ESPECIALIZACIÓN EN ESTRATEGIA OPERACIONAL Y PLANEAMIENTO MILITAR CONJUNTO

TRABAJO FINAL INTEGRADOR

TEMA:

Ciberdefensa

TÍTULO:

La resiliencia aplicada al nivel operacional en el ambiente cibernético. Caso de estudio: Tallinn (Estonia) y su evolución hacia la ciber-resiliencia (2007/2017)

AUTOR: My Mariano Oscar Gómez.

PROFESOR: Miguel Gratacos.

Año 2017

RESUMEN

Producto del análisis realizado sobre la problemática que dicta el estado del arte respecto a las operaciones en el ambiente cibernético, es posible apreciar que las amenazas que se pueden presentar en el campo de batalla moderno se extienden en la actualidad efectivamente más allá del marco tridimensional de la campaña, sumándose una cuarta dimensión (ciberespacio) que merece ser atendida.

Resulta entonces imperioso que las operaciones en el ciberespacio sean planificadas en todos los niveles, siendo particularmente necesario dicho planeamiento en el nivel operacional para que el resguardo de los sistemas propios contra las amenazas cibernéticas sea concebido desde el máximo nivel del Teatro de Operaciones.

Dicho resguardo se logra mediante la articulación de fines, modos y medios para lograr un sistema ciber-resiliente, el cual, sumado a la necesaria cooperación regional e internacional, hará posible que, bajo la premisa de que no existe sistema informático invulnerable, sea posible reaccionar con la mayor celeridad posible, mitigando el accionar cibernético enemigo, y restableciendo los sistemas y servicios afectados a su estado inicial.

Es por ello que con el presente estudio se pretende identificar la importancia que reviste la inclusión de herramientas de análisis en el planeamiento de nivel operacional para el tratamiento de aspectos referidos al ámbito cibernético, con la intención de favorecer de esta manera al logro de la resiliencia en las redes y sistemas propios.

El caso de estudio “Tallinn (Estonia) y su evolución hacia la ciber-resiliencia (2007/2017)” permite dimensionar, en cierta medida, cómo un sistema puede transformarse en resiliente de manera efectiva.

PALABRAS CLAVES

Resiliencia, Ambiente, Cibernético, Riesgo, Diseño, Estonia.

ÍNDICE

INTRODUCCIÓN

Las operaciones en el ambiente cibernético han sido consideradas en el ámbito de la campaña a partir del año 1988, oportunidad en la cual Internet fue víctima de un ataque con virus informático, dejando al sistema totalmente vulnerable a amenazas electrónicas. Como consecuencia de este evento, las organizaciones militares más expuestas y relevantes del momento (Estados Unidos y OTAN) comenzaron a implementar medidas de contingencia ante esta nueva modalidad de amenaza.

El bautismo de fuego en cuanto a la afectación de organizaciones militares se dio recién en el año 1998, cuando fuerzas aliadas de la OTAN fueron objeto de un ataque cibernético y Estados Unidos se vio vulnerable al haberse detectado al acceso remoto de operadores no autorizados ni identificados a la red de computadores del Pentágono.

Sin embargo, el hito histórico que despertó el interés militar en el marco global respecto a la protección de los sistemas informáticos se remonta al 27 de abril del año 2007, oportunidad en la cual Estonia resulta blanco de un ataque cibernético sin precedentes. Las páginas de los bancos estaban saturadas, no era posible extraer dinero de los cajeros automáticos, las transacciones virtuales eran denegadas y las páginas de gobierno estaban colapsadas.

El ataque afectó a más de 1.300.000 habitantes. La razón, deducida por parte del gobierno estonio, era el retiro de una vieja estatua de bronce de un soldado de la Unión de Repúblicas Socialistas Soviéticas del centro de Tallinn, ya que, para el gobierno ruso, esa estatua simbolizaba su poder geopolítico en el Báltico.

Asimismo, debido a que los ataques informáticos eran impredecibles y anónimos, no existía alegato alguno para atribuir el ataque a Rusia.

En virtud de ese acontecimiento relevante que modificó las características del ambiente operacional conocido hasta el momento, el estudio de esta temática se ha ido incrementando, se han incorporado medios y fuerzas que atienden a esta problemática, y hasta se ha llegado a considerar al ciberespacio como una dimensión más del campo de batalla.

En las diferentes Escuelas de Guerra que conforman el Centro Educativo de las Fuerzas Armadas de la República Argentina, también se ha escrito e investigado al respecto, tanto sea en el marco de trabajos finales integradores de cursantes de

distintos cursos superiores, como es el caso de los Trabajos Finales Integradores de:

- Sergio David Miranda (Año 2014) que, bajo el título "La Ciberguerra como Amenaza a los Sistemas de Defensa Integrados y Basados en Redes del Teatro de Operaciones", desarrolla la relevancia de los sistemas integrados en redes y la proliferación de los ataques a través del ciberespacio sobre los mismos. Formula la necesidad de replantear la seguridad de los enlaces y describe las medidas necesarias para incrementar la capacidad de ciberdefensa identificando para ello: la organización necesaria, las vulnerabilidades del sistema y la formación del personal para integrar la organización.
- Eduardo Pablo Páez (Año 2014) que, en su trabajo final integrador titulado "La Guerra Cibernética en el Nivel Operacional", considera la organización y funcionamiento de los distintos servicios de informática de las tres Fuerzas Armadas y la interrelación entre estos y las capacidades para desempeñarse en un escenario virtual para hacer frente a las amenazas en el nivel operacional. Plantea como finalidad establecer una organización de nivel conjunto que permita mantener la capacidad y la efectividad de las operaciones militares en un Teatro de Operaciones en el ámbito de la ciberdefensa.
- Daniel Edgardo Giudici (2013) plantea, en su trabajo titulado "Lineamientos para la Seguridad Cibernética en el Teatro de Operaciones", la necesidad de comprender cómo el empleo efectivo de los medios y tecnologías cibernéticas facilitan y favorecen el dominio de las Fuerzas Armadas en un Teatro de Operaciones. Desde el punto de vista de personal, fundamenta el requisito de contar con profesionales especializados y orientados al desarrollo de medidas de seguridad, tratamiento de la información, supervisión de la aplicación de medidas de seguridad cibernética y análisis de riesgo.

Pertenecientes a esta misma casa de estudios, el General de División Retirado Evergisto De Vergara y el Contralmirante Retirado Gustavo Trama llevan adelante una serie de investigaciones respecto a las operaciones en el espectro cibernético. Los resultados de las mismas se traducen en clases magistrales sobre "Ciberdefensa" dirigidas al alumnado de la Escuela Superior de Guerra Conjunta,

en inclusión de roles de combate dentro de los estados mayores de los ejercicios de nivel operacional del Departamento Simulación, y en invitación a expertos en la temática para que diserten frente a los alumnos de los diferentes cursos que se dictan en el Instituto.

Otro referente en la materia es Alejandro Corletti Estrada, Mayor Retirado del Ejército Argentino, Ingeniero Militar formado en la Escuela Superior Técnica y Doctor en Telemática de la Universidad Politécnica de Madrid, España. Actualmente dirige su propia consultora (DarFe.es) y oficia como conferencista internacional en aspectos referidos a la ciberseguridad. En su amplia bibliografía escrita, conferencias dictadas y documentadas y artículos científicos presentados, es posible citar libros tales como: "Seguridad en Redes" y "Seguridad por Niveles", o los artículos: "Presentación, conceptos y situación de Ciberseguridad, ¿de quién nos defendemos?", "Estrategias de Ciberseguridad en grandes redes (seguir y perseguir – proteger y proceder)", "Ciberdefensa en profundidad y en altura (la conquista de las cumbres)", "Ciberseguridad: la importancia de los procesos", "Ciberseguridad: Plataformas / infraestructuras de seguridad en red", "Ciberseguridad: ¿Cómo son las entrañas de esta gran red mundial?", o su tesis doctoral: "Estrategia de Seguridad Informática por capas, aplicando el concepto de Operación Militar por Acción Retardante".

Julio Ardita y la consultora Cybsec representan una importante fuente de información referida al objeto de estudio. Julio Ardita, como referente en la materia, además de proporcionar importantes artículos tales como "Casos de Ciberataques a Infraestructuras Críticas frente a un mundo interconectado e interdependiente" o "Ciberdefensa Nacional", también ha sido conferencista de este Instituto durante el año 2017, bajo la temática: "El estado del arte en materia de ciberdefensa de infraestructuras críticas".

En relación a lo expuesto, cabe destacar que específicamente nadie ha abordado en este Centro de Estudios a la "Resiliencia" como concepto regenerador de capacidades, luego que el sistema haya recibido una afectación por acciones cibernéticas del enemigo.

En la actualidad, no sólo las Fuerzas Armadas de los países más desarrollados del mundo sino también las de los países emergentes, se encuentran desarrollando e implementando medidas para "proteger" los sistemas propios ante acciones enemigas en el ambiente cibernético y, exclusivamente las Fuerzas Armadas de

países más desarrollados, para “seguir y perseguir” enemigos reales y potenciales por medio de la explotación del ambiente cibernético.

Para lograr sistemas robustos y seguros, los organismos de ciberdefensa de las Fuerzas Armadas que disponen de ellos poseen dependencias específicas de “Resiliencia”, concebidas para “resistir” la acción enemiga sobre los propios sistemas y, para estar en capacidad de “volver al estado inicial” en un período de tiempo aceptable.

Asimismo, para que estas acciones sean efectivas, las Fuerzas Armadas que más desarrollados tienen los aspectos referidos a las operaciones en el ambiente cibernético y las implicancias que conllevan la no observancia de este espectro en la concepción de las operaciones, planifican las operaciones cibernéticas de manera particular, empleando el Arte y Diseño Operacional y diferentes matrices de análisis de riesgo, integradas al planeamiento general de la campaña. Este es un aspecto clave que es necesario reforzar en el planeamiento operacional de las Fuerzas Armadas de la República Argentina, rompiendo la inercia propia de la cultura organizacional vigente.

Luego de lo sucedido en Estonia (Tallinn) en el año 2007, la Unión Europea ha tomado ese país como caso de estudio y aplicación, llegando en la actualidad a que Estonia sea considerada la región más segura y resiliente del mundo (desde el punto de vista del ambiente cibernético).

El presente trabajo constituye un aporte importante a la inclusión del ambiente cibernético en el planeamiento de nivel operacional, a partir de la concepción de un sistema resiliente que posibilite “proteger y proceder” para luego poder “seguir y perseguir”.

Al presentar un caso de estudio que demuestra los efectos que puede provocar una ataque cibernético a gran escala, cómo un sistema puede evolucionar hasta convertirse en resiliente y como lo es en la actualidad, es posible apreciar, mediante una prueba real y fehaciente, la necesidad y relevancia del tratamiento del objeto de estudio presentado.

Es entonces que surge como problema de estudio el siguiente: ¿en qué medida la falta de conocimiento respecto a la ciber-resiliencia en el planeamiento del nivel operacional genera vulnerabilidades en el empleo efectivo de la fuerza?.

Para dar respuesta al interrogante precedente, se procurará cumplir con el objetivo general de “identificar la inclusión de herramientas de análisis del centro

de gravedad y de análisis de riesgo para el tratamiento de aspectos referidos al ámbito cibernético, a fin de favorecer el logro de la resiliencia en los sistemas digitales en el planeamiento de nivel operacional".

Y con los objetivos específicos de:

- Identificar las herramientas de análisis en el nivel operacional que favorezcan al logro de la resiliencia en el ambiente cibernético.
- Analizar la evolución de los sistemas digitales hacia la resiliencia, en el caso de estudio "Tallinn – Estonia – (2007/2017)".

La hipótesis que tiene lugar en esta trabajo integrador es "la inclusión de herramientas de análisis del centro de gravedad y de análisis de riesgo aplicadas, durante el proceso de planeamiento de nivel operacional, al espectro cibernético, favorecen la detección de vulnerabilidades propias y contribuyen a la conformación de un sistema ciber-resiliente eficiente".

Para abordar el presente estudio, se llevará adelante un tipo de investigación descriptiva, puesto que se pretenden analizar en profundidad las distintas bibliografías referidos a estos conceptos (muchas veces mal interpretadas), para lo cual se utilizará un diseño cualitativo, en virtud de que se pretende tomar en cuenta la visión de distintos autores vinculados al principio de resiliencia.

Para ello, se utilizará como guía de observación las publicaciones más recientes presentadas en el mundo referentes al objeto de estudio, para luego cotejar con la doctrina propia la mejor articulación lógica posible para detectar las vulnerabilidades de los sistemas propios ante las amenazas cibernéticas.

Finalmente, se describirá la evolución cualitativa y cuantitativa que ha tenido Estonia desde el año 2007 al 2017, como caso de estudio.

CAPÍTULO I

Herramientas de análisis en el nivel operacional para favorecer el logro de la resiliencia en el ambiente cibernético.

En el presente capítulo se abordarán los conceptos referidos a la resiliencia aplicable al ámbito cibernético, y su relación con los niveles de la conducción; el análisis de los factores críticos del Centro de Gravedad en el ambiente cibernético y su conveniente análisis de riesgo (indispensable en el Nivel Operacional); y se planteará una posible estrategia de seguridad cibernética para concebir y procurar un sistema ciber-resiliente.

1. La ciber-resiliencia

Relacionar la resiliencia con el ámbito cibernético no responde a una innovación del autor, sino que es un concepto que ya viene siendo implementado por las principales organizaciones que atienden en el ámbito de la ciberseguridad / ciberdefensa. Para tomar dos ejemplos concretos de ello, la Unión Europea ha planteado como estrategia de ciberseguridad el "logro de la ciber-resiliencia", y el Comando Conjunto de Ciberdefensa del Estado Mayor Conjunto de las Fuerzas Armadas de la República Argentina ha creado y articulado un "Departamento Ciber-resiliencia" en el marco de su orgánica.

Lo que se pretende es abordar la problemática de la ciber-resiliencia desde una visión operacional incluyéndolo en el planeamiento de este nivel y vinculándolo con lo que un Estado Mayor debe identificar al respecto en la concepción de la campaña.

Como término genérico, responde a un concepto empleado en el ámbito de la ingeniería por el cual se llama resiliencia de un material a la energía de deformación (por unidad de volumen) que puede ser recuperada de un cuerpo deformado cuando cesa el esfuerzo que causa la deformación. Es decir, sería su límite elástico, por lo cual, una vez superado esto, el material ya no se puede recuperar y queda "deformado".

Haciendo un paralelismo con una infraestructura informática, sería justamente la capacidad de recuperar su estado inicial luego de haber sido afectada por algún agente (capacidad "elástica").

Por lo tanto, podría definirse entonces a la ciber-resiliencia como la capacidad de respuesta y recuperación ante incidentes de seguridad.

2. Relación entre la ciber-resiliencia y los niveles de la conducción

A nivel Estado, hace cientos de años que le concepto de Defensa es uno de sus pilares básicos pues hace a la soberanía de todo País. La dependencia tecnológica está llegando a una masa crítica que, cuando se explote adecuadamente, podría llegar a dejar fuera de combate a una población o territorio completo.

Es por ello que, de la misma manera que se identifican los niveles de la conducción, en el ambiente cibernético también es necesario concebir distintos niveles de análisis, aunque en el caso de la República Argentina, con algunas diferencias respecto a lo que dicta el mundo.

Tomando como modelo los niveles propuestos por Alejandro Corletti Estrada en su tesis doctoral ("Estrategia de Seguridad Informática por capas, aplicando el concepto de Operación Militar de Acción Retardante"), publicada el año 2011 en la Universidad Nacional de Educación a Distancia de la Escuela Técnica Superior de Ingeniería Informática de Madrid (España), y adaptándola a la realidad fáctica y legal del ámbito de Defensa de la República Argentina, es posible arribar a las siguientes consideraciones particulares referidas a los distintos niveles de la conducción:

2.1. Nivel Estratégico: este nivel debe involucrarse en lo concerniente a la "ciberseguridad", en base a los estudios realizados en un horizonte temporal extenso. Es el punto de partida para determinar las infraestructuras críticas y definir las prioridades en cuanto a la seguridad cibernética al máximo nivel del Estado.

En este nivel es donde se asumen los presupuestos y dimensionan y asignan los recursos necesarios para el mediano y largo plazo.

La responsabilidad primaria de este nivel pasa por el equilibrio justo entre los riesgos asumidos y las estrategias de mitigación.

2.2. Nivel Operacional: es el responsable de dos actividades fundamentales, el planeamiento de la seguridad y el gobierno de la seguridad.

El planeamiento debe definir el ciclo de vida de la seguridad y diseñar la implementación de las medidas técnicas a aplicar para la mitigación de los riesgos que definió el nivel Estratégico.

El gobierno es la actividad que mantiene vivo el estado de seguridad. Supervisa, audita y diseña las acciones de mejoras necesarias para mantener el ciclo.

En este nivel se realiza:

- El análisis de riesgo (identificación de recursos, interacción entre ellos, cuantificación, amenazas, riesgo e impacto, medidas mitigatorias).
- Diseña o define cada uno de estos recursos, pensando en la resiliencia, es decir: definir *Backus*, puntos de recuperación, tiempos de recuperación, procedimientos de recuperación, planes de prueba, redundancias, alta disponibilidad, generación de registros y alarmas, protocolos de monitorización y supervisión, capacitación y redundancia de operadores y administradores, etc.
- Diseña la seguridad informática por capas, es decir, aplicar una robusta política de segmentación de redes basada en zonas.
- Organiza las capas por niveles de seguridad hasta llegar a una última capa de máxima seguridad.
- En esta última capa de máxima seguridad es donde se ubicarán todos los elementos que se han identificado como “críticos” para la organización.
- Implanta robustos procedimientos que regulen toda la actividad que se desarrolle en cada zona.
- Implanta mecanismos para obtener información del adversario.
- Define medidas para intercambiar tiempo por recursos (operaciones de velo y engaño y operaciones de información).
- Puede evaluar permanentemente el balance de fuerzas y el debilitamiento sufrido en cada enfrentamiento.
- Asegurar la capa de máxima seguridad: no se propone mantener al intruso fuera del propio sistema informático, sino dejarlo ingresar poco a poco, para identificarlo y poder accionar sobre él.

2.3. Nivel Táctico: es el nivel responsable de llevar adelante el "cómo" de la operación. No deben existen improvisaciones, ni despliegues que no responsan directamente a las pautas y lineamientos establecidos por el Nivel Operacional. Se aplicarán en este nivel herramientas tales como: de gobierno, riesgo y cumplimiento legal, de mitigación de ataques, de centralización y correlación de *logs*, *Firewalls*, de gestión de *firewalls*, de detección y prevención de intrusiones, de monitorización y supervisión de red, control de acceso, NOC (*Network Operation Center*), SOC (*Security Operation Center*), etc.

En el ámbito de la defensa cibernética, la incertidumbre es total. Si los responsables del subsistema informático son eficientes, podrán acceder a un sin número de herramientas, procedimientos y medidas de protección que permitan estructurar un aceptable sistema de seguridad informática. Pero, aunque estas medidas de eficiencia demandan muchos años de ajustes y mejoramiento, el problema radical no es este, sino que recae en el máximo nivel de la conducción (Estratégico), debido a que, este nivel, debe concebir la seguridad cibernética para que toda su articulación sea coherente.

3. Análisis de los factores críticos del Centro de Gravedad en el ambiente cibernético

Eikmeier (2010) sostiene la necesidad de un tratamiento holístico del análisis del centro de gravedad, debido a que este último funciona dentro de un sistema, el cual está constituido por partes que le dan valor al todo. Es a partir de esta afirmación que Eikmeier sugiere como primer paso del análisis tener claramente descripto el sistema y sus subsistemas componentes para entenderlo y visualizarlo de modo de estar en capacidad de discernir de dónde proviene la fuerza.

Un método aplicable para identificar el escenario sería: primero conocer los actores, luego identificar sus relaciones (conexión entre actores), sus funciones (descripción de sus relaciones) y luego las tensiones (caracterizaciones de las relaciones y de las funciones, como por ejemplo: positivas, negativas, fuertes, débiles, etc).

Una vez que se visualiza esto es posible trazar un mapa, que es un pre requisito para entender el centro de gravedad.

La primera cuestión se relaciona a los fines: ¿cuál es el objetivo de esta entidad o sistema?. ¿Qué es lo que se desea lograr?. El centro de gravedad va a estar siempre en relación al Estado Final Deseado.

La segunda pregunta está relacionada con los modos. ¿Cómo la entidad o sistema pretende alcanzar el objetivo?. ¿Qué acciones se deben ejecutar?. A estas acciones se las denominan capacidad crítica.

La siguiente pregunta conecta a las capacidades con los medios. ¿Quién o qué posee esta capacidad crítica que va a alcanzar la meta u objetivo?. El actor del sistema que la posee entonces es el centro de gravedad.

Como el centro de gravedad (ente primario que posee la capacidad para alcanzar el objetivo) no actúa sólo sino en el marco de un esfuerzo sistémico, es necesario revisar nuevamente: ¿quién es el poseedor primario de esta capacidad?; ¿quién está apoyándolo?; ¿quiénes son los elementos o actores que están siendo apoyados?.

Utilizando este método será posible identificar el centro de gravedad lógicamente y diferenciarlo claramente de los demás actores del sistema que serán probablemente requerimientos, algunos de ellos críticos. A partir de ello, a los requerimientos es necesario identificarles su debilidad para transformarlos en vulnerabilidad crítica.

A partir de lo expuesto será posible deducir que resultaría muy difícil, en una operación militar planificada en el nivel operacional, que dicho Centro de Gravedad sea un factor referido al ambiente cibernético.

Lo que sí indefectiblemente constituirá el espectro cibernético será una conjunción de factores críticos que nutren el sistema de análisis del centro de gravedad. Es decir, existirán capacidades críticas, requerimientos críticos y vulnerabilidades críticas.

De Vergara, Trama (2017) plantean:

> *"Para asegurarse la comprensión del ambiente cibernético, es necesario cerciorarse que en el análisis del Centro de Gravedad se incluya al espacio cibernético. Eso va a permitir identificar capacidades críticas, requerimientos y vulnerabilidades cibernéticas,*

ayudando al Comandante a identificar avenidas de aproximación importantes, y terrenos claves cibernéticos para concentrarse en el esfuerzo defensivo".

A modo de ejemplo, se presenta a continuación un análisis del centro de gravedad desde el punto de vista cibernético, experimentado durante el Ejercicio de Nivel Operacional Alianza – Choique 9, llevado a cabo por los alumnos del Nivel I (Especialización en Planeamiento de Nivel Operacional) de la Escuela Superior de Guerra Conjunta, durante el año 2017:

- Capacidad Crítica:
  - Capacidad de acceso a internet seguro.
  - Capacidad de comando y control de herramientas de la infraestructura crítica.
  - Capacidad de accionar legalmente en el ambiente cibernético.
  - Capacidad de operar con todas las agencias del Estado.

- Requerimiento Crítico:
  - Control activo del ciberespacio de responsabilidad.
  - Máximo empleo de la inteligencia cibernética.
  - Uso del espectro cibernético legalizado.
  - Auditoría y control de puntos de acceso a internet.
  - Uso del espectro cibernético coordinado interagencialmente.
  - Implementación de protocolos del Nivel Operacional en el táctico.
  - Apoyo de medios y personal de ciberdefensa de Verde.
  - Protección y control de infraestructura crítica.

- Vulnerabilidad Crítica:
  - Control activo del ciberespacio de responsabilidad perdido.
  - Uso de actividades de inteligencia cibernética limitado.
  - Legalidad del uso del espectro cibernético no regulado.
  - Auditoría de puntos de acceso a internet no controlado.
  - Coordinación interagencial en el uso del espectro cibernético no lograda.

- Articulación de medidas cibernéticas en el nivel táctico perdidas.
- Apoyo de medios y personal de ciberdefensa de Verde perdido.
- Protección cibernética de infraestructura crítica perdida.

El análisis sistémico de los factores críticos anteriormente mencionados, permite arribar a la conclusión que el Centro de Gravedad desde el punto de vista cibernético en este caso podría ser un "Telepuerto Satelital", o un "Centro de Comando y Control".

4. Análisis de Riesgo que debe llevar adelante el Nivel Operacional a partir de la concepción estratégica

Como ya se ha expresado precedentemente, el Nivel Operacional es el responsable de dos actividades fundamentales: el planeamiento de la seguridad y el gobierno de la seguridad.

El análisis de riesgo le compete al planeamiento del Nivel Operacional, con la intención de mitigar aquellos riesgos que definió el Nivel Estratégico.

Un análisis de riesgo tradicional, según lo expresa Alejandro Corletti Estrada (2011), comprende los siguientes aspectos:

- Identificación de recursos.
- Interacción entre ellos.
- Cuantificación de amenazas, riesgos e impacto.
- Medidas mitigatorias.

A continuación se presentan una serie de procesos y subprocesos a tener en cuenta para la realización de un análisis de riesgo de orden cibernético, a los efectos de estructurar un sistema ciber-resiliente. Dichos procesos y subprocesos responden al análisis comparativo, estudio analítico e interpretación comprensiva llevada a cabo durante la investigación, particularmente de Brett (2014), Carneiro (2012), Corletti Estrada (2011), Harrington (2015), Uzal (2014), Carvalho (2012), entre otros autores complementarios, habiéndose comprobado su aplicación también durante el mencionado ejercicio Alianza – Choique 9 (2017).

4.1. Proceso de concepción de la plataforma informática:

4.1.1. Análisis técnico.

4.1.2. Pruebas de laboratorio.

4.1.3. Documentación de registro.

4.1.4. Informe de seguridad informática.

4.1.5. Informe de pruebas de red.

4.1.6. Análisis de Infraestructuras Críticas.

4.1.7. Determinación de las Infraestructuras Críticas as proteger.

4.2. Proceso de gestión de cambios:

4.2.1. Análisis y gestión de usuarios.

4.2.2. Identificación de usuarios.

4.2.3. Plataforma de seguimiento.

4.2.4. Gestión de incidencias.

4.2.5. Autenticación y control de acceso.

4.2.6. Difusión de protocolos a los sistemas de redes dependientes.

4.3. Proceso de gestión de accesos:

4.3.1. Existencia y cumplimiento de documento de "Control de Accesos", compartiéndolo recurrentemente con los sistemas de redes dependientes.

4.3.2. Mantenimiento actualizado de registro y gestión de identidades por parte de la figura de "gestor de usuarios".

4.3.3. Establecimiento y práctica del ciclo de vida de las cuentas.

4.3.4. Empleo de herramientas de seguimiento y monitoreo para control de accesos.

4.3.5. Documentación y definición de perfiles de usuarios para los diferentes accesos, convenientemente aprobadas por el máximo nivel del sistema.

4.3.6. Eliminación de cuentas genéricas y locales en los dispositivos.

4.3.7. Empleo de privilegios y categorías de acuerdo al nivel de acceso.

4.3.8. Permisos de acceso.

4.3.9. Implementación de plataformas de trazabilidad de accesos.

4.3.10. Implemento de medidas de control sobre potencial evasión del control de acceso.

4.3.11. Difusión de protocolos respecto al proceder de los usuarios ante posibles intrusiones.

4.4. Proceso de configuraciones e inventario:

4.4.1. Procedimiento de configuraciones y gestión de inventario.

4.4.2. Integración de este proceso con el control de cambios.

4.5. Proceso de gestión de resguardo:

4.5.1. Existencia de un procedimiento de respaldo y recuperación.

4.5.2. Alcance del procedimiento de respaldo y recuperación.

4.5.3. Análisis y seguimiento de la criticidad de elementos de la red.

4.5.4. Análisis de criticidad de tiempos de fallo y recuperación.

4.5.5. Plan de pruebas.

4.5.6. Implantación de mecanismos de: redundancia, rotación, extracción de discos y cintas, registro de entrada, salida y destrucción de soportes.

4.5.7. Detalle en cuanto a la asignación de roles y responsabilidades.

4.5.8. Concordancia entre el plan general y la estrategia de seguridad informática a aplicar.

4.6. Proceso de Gestión de Incidencias:

4.6.1. Metodología para la notificación, gestión y respuesta de incidentes de seguridad de la información.

4.6.2. Alcance del procedimiento.

4.6.3. Integración con seguimiento de la organización.

4.6.4. Nivel de integración con “control de cambios”.

4.6.5. Distribución de roles, responsabilidades y funciones convenientemente definidas bajo la premisa de la Inteligencia de “Necesidad de Saber”.

4.6.6. Mecanismos de monitorización, alarmas y escalado de incidencias.

4.6.7. Informes, estadísticas y acciones de mejora para mitigar riesgos y potenciar capacidades.

4.6.8. Recopilación de evidencias, forensia y aprendizaje para robustecer los sistemas propios.

4.7. Proceso de supervisión y monitorización:

4.7.1. Registro de actividad de los administradores y operadores de los sistemas de información.

4.7.2. Análisis para determinar la profundidad o cantidad de eventos a registrar en un sistema de información o red de comunicaciones.

4.7.3. Supervisión y monitoreo adecuado de los siguientes eventos de seguridad:

4.7.3.1. Eventos requeridos por la legislación aplicable.

4.7.3.2. Intentos de autenticación fallidos.

4.7.3.3. Accesos de usuarios a los dispositivos, tanto autorizados como los intentos no autorizados.

4.7.3.4. Los eventos de operación y administración de los sistemas.

4.7.3.5. Uso de programas y utilidades de administración, la instalación o desinstalación de dispositivos de almacenamiento, etc.

4.7.3.6. Cambios de parámetros de configuración de los sistemas.

4.7.3.7. Errores de funcionamiento de los sistemas y las redes.

4.7.3.8. Los accesos a redes de comunicación, tanto autorizados como los intentos no autorizados.

4.7.3.9. El tráfico no permitido o rechazado por los contrafuegos y los dispositivos de encaminamiento.

4.7.3.10. Las alertas generadas por los dispositivos de detección / prevención de intrusos.

4.7.3.11. Los cambios de privilegios de acceso: alta, baja, modificación, cambios de perfiles, etc.

4.7.3.12. Los cambios en los sistemas de seguridad.

4.7.3.13. Acceso al código fuente de los sistemas desarrollados.

4.7.3.14. Activación/desactivación o cambios en la configuración de los mecanismos.

4.7.3.15. Modificaciones o borrado de los ficheros con registros de auditoría.

4.7.3.16. El acceso a datos de carácter sensible.

4.8. Proceso de Gestión de Registros:

4.8.1. Nivel de implantación y explotación alcanzada de registros.

4.8.2. Nivel de seguridad en la gestión de la plataforma de centralización y/o corrección.

4.9. Proceso de Gestión de Actualizaciones:

4.9.1. Tiempo que transcurre entre la primera observación de un archivo desconocido y la detección de una amenaza.

4.9.2. Tiempo que el ciberagresor tarde en volver a atacar.

4.9.3. Ciclo de identificación de vulnerabilidades y solución.

4.9.4. Investigación de actualizaciones.

4.9.5. Evaluación de actualizaciones.

4.9.6. Pruebas de laboratorio.

4.9.7. Pruebas con aplicativos y servidores puntuales.

4.9.8. Pruebas de funcionamiento de pre-producción.

4.9.9. Instalación.

4.9.10. Monitorización.

4.9.11. Aprobación.

4.9.12. Inventariado.

Los procesos y subprocesos enunciados precedentemente, convenientemente insertados en un esquema de análisis de riesgo tradicional (identificación de recursos, interacción entre ellos, cuantificación de amenazas, riesgos e impacto y medidas mitigatorias), permitirán al área de Ciberdefensa del Estado Mayor, diagnosticar la criticidad de la red propia y adoptar las medidas mitigatorias necesarias para contribuir con la conformación de sistemas informáticos seguros y confiables.

5. Estrategias de seguridad cibernética

En la actualidad no es posible concebir un sistema informático eficiente sin el conveniente acceso a Internet. Lógicamente es aquí donde la estrategia de

seguridad cibernética debe primar para interponer las medidas de protección necesaria que aseguren los sistemas.

Asimismo, Internet ofrece una serie de recomendaciones llamadas “RFC” (*Request For Comments*) que constituyen una serie de documentos que establecen pautas a seguir para su buen uso. El RFC-1244 (Política de Seguridad), en su apartado 2.5., propone dos estrategias de seguridad:

5.1. Proteger y proceder.

La premisa de esta es la preservación de los componentes del sistema. El gran problema es que si el intruso no pudo ser identificado, este podrá regresar por la misma falla de seguridad o por cualquier otra.

Esta estrategia propone que, ante un incidente de seguridad, se corten los vínculos, se apaguen equipos, se aíslen áreas. El gran problema reside en que una vez que se decida restablecer los servicios, las debilidades o los intrusos seguirán allí, y volverán a hacer lo mismo, puesto que existe una situación de incertidumbre respecto a la intrusión recibida.

5.2. Seguir y perseguir.

Se permite al intruso continuar sus actividades hasta identificarlo y evidenciar las vulnerabilidades del sistema que fueron aprovechadas. Se requiere aquí el conocimiento en el manejo de incidentes y herramientas adecuadas pues se está arriesgando demasiado la gran ventaja de este proceder es que es la única forma eficiente de llegar a las causas del problema para que este no vuelva a repetirse.

Esta estrategia es más audaz, permitiendo llegar al origen de la vulnerabilidad, determinar las causas, los pasos que siguió el intruso, obtener toda la información probatoria, e inclusive hasta generar ataques inversos.

El principal problema de esta estrategia será que el riesgo de afectación de los sistemas puede llegar a ser catastrófico si no es adecuada y coherentemente conducida.

La lógica de la aplicación de estas dos metodologías sería “proceder y proteger” si las capacidades propias son ciertamente vulnerables. Con un

sistema robusto de seguridad cibernética, se debería progresar hacia la estrategia de "seguir y perseguir", ya que esta modalidad hará posible que las redes y sistemas propios estén orientados hacia la Resiliencia, es decir que, al sufrir cualquier tipo de incidente de seguridad, será posible garantizar que, en primer lugar los sistemas estén en capacidad de resistir el ataque, y en segundo lugar que esté en capacidad de volver a su estado inicial (en un período de tiempo aceptable).

6. Estrategia de Seguridad Informática enmarcada en una Operación Táctica Defensiva de Acción Retardante en procura de un sistema resiliente.

Retomando el raciocinio presentado por Alejandro Corletti Estrada (2011) en su tesis doctoral "Estrategia de Seguridad Informática por capas, aplicando el concepto de Operación Militar de Acción Retardante", y ubicándonos específicamente en el Nivel Operacional, es posible apreciar que para las estrategias de "Proteger y Proceder", y de "Seguir y Perseguir", se podrían aplicar tácticas de carácter netamente militares adecuadas convenientemente al ambiente cibernético.

Así entonces, la estrategia de "proteger y proceder" se equipara con una operación defensiva (defensa de zona) de orden estática, y la estrategia de "seguir y perseguir" también con una operación defensiva (acción retardante), de orden principalmente dinámica.

Alejandro Corletti Estrada (2011) propone, para que esta estrategia tenga éxito, tener especialmente en cuenta lo siguiente:

- *"Determinar los distintos grados de calificación de los recursos, con especial atención en cuáles se podrán intercambiar o interactuar, y cuáles definitivamente no (críticos)".*
- *"Delimitar líneas de retardo (zonas de red) donde se deberán estudiar los sistemas de alarma y la estrategia en ellas".*
- *"Planificar los cursos de acción ante presencia de intrusiones en cada línea, sus probables líneas de aproximación y evaluación de probables metodologías".*

- *"Planificar y llevar a cabo operaciones complementarias de velo y engaño, seguridad, e información como proponen los reglamentos militares".*
- *"Definir una línea de retardo final o línea a no ceder, dentro de la cual deberán encontrarse los recursos críticos y excluirse todo aquel que no pueda garantizarse su fiabilidad".*
- *"Definir zonas de sacrificio y contraataques (Honey Pots), para quebrar el avance de intrusos (IDSs y/o IPSs: Intrusion Detection / Prevention System)".*

El autor de esta teoría plantea que el sistema de seguridad cibernética propuesto se podrá presentar inicialmente como una "Defensa en Profundidad", no manteniendo al intruso fuera del propio sistema informático sino dejándolo ingresar de manera controlada para cumplir con la metodología estratégica de "seguir y perseguir", aplicando la dinámica de la defensa como herramienta.

Se deberá planificar detalladamente esta acción determinando un punto culminante que tácticamente puede ser llamado como "línea no ceder" o "línea de retardo final".

También, es necesario reconocer que existirá una ventana de desconocimiento (como en cualquier operación militar, y más en este nivel de la conducción), en la cual se tendrá absoluta incertidumbre sobre el accionar del enemigo en el ambiente cibernético. Esa ventana de desconocimiento podría definirse entonces como el espacio de tiempo en que la organización aún no ha detectado una vulnerabilidad que le afecte.

Estos conceptos, que parecerían novedosos, no son más que la interpretación de las pautas propuestas en el RFC-1244 referentes a "seguir y perseguir" o "proteger y proceder", y contribuyen a la generación de un sistema cibernético resiliente.

7. Conclusiones Parciales:

Es posible tener la capacidad, los recursos, los conocimientos, y la experiencia para que las redes propias se encuentren protegidas y revestidas de cierta confiabilidad, pero resulta fundamental tener siempre presente que no existen sistemas totalmente seguros e invulnerables. El máximo objetivo

que se requiere perseguir entonces, en lo que a la ciberdefensa se refiere, será la “resiliencia” para soportar el accionar enemigo en este ambiente.

Para lograrlo se debe partir de un adecuado análisis de los factores críticos del Centro de Gravedad, principalmente para identificar requerimientos críticos y vulnerabilidad críticas, sumadas a un conveniente análisis de riesgo tendiente a disminuir la criticidad de dichas vulnerabilidades y adoptar medidas mitigatorias que posibiliten contrarrestar las falencias existentes.

De la misma manera que se planifica la maniobra operacional, será necesaria la implementación de estrategias de seguridad cibernética que permitan no sólo contrarrestar intrusiones, agresiones y/o ataques cibernéticos enemigos, y proteger consecuentemente los propios sistemas, sino también canalizarlo para poder identificarlo, aprender de él y repelerlo, atacarlo y desgastarlo, y todo tipo de acciones llevadas a cabo tendientes a lograr la supremacía en el espectro cibernético.

CAPÍTULO II

Análisis de la evolución de los sistemas digitales hacia la resiliencia, en el caso de estudio "Tallinn, Estonia – (2007/2017)

En el presente capítulo se abordará el caso de Estonia (Tallinn) como Estado Ciber-Resiliente, considerando el período 2007/2017. Se desarrollará el hecho histórico en cuestión y luego se analizará el mismo, para finalmente exponer un muestrario del estado del arte en el mundo referente al tema de estudio.

1. Introducción

En el mes de abril del año 2007, redes y sistemas de datos de Estonia fueron objeto de un ataque de denegación de servicio masivo originado en el extranjero.

Servicios gubernamentales, red de correo electrónico del Ministerio de Defensa, servicios privados, sitios de internet bancarios, redes de cajeros automáticos, entre otros, quedaron fuera de servicio, incapacitando efectivamente a la mayoría de las empresas públicas y privadas durante las aproximadamente 48 horas que duró el ataque. Si bien no hubo daños físicos, el ataque paralizó las actividades financieras y gubernamentales del país durante semanas.

Este incidente dio como resultado el fortalecimiento y protección de los sistemas informáticos públicos y privados de Estonia, implementando firmas electrónicas fortificadas, cortafuegos y sistemas de respaldo, convirtiendo a Estonia en un verdadero líder de la seguridad cibernética, en un verdadero Ciber-Estado Resiliente.

2. Desarrollo del Hecho Histórico

Después de una controversia política originada por un monumento de la Segunda Guerra Mundial, los rusos llevaron a cabo una serie de ataques a sitios de internet de Estonia. La motivación de estos ataques se remonta a principios de 2007, cuando Estonia había anunciado que trasladaría un monumento de la Segunda Guerra Mundial desde el centro de su capital Tallin a un cementerio en el límite exterior de la ciudad. El monumento

revestía un fuerte simbolismo para los rusos étnicos que vivían en Estonia y para los rusos nativos, pues representaba la victoria soviética sobre la Alemania Nacional Socialista. Para algunos estonios, sin embargo, el monumento era un símbolo de la opresión rusa durante el régimen de la Unión de Repúblicas Socialistas Soviéticas.

Como Estonia calificó los ataques como de origen ruso, la cooperación internacional (algunos países europeos y Finlandia), surgió de manera espontánea. Esta cooperación incluyó a profesionales técnicos extranjeros, empresas proveedoras de servicios de Internet, compañías de la red, y otros agentes privados y públicos.

Si bien los ataques son atribuidos a Rusia, su participación no ha sido probada. Asimismo, los políticos estonios y altos funcionarios de los medios de comunicación hicieron completamente responsable a Rusia después del ataque.

Estonia era un blanco ideal para un ataque cibernético debido a su Infraestructura de Tecnología de la Información y de las Comunicaciones y uso generalizado de Internet.

A partir de estos acontecimientos, Estonia se convirtió en un centro de seguridad cibernético. Surgió a partir de ello el Centro de Excelencia Cooperativa de la Ciberdefensa de la OTAN y la Agencia de la Unión Europea para los sistemas informáticos de gran escala.

3. Análisis del Hecho Histórico

El análisis histórico de este hecho, hito para el desarrollo de las operaciones en ámbito cibernético, sumado a las contribuciones académicas suministradas por el Coronel César Cicerchia (2017), nos permite identificar como actores involucrados a:

- Estonia: gobierno, actores privados, opinión pública, asociaciones técnicas, hackers estonianos y ciudadanos de Estonia.
- Rusia: gobierno, hackers rusos y rusos-estonianos.
- OTAN y Aliados: actores públicos y privados (Finlandia, Israel, Eslovenia).
- Espectro cibernético.

La controversia que dio lugar al hito en cuestión fue la mudanza del monumento de la Segunda Guerra Mundial al Soldado Ruso, que afectaba los sentimientos patrióticos de los rusos.

Como hecho relevante a destacar, para el año 2007 en Estonia el 97 % de las transacciones bancarias eran "en línea" y el 60 % de la población hacía uso diario de Internet.

El hecho tuvo lugar entre el 17 de abril y el 18 de mayo de 2007, logrando una afectación total de los sistemas por el lapso de un mes.

Las acciones llevadas a cabo durante el período en que Estonia fue sometido a este flagelo cibernético fueron:

- Infiltración e incursión cibernética.
- Manipulación cibernética mediante el escalonamiento de privilegios de sitios de internet y sabotaje de diversas páginas de internet.
- Asalto cibernético con denegación de servicio distribuido.
- Se generó, como efecto inmediato, un caos digital materializado por: la pérdida del control de más del 90 % de los servicios esenciales y comerciales por parte de Estonia.
- Se generó también un caos urbano, particularmente en la localidad de Tallin, materializado por violencia de la población por la pérdida de acceso a los servicios esenciales y comerciales.

Asimismo, esta situación repercutió en incidentes ulteriores, tales como:

- Acción estratégica de la OTAN a partir de la localización en Estonia del "Centro de Cooperación y Excelencia en Ciberdefensa de la OTAN".
- Acción estratégica de la Unión Europea, a partir de la localización en Estonia de la "Agencia de Sistemas de Tecnologías de la Información de Gran Escala de la Unión Europea".

En Estonia, en aquel año 2007, se dio un escenario propicio para las operaciones del Ciberespacio, en el cual el gobierno y el comercio electrónico hacían uso masivo de los sistemas informáticos conectados.

Al tratarse de un nuevo escenario desconocido como tal en la dimensión en la cual se manifestó, el caso de Estonia se transformó en un conflicto no declarado dirimido en el ciberespacio.

El mundo entero se vio sumergido en una profunda sorpresa tanto sea por su impacto como por su duración, generando en un estado soberano una

situación de emergencia nacional sin que el agresor haya podido ser identificado como tal.

Este ciberataque afecto objetivos de valor estratégico de Estonia, materializados en infraestructuras críticas tales como servicios esenciales del gobierno, energía, financieras, entre otros.

También afectó sistemas de uso diario y cotidiano, tales como las compras en línea, el acceso a los medios de prensa digitales, entre otros.

4. Desarrollo del ámbito cibernético en el mundo

A partir de ello, es posible medir una marcada evolución en materia de ciberdefensa, como se detalla a continuación (datos obtenidos de la investigación y de las contribuciones académicas del Cnl César Cicerchia (2017)):

- **Alemania**, el primero de abril del año 2017, crea el Comando del Ciberespacio e Información, con un efectivo inicial de 260 hombres, y una proyección hacia el año 2021 de 131500 hombres, entre militares y civiles, conformando de esta manera una Cuarta Fuerza Armada con el objetivo de garantizar la protección de las infraestructuras militares y los sistemas de armamento de las Fuerzas Armadas.

- **Brasil**, por su parte, en agosto de 2010 activa un "Equipo Núcleo Cibernético", dependiente del Ejército. En septiembre de 2012 crea el Centro de Defensa Cibernético, también dependiente del Ejército, y en julio de 2015 activa dos núcleos, el Comando de Defensa Cibernético y la Escuela de Defensa Cibernética, ambos subordinados al Ejército y con participación conjunta.

- **Colombia**, en octubre de 2012, crea por orden del Ministerio de Defensa el Comando Conjunto Cibernético de las Fuerzas Militares.

- **China**, también en el año 2010, crea la primera base de seguridad de la información, y en 2015 el gobierno chino reconoce poseer "Ciber-Unidades Militares y Civiles".

- **España**, entre los años 2011 y 2012, desarrolla su visión, concepto y plan de acción de "Ciberdefensa Militar", creando el febrero de 2103 el

"Mando Conjunto de Ciberdefensa", subordinado al Jefe de Estado Mayor de la Defensa.

- **Estados Unidos** en junio del año 2009 crea el "Ciber-comando", subordinado al Comando Estratégico, el cual, en octubre de 2010, alcanza su capacidad operativa completa.
- **Israel**, en el año 2015, inicia el desarrollo de la capacidad de "Ciberdefensa Militar Defensiva", dependiente de la Dirección de Comando, Control, Comunicaciones, Computación e Informática, y de "Ciberdefensa Militar Ofensiva", dependiente de la Dirección de Inteligencia Militar, y arribando al año 2017 logra concentrar todas las capacidades de ciberdefensa en la figura de un "Ciber-comando", subordinado al Jefe del Estado Mayor de la Defensa.
- **Rusia**, en el año 2013, crea el "Ciber Comando Militar".

Ante la marcada tendencia que fueron dictando los países más evolucionados en materia Cibernética, Argentina comenzó a tomar cuenta de esta problemática en el año 2011 cuando, por iniciativa de la Jefatura de Gabinete de Ministros, crea el "Programa Nacional de Infraestructuras Críticas de la Información y Ciberseguridad".

A partir de ello, el Estado Mayor Conjunto de las Fuerzas Armadas incorpora el Plan Transversal Sistémico "Tecnologías del Ciberespacio" en el Plan de Capacidades Militares.

Entre los años 2012 y 2013, a partir del motor del planeamiento estratégico, se crea la "Unidad de Coordinación de Ciberdefensa", concentrada en el Ministerio de Defensa / Estado Mayor Conjunto de las Fuerzas Armadas, organismo este que dio lugar, 14 de mayo de 2014, a la creación del "Comando Conjunto de Ciberdefensa" bajo dependencia del Jefe de Estado Mayor Conjunto de las Fuerzas Armadas.

En 2015 el Ministerio de Defensa crea la "Dirección General de Ciberdefensa" y en el 2016 eleva esa Dirección General a la categoría de "Subsecretaría".

Ese mismo año 2016, por resolución del Ministerio de Defensa, cada Fuerza Armada debía comenzar con un plan de conformación de Direcciones

(dependientes de los Subjefes de Estados Mayores Generales de las Fuerzas Armadas), y posteriormente de Direcciones Generales (dependientes de los Jefes de Estados Mayores Generales de las Fuerzas Armadas). Este plan debería verse completado para inicios del año 2018.

En la actualidad cada Fuerza Armada se encuentra articulando recursos para dar cumplimiento a la resolución ministerial, disponiéndose a la fecha de células de ciberdefensa en cada una de ellas, algunas bajo la figura de Departamentos y otras bajo la figura de Direcciones.

Pero estas medidas no son suficientes para estar a la altura que dicta el estado del arte. Resulta imperioso incidir en la cultura organizacional mediante la ejecución de una política abierta de concientización y difusión de la importancia de la Ciberdefensa en el ambiente operacional moderno.

Acompañado de esto, será necesario incrementar los vínculos de conectividad existentes en las redes militares a los efectos que las plataformas de seguimiento y monitorización posibiliten la vigilancia del ciberespacio de interés para negarlo a potenciales amenazas.

Como lo ha hecho la Unión Europea, la cooperación resulta vital para incrementar la eficiencia en la integración de los sistemas regionales, difundiendo el prestigio del desarrollo de la Ciberdefensa en Sudamérica, de modo de poder acceder a un relacionamiento más acabado con las potencias de primer orden en la materia.

Pero para que este crecimiento y difusión sea tangible y realizable, será necesario el incremento de la planta de personal, no sólo en aspectos cuantitativos sino también cualitativos. La generación de una cadena de conocimiento debería ser el pilar fundamental del crecimiento, capacitando al personal mediante un plan de formación y concientización, estableciendo un núcleo virtuoso de personal que, a partir de su rotación, disemine sus conocimientos y posibilite una mayor eficiencia operativa del sistema.

5. Conclusiones Parciales

Estonia representa un verdadero baluarte de la Resiliencia en Operaciones Cibernéticas. Fue blanco de uno de los ataques cibernéticos más importantes en la historia mundial que lo dejó literalmente incomunicado del mundo y librado a la suerte de su agresor.

Supo reponerse, aprender de sus errores, robustecer sus sistemas informáticos, hasta llegar a concentrar la atención del mundo como “Estado Modelo” en cuanto a la ciber-resiliencia.

Pero esta consolidación fue posible a partir de la cooperación regional, de la integración de conocimientos, habilidades, medios y recursos puestos a disposición por los países integrantes de la Unión Europea en pos de transformar a este país soberano en un verdadero laboratorio de implementos cibernéticos, aprender de él y demostrar el mundo la eficiencia de una organización sólida y competente.

CONCLUSIONES FINALES

A partir del problema de estudio planteado ("¿en qué medida la falta de conocimiento respecto a la ciber-resiliencia en el planeamiento del nivel operacional genera vulnerabilidades en el empleo efectivo de la fuerza?), y luego del análisis y desarrollo expuesto en el presente trabajo, es posible apreciar que la ciber-resiliencia en el planeamiento de nivel operacional resulta fundamental para disminuir las debilidades que posee todo sistema informático y reducir la posibilidad de que las mismas se transformen en vulnerabilidades, generando estructuras más flexibles y adaptables y permitiendo reaccionar con mayor rapidez y eficiencia a la acción enemiga en el ambiente cibernético.

Fue posible apreciar también que la inclusión de herramientas de análisis del centro de gravedad (principalmente para identificar requerimientos críticos y vulnerabilidad críticas), sumadas a un conveniente análisis de riesgo tendiente a disminuir la criticidad de dichas vulnerabilidades y adoptar medidas mitigatorias que posibiliten contrarrestar las falencias existentes para el tratamiento de aspectos referidos al ámbito cibernético, favorecen al logro de la resiliencia en los sistemas digitales en el planeamiento de nivel operacional.

En virtud de esto, la hipótesis planteada referente a "*la inclusión de herramientas de análisis del centro de gravedad y de análisis de riesgo aplicadas, durante el proceso de planeamiento de nivel operacional, al espectro cibernético, favorecen la detección de vulnerabilidades propias y contribuyen a la conformación de un sistema ciber-resiliente eficiente*", merece una consideración positiva, fundamentada en lo convenientemente explicitado en los párrafos precedentes.

Finalmente se concluye que es necesario diseñar e implementar estrategias de seguridad cibernética que permitan no sólo contrarrestar intrusiones, agresiones y/o ataques cibernéticos enemigos, y proteger consecuentemente los propios sistemas, sino también canalizarlo para poder identificarlo, aprender de él y repelerlo, atacarlo y desgastarlo, y todo tipo de acciones llevadas a cabo tendientes a lograr la supremacía en el espectro cibernético. Así reaccionó

Estonia, supo reponerse, aprender de sus errores, robustecer sus sistemas informáticos, hasta llegar a concentrar la atención del mundo como "Estado Modelo" en cuanto a la ciber-resiliencia.

Lo expresado precedentemente da lugar a definir como condición esencial para alcanzar la condición de estado ciber-resiliente la cooperación regional, sin la cual hubiese sido imposible para Estonia reponerse a la afectación cibernética a la cual fue sometida en aquel año 2007, y transformarse, diez años después, en país emblema y ejemplo en cuanto a sofisticación y seguridad cibernética.

BIBLIOGRAFÍA

Ardita, Julio César. (2016). "Casos de Ciberataques a Infraestructuras Críticas frente a un mundo interconectado e interdependiente". *Seminario de CYBSEC*. Buenos Aires, Argentina.

Ardita, Julio; Corletti Estrada, Alejandro. (2016). "Ciberdefensa Nacional". *DarFe Learning Consulting S.L*. Madrid, España.

Asamblea General del Reino de España. (2016). "ODA/11-2016/IS - Avances en la esfera de la información y las telecomunicaciones en el contexto de seguridad internacional". *Asamblea General Reino de España*. Madrid, España.

Bejarano, José Caro. (2012). El Control de Armas en la Era de la Información. *Instituto Español de Estudios Estratégicos*. Madrid, España.

Berman, Ilan. (2011). Iranian Cyberwar. *U. S. Must Prepare for Possible Confrontation, Defense News*. Estados Unidos.

Brett, Williams, (2014). The Joint Force Commander's Guide to Cyberspace Operations. *Indupress*. Estados Unidos.

Carneiro, J. M. (2012). A Guerra Cibernética: uma proposta de elementos para formulação doutrinária no Exército Brasileiro. *Tesis (Doctorado en Ciencias Militares)* – Escola de Comando e Estado-Maior. Río de Janeiro, República Federativa del Brasil.

Carrasco, Luis Salvador. (2015). Ciber-Resiliencia. *Instituto Español de Estudios Estratégicos*. Madrid, España.

Carvalho, Paulo Sérgio. (2012). A Defesa Cibernética e as Infraestruturas Críticas Nacionais. *Escola de Comando e Estado-Maior*. Río de Janeiro, Brasil.

Cicerchia, César. (2017). Conferencia sobre Ciberdefensa y el Comando Conjunto de Ciberdefensa. *Estado Mayor Conjunto de las Fuerzas Armadas – Escuela Superior de Guerra Conjunta*. Buenos Aires, Argentina.

Comando General de las Fuerzas Militares de Colombia. (2015). "Plan

Estratégico Militar 2030 (PEM 2030) - Planeación Estratégica y Transformación". *Comando General de las Fuerzas Militares de Colombia*. Bogotá, Colombia.

Comisión de Regulación de Comunicaciones de la República de Colombia. (2015), "Identificación de posibles acciones regulatorias a implementar en materia de ciberseguridad". *Documento de análisis y consulta de Coordinación de Relaciones de* Gobierno y Asesoría. Bogotá, Colombia.

Corletti Estrada, Alejandro. (2011). Estrategia de Seguridad Informática por capas, aplicando el concepto de Operación Militar por Acción Retardante. Tesis Doctoral. *Universidad Nacional de Educación a Distancia – Escuela Técnica Superior de Ingeniería Informática*. Madrid, España.

Corletti Estrada, Alejandro. (2011). Seguridad por Niveles. *DarFe Learning Consulting S.L*. Madrid, España.

Corletti Estrada, Alejandro. (2016). Seguridad en Redes. *DarFe Learning Consulting S.L*. Madrid, España.

De Vergara, Trama. (2016). "Trabajo de Investigación: Las Operaciones Cibernéticas en el Planeamiento y Ejecución de las Operaciones Militares de Nivel Operacional". Contribución Académica. *Escuela Superior de Guerra Conjunta*. Buenos Aires, Argentina.

Department of Defense. (2016). Joint Publication 1-02. *Department of Defense Dictionary of Military and Associated Terms*. Estados Unidos.

Department of Defense. (2013). *Joint Publication 12-03 (R) – Cyberspace Operational*. Estados Unidos.

Descalzo, Fabián. (2015). "La Importancia del factor humano". *Cybsec, Revista Magazcitum*. Buenos Aires, Argentina.

Diez Molina, Carlos; Perojo, Javier; Penide Blanco, José; Arias, Mikel. (2011). Ciber-terrorismo, definición de políticas de seguridad para proteger infraestructuras críticas frente a ciber-ataques terroristas. *Escuela Politécnica de la Universidad Europea de Madrid*. Madrid, España.

Eikmeier, Dale. (2010). Redefiniendo el Centro de Gravedad. *Military Review*.

Estados Unidos.

Escuela Superior de Ingenieros de Telecomunicaciones. (2013). Seguridad Nacional y Ciberdefensa. Aproximación conceptual: ciberseguridad y ciberdefensa. *Conferencia de la Universidad Politécnica de Madrid*. Madrid, España.

Ferrari, Bruno; Cornachione, Daniella; Loyola, Leandro. (2011). A Guerra Virtual Começou. *Editorial Época*. Río de Janeiro, Brasil.

Gamero Garrido, Alexander. (2014). "Cyber Conflicts in International Relations: Framework and Case Studies". *Seminario sobre Cyber International Relations*. Estados Unidos.

Geers, Kenneth. (2011). *Strategic Cyber Security. NATO Cooperative Cyber Defense Centre of Excelence*. Tallinn, Estonia.

Harrington, Anne; Theohary, Catherine. (2015). Cyber Operations in DOD Policy and Plans: Issues for Congress. Congressional Research Service. *CRS Report – Prepared for Members of Commitees of Congress*. Estados Unidos.

Justribó, Candela; Gastaldi, Sol; Fernández, Jorge. (2014). "Las estrategias de ciberseguridad y ciberdefensa en Argentina: marco político – institucional y normativo". *EDENA*. Buenos Aires, Argentina.

Klimburg, Alexander. (2014). National Cyber Security: Framework Manual. *NATO Cperation Cyber Defense Centre of Excelence.* Tallinn, Estonia.

Kramer, Franklin; Starr, Stuart; Wentz, Larry. (2009). Cyberpower and National Security. Center for Technology and National Security Policy. *National Defense University Press*. Estados Unidos.

Libicki, Martin. (2009). Ciberdeterrence and Cyberwar. *Rand Corporation*. Estados Unidos.

Manera Benítez, Pablo. (2014). "Los 10 errores más comunes de seguridad de aplicaciones móviles". *Cybsec*. Buenos Aires, Argentina.

Manual de Tallin. (2014). Sobre el derecho internacional aplicable a la guerra cibernética. *Traducción oficial por el Ministerio de Defensa Argentino*.

Buenos Aires, Argentina.

Ministerio de Defensa. (2013). MC-20-01 – 2013 - Manual de Estrategia y Planeamiento para la Acción Militar Conjunta, Nivel Operacional- La Campaña. *Estado Mayor Conjunto de las Fuerzas Armadas.* Buenos Aires, Argentina.

Ministerio de Defensa. (2002). RFD–99–01 - Terminología Castrense de uso en el Ejército Argentino. *Ejército Argentino*. Buenos Aires, Argentina.

Ministerio de Defensa del Reino de España. (2010). "Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio". *Cuaderno de Estrategia Nro 149, Instituto Español de Estudios Estratégicos – Instituto Universitario General Gutiérrez Mellado*. España.

Newmeyer, Kevin. (2015). *Ciberespacio, Ciberseguridad y Ciberguerra. II Simposio Internacional de Seguridad y Defensa*. Perú.

Schmitt, Michel. (2013). Manual de Tallinn sobre el Derecho Internacional aplicable a la Guerra Cibernética. *Cambridge University Press*. Nueva York, Estados Unidos.

Silva, Héctor Rubén. (2013). "Ataques Virtuales y la seguridad Informática". *Escuela Superior de Guerra Naval*. Buenos Aires, Argentina.

Taleb, Nassim Nicholas. (2012). Antifragile. Things that gain from discorder. *Random House*. Estados Unidos.

The International Institute for Strategic Studies. (2015). "Evolution of the Cyber Domain: The Implications for National and Global Security". *IISS Strategic Dossier*. Estados Unidos.

Uzal, Roberto. (2014). "¿Guerra Cibernética: un desafío para la Defensa Nacional?". *Revista Visión Conjunta Nº 7.* Buenos Aires, Argentina.

Vargas, Edisson Mauricio. (2014). Tesis de Grado: Ciberseguridad y Ciberdefensa: ¿qué implicaciones tiene para la seguridad nacional?. *Facultad de Relaciones Internacionales, Estrategia y Seguridad*. Bogotá, Colombia.