Planeamiento Estratégico Informático: Planeamiento Basado en Capacidades aplicado al Planeamiento Estratégico de la Ciberdefensa

Roberto Uzal, Daniel Riesco, German Montejano, and Mario Beron

Universidad Nacional de San Luis,

San Luis, Ejército de los Andes 950, Argentina

ruzal@arnet.com.ar

{driesco,gmonte,mberon}@unsl.edu.ar

http://www.unsl.edu.ar

Resumen Las agresiones entre estados naciones utilizando malware sumamente sofisticado, causando en algunos casos efectos devastadores, se ha venido verificando, con especial intensidad, desde el año 2007. Nuestra región no ha permanecido ajena a estos actos hostiles entre países. Al capítulo de la *Seguridad Informática* al que le incumben las agresiones entre estados naciones, se lo ha denominado *Ciberdefensa*. En este artículo se desarrollan algunos conceptos relacionados con la Ciberdefensa, se pone especial énfasis en el *Planeamiento Estratégico* de la Ciberdefensa, se destacan las ventajas de utilizar una adecuada instanciación de la *Metodología de Planeamiento Basado en Capacidades* para elaborar el *Plan Estratégico de Ciberdefensa* de la Argentina, se suministran algunos ejemplos de algunos de los capítulos de un Plan Es-

tratégico de Ciberdefensa que se ha venido elaborando en el ámbito de la Universidad Nacional de San Luis y se adelantan las propuestas que se efectuarán, respecto de dicho plan, a las autoridades nacionales. Un aspecto destacado de Ciberdefensa que es tratado en este artículo lo es el de la naturaleza eminentemente interdisciplinaria de la Ciberdefensa; de ninguna manera se trata de un tema eminentemente militar. También se destaca, con especial énfasis, el muy relevante rol que debe encarar la academia para que la Argentina pueda contar con un *Ciberespacio* seguro y confiable.

Keywords: Ciberdefensa; Planeamiento Estratégico de la Ciberdefensa; Planeamiento Basado en Capacidades; Seguridad Informática.

1. Introducción: La Ciberdefensa

En una primera aproximación se puede interpretar a la *Ciberdefensa* como *Seguridad Informática* pero aplicada a la Defensa Nacional. Asimismo, el *Planeamiento Estratégico de la Ciberdefensa*, sin dudas, constituye una variante singular del *Planeamiento Estratégico Informático*. La diferenciación de Ciberdefensa [6,2], respecto de *Seguridad Informática Canónica* es que, en la primera, detectado un ataque al país, claramente proveniente desde otro estado nación, mediante malware de alta sofisticación destinado a dañar la Infraestructura Crítica o Servicios Esenciales y, también detectados sin lugar a dudas los denominados *Servidores de Comando y Control* [4,12] de dicho ataque, el Poder Ejecutivo del país afectado puede, eventualmente, disponer la *neutrali-*

zación de dichos Servidores de Comando y Control emisores de la agresión (artículo 51 de la Carta de las Naciones Unidas).

Ciberdefensa comprende, en principio [9,8]: Planear, coordinar, integrar, sincronizar, conducir y eventualmente ejecutar actividades relacionadas con la protección de las redes de computadoras del Área Defensa de un país, la ejecución de operaciones cibernéticas de todo tipo relacionadas con intrusiones desde otros estados naciones destinado a dañar la Infraestructura Crítica o Servicios Esenciales, e impedir que otros estados naciones utilicen al territorio nacional como base de lanzamiento de ataques cibernéticos a terceros países.

Nada de lo expresado en el párrafo anterior es *abstracto*. Desafortunadamente, las agresiones cibernéticas entre estados naciones se han transformado en algo *cotidiano*. También desafortunadamente no se tiene que buscar *muy lejos* para encontrar ejemplos concretos.

Ciberdefensa [8] es un concepto eminentemente *asimétrico*. En otras palabras, Ciberdefensa no es un “lujo” que incumbe sólo a los países más poderosos. Paradójicamente, los estados naciones cuyas Fuerzas Armadas más han avanzado en la adopción de sistemas de Comando y Control integrados del tipo C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance), son los que más deben esforzarse en cubrir sus *flancos débiles* o *vulnerabilidades*. Estas características son derivadas del uso intensivo de redes teleinformáticas complejas, las cuales están implementadas sin tener en cuenta de que el ciberespacio se transformaría en un nuevo ámbito de los conflictos entre estados naciones.

Este nuevo escenario de conflictos hace que países medianamente desarrollados, que adquieran las correspondientes capacidades de Ciberdefensa, podrán lograr un importante re-posicionamiento favorable, en cuanto a defensa se refiere, en el contexto global. En Ciberdefensa lo cualitativo prevalece respecto de lo cuantitativo.

Contar con capacidades en el ámbito de la Ciberdefensa es mandatorio para todo país. El peor de las escenarios que se le puede presentar a un estado nación genérico es recibir Ciber ataques y, por incapacidad Tecnológica y/o de Gestión, terminar adjudicando la devastación ocasionada por dichos Ciber ataques a accidentes impredecibles. Esta aseveración no es *abstracta*. Hechos de este tipo han ocurrido y tampoco se tiene que ir muy lejos para encontrar ejemplos concretos [15].

Es importante distinguir claramente entre Guerra Cibernética y Guerra Electrónica [15]. Los países que cometieron el error de confundirlas se han posicionado con desventajas competitivas. Confundir al *espectro radioeléctrico* (*campo de batalla* de la Guerra Electrónica) con el *Ciberespacio* (*dominio* de las agresiones cibernéticas) es un error inadmisible. La *Guerra Electrónica* se corresponde con los ámbitos *tradicionales* de los conflictos entre países: Tierra, Mar y Aire. La *Guerra Cibernética* se desarrolla en un nuevo ámbito de las hostilidades entre estados naciones: El Ciberespacio.

Ciberdefensa no implica previsiones para el futuro; el mundo está ya inmerso en ella. Sólo a modo de ejemplo se citan [17,15]:

- La masiva y devastadora agresión cibernética de Rusia a aeropuertos, sistemas ferroviarios, hospitales, sistema financiero y medios periodísticos de Estonia en el 2007. El ataque provocó la reacción de Alemania en ayuda de Estonia y luego la intervención de la NATO (Organización de Naciones del Atlántico Norte). A partir de este conflicto la NATO replantea lo que hasta entonces constituía su política y estructura de *Guerra Electrónica*. Conviene destacar que miembros europeos de la Alianza del Norte excluyen parcialmente de este esquema a los EEUU. Esto se debe a que comprobaron los gobiernos de Francia y Alemania que miembros de las agencias de inteligencia estadounidenses trabajaban junto a los desarrollistas de los productos Microsoft. Dicho productos serían vendidos en Francia y Alemania y que algunas de dichas agencias disponía del *código fuente* de versiones de productos de esa marca adquiridos por los gobiernos de esos países.

- La alteración, mediante Armas Cibernéticas, del software de un Sistema de Radar de origen Ruso en el Norte de Siria, a orillas del Éufrates, en 2007. Esta alteración impidió detectar a cazas bombarderos de Israel que atacaron y destruyeron construcciones realizadas, aparentemente, por norcoreanos.

- La intrusión de China en sistemas satelitales de Estados Unidos El prácticamente confirmado acceso, también por parte de China, a información del área Defensa altamente sensitiva, residente en la Intranet del Jet Propulsion Laboratory (California Institute of Technology – NASA).

- La intrusión de China en la “grilla” de producción y distribución de electricidad de EEUU.
- El prácticamente confirmado acceso, también por parte de China, a información del área Defensa altamente sensitiva, residente en la Intranet del Jet Propulsion Laboratory (California Institute of Technology – NASA)
- La voladura, utilizando “virus de red” o “gusanos”, de las baterías centrífugas en la planta de enriquecimiento de uranio en Natanz, Irán.
- La presencia de las más sofisticada Arma Cibernética, *Flame*, en las plataformas de explotación petrolera de Irán.
- La Guerra Cibernética de carácter *sine die* entre Pakistán e India. Así como, en la guerra con Irak, se reclutaron a marginales expulsados de las fuerzas especiales de diversos países (*contractors*) para operaciones *sucias*, tanto la India como Pakistán están recurriendo a hackers privados llevándolos a una suerte de categoría de *Cyber Contractors*.
- La fuerte presunción, por parte del Gobierno de Brasil, de que el *gran apagón* del año 2009 no se trató casualmente de un accidente. Esta fuerte presunción llevó a la decisión de la creación de la primera unidad de Ciberdefensa de Brasil (CDCIBER-Centro de Defensa Cibernética).

Es importante distinguir entre Ciberdefensa (agresiones entre países) de Ciberseguridad (a la que le incumben el Ciber crimen, el Ciber terrorismo, el Activismo Hacker y el Ciberespionaje).

También es importante saber que todos los conceptos mencionados deben ser tratado con un enfoque sistémico, tal como se muestra en la figura 1.

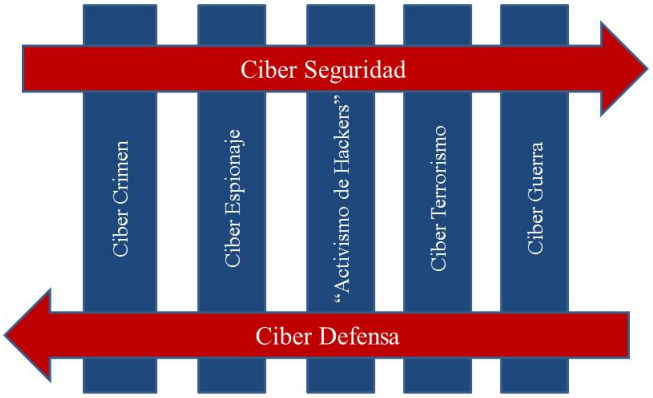

Figura 1. Enfoque Sistémico

Este artículo, orientado específicamente al Planeamiento Estratégico de la Ciberdefensa, describe esquemáticamente al enfoque metodológico Planificación Basado en Capacidades, reporta la aplicación de la Planificación Basada en Capacidades al Planeamiento Estratégico de la Ciberdefensa a nivel estado nación, extrae conclusiones y suministra referencia abundantes para quienes deseen profundizar en los temas tratados y también en los mencionados.

2. Planificación Basada en Capacidades

Planear en condiciones de *indeterminación* y de *incertidumbre* se ha transformado casi en un estándar para organizaciones de distinto tipo. El Planeamiento Estratégico Informático y el Planeamiento de la Seguridad Informática,

a nivel estratégico, se ha constituido en ejemplos de lo aseverado. El contexto cambiante, turbulento e impredecible constituye un gran desafío para el ejercicio del liderazgo en general y para quien lidere el Planeameinto Estratégico Informático en particular. Un lego en planeamiento podría expresar: *Si el contexto es cambiante, turbulento, impredecible y casi imposible de ser caracterizado, no resulta posible planear*. En contraposición, lo que expresaría una persona informada sería: *El contexto cambiante, turbulento e impredecible constituye un apasionante desafío para quien planea. Confundir planeamiento con pronóstico constituye un despropósito insalvable*.

El denominado Planeamiento basado en Capacidades [3,11,7] (*Capabilities-based planning*) es una de las opciones metodológicas más adecuadas para encarar el planeamiento en un contexto de Indeterminación y de Incertidumbre. El desafío consiste en adquirir, desarrollar, fortalecer y ampliar Capacidades que fácilmente puedan ser instanciadas a casos específicos de un muy amplio espectro de amenazas y escenarios peligrosos. El Planeamiento basado en Capacidades facilita acotar las previsiones incluidas en el plan a las restricciones de la viabilidad económico, es decir financiara mediante la priorización de necesidades.

La figura 2 constituye una extrema y simplificada síntesis de la estructura del Planeamiento basado en Capacidades

Si bien el esquema anterior es muy claro y representativo, puede llegar a dejar la impresión de que el Planeamiento Basado en Capacidades responde a un esquema lineal-secuencial. De ninguna manera es así, se trata, como toda

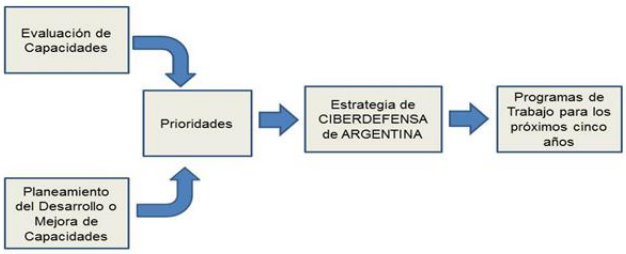

Figura 2. Visión Simplificada del Planeamiento Basado en Capacidades

metodología de planeamiento moderna, de un esquema iterativo (aproximaciones sucesivas al *mejor* plan) e interactivo (necesidad de recibir la correspondiente *realimentación* del entorno afectado por el plan). Una visión alternativa de esta metodología es la que se muestra en la figura 3.

El Planeamiento Basado en Capacidades presenta un esquema flexible, debe instanciarse a cada caso. No se lo debe interpretar como una suerte de *Cook Book* que permite elaborar Planes Estratégicos exitosos a: i) desconocedores de la esencia de Planeamiento Estratégico, o ii) personas sin la adecuada experiencia Gerencial y en Planeamiento, o iii)personas sin conocimientos del *espacio del problema*, en este caso la Seguridad Informática ante un nuevo paradigma de la misma y a nivel estratégico. Planeamiento Basado en Capacidades ha mostrado ser especialmente apto para ser utilizado en el ámbito de la Ciberdefensa.

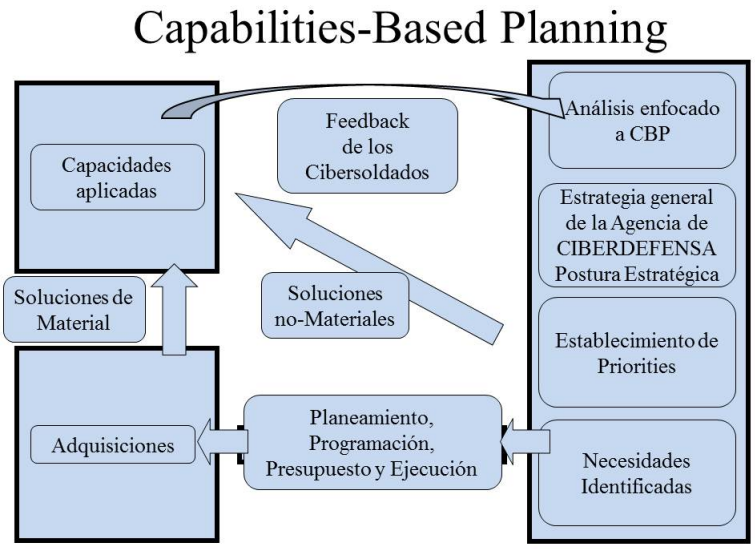

Figura 3. Visión Simplificada del Planeamiento Basado en Capacidades

En el caso abordado en este artículo, los componentes del ciclo del Planeamiento Estratégico de Ciberdefensa, *instanciando* adecuadamente al Planeamiento Basado en Capacidades, podrían ser, en principio, las siguientes:

- Evaluación de Capacidades o Análisis enfocado a la Planificación Basada en Capacidades.
- Planeamiento de la adquisición, desarrollo, fortalecimiento y ampliación de Capacidades (Estrategia *general* de Ciberdefensa).
- Determinación de las Prioridades.
- Definición de soluciones *no materiales* (selección de los Recursos Humanos, formación de los Recursos Humanos, incorporación paulatina de Recursos Humanos formados y capacitados a la Agencia de Ciberdefensa), defensa.

- Necesidades identificadas.
- Planeamiento propiamente dicho:
  - Elaboración del plan propiamente dicho:
    - Visión.
    - Misión.
    - Políticas.
    - Objetivos.
    - Metas.
  - Elaboración de los Programas de Trabajo:
    - Asignar un cronograma a las Metas debidamente desagregadas.
    - Identificar las Tareas correspondientes al logro de cada Meta debidamente desagregada.
    - Identificar las *precondiciones* para el inicio de cada Tarea (Tareas correlativas anteriores de cada Tarea).
    - Identificar el *Camino Crítico* asociado a los Programas de Trabajo.
  - Elaboración del Presupuesto:
    - Asignar, en función del tiempo, valores económicos a cada Meta debidamente desagregada.
    - Elaborar el presupuesto financiero.
  - Ejecución:
    - Ejecución de las Tareas correspondientes al Programa de Trabajo.
    - Ejecución presupuestaria según lo establecido en el presupuesto financiero.

- Especificación de las Adquisiciones.
- Evaluación de la aplicación de las Capacidades:
  - Definición de Indicadores Clave.
  - Monitoreo de los Indicadores Clave.
  - Realimentación (optimización o replanteo de las Capacidades a ser generadas u optimizados).

En el siguiente punto se suministrarán algunos ejemplos de sólo algunos de los componentes listados. Estos ejemplos se refieren a una aplicación concreta de la Planificación Basada en Capacidades. Razones de límites de extensión de este artículo impiden un desarrollo completo.

3. La Aplicación de la Planificación Basada en Capacidades al Planeamiento Estratégico de la Ciberdefensa a nivel Estado Nación

En este punto, como se anticipó en la sección previa, se suministrarán algunos ejemplos de los componentes del ciclo del Planeamiento Estratégico de Ciberdefensa, *instanciando* adecuadamente al Planeamiento Basado en Capacidades al caso de nuestro país:

- Ejemplos de la evaluación de Capacidades o Análisis enfocado en el Planeamiento Basado en Capacidades.
  - Consiste, en este caso, en:

- El establecimiento de una *Línea de Base* definida por la evaluación de las amenazas conocidas, y
- Las vulnerabilidades detectadas *contra* las capacidades a ser adquiridas, desarrolladas, fortalecidas y ampliadas. La evolución de capacidades respecto de las posibilidades de enfrentar amenazas y mitigar/anular vulnerabilidades constituye el indicador (en realidad conjunto de indicadores) esenciales para evaluar la ejecución de lo planeado. Se muestra como ejemplo *sólo una parte* de la tabla con la correspondencia entre Vulnerabilidades detectadas en nuestro país y las Capacidades que permitirían superarlas o mitigarlas.

Número	Vulnerabilidad	Capacidad a ser Generada
1	Ante un evento devastador del tipo estallido de un oleoducto, incendio en una refinería,etc. , no contar ni con el personal calificado ni con las herramientas para poder determinar si se está frente a un accidente o un Ciber ataque proveniente de FFAAs de otros estados naciones (hasta hoy sólo los estados naciones pueden desarrollar malware sumamente sofisticado y de alta complejidad que no es detectado ni por el software de base hoy disponible comercialmente ni por los productos *anti – malware* disponible comercialmente)	Capacidad de detección de Ciber armas, es decir de malware sumamente sofisticado que no es detectado ni por el software de base hoy disponible comercialmente ni por los productos anti – malware disponible comercialmente. Esta capacidad incluye la capacidad de identificación y de aislamiento de Ciber armas. Nota: No le incumben a la Agencia de Ciberdefensa los *ladrones de gallinas* del Ciberespacio (robo de identidad en tarjetas de crédito, etc.)

Número	Vulnerabilidad	Capacidad a ser Generada
2	No contar ni con el personal calificado ni con las herramientas para la detección temprana de malware sumamente sofisticado que no es detectado ni por el software de base hoy disponible comercialmente ni por los productos anti – malware disponibles comercialmente.	Capacidad de detección temprana de Ciber armas, es decir de malware sumamente sofisticado que no es detectado ni por el software de base hoy disponible comercialmente ni por los productos anti – malware disponible comercialmente. Esta capacidad incluye la capacidad de identificación y de aislamiento de Ciber armas.
3	No contar ni con el personal calificado ni con las herramientas para asistir en la recuperación de un sistema (fábrica, hospital, aeropuerto,etc.) objeto de un Ciber ataque.	Capacidad para la *integración dinámica* de grupos de tipo CERT (Computer Emergency Response Teams).
4	No contar ni con el personal calificado ni con las herramientas para realizar las tareas “forenses” que permitan presentar pruebas admisibles, de haber recibido un Ciber ataque. Ante organismos o foros internacionales.	Capacidad para que, ante Ciber ataques, queden conformadas pruebas que sean admisibles por organismos internacionales (ejemplo: Consejo de Seguridad de las Naciones Unidas).
5	No contar ni con el personal calificado ni con las herramientas para identificar a *las fuentes* de un ataque cibernético diferenciando los computadores *zombies* de los verdaderos Servidores de Comando y Control.	Capacidad de Análisis de Flujo de Redes, es decir poder identificar a “las fuentes” de un ataque cibernético diferenciando los computadores zombies de los verdaderos Servidores de Comando y Control.
6	No contar ni con el personal calificado ni con las herramientas para poder llegar a obtener el *código fuente* del malware a partir del *código ejecutable* identificado y aislado.	Capacidad de Ingeniería Reversa de Ciber armas es decir, a partir de la identificación y de aislamiento de Ciber armas, poder llegar a obtener el código fuente del malware a partir del código ejecutable identificado y aislado.
7	No contar ni con el personal calificado ni con las herramientas para, a partir de contenidos de una Bases de Datos / Bases de Conocimiento de la Agencia de Ciberdefensa, utilizando técnicas del tipo *Reconocimiento mediante Patrones* aportar a la identificación de los desarrollistas de la Ciber armas.	Capacidad de Análisis de Ciber armas a partir de contenidos de Bases de Datos / Bases de Conocimiento de la Agencia de Ciberdefensa utilizando técnicas del tipo *Reconocimiento mediante Patrones* (aportar a la identificación de los desarrollistas de la Ciber armas).

Número	Vulnerabilidad	Capacidad a ser Generada
8	Carecer de todos los elementos correspondientes a la Defensa Cibernética Indirecta.	Capacidad de respuesta ante agresiones Cibernéticas desde otros estados naciones cuando así lo disponga la Presidencia de la Nación y capacidad, también cuando así lo disponga la Presidencia de la Nación, de neutralización preventiva de Servidores de Comando y Control de potenciales atacantes.
9	Carencia de posibilidad de desarrollo de *Software para la Respuesta preventiva* a agresores cibernéticos perfectamente identificados o para la *neutralización preventiva* de dichos agresores.	Capacidad de desarrollo de Software para la Respuesta a agresores cibernéticos perfectamente identificados (¡estar atentos a la trampa tendida por los países que más han avanzado en armamento cibernético!: *evitar la proliferación de armas cibernéticas* - limitar la capacidad de respuesta ante agresiones - Argentina no puede renunciar a tener *capacidad de disuasión cibernética*).
10	Carencia de personal calificado y de herramientas que hagan viable el lograr evitar que, el territorio argentino, sea utilizado por otros países, para lanzar Ciber ataques a terceros estados naciones.	Capacidad de evitar el uso del territorio argentino, por parte de otros países, para lanzar Ciber ataques a terceros estados naciones.

- Planeamiento de la adquisición, desarrollo, fortalecimiento y ampliación de Capacidades:
  - Ejemplos de Capacidades a ser adquiridas, identificadas a partir de la tabla anterior, debidamente desagregadas:

- Capacidad de detección de Ciber armas, es decir de malware sumamente sofisticado que no es detectado ni por el software de base hoy disponible comercialmente ni por los productos anti – malware disponible comercialmente. Esta capacidad incluye la capacidad de identificación y de aislamiento de Ciber armas[1]:
  - Capacidad de identificación de las *arquitecturas tipo* de Ciber armas,
  - Capacidad de simulación de Ciber ataques en distintos escenarios de manera de mantener al equipo en entrenamiento permanente,
  - Capacidad para generar esquemas asociativos para acceder a ambientes de simulación de Ciber ataques que actualmente estén utilizando países amigos,
  - Capacidad para desarrollar ambientes de simulación de Ciber ataques de alto nivel de sofisticación,
  - Capacidad para la *integración dinámica* de grupos de tipo CERT (Computer Emergency Response Teams),
  - Capacidad de desarrollo propio de herramientas de software para asistir en la detección de Ciber ataques de alto nivel de sofisticación,
  - Capacidad de *confinamiento* de una Ciber arma detectada,

[1] No le incumben a la Ciberdefensa los ladrones de gallinas del Ciberespacio (robo de identidad en tarjetas de crédito, etc.)

- ◇ Capacidad para asistir en la recuperación de los *blancos* de Ciber ataques, y
- ◇ Capacidad para realizar los puntos anteriores de manera que queden conformadas pruebas que sean admisibles por organismos internacionales (ejemplo: Consejo de Seguridad de las Naciones Unidas).

- Capacidad de Análisis de Flujo de Redes [10,5,1], es decir poder identificar a "las fuentes" de un ataque cibernético diferenciando los computadores "zombies" de los verdaderos Servidores de Comando y Control:
  - ◦ Capacidad de detección y caracterización de problemas en las redes de computadoras y suministrar elementos de juicio para su análisis.
  - ◦ Capacidad para contar con informes periódicos / monitoreo *en tiempo real* del tráfico en redes de computadoras.
  - ◦ Capacidad para el *reconocimiento de patrones* en el tráfico en redes de computadoras.
  - ◦ Capacidad para la detección temprana de intrusiones.
  - ◦ Capacidad para optimizar redes de computadoras (topología, etc.) para minimizar la probabilidad de intrusiones a través de las mismas.
  - ◦ Capacidad de detección de *botnet* y Servidores de Comando y Control de Ciber ataques a través análisis de flujos de redes en gran escala.

- Capacidad de Ingeniería Reversa de Ciber armas [13,18,21,20,19] es decir, a partir de la identificación y de aislamiento de Ciber armas, poder llegar a obtener el código fuente del malware a partir del código ejecutable identificado y aislado.
- Capacidad de *inspección* del código ejecutable en estudio.
- Capacidad de desarrollo de herramientas de *inspección*.
- Capacidad de construir *perspectivas* [2] del código ejecutable en estudio.
- Capacidad para construir *vistas* del código ejecutable en estudio.
- Capacidad para desarrollar herramientas que posibiliten la *visualización dinámica* del código ejecutable en estudio.
- Capacidad para lograr la comprensión plena de la lógica de funcionamiento del código ejecutable en estudio.
- Capacidad para definir y para ejecutar distintas estrategias de Ingeniería Reversa.
- Capacidad para no sólo llegar al código fuente del código ejecutable en estudio sino para exponer en forma gráfica y dinámica el funcionamiento integral de la Ciber arma estudiada.
- Capacidad para realizar los puntos anteriores de manera que queden conformadas pruebas que sean admisibles por organismos internacionales (ejemplo: Consejo de Seguridad de las Naciones Unidas).

[2] Perspectiva: criterios de agrupamiento de características o atributos

- Capacidad de Análisis de Ciber armas a partir de contenidos de Bases de Datos/Bases de Conocimiento de una futura Agencia de Ciberdefensa utilizando técnicas del tipo Reconocimiento mediante Patrones [16,14] (aportar a la identificación de los desarrollistas de la Ciber arma):
  - Capacidad de detección y caracterización de problemas en las redes de computadoras y suministrar elementos de juicio para su análisis.
  - Capacidad para contar con informes periódicos/monitoreo en tiempo real del tráfico en redes de computadoras.
  - Capacidad para el reconocimiento de patrones en el tráfico en redes de computadoras.
  - Capacidad para la detección temprana de intrusiones.
  - Capacidad para optimizar redes de computadoras (topología, etc.) para minimizar la probabilidad de intrusiones a través de las mismas.
  - Capacidad de detección de “botnet” y Servidores de Comando y Control de Ciber ataques a través análisis de flujos de redes en gran escala.
  - Capacidad de Ingeniería Reversa de Ciber armas [22,13,18,21,20,19] es decir, a partir de la identificación y de aislamiento de Ciber armas, poder llegar a obtener el código fuente del malware a partir del código ejecutable identificado y aislado.

- Capacidad de *inspección* del código ejecutable en estudio.
- Capacidad de desarrollo de herramientas de inspección.
- Capacidad de construir *perspectivas* del código ejecutable en estudio.
- Capacidad para construir *vistas* del código ejecutable en estudio.
- Capacidad para desarrollar herramientas que posibiliten la *visualización dinámica* del código ejecutable en estudio.
- Capacidad para lograr la comprensión plena de la lógica de funcionamiento del código ejecutable en estudio.
- Capacidad para definir y para ejecutar distintas estrategias de Ingeniería Reversa.
- Capacidad para no sólo llegar al código fuente del código ejecutable en estudio sino para exponer en forma gráfica y dinámica el funcionamiento integral de la Ciber arma estudiada.
- Capacidad para realizar los puntos anteriores de manera que queden conformadas pruebas que sean admisibles por organismos internacionales (ejemplo: Consejo de Seguridad de las Naciones Unidas).

- Como se expresó con anterioridad, mediante un esquema lógico formal consistente, suministrado por la Planificación Basada en Capacidades, se llega a la Visión, Misión, Políticas y Objetivos y Metas contenidas en un Plan Estratégico de Ciberdefensa. De ese conjunto, por estimarse que son los que más interés despiertan, se exponen, de los aspectos

mencionados, sólo algunos de los objetivos (que en la realidad suman 74):

- Adquirir los conceptos, desarrollar las habilidades y construir las herramientas para lograr la identificación de las *arquitecturas tipo* de Ciber armas (primer *alerta* de la detección).
- Acceder en lo inmediato a ambientes de simulación de Ciber ataques que actualmente estén utilizando países amigos.
- Lograr la integración dinámica de los especialistas en detección de malware de alto nivel de sofisticación a grupos de tipo CERT (Computer Emergency Response Teams).
- Desarrollar, con know how propio, herramientas de software para asistir en la detección temprana de Ciber ataques de alto nivel de sofisticación (completar lo iniciado con la construcción de las herramientas para lograr las identificación de las *arquitecturas tipo* de Ciber armas.
- Adquirir las capacidades para lograr que, ante un Ciber ataque, queden conformadas pruebas, derivadas del malware localizado y analizado, que sean admisibles por organismos internacionales (ejemplo: Consejo de Seguridad de las Naciones Unidas).
- Desarrollar las herramientas y las habilidades de detección y caracterización de problemas en las redes de computadoras y suministrar elementos de juicio para su análisis (Análisis de Flujo).

- Obtener las habilidades y las herramientas de detección de botnet y Servidores de Comando y Control de Ciber ataques a través Análisis de Flujos de Redes en gran escala.
- Lograr las habilidades para la “integración dinámica” de grupos de tipo CERT (ComputerEmergency Response Teams) aportando en el ámbito de Análisis de Flujos de Redes.
- Adquirir las habilidades para lograr que queden conformadas pruebas, mediante el Análisis de Flujo de Redes, que sean admisibles por organismos internacionales (ejemplo: Consejo de Seguridad de las Naciones Unidas).
- Obtener las habilidades y las herramientas para la inspección del código ejecutable en estudio (primera fase de la Ingeniería Reversa).
- Obtener las habilidades y las herramientas para definir y para ejecutar distintas estrategias de Ingeniería Reversa.
- Obtener las habilidades y las herramientas para no sólo llegar al código fuente del código ejecutable en estudio sino para exponer en forma gráfica y dinámica el funcionamiento integral de la Ciber arma estudiada.
- Obtener las habilidades y las herramientas para que, a través de la Ingeniería Reversa del malware, queden conformadas pruebas que sean admisibles por organismos internacionales (ejemplo: Consejo de Seguridad de las Naciones Unidas).

- Desarrollar las habilidades de diseño e implantación de Bases de Datos/Bases de Conocimiento específicas de la Agencia de Ciberdefensa.
- Obtener las habilidades y las herramientas para que queden conformadas pruebas, obtenidas mediante un enfoque del tipo reconocimiento de patrones que sean admisibles por organismos internacionales (ejemplo: Consejo de Seguridad de las Naciones Unidas).
- Obtener las habilidades y las herramientas para el desarrollo de *Software para la Respuesta* a agresores cibernéticos perfectamente identificados (¡estar atentos a la trampa tendida por los países que más han avanzado en armamento cibernético!, evitar la proliferación de armas cibernéticas - limitar la capacidad de respuesta ante agresiones - Argentina no puede renunciar a tener capacidad de ejercer lo previsto en el Artículo 51 de la Carta de las Naciones Unidas - Legítima Defensa).
- Asegurar un efectivo control de la Presidencia de la Nación respecto del mencionado de *software para la respuesta* a agresores cibernéticos sobre todo para evitar su transferencia al *mercado negro cibernético*; error cometido, por ejemplo, por los Estados Unidos.
- Definir las *reglas de empeñamiento* de manera que sea sólo de la Presidencia de la Nación la atribución de utilización de *software para la respuesta* a agresores cibernéticos (otros estados naciones),

- Evitar el uso del territorio argentino, por parte de otros países, para lanzar Ciber ataques a terceros estados naciones.

- A partir de los Objetivos, para elaborar el documento de Planeamiento Estratégico de la Ciberdefensa completo, se desarrollaron los siguientes puntos:
  - Elaboración de los Programas de Trabajo (cronograma de ejecución):
    - Asignación de un cronograma a las Metas, derivadas de los Objetivos, a su vez debidamente desagregadas.
    - Identificación de las Tareas correspondientes al logro de cada Meta debidamente desagregada.
    - Identificación de las *precondiciones* para el inicio de cada Tarea (Tareas correlativas anteriores de cada Tarea).
    - Identificación del *Camino Crítico* asociado a los Programas de Trabajo.
  - Elaboración del Presupuesto:
    - Asignación, en función del tiempo, valores económicos a cada Meta debidamente desagregada.
    - Elaboración del presupuesto financiero.
  - Previsiones para la Ejecución:
    - Ejecución de las Tares correspondientes al Programa de Trabajo.

- ◇ Ejecución presupuestaria según lo establecido en el presupuesto financiero.
- ◇ Especificación de las Adquisiciones.
- ◇ Evaluación de la aplicación de las Capacidades.

- Uso de los Indicadores Clave:
  - ○ Monitoreo de los Indicadores Clave.
  - ○ Realimentación (optimización o replanteo de las Capacidades a ser generadas u optimizados).

Se insiste en que sólo se han presentado partes de sólo algunos puntos del Planeamiento Estratégico de Ciberdefensa para dar ejemplos concretos.

4. Conclusiones

La Ciberdefensa es un requerimiento mandatorio para los estados naciones. Poseer métodos, técnicas y herramientas que posibiliten la detección y prevención de ataques ciberneticos proporcionan una mayor seguridad para los habitantes de los estados naciones. Claramente, implementar mecanismos de ciberdefensa no es una tarea sencilla, implica un estudio profundo tanto de los conocimientos técnicos como así también de la realidad en la que el estado nación se encuentra. Demás está pensar en utilizar el mejor método de ciberdefensa cuando la coyuntura actual del estado nación no da las garantías necesarias para su correcta aplicación. De igual manera, la utilización de planes de ciberdefensa austeros, en estados naciones solventes, puede dejar a los mismos indefensos ante ataques sofisticados. La afirmación mencionada

previamente, permite percibir la importancia de la correcta conceptualización e interpretación de los conceptos involucrados en ciber defensa y de la elaboración de un plan estrategico acorde con la situación del estado nación.

La temática mencionada previamente ha sido abordada en este artículo de una manera concienzuda y profunda a nivel conceptual, de manera tal de evitar falacias que en el futuro puede a llevar situaciones catastróficas. Luego de realizada la tarea antes mencionada y de haber comprobado la importancia de la ciberdefensa para la República Argentina se elaboró un plan estratégico informático. Este plan tiene como finalidad establecer los requerimientos necesarios y proponer soluciones que permitan cubrir dichos requerimientos tomando en consideración la situación actual de Argentina.

Luego de haber llevado a cabo las tareas previamente mencionadas se puede concluir que:

- Constituye un error conceptual profundo el sólo pensar que la Ciberdefensa es un problema de exclusiva incumbencia militar. Diversos sectores de la sociedad deben aportar. A la academia le cabe un rol fundamental, en este sentido la Universidad Nacional de San Luis viene aportando a la Ciberdefensa desde hace años.
- En dicho rol esencial de la academia están incluidos, entre otros, los siguientes aspectos: i) Formación de Recursos Humanos aptos para actuar en los diversos aspectos relacionados con la Ciberdefensa. El personal militar asignado a temas de ciberdefensa deberá tener formación universitaria de cuarto nivel (mínimo Maestría) con una tesis desarrollada en el mismo

ámbito que se le asigne en Ciberdefensa, ii) Generar conocimiento, en forma permanente en el ámbito de las capacidades de detección de malware cuyo nivel de sofisticación evoluciona permanentemente, iii) General conocimiento, en forma permanente, en el ámbito de la Ingeniería Reversa de malware sofisticado y construido con un enfoque de programación multi paradigma. La Universidad Nacional de San Luis ha trabajado en este ámbito hasta el nivel de tesis doctorales, iv) Generar conocimiento en lo que hace al Análisis de Flujo de Redes, y v) Formar Recursos humanos aptos para Gestionar las actividades de Ciberdefensa.

- Argentina tiene ante sí oportunidades concretas para contar con un Ciberespacio seguro y confiable sin depender para ello de un "Gran Hermano". Este tipo de esquema, si se adopta, constituiría un gravísimo error estratégico del Gobierno Nacional.
- El documento completo de Planeamiento Estratégico de Ciberdefensa debe ser re elaborado a partir de discusiones con: i) el Ministerio de Defensa (en parte ya desarrolladas), ii) con el Grupo Especial de Temas Tecnológicos de Cancillería (con el que la UNSL está en contacto) y iii) con la Oficina Nacional de Tecnología Informática (ONTI) con cuya Dirección Nacional también está en contacto la UNSL.
- La Argentina, según numerosos estudios comparativos realizados por los autores, no sólo puede y debe ser autosuficiente para protegerse de Ciber ataques provenientes desde otros estados naciones (tema no abstracto), sino que podría llegar a cooperar con países vecinos.

- Argentina posee tanto ventajas comparativas como así también ventajas competitivas en el ámbito de la Ciberdefensa que no deferían ser desaprovechadas.

Referencias

1. $http://cnets.indiana.edu/groups/nan/flowanalysis.$
2. $http://csis.org/files/publication/Twenty-Critical-Controls-for-Effective-Cyber-Defense-CAG.pdf.$
3. $http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap32.html.$
4. $http://security.radware.com/knowledge-center/DDoSPedia/command-and-control-server/.$
5. $http://tools.netsa.cert.org/silk/.$
6. $http://www.cnas.org/files/documents/publications/CNAS-ActiveCyberDefense-Lachow-0.pdf.$
7. $http://www.defensa.gob.es/Galerias/ooee/emad/fichero/EMD-planeamiento.pdf.$
8. $http://www.egov.ufsc.br/portal/conteudo/la-guerra-cibernetica-en-las-fuerzas-armadas-un-desafio-global.$
9. $http://www.gwu.edu/nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-038.pdf.$
10. $http://www.nas.nasa.gov/assets/pdf/papers/boscia_n_flow_analysis_tools-2012.pdf.$
11. $http://www.rand.org/topics/capabilities-based-planning.html.$
12. $http://www.sba-research.org/wp-content/uploads/publications/acsac12-disclosure.pdf.$

13. R. Berón M. y Henriques P. y Varanda M. y Uzal. Inspección de código para relacionar los dominios del problema y programa para la comprensión de programas. *X Workshop de Investigadores en Ciencias de la Computación. WICC 2008.*, 1:549–553, 2008. Estado: Publicado. Editorial: Universidad Nacional de la Pampa. ISBN: 978-950-863-101-5. Ciudad: General Pico. País: Argentina. Idioma: Castellano. Año: 2008. Edición: 10. Soporte: CD-ROM. Página Web: http://mdk.ing.unlpam.edu.ar/wicc2008/index.php. Área de Conocimiento: Ingeniería de Software y Base de Datos.
14. Christopher M. Bishop. *Pattern Recognition and Machine Learning (Information Science and Statistics)*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006.
15. R. Clarke. Cyber war. 2012.
16. W. Gibson. *Pattern recognition*. Berkley Books. Berkley Publishing Group, 2005.
17. R. Uzal. El desafío más relevante de la defensa. In *Visión Conjunta*.
18. Berón M. y Cruz D. y Pereira M. y Henriques P. y Uzal R. Evaluation criteria of software visualization system used for program comprehension. *3a Conferencia Nacional em Interacção Pessoa-Máquina*, 3:81–86, 2008. Estado: Publicado. Editorial: Universidade de Évora. ISBN: 972-9464-9-9. Ciudad: Évora. País: Portugal. Idioma: Inglés. Año: 2008. Edición: 3. Soporte: Página Web y CD-ROM. Página Web: http://bibliotecadigital.ipb.pt/dspace. Área de Conocimiento: Ingeniería de Software.
19. Berón M. y Henriques P. y Varanda M. y Uzal R. Program inspection to inter-connect the operational and behavioral views for program comprehension. *First Doctoral Symposium on Computing.*, 1:65–72, 2007. Estado: Publicado. Editorial: University of York. ISBN: -. Ciudad: York. País: United Kingdom. Idioma: Inglés. Año: 2007. Edición: 1. Soporte: Papel. Página Web: http://www.cs.york.ac.uk. Área de Conocimiento: Ingeniería de Software.

20. Berón M. y Henriques P. y Varanda M. y Uzal R. Técnicas de inspecção de programas para inter-relacionar as vistas comportamental e operacional. *Simpósio Doutoral em Inteligência Artificial*., 1:87–96, 2007. Estado: Publicado. Editorial: Universidade do Minho. ISBN: 978-989-95618-1-6. Ciudad: Guimaraes. País: Portugal. Idioma: Portugués. Año: 2007. Edición: 1. Soporte: Papel. Página Web: http://www.epia2007.appia.pt/sdia. Área de Conocimiento: Inteligencia Artificial. Robótica.
21. Berón M. y Henriques P. y Varanda Pereira M. y Uzal R. Simplificando la comprensión de programas a través de la interconexión de dominios. *XIV Congreso Argentino de Ciencias de la Computación. CACIC 2008*., 1, 2008. Estado: Publicado. Editorial: Universidad Nacional de la Rioja. ISBN: 978-987-24611-0-2. Ciudad: Chilecito. País: Argentina. Idioma: Castellano. Año: 2008. Edición: 14. Soporte: CD-ROM. Página Web: http://cacic2008.undec.edu.ar. Área de Conocimiento: Ingeniería de Software y Base de Datos.
22. Berón M. y Henriques P. y Varanda Pereira M. y Uzal R. Comprensión de programas. *XI Workshop de Investigadores en Ciencias de la Computación*., 1, 2009. Estado: Publicado. Editorial: Universidad Nacional de San Juan. ISBN: 978-950-605-570-7. Ciudad: San Juan. País: Argentina. Idioma: Castellano. Año: 2009. Edición: 11. Soporte: CD-ROM. Página Web: http://www.wicc2009.com.ar Área de Conocimiento: Ingeniería de Software y Base de Datos.