferencia entre conexiones consecutivas.

La expresión **t** i,j,k representa al elemento k ésimo de de la serie Ti,j. Estimaciones estadísticas son elaboradas a partir de las secuencias inter arribos, incluyendo mínimo, máximo, media y desviación típica.

Estos valores configuran patrones que pueden ser asociados a la actuación de distintos tipos de software malicioso en la red monitoreada.

En la Figura 9 se observa cómo funcionan la fase de aprendizaje (color azul) y la fase operativa (color rosa) de una herramienta de detección de malware en la Red mediante Análisis de Flujo de Redes.

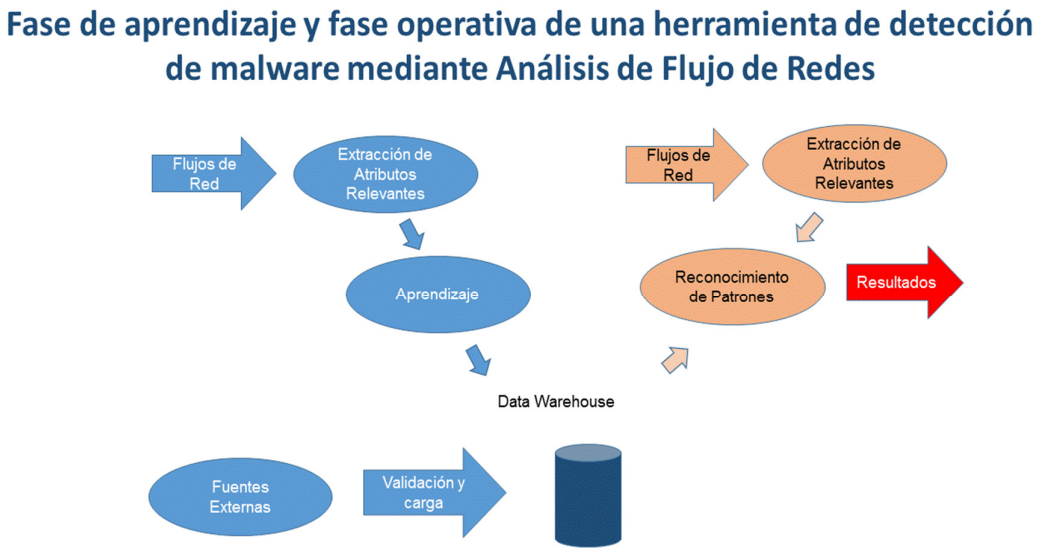

Figura 9

Conclusiones parciales de este punto: a) Es posible detectar, con llamativa efectividad, Flujos de Red que se correspondan con distintas Ciber Agresiones[28]; las correspondientes a "cyber gambling" (apuestas en línea) se detectan con cierta facilidad, b) Está experimentalmente probado que el "Problema de la Atribución" tiene solución; posibilidad concreta de detección del o de los servidores de comando y control (BAIELI, C., CUNHA, I., UZAL, R., - 2014), c) Está demostrado que es posible implementar medidas de vigilancia en el Ciberespacio sin afectar ningún Derecho Humanos (privacidad, libertad, etc.)[29]; d) Es posible y por otro lado muy conveniente desarrollar e implantar, en países de Sudamérica, aspectos conceptuales e instrumentales, como los citados en este punto del artículo, en el ámbito de la Seguridad Cibernética y de la Defensa Cibernética.

8. ¿Es aplicable el Artículo 51 de la Carta de las Naciones Unidas en el caso de Lavado Transnacional de Activos en el Ciberespacio?

El Artículo 51 de la Carta de las Naciones Unidas[30] establece (transcripción): "Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los Miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales".

Por otro lado, "The United Nations Office on Drugs and Crime (UNODC)" estima que el "negocio" del lavado de activos tiene asociado ingresos anuales que implican entre el 3 al 5 % del Producto Bruto

[28] https://www.acsac.org/2012/openconf/modules/request.php?module=oc_program&action=view.php&a=&id=73&type=4
[29] http://content.netmundial.br/contribution/internet-roadmap-topics-freedom-and-security-in-cyberspace-a-cyber-defense-perspective/61
[30] http://www.un.org/es/documents/charter/chapter7.shtml

Global. Utilizando el léxico anglo sajón, estaríamos en el orden de "trillones" de U$D, es decir, trece cifras significativas a la izquierda del punto (o coma) decimal.

Está claro que, cuando cifras del orden de magnitud como el de las citadas impactan en la economía de un país, causan daños igual o mayores que las correspondientes a un "ataque armado" (referencia utilizada en el citado Artículo 51).

Un país quedaría habilitado al ejercicio del derecho inmanente de legítima defensa en el caso de que organizaciones claramente alineadas con el crimen organizado transnacional comprometieran la existencia o la estabilidad del correspondiente estado nación impactando su economía mediante operaciones que involucraran, directa o indirectamente a su economía, con cifras del orden de las estimadas por UNODC.

Existe un importante consenso respecto de considerar a un ciber ataque a un estado nación, que destruya componentes importantes de su infraestructura crítica, equivalente a las agresiones bélicas "tradicionales" (bombardeos, desembarcos de tropas hostiles, etc.). El Ciber Lavado Transnacional de Activos utiliza, asimismo, conceptos, métodos e instrumentos análogos a los que se usan en la Ciber Guerra.

La destrucción remota de un servidor de comando y control del que se pueda probar que su función es la de manejar un esquema de Lavado Transnacional de Activos en el Ciberespacio, en determinadas condiciones, constituiría un acto de legítima defensa con independencia de la localizaciones geográficas, tanto del citado servidor de comando y control como la del estado nación que, sintiéndose agredido, haga ejercicio de su derecho a la legítima defensa.

Aseveración a ser discutida: El narcotráfico no se incrementa por el incremento de la producción de drogas ilegales, el tráfico ilegal de armas no crece por un supuesto incremento en la producción global de armamentos y la corrupción gubernamental no crece porque ahora los funcionarios sean más corruptos que antes. Dichas tres actividades delictivas cuentan hoy con servicios de lavado transnacional de dinero sumamente especializados y altamente tecnificados que disminuyen significativamente el riesgo. Ofertas de servicios de Lavado Transnacional de Activos en el Ciberespacio están incrementando la atracción y la rentabilidad de los delitos precedentes mencionados.

Elementos de juicio:

- El Lavado Transnacional de Activos en el Ciberespacio puede causar daños mayores, a un país, que Ciber Armas como Stuxnet[31] o Flame[32].
- La Carta de las Naciones Unidas fue firmada en San Francisco, Estados Unidos el 26 de junio de 1945. Entró en vigor el 24 de octubre de 1945. Sus contenidos se correspondía con la visión de los ámbitos o dominios de los conflictos que se tenía en ese entonces: Tierra, Mar y Aire. Nadie imaginaba que el Espacio Exterior primero y luego el Ciberespacio se constituirían en nuevos ámbitos o dominios de graves conflictos.
- La principal fuente de ventajas competitiva de las organizaciones criminales que brindan servicios de Lavado Transnacional de Activos en el Ciberespacio es que quienes deben combatirlas suelen aferrarse a criterios geográficos de la soberanía anteriores al concepto de Ciberespacio.
- Quienes claramente estén orientados a una efectiva mitigación del impacto negativo causado por el Lavado Transnacional de Activos en el Ciberespacio, es probable que coincidan en que los contenidos de este punto del presente trabajo ajustan al espíritu del Artículo 51 de la Carta de las Naciones Unidas. El pasaje del tiempo provocó que "la letra" de dicha normativa no ajuste estrictamente a la actual naturaleza de los conflictos globales.

[31] http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
[32] http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html

- Si un estado nación es atacado tiene derecho a defenderse. El Lavado Transnacional de Activos en el Ciberespacio constituye un gravísimo ataque a la economía, a la seguridad, a la estabilidad social y a la estabilidad política.

9. Posible intervención de la Unión Internacional de Telecomunicaciones

Como está expresado en su página web, la UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación.

La UIT está basada en el principio de la cooperación internacional entre los gobiernos (Estados Miembros) y el sector privado (Miembros de Sector, Asociados e Instituciones Académicas), la UIT es el primer foro mundial en el que las partes colaboran para lograr un consenso sobre una amplia gama de cuestiones que afectan a la futura orientación de la industria de las TIC.

La UIT ya ha tenido una más que destacada intervención en caso de los conflictos en el Ciberespacio. Se menciona como ejemplo la brillante intervención cuando se produjo el ataque, mediante la Ciber Arma Flame, a las plataformas petroleras de Irán (UZAL, R., MONTEJANO, G., RIESCO, D., - 2014).

Cuando un estado nación diseñe e implemente sistemas de detección de esquemas de Lavado Transnacional de Activos en el Ciberespacio y de neutralización / destrucción de los correspondientes servidores de comando y control, será muy conveniente que dichas facilidades estén homologadas por la UIT. La probabilidad de éxito en las detecciones debería estar por encima del 99 % y la de generación de falsos positivos por debajo del 0,01 %.

Las citadas facilidades de detección y neutralización de esquemas de Lavado Transnacional de Activos en el Ciberespacio deberán incluir en sus prestaciones la posibilidad de producir evidencias forenses cuasi irrefutables para ser presentadas ante foros y tribunales internacionales.

10. Propuestas

10.1. Difundir que el Lavado Transnacional de Activos en el Ciberespacio constituye una Ciber Agresión que puede superar en gravedad a acciones de Ciber Guerra, es decir aquellas destinadas a destruir elementos esenciales de la infraestructura crítica de un país, tales como destilerías de petróleo, instalaciones nucleares, sistemas de distribución de energía, etc. Recalcar que el Lavado Transnacional de Activos en el Ciberespacio constituye un desafío mayor para la gestión gubernamental. Los efectos negativos en la economía de un estado nación, provenientes del Lavado Transnacional de Activos pueden ser devastadores.

10.2. Difundir que el Lavado Transnacional de Activos produce sobre los estados naciones efectos más perniciosos que los delitos precedentes: Narcotráfico, corrupción gubernamental y tráfico ilegal de armas. Sin Lavado Transnacional de Activos las “tasas internas de retorno” del narcotráfico, de la corrupción gubernamental y del tráfico ilegal de armas decrecerían muy significativamente.

10.3. Discutir, en distintos foros, si realmente las Ciber Agresiones, de acuerdo a su naturaleza y a los daños reales o potenciales que produzcan, quedan potencialmente encuadradas en el espíritu del Artículo 51 de la Carta de las Naciones Unidas.

10.4. Difundir y motivar para que se desarrollen conceptos, métodos y herramientas que permitan detectar, identificar fehacientemente y eventualmente neutralizar el funcionamiento de “empresas de servicios de lavado” Transnacional de Activos (AGÜERO, W. MACEDO, D., UZAL, R. 2014)

10.5. Interactuar efectivamente, con la Unión Internacional de Telecomunicaciones, para implementar mecanismos efectivos para mitigar los efectos perniciosos del el Lavado Transnacional de Activos en el Ciberespacio homologados por la UIT.

10.6. Difundir la clara tendencia hacia el Lavado Transnacional de Activos en el Ciberespacio del actual monto total anual de Lavado de Activos estimado en el orden del 5% del Producto Bruto Global. Esas cifras tienen la capacidad para desestabilizar la economía de cualquier país del mundo.

11. Conclusiones

11.1. Existen Ciber Agresiones, inicialmente encuadrables como Ciber Crímenes, que pueden llegar a afectar contundentemente a la economía de los países más poderosos del mundo. Obviamente los países afectados tiene derecho a la autodefensa. La naturaleza del Ciberespacio obliga a rever el tradicional concepto de jurisdicción basado en criterios eminentemente geográficos.

11.2. Además de las capacidades de detección y neutralización de las Ciber Agresiones, los estados naciones deben desarrollar capacidades forenses para poder demostrar, ante organismos internacionales, que realmente el derecho a la autodefensa fue ejercido legítimamente.

11.3. El desarrollo de capacidades de detección y neutralización, sumado a las mencionadas capacidades forenses, ejercerá una suerte de Ciber Disuasión respecto de las ""empresas de servicios" de Lavado Transnacional de Activos en el Ciberespacio. Dicha Ciber Disuasión incrementará la percepción del riesgo de funcionamiento por parte de dichas "empresas de servicios". El incremento de la percepción del riesgo impactará negativamente en la "Tasa Interna de Retorno" de los "empresarios" del Ciber Lavado. Esta disminución de la rentabilidad afectará negativamente al "negocio" de los delitos precedentes (narcotráfico, corrupción gubernamental y tráfico ilegal de armas). Es más que evidente que la "batalla decisiva" contra dichos "delitos precedentes" debe darse en los mecanismos de Lavado de Activos. Una proporción importante y creciente del Lavado de Activos se verifica hoy en el Ciberespacio.

11.4. Neutralizar los sistemas transnacionales de Lavado de Activos en el Ciberespacio ("empresas de servicio") es más sencillo y efectivo que seguir caso por caso cada una de las acciones de Lavado. Esto último es desgastante y aparentemente inconducente.

12. Referencias

Sitios Web

[1] http://www.fbi.gov/about-us/investigate/organizedcrime/italian_mafia
[2] http://www.unis.unvienna.org/unis/pressrels/2000/shc302.html
[3] http://www.npr.org/2012/06/02/154188937/flame-sheds-light-on-politics-of-cyberwarfare
[4] https://www.youtube.com/watch?v=vrRj-kRofRg
[5] http://lema.rae.es/drae/?val=ciberespacio

Libros

MADINGER, J. (2011), Money Laundering: A Guide for Criminal Investigators, Publisher CRC Press, New York

HOLT, T., BOSSLER, A. (2015), Cybercrime and Digital Forensics, Publisher: Routledge, Londres

GOMEZ VIEITES, A. (2011), Enciclopedia de la Seguridad Informática, Alfaomega, México D.F.

CLARKE, R., KNAKE, R. (2010), Cyber War, Harper Collins Publishers, New York

Publicaciones científicas

BILGE, l., BALZAROTTI, D., ROBERTSON, W., KIRDA, E., KRUEGEL, C., (2012) DISCLOSURE: Detecting Botnet Command and Control Servers Through Large-Scale NetFlow Analysis, ACM Digital Library, http://dl.acm.org/citation.cfm?id=2420969 leylya_yumer@symantec.com

BAIELI, C., CUNHA, I., UZAL, R., (2014) Aportes para la detección de Ciber Agresiones, Tesis de Maestría (Universidad Nacional de San Luis – Argentina / Universidad Federal de Minas Gerais – Brasil) a ser defendida en el primer semestre de 2015 cbaieli@hotmail.com

UZAL, R., MONTEJANO, G., RIESCO, D., (2014 - 1) Internet Roadmap topics: Freedom and Security in Cyberspace - A Cyber Defense perspective, NETmundial Contributions, San Paulo, http://content.netmundial.br/contribution/internet-roadmap-topics-freedom-and-security-in-cyberspace-a-cyber-defense-perspective/61

UZAL, R., RIESCO, D. MONTEJANO, G., (2014 - 2), Conflictos en el Ciber Espacio entre estados naciones: Potenciales aportes para la eventual actuación de las Naciones Unidas y de la Unión Internacional de las Telecomunicaciones, 43 Jornadas Argentinas de Informática Proceedings, Sociedad Argentina de Informática, Buenos Aires http://43jaiio.sadio.org.ar/proceedings/SIE/16-SIE704.pdf

AGÜERO, W. MACEDO, D., UZAL, R. (2014) Aportes para la neutralización de Ciber Agresiones, Tesis de Maestría (Universidad Nacional de San Luis – Argentina / Universidad Federal de Minas Gerais – Brasil) a ser defendida en el primer semestre de 2015 l.com