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

Roberto Uzal (*), Daniel Riesco (*), Germán Montejano (*), Claudio Baieli (*), Walter Agüero (*)
ruzal@unsl.edu.ar, driesco@unsl.edu.ar, cbaieli@hotmail.com, wfaguero@gmail.com

(*) Universidad Nacional de San Luis

Keywords: Internet-roadmap; Internet Freedom&Security; Cyber-Defense; Cyber-Attacks; Cyber-Espionage; Futuro de Internet; Libertad y Seguridad en Internet; Ciber Defensa; Ciber Ataques; Ciber Espionaje

Resumen

Esta contribución está orientada a proponer algunos aspectos específicos a ser utilizados en una eventual actuación de las Naciones Unidas en general, o en particular de la Unión Internacional de Telecomunicaciones, en el caso de continuar concretándose agresiones entre estados naciones en el Ciber Espacio. Estas agresiones han sido analizadas en foros globales en los que han participado los autores. Los resultados de dichas participaciones, las consultas efectuadas a expertos reconocidos mundialmente y los cambios que necesariamente se verificarán en la gobernanza de Internet en el corto y en el mediano plazo, han sido las circunstancias motivadoras de la elaboración de este reporte. Se informa sobre un proceso de adquisición de conocimiento y habilidades, desarrollado en el contexto de la Línea de Investigación “Ciber Defensa” de la Universidad Nacional de San Luis. Los aspectos que se exponen en este trabajo han sido o están siendo desarrollados por tesistas de la Maestría en Ingeniería de Software y por doctorandos pertenecientes al Doctorado en Ingeniería Informática, ambos postgrados de la citada universidad. Se espera que, el éxito de los emprendimientos correspondientes a la Línea de Investigación “Ciber Defensa”, aporte a un Ciber Espacio más confiable y que se logre un impacto global.

Introducción

Los autores de este trabajo, invitados por los organizadores de NETmundial (NETmundial, 2014), participaron y contribuyeron muy específicamente en el ámbito de la “Reunión Global de Múltiples Partes Interesadas” sobre el “Futuro de la Gobernanza de Internet”, realizada en San Pablo, Brasil, los días 23 y 24 de abril de 2014. La reunión constituyó una iniciativa conjunta del Comité Gestor de Internet en Brasil (CGI.br) y /1Net, es decir, el foro que reúne a las entidades internacionales de los distintos sectores que participan en la gobernanza de Internet.

NETmundial debería ser interpretada, en parte, como una consecuencia de los Ciber Ataques / Ciber Espionaje entre estados naciones, tal como se destacó, por ejemplo, en la última Asamblea General de las Naciones Unidas (Rousseff, 2013) y en la última reunión de la Comunidad de Estados Latinoamericanos y Caribeños - CELAC (CELAC, 2014).

En el contexto de NETmundial los autores contribuyeron con un trabajo titulado “Internet Roadmap topics: Freedom and Security in Cyberspace - A Cyber Defense perspective” (Uzal, 2014). Dicha contribución, aún antes de desarrollarse NETmundial, despertó interés en diversos países. En cierta forma el presente trabajo es la continuación, en lo conceptual y en lo instrumental, de la contribución a NETmundial y, por otro lado, es una síntesis del proceso de adquisición de conocimiento sobre Ciber Defensa en el entorno de una Línea de Investigación “Ciber Defensa” del Proyecto “Ingeniería de Software: Aspectos de alta sensibilidad en el ejercicio de la profesión de Ingeniero de Software", de la Universidad Nacional de San Luis.

Los autores también participaron intensamente en las discusiones asociadas a la elaboración del “Outcome Document” de NETmundial.

La Ciber Defensa, como objeto de estudio, es sumamente atractiva porque en ella se produce una suerte de síntesis de los conceptos y técnicas más avanzados de la Tecnología de la Información y de la Ingeniería de Software. Por otro lado, dichos conceptos y técnicas se encuentran en una evolución cuya velocidad es realmente sorprendente.

El Ciber Espacio ha sido reconocido como un nuevo dominio de los actos hostiles entre estados naciones pero, hasta ahora y posiblemente en el mediano plazo, sin la existencia de un acuerdo internacional de Ciber Defensa, las "soluciones" unilaterales, muy probablemente, continuarán teniendo, desafortunadamente, un rol central en el campo de los incidentes en el Ciber Espacio (Uzal, 2012) (Geiss & Lahmann, 2013). Se espera que los resultados de NETmundial lleguen a contribuir al mencionado acuerdo internacional.

El "Problema de la Atribución" de los Ciber Ataques y del Ciber Espionaje, constituye un desafío mayor, tanto para los estados naciones como para los organismos internacionales (Geiss & Lahmann, 2013). Sobre este aspecto y otros íntimamente asociados, aportaron los autores de este trabajo en NETmundial.

En este ámbito, constituye un tópico tecnológico de muy alta importancia la detección de botnets (redes de computadores zombis) y de los verdaderos Servidores de Comando y Control de Ciber Ataques y de Ciber Espionaje. La propuesta integral de los autores incluye, entre otros aspectos, la utilización de "Análisis de Flujos de Redes / Reconocimientos por Patrones en Gran Escala". El uso de "Large Scale Net Flow Analysis (LSNFA) / Pattern Recognition (PR)" es factible tanto en lo tecnológico como en lo económico. Es posible obtener tasas de detección significativamente altas con tasas asociadas de "falsos positivos" realmente muy bajas (Baieli, Cunha, Uzal, 2014).

Surge como evidente que, si organismos internacionales como las Naciones Unidas / Unión Internacional de Telecomunicaciones, contaran con el ya citado acuerdo internacional, la detección de botnets y Servidores de Comando y Control utilizando LSNFA / PR permitiría resolver, casi en tiempo real, con una muy alta tasa de efectividad y muy baja tasa de falsos positivos, el "Problema de la Atribución" en el contexto de Ciber Ataques y Ciber Espionaje (Bilge et al, 2012) (Brauckhoff et al, 2009) (Claise, 2004) (Cook, et al 2005).

Sabemos que la "fuente de datos" ideal para la detección de botnets y sus Servidores de Comando y Control no existe actualmente. Sin embargo son válidos, como alternativa, los datos provenientes de los "Flujos de Redes"; en otras palabras, series numéricas que tomarán la forma de histogramas y que son representativas del comportamiento de los switches y routers en las capas II y III del modelo de interconexión ISO/OSI (Cisco, 2013) (Bilge et al, 2012) (Baieli, Cunha, Uzal 2014) (Uzal, Montejano, Riesco, 2013 / 14).

Un aspecto central: El hecho de trabajar casi exclusivamente con histogramas que modelan el comportamiento de las redes en las capas II y III, "alejados" de la Capa de las Aplicaciones (capa VII del modelo ISO/OSI), asegura que cuestiones relacionadas con la Privacidad, Confidencialidad y otros Derechos Humanos Básicos, de ninguna manera se verán afectados por las tareas que se propone que sean encaradas por organismos internacionales como las Naciones Unidas y la Unión Internacional de Telecomunicaciones.

En otras palabras, el actual know how tecnológico permite, de ser utilizado en forma adecuada, la existencia de una Internet donde la Libertad, Privacidad y la Seguridad puedan coexistir en un contexto en el cual los Derechos Humanos sean la principal referencia.

En la contribución que los autores realizaron para NETmundial, se remarcó que los conceptos y fundamentos de tipo tecnológico contenidos en el trabajo (LSNFA/PR) pueden ser utilizados también en la lucha contra el lavado internacional de activos en su modalidad más efectiva: "Apuestas en Lìnea" - Cyber Money Laundering – Cyber Gambling" (Uzal, 2013). Este aspecto también se destaca en este trabajo.

Además de Análisis de Flujo de Redes, otros aspectos asociados fueron encarados. El estudio de herramientas que se han utilizado en agresiones entre estado naciones ha sido objeto de estudios y de desarrollos en curso; protocolos y herramientas correspondientes a test de penetración fueron probados y continúan perfeccionándose.

Retomando el análisis de los efectos de NETmundial, los resultados de dicha reunión han motivado para que se reporte, como aspecto importante de este informe, la elaboración en curso de las bases de un Proyecto que serán puestas a consideración de las Naciones Unidas. Este trabajo, "ex ante" NETmundial, habría sido considerado como inconducente por estudiosos de las relaciones internacionales y del funcionamiento de los organismos con incumbencias globales. Lo "imposible", hasta hace muy poco, respecto de los responsabilidades de la gobernanza de Internet, es motivo de profundas y muy serias discusiones "ex post" NETmundial.

Dieciséis doctorandos de la Universidad Nacional de San Luis (UNSL, 2013) están trabajando en la elaboración de las mencionadas "bases para la elaboración del Proyecto". El gran desafío lo constituye, más allá de la complejidad técnica del proyecto, el enfoque eminentemente "multi interesados" (multistakeholders) de este emprendimiento. Gran parte de los factores críticos de éxito del Proyecto en ciernes, se encuentran comprendidos en el Área de Conocimiento "Stakeholder Management" de la Guía del Project Management Body of Knowledge (v. 5) del Project Management Institute (PMI, 2013).

Los resultados de detalle obtenidos, las herramientas desarrolladas y el conocimiento adquirido en la Línea de Investigación "Ciber Defensa" de la Universidad Nacional de San Luis, están a disposición de aquellos organismos del gobierno que, convenio mediante, así lo requieran.

Para finalizar esta Introducción, se adelanta que la estructura de este trabajo consta de, a) la mención de la necesidad de un acuerdo internacional en el ámbito de la Ciber Defensa; b) una breve referencia al Análisis de Flujo de Redes a Gran Escala – Reconocimiento por Patrones; c) aspectos relacionados con la puesta en práctica de los derechos enunciados en el artículo 51 de la Carta de las Naciones Unidas y sus potenciales consecuencias; d) citas respecto del "valor agregado" de los conceptos y herramientas contenidos al poder ser usados en la lucha contra lavado internacional de activos en su modalidad más efectiva: "Apuestas en Línea" - Cyber Money Laundering – Cyber Gambling; e) reporte de la elaboración, en curso, de las bases de un proyecto que permita a las Naciones Unidas / Unión Internacional de Telecomunicaciones tener un rol activo, efectivo y positivo en la mitigación / eliminación de las agresiones entre estados naciones en el Ciber Espacio. El trabajo finaliza con las conclusiones del mismo y las referencias en las que se sustentan varias de las aseveraciones contenidas.

La necesidad de un acuerdo internacional en el ámbito de la Ciber Defensa

Se había adelantado en la Introducción que, actualmente y seguramente en el mediano plazo, sin un acuerdo internacional acerca de Ciber Defensa, los enfoques unilaterales probablemente seguirán teniendo un rol predominante en el caso de incidentes entre estados naciones en el Ciber Espacio.

Uno de los aspectos relevantes de esta presentación lo es el hecho de proponer una alternativa consistente que complementa el foco unilateral basado en el Artículo 51 de la Carta de las Naciones Unidas (derecho a la legítima defensa por parte de los estados naciones). Este trabajo presenta tanto aspectos tecnológicos como nuevas incumbencias / responsabilidades a ser encaradas por las Naciones Unidas / Unión Internacional de Telecomunicaciones u otros organismos internacionales, esta última cuestión será motivo de posteriores intercambios de opiniones.

Los autores, en el contexto de NETmundial, efectuaron enfáticas propuestas respecto de un acuerdo internacional en el ámbito de la Ciber Defensa, con un estricto enfoque "multistakeholder" (NETmundial, 2014).

Análisis de flujo de redes a gran escala – Reconocimiento por patrones

Análisis de Flujo de Redes en un ítem tecnológico que tiene su relevancia en el contexto de esta presentación. Mediante la secuencia de pasos incluidos en el Análisis de Flujos de Redes es posible obtener registros que pueden ser asociados a alertas de intrusiones o de actividades sospechosas en una red monitoreada. En una "etapa de aprendizaje", los citados registros, en la forma de histogramas, son asociados a distintos tipos de agresiones. Estas asociaciones histograma/agresión deben ser almacenadas en una sofisticada data warehouse asociada a mecanismos de data mining de alta eficacia. Agresiones como ataques distribuidos masivos, para obtener "denegaciones de servicios", acciones destinadas a la detección de vulnerabilidades y, muchas otras actividades vinculables de Ciber Ataques, pueden ser detectadas con tasas de efectividad muy altas y también con tasas de falsos positivos realmente bajas.

Se construyó, a nivel prototipo, una herramienta basada en "Análisis de Flujo de Redes a Gran Escala. La herramienta genera flujos de datos de red a partir de paquetes capturados; se los exporta a un colector de flujos donde son analizados para determinar su compatibilidad o no con comportamientos sospechosos en la Red: Ciber Ataques, Ciber Espionaje, ejecución de Análisis de Vulnerabilidades, etc. Esta capacidad de generación de flujos, a partir de paquetes, la disponen routers de distintas marcas y tipo (CISCO, 2014). Una adecuada selección de routers, ubicados estratégicamente en distintos segmentos de la Red, posibilita el mencionado "Análisis a Gran Escala".

La herramienta fue desarrollada en un contexto de programación multiparadigma. Además se desarrollaron e hicieron funcionar exitosamente rutinas de prueba y pequeños script para comparar registros en lenguaje PYTHON con los contenidos de una base de datos MYSQL (14000000 registros extraídos de segmentos de red) de otra universidad.

La herramienta fue testeada en un servidor de 6 Gb de memoria RAM y un disco 1 Terabyte y un procesador INTEL de 2 NUCLEOS

Se realizaron tests "de campo", en espacios geográficos importantes, 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, que dieron lugar a histogramas, tomando como base, por ejemplo:

- 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
- Volumen de flujos (entrante o saliente) cada 5 minutos (por ejemplo)
- Cantidad de flujos por protocolo de red (TCP, ICMP o UDP)
- Otros
- Combinación de los anteriores

La puesta en práctica de los derechos enunciados en el artículo 51 de la Carta de las Naciones Unidas

El derecho a ejercer la legítima defensa por parte de los estados naciones, está consagrado en el artículo 51 de la Carta de las Naciones Unidas. Considerando los numerosos casos de Ciber Ataques a la infraestructura crítica de varios países, registrados en los últimos años (Uzal, 2012), el estar preparado para la legítima defensa, desde el punto de vista de los estados naciones, podría llevar a una no conveniente proliferación de Ciber Armas. Estudiosos de diversos lugares del mundo han acordado (Ahmadi, 2013) que la proliferación de Ciber Armas podría ser aún más perniciosa que la proliferación de Armas Nucleares.

Con la finalidad adquirir conocimientos y llegar a un aceptable nivel de habilidades en el ámbito de las denominadas Ciber Armas, se tomó como referencia al software malicioso sumamente sofisticado denominado "Flame", detectado en la plataformas petroleras de Irán (Uzal, 2012) (Ahmadi, 2013).

Aparentemente la arquitectura conceptual de “Flame” podría guardar una cierta analogía con una suerte de “bus de software” en cada uno de cuyos “slots” podían ser asignados, con cierto carácter dinámico, distintos módulos de malware de muy alta efectividad. La orientación principal para definir la arquitectura de la herramienta fue suponer cuál habría sido la arquitectura conceptual de “Flame”. Con esa orientación se comenzó a trabajar tanto en la arquitectura general y como con la de algunos de los potenciales módulos. Se comenzaron las tareas, correspondientes a uno de los módulos, analizando las vulnerabilidades de uno de los protocolos de la pila de Bluetooth, el perfil Obex, (OBject EXchange). En primera instancia se estudiaron las posibilidades de hardware y/o software existentes. En el ámbito del hardware, por ejemplo, se analizó Frontline pues trabaja con dispositivos que podrían ayudar en la detección de vulnerabilidades en las distintas capas de Bluetooth y es utilizado por fabricantes de teléfonos celulares. Se encontraron funcionalidades que podrían facilitar la comprensión del ámbito estudiado. Como ejemplo de la búsqueda de conocimientos y de posibilidades a nivel de software, se contactó con distintos proyectos en curso en otras instituciones; uno de los autores de este trabajo se asoció al grupo de detección de vulnerabilidades de Bluetooth SIG.

En cuanto a la herramienta que se utiliza para trabajar sobre la pila OBEX, se destaca que la misma utiliza la “confianza” en dispositivos previamente “emparejados”. Se profundizó el estudio y perfeccionamiento de un emprendimiento implementado en lenguaje Python que permite extraer y/o almacenar datos / información en equipos Bluetooth previamente “emparejados” sin que el usuario del equipo lo detectara en los ensayos que se realizaron.

Los primeros aspectos experimentales se realizaron en un pequeño equipo con 2 Mb RAM, con un disco de 80 Gb, “dongle Bluetooth” (dispositivo Bluetooth externo), sistema operativo Ubuntu y la herramienta del “proyecto Obex” instalada y compilada. Primero se “emparejó” un dispositivo celular (confianza) y luego, sin acciones adicionales, desde la PC fue posible listar las carpetas del teléfono móvil; también se efectuaron extracciones y o transferencias de archivos al celular sin que el usuario / operador, en ningún caso, lo detectara.

Otras de las tareas encaradas en este contexto:

a. Descarga, compilación y prueba de más de treinta scripts Python y C++ disponibles en Internet que actúan sobre distintos protocolos y perfiles.
b. Descarga, compilación y prueba de distintos proyectos análogos disponibles en Internet, realizados en Python y C++
c. Las tareas mencionadas en a. y b. se replicaron en distintos sistemas operativos: Linux, Ubuntu (varias versiones), CentOS y Windows, también varias versiones.
d. Con los respectivos script estables y funcionado correctamente, se analizaron vulnerabilidades en distintos tipos y marcas de teléfonos celulares.
e. Los éxitos alcanzados, en todos los casos, fueron avalados por los Profs. Drs. Daniel Macedo y José Marcos Nogueira del Departamento Ciencias de la Computación de la Universidad Federal de Minas Gerais (Agüero, Macedo, Uzal, Nogueira, 2013/14)

Respecto del ya citado “bus de software” símil “Flame”, se estudia el desarrollo de módulos prototipos adicionales.

Complementariamente al estudio de herramientas de intrusión, se definieron protocolos de test de penetración y se desarrollaron / adquirieron herramientas asociadas a dichos protocolos. Las capacidades de las mencionadas “asociaciones” protocolos / herramientas se encuentran en etapa de prueba. Los primeros resultados obtenidos han sido satisfactorios.

Un “valor agregado” relevante

En paralelo a lo mencionado en el ámbito de la Ciber Defensa, se ha venido estudiando la utilización del enfoque y de las herramientas de “Análisis de Flujo de Datos” como medio idóneo para encarar la prevención y la lucha contra el denominado Cyber Money Laundering - Ciber Lavado de Dinero. Aparece como evidente que el “seguimiento de la ruta del dinero”, en el caso de Cyber Money

Laundering es, en general, inconducente e ineficaz. Se estudia 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 otros trabajos (CARI, 2013) 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.

La variante de Cyber Money Laundering denominada Cyber Gambling - Apuestas utilizando Internet es la más efectiva, según lo relevado por el equipo, 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.

La elaboración de un proyecto a ser presentado a las Naciones Unidas

En el contexto del Doctorado en Ingeniería Informática de la Universidad Nacional de San Luis, el primer módulo puesto a disposición de los doctorandos, ha sido “Gestión de Proyectos de Ingeniería”. Dieciséis doctorandos se encuentran cursando dicho módulo el cual está implementado sobre un caso práctico: Desarrollar y formalizar los aspectos esenciales que permitirán contar con las bases para la elaboración de un proyecto que posibilite una adecuada intervención de las Naciones Unidas / Unión Internacional de las Telecomunicaciones en los conflictos estado nación / estado nación desarrollados en el Ciber Espacio.

Los doctorandos están aportando significativamente para instanciar, al caso particular del citado emprendimiento, los contenidos genéricos de las Áreas de Conocimiento del Cuerpo de Conocimiento de la Gestión de Proyectos del Project Management Institute.

1. Administración de la Integración de Proyectos: Se refiere los procesos requeridos para asegurar que los elementos varios de un proyecto están coordinados apropiadamente.
2. Administración del Alcance del Proyecto: Se refiere el proceso requerido para asegurar que el proyecto incluye todo trabajo requerido, y sólo el trabajo requerido.
3. Administración del Tiempo del Proyecto: Se refiere los procesos requeridos para asegurar la terminación a tiempo del proyecto.
4. Administración de los Costos del Proyecto: Se refiere los procesos requeridos para asegurar que el proyecto es completado dentro del presupuesto aprobado.
5. Administración de la Calidad del Proyecto: Se refiere los procesos requeridos para asegurar que el proyecto va a satisfacer las necesidades para lo cual fue desarrollado.
6. Administración de los Recursos Humanos del Proyecto: Se refiere los procesos requeridos para hacer el uso más eficiente de las personas directamente involucradas en el proyecto.
7. Administración de las Comunicaciones del Proyecto: Se refiere los procesos requeridos para asegurar la generación apropiada y a tiempo, colección, diseminación, almacenamiento, y la disposición final de la información del proyecto.
8. Administración de Riesgos del Proyecto: Se refiere los procesos concernientes con la identificación, análisis, y respuesta al riesgo del proyecto.
9. Administración de la Procuración del Proyecto: Se refiere los procesos requeridos para adquirir bienes y servicios de fuera de la organización ejecutora.
10. Gestión de los Interesados en el Proyecto: Esta área de conocimiento incluye los procesos necesarios para identificar todas las personas y organizaciones afectadas por el proyecto, analizar sus expectativas y potencial impacto sobre el proyecto y desarrollar estrategias adecuadas para implicarles de forma efectiva en las decisiones y ejecución del proyecto.

También se ocupa de mantener un diálogo fluido y continuo con los stakeholders para satisfacer sus necesidades y expectativas, resolver los problemas conforme ocurran y promover su implicación activa en las decisiones y actividades del proyecto

Casualmente la Gestión de los Interesados (stakeholders) es el aspecto clave del proyecto. Los "interesados", en este caso, son organismos internacionales, alianzas regionales, países, corporaciones empresariales, organizaciones de distinto tipo, personas jurídicas y personas físicas de diversa naturaleza, diverso origen y con motivaciones heterogéneas.

En la primera parte del desarrollo del módulo del Doctorado en Ingeniería Informática de la Universidad Nacional de San Luis, denominado, como se adelantó, "Gestión de Proyectos de Ingeniería", se analizaron los antecedentes del emprendimiento y se avanzó, razonablemente, en lo que hace a "Gestión de los Interesados". También se inició el proceso de elaboración de la Descomposición de la Estructura de Trabajo (Work Breakdown Structure). Esta herramienta permitirá:

- Discutir en forma coherente y consistente el Alcance del Proyecto
- Elaborar un Programa del Proyecto totalmente consistente con el Alcance
- Elaborar el Presupuesto del Proyecto llegándose inclusive a contar con la "Línea de Base" del mismo.

En la segunda reunión correspondiente al desarrollo del módulo de doctorado "Gestión de Proyectos de Ingeniería", los doctorandos deberán realizar sus aportes para perfeccionar lo atinente a "Gestión de los Interesados" y deberán exponer sus avances en cuanto a la Descomposición de la Estructura de Trabajo. Posteriormente, en equipo, se iniciará el tratamiento de los primeros aspectos relacionados con "Administración de los Costos" del Proyecto.

Cuando los progresos logrados por los doctorandos alcancen un status de "Bases para la elaboración de un proyecto que posibilite una adecuada intervención de las Naciones Unidas / Unión Internacional de las Telecomunicaciones en los conflictos estado nación / estado nación desarrollados en el Ciber Espacio", los trabajos serán puestos a consideración de dichos organismos.

La participación de la Universidad Nacional de San Luis en NETmundial ha permitido establecer contactos que hacen viable dicha puesta a disposición.

Conclusiones

1. La Línea de Investigación "Ciber Defensa" de la Universidad Nacional de San Luis ha generado conocimientos y desarrollado herramientas, correspondientes a Ciber Defensa, que están a disposición de aquellos organismos del gobierno que, convenio mediante, los requieran. De hecho, investigadores de la citada Línea de Investigación ya han colaborado con el Gobierno Nacional en este ámbito.

2. En este trabajo se describe un proceso representativo de diversos emprendimientos encarados en el contexto de dicha Línea de Investigación.

3. Los investigadores de la Línea de Investigación "Ciber Defensa" han desempeñado un rol importante en el contexto de "NETmundial - Global Multistakeholder Meeting on the future of Internet Governance" en San Pablo – Brasil. Por otro lado, la asistencia a dicho foro les ha permitido establecer una red de contactos personales que viabiliza los propósitos enunciados en este trabajo, tal el de poder efectuar propuestas a las Naciones Unidas / Unión Internacional de Telecomunicaciones.

4. Encarar debidamente problemas como la proliferación del Uso Militar de Internet (Cyber Warfare), el Ciber Espionaje y el Ciber Crimen Organizado Trasnacional, requiere de acuerdos internacionales que no serán establecidos, desafortunadamente, en el corto plazo. Sin embargo, conceptos y herramientas citados en este trabajo pueden ser utilizados parcialmente

con la legislación internacional vigente, tal por ejemplo, la Carta de las Naciones Unidas y algunos acuerdos de cooperación en la lucha contra el Crimen Trasnacional Organizado. Los acuerdos de fondo deberán serlo mediante una convocatoria del tipo “Multistakeholders”. La carencia de dicho enfoque “Multiinteresados” le ha quitado efectividad a algunos “pasos” que se han tratado de dar en este sentido.

5. La viabilidad técnica y económica de los aspectos tecnológicos para resolver el “Problema de la Atribución” (Ciber Defensa y Ciber Espionaje) y para enfrentar el Ciber Delito Trasnacional y Organizado está prácticamente probada. Ocurre que sí se está aún lejos de lograr los acuerdos internacionales que son necesarios para utilizar efectivamente la disponibilidad de know how tecnológico citado.

6. En lo militar, la no existencia de acuerdos se plasmará en una peligrosa proliferación de Armas Cibernéticas. Dicha proliferación podría llegar a ser más perniciosa que la proliferación de Armamento Nuclear.

7. Ciber Defensa implica incursionar y consolidarse en capítulos de la Ingeniería de Software y de la Tecnología Informática que constituyen verdaderos desafío, por ejemplo, diseño e implantación de algoritmos computacionales de alta complejidad, programación multiparadigma, ingeniería reversa, arquitecturas de software, arquitecturas de hardware, arquitecturas de redes, distribución, concurrencia, tiempo real, data warehousing, data mining, adquisición de conocimiento, reconocimiento de patrones, etc.

8. Temas clave, tales como la detección de botnets y Servidores de Comando y Control de Ciber Ataques o Ciber Espionaje, utilizando Análisis de Flujo de Redes – Reconocimiento por Patrones, ya están siendo manejados con una interesante solvencia en el contexto de la Línea de Investigación “Ciber Defensa” de la Universidad Nacional de San Luis.

9. El nivel tecnológico alcanzado, adecuadamente utilizado, puede llegar a permitir la existencia de un Ciber Espacio en el cual la Libertad, la Privacidad y los Derechos Humanos en general sean respetados coexistiendo con herramientas que permitan detectar el uso delictivo de Internet y también mitigar el uso del Ciber Espacio como un nuevo “dominio” o “espacio” en el que se desarrollen los conflictos militares entre estados naciones.

10. Se continuará trabajando, en el contexto de la Línea de Investigación “Ciber Defensa” de la Universidad Nacional de San Luis, perfeccionando y ampliando los conocimientos adquiridos y habilidades desarrolladas, de manera de poder seguir suministrando sustento al Estado, en el ámbito de la Ciber Defensa y de la Ciber Seguridad, tal como ha venido ocurriendo en el último año y medio.

Referencias

- (NETmundial, 2014) http://netmundial.br/
- (Rousseff, 2013) http://www.youtube.com/watch?v=J9mV1WoPN1o
- (CELAC, 2014) http://www.youtube.com/watch?v=tz3gBMYaK_4
- (Uzal, 2014) http://content.netmundial.br/contribution/internet-roadmap-topics-freedom-and-security-in-cyberspace-a-cyber-defense-perspective/61
- (Uzal, 2012) R. Uzal “Guerra Cibernética” Visión Conjunta” Año 4, Número 1, 2012 (Armed Forces Joint War College Magazine – Argentina)
- (Geiss & Lahmann, 2013) R. Geiss, & H. Lahmann “Freedom and Security in Cyberspace”, http://www.ccdcoe.org/publications/books/PeacetimeRegime.pdf, Tallin, 2013
- (Bilge et al, 2012) L. Bilge et al “DISCLOSURE: Detecting Botnet Command and Control
- Servers Through Large-Scale Net Flow Analysis”, 2012 http://www.cs.ucsb.edu/~chris/research/doc/acsac12_disclosure.pdf

- (Brauckhoff et al, 2009) D. Brauckhoff, X. Dimitropoulos, A. Wagner, and K.Salamatian. “Anomaly extraction in backbone networks using association rules”. ACM Internet Measurement Conference (IMC'09), 2009.
- (Claise, 2004) B. Claise, “Cisco systems Net Flow services export version 9”, 2004.
- (Cook, et al 2005) E. Cooke, F. Jahanian, and D. McPherson. “The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets”. 1st Workshop on Steps to Reducing Unwanted Traffic on the Internet, pages 39- 44, 2005.
- (Cisco, 2013) http://www.cisco1900router.com/what-is-ios-model-the-overall-explanation-of-ios-7-layers.html
- (Baieli, Cunha, Uzal 2014) C. Baieli, I. Cunha, R. Uzal. Claudio Baielli MSc Thesis work (I. Cunha – UFMG & R. Uzal – UNSL are the thesis development advisors)
- (Uzal, Montejano, Riesco, 2013 / 14) On going research work at Universidad Nacional de San Luis – Argentina
- (Uzal, 2013) R. Uzal, www.cari.orghttp://argentina.afceachapters.org/wp-content/uploads/2013/07/presentacionDrUzal.pdf
- (UNSL, 2013) http://www.dirinfo.unsl.edu.ar/noticias/articulo/un-nuevo-doctorado-del-departamento-de-informatica.html
- (PMI, 2013) http://search.pmi.org/?q=pmbok+5
- (CISCO, 2014) http://www.cisco.com/en/US/products/sw/netmgtsw/ps1964/products_implementation_design_guide09186a00800d6a11.html#wp1053288
- (Ahmadi, 2013) http://www.youtube.com/watch?v=vrRj-kRofRg
- (Agüero, Macedo, Uzal, Nogueira, 2013/14) Tesis de Maestría en Ingeniería de Software co tutelada UNSL / UFMG (en elaboración).
- (CARI, 2013) http://www.cari.org.ar/pdf/crimenorganizado-uzal-2013.pdf