Capítulo 7

Desafíos para afrontar la ciberguerra

Equipo CEEAG

Hacia los alcances de la resiliencia de un cibersistema

A nivel regional[1], los países que han destacado por ser víctimas de un gran número de ciberataques en Latinoamérica fueron Brasil, Argentina, Colombia, México y Chile. Los accesos o robo de información desde un ordenador infectado –denominados *botnets*– predominaron en la región. Incluso, un tipo específico de este código malicioso llamado *dorkbot* generó más de 80 mil acciones contra el sistema virtual, concentrándose en Chile (44%), Perú (15%) y Argentina (11%). Con ello evidenciamos que hace bastante tiempo que el ciberespacio dejó de ser parte de la ciencia ficción para convertirse en uno de los principales espacios de interacción social[2].

El concepto de resiliencia es definido por Holling como "las condiciones de un sistema complejo alejado del equilibrio, donde las inestabilidades pueden transformar al mismo para que presente otro régimen de comportamiento, así la resiliencia es medida por la magnitud de perturbaciones que pueden ser absorbidas por el sistema antes de que sea reorganizado con diferentes variables y procesos"[3]. Entonces, el concepto de la resiliencia está directamente asociado con la sustentabilidad de todo sistema complejo.

1 P. Prandini y M. Maggiore, M. 2013. *Ciberdelito en América Latina y el Caribe.* Una visión desde la sociedad civil. Proyecto Amparo, Sección de Estudios. LACNIC Registro de Direcciones de Internet para América Latina y el Caribe, p. 3.

2 Marcos Robledo Hoecker, Subsecretario de Defensa Secretario Ejecutivo, Comité Interministerial sobre Ciberseguridad, PNCS 2017, p. 9.

3 Arturo M Calvente, *Resiliencia: un concepto clave para la sustentabilidad*, Universidad Abierta Interamericana, Centro de Altos Estudios Globales.

La resiliencia no es una propiedad absoluta y fija sino que, por el contrario, es variable en el tiempo y el espacio y depende, en gran medida, de las acciones y relaciones del sistema y la volatilidad ambiental del contexto en el que se encuentre.

Entonces, si por motivos antes mencionados un sistema comienza a "perder" resiliencia, se incrementa el "potencial de cambio", es decir, aumentan las posibilidades de pasar a un estado o configuración organizacional diferente, incluso si está sujeto a perturbaciones pequeñas o perturbaciones que anteriormente eran insignificantes o no producían ningún efecto adverso.

Al hablar de un sistema robusto, ello debe ser entendido como la magnitud de volatilidad que puede ser compensada por el sistema complejo antes de llegar al colapso de sus características, procesos y funciones principales. Para ello, el diseño debería contemplar dentro del sistema un arquetipo de detección, otro de protección, uno compensatorio, y por último uno de desafío o contraagresión (eventual). Cada uno juega un rol en el proceso y no necesariamente son secuenciales en su actuar, sino que pueden operar en forma simultánea, cooperativa y coordinada. Así el modelo de detección estará monitoreando constantemente la red, para una vez detectada una amenaza real o potencial, activar las alertas o alarmas.

Acá inicia su labor el modelo de protección, con las contramedidas que estén asociados al tipo de evento malicioso captado, las que pueden contener acciones automatizadas como también otras que el controlador aplique a criterio, dando así dinamismo a la respuesta.

El modelo compensatorio operará sobre la base de los recursos de redundancia y robustez del sistema, logrando con ello un grado abordable de resiliencia.

A lo anterior podría sumarse el modelo de desafío, que junto con tener una capacidad exploratoria (control de daños) y otra ciberforense, van en busca de la fuente de la agresión y aplican medidas de bloqueo, neutralización o mitigación de la acción hostil.

El concepto CSIRT

Una de las herramientas más usadas y de respuesta más oportuna ante eventos cibernéticos corresponde al CSIRT. La sigla CSIRT proviene de la expresión en idioma inglés Computer Security Incident Response Team, que traducido al español es Equipo de Respuesta ante Incidencias de Seguridad. Su practicidad se basa en su capacidad de monitoreo constante de las redes, disponiendo de herramientas tecnológicas y personal especializado que

pueden detectar anomalías en el sistema, pero principalmente en disponer de medios de defensa para el bloqueo, reparación o mitigación del efecto de ataques o alteraciones.

Para garantizar la efectividad de un CSIRT[4], la confianza es un requisito muy importante, y la única manera de desarrollar esta condición mediante un historial de colaboración y participación en la comunidad de seguridad. Tiene una importancia menor que el CSIRT sea operado por el gobierno, un proveedor de red, una entidad comercial o la academia, siempre y cuando se desarrolle en asociación con toda la comunidad de trabajo en red y seguridad dentro de la región.

No puede subestimarse la necesidad de contar con CSIRT robustos en empresas, la academia y el gobierno. Los gobiernos tienen un importante papel que desempeñar en motivar el desarrollo de estos equipos, así como percatarse que no pueden "imponer" la confianza que les permita alcanzar sus metas: deben identificar quién les otorga seguridad, fomentar su crecimiento para el país en general y trabajar con todos. La confianza también está ligada a los servicios que un CSIRT ofrece. Cuando un CSIRT se centra correctamente en responder y mitigar un incidente, a menudo las corporaciones y organizaciones extranjeras confiarán más en ellos y proveerán mayor información para apoyar su misión.

Esta información puede limitarse cuando el CSIRT cumple un papel en la persecución criminal o es parte de un servicio de inteligencia. El tipo de información proporcionada a cualquiera de estas organizaciones tiende a ser diferente y los roles, por tanto, deben segregarse debidamente.

Cuando existe una red de CSIRT, es importante la creación continua de su capacidad. Vemos tres niveles diferentes de mejoramiento en la prestación de servicios de los CSIRT:

Competencia

Una competencia define una actividad medible que puede ser desempeñada como parte de las funciones y responsabilidades de una organización. Para el propósito del marco de servicios de los CSIRT, las competencias pueden definirse como los servicios más amplios o como tareas, subtareas o funciones necesarias.

[4] Observatorio de la Ciberseguridad en América Latina y el Caribe, *Ciberseguridad, ¿Estamos preparados en América Latina y el Caribe?*, Informe Ciberseguridad 2016, presentado por OEA y BID.

Capacidad

La capacidad define el número de ocurrencias simultáneas de una competencia en particular que una organización puede ejecutar antes de alcanzar alguna forma de agotamiento de recursos.

Madurez

¿Qué tan bien puede usted hacerlo? La madurez define el grado de eficacia con el que una organización ejecuta una competencia, en particular dentro de la misión y las autoridades de la organización.

Es necesario centrarse en cada uno de estos tres elementos con el fin de tener éxito en el aumento de la eficacia de un programa de CSIRT.

Como tal, es importante para la comunidad de respuesta a incidentes reconocer estas diferencias y trabajar respecto de las maneras de abordarlas, lo que podrían hacer siguiendo estos (o algunos) lineamientos[5].

- Los Equipos de Respuesta a Incidentes que actúen en primera instancia pueden hacer contacto con otros para mitigar ataques.
- Los CSIRT, al trabajar coordinados y en equipo frente a un incidente, deben tender a hablar el mismo idioma operativo y contar con procedimientos claros y expectativas precisas acerca de. uso de la información proporcionada.
- La comunidad CSIRT debe estar dotada de herramientas y técnicas que permitan el intercambio automatizado de información.

Los analistas aprovechan la información para comprender verdaderamente las ramificaciones del incidente y toman las decisiones acertadas para reducir los riesgos mientras mitigan el ataque. Para llegar a este punto, vemos necesario el desarrollo de una red de CSIRT sólida e incluyente, la disponibilidad de formación y educación para los miembros de la comunidad y la necesidad de contar con prácticas estandarizadas dentro de esta estructura de colaboración.

Idealmente la comunidad de CSIRT debería lograr que cada organización cuente con una capacidad de respuesta a incidentes bien equipada. Puede ser un solo individuo o un equipo pequeño, pero cada organización debe poder asumir la responsabilidad por el tráfico que genera. Sin embargo a causa del gran número de redes y su respectivo crecimiento, esto podría considerase

5 Op. cit., *Observatorio de la Ciberseguridad*, OEA y BID.

un panorama complejo de lograr. Una alternativa es que cada país desarrolle su "CSIRT de último recurso", es decir, que puede ser punto de coordinación para aquellas redes que puedan no tener un equipo de respuesta a incidentes bien entrenado y directamente accesible. Se debe entender que, al final, cada organización es responsable de su propia seguridad; un equipo nacional solo puede apoyar en la coordinación pero no podrá "desconectar" o investigar cada máquina comprometida.

Pero la ciberdefensa también debe contar con un vector ofensivo. Si consideramos que la guerra se gana poniendo al enemigo en una situación en que acceder a lo que se le está requiriendo sea menos malo para él que resistir a ello, y la forma de ponerlo en esta situación es mediante una combinación de acciones militares, económicas, diplomáticas y psicológicas que lo lleven a una o más de las siguientes condiciones: la destrucción de sus fuerzas militares; la conquista y ocupación de su territorio; el quiebre de la voluntad de lucha de su ejército, de su gobierno, de su opinión pública, o de todos ellos[6], son todos factores en que el ariete ofensivo de la ciberdefensa ciertamente va a aportar.

Ese plan de acción debe ser coherente y creíble para así generar disuasión.

Esta capacidad de actuar por el disuasor posee una limitación clara en los requisitos de la proporcionalidad y la coherencia. El primero exige una proporcionalidad entre la conducta que se desea inducir en el actor disuadido y los efectos del uso del poder coactivo con el que se le amenaza. Precisamente este criterio de la proporcionalidad de la disuasión exige que esta sea graduable, es decir, que la amenaza del poder coactivo pueda incrementarse o reducirse en correspondencia con la conducta que siga la parte disuadida[7].

A mejor entendimiento de la amplitud del escenario a cubrir[8], un esbozo de la infraestructura de la información de los siguientes sectores será considerada como crítica: energía, telecomunicaciones, agua, salud, servicios financieros, seguridad pública, transporte, administración pública, protección civil y defensa, entre otras. Complementa lo anterior la lectura de la Estrategia Nacional de Seguridad del Reino Unido del 2010[9]. En ella se incluye como aspecto prioritario la protección de las infraestructuras críticas del país, y se determina que Internet es parte de estas infraestructuras, y

6 Fernando Thauby García, "Disuasión y Defensa", *Revista de Marina*, Armada de Chile, 1992.

7 Rafael Calduch Cervera, La Ocupación del Territorio Nacional y la Disuasión para su Defensa: La Cambiante Perspectiva Europea, Universidad Complutense de Madrid.

8 Propuesta de Política Nacional de Ciberseguridad (PNCS) 2016-2022.

9 Ministerio de Defensa del Reino Unido, *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, Reino Unido.

que puede ser tanto un objetivo como un medio para terroristas, criminales y naciones hostiles.

Es tanto el impacto y la necesidad de coordinación transversal en todos los campos de acción, que se ha planteado que la ciberdefensa requiere ser considerada como un nuevo eje estratégico.

La respuesta para ello contemplada en el *Libro Blanco de la Defensa de Francia 2013*[10] plantea un concepto en extremo interesante y que encaja plenamente dentro de lo que son actividades propias de ciberdefensa. La visión gala considera una postura estratégica para determinar el origen de los ataques, organizar la resiliencia de la Nación y responder a ellos, también mediante una respuesta agresiva, denominada "Lucha Informática Ofensiva" (LIO) y que parte del principio que para saber defenderse es necesario también saber atacar. Para poder lograr esta capacidad se debe invertir en los siguientes ejes principales:

- Definición de un marco de uso que cubra específicamente el conjunto de acciones relevantes de la lucha informática.
- El desarrollo de herramientas especializadas (laboratorios técnico-operativos, redes de ataque, etc.).
- La formulación de una doctrina de empleo de las capacidades de LIO (planificación, realización y evaluación de las operaciones).
- Puesta en marcha de una formación adaptada, y regularmente actualizada, para personal identificado y reunido dentro de células de especialistas.

En el contexto regional[11] se puede apreciar claramente un mayor entendimiento y compromiso por el diseño y concreción de un grado de protección de la infraestructura, redes estratégicas, información electrónica y el fortalecimiento de organismos interinstitucionales para hacer frente a las amenazas que atentan a la seguridad del Estado, llegando a constituir el concepto estratégico que la ciberdefensa debe ser entendido como bien público.

Las ideas van desde lo meramente conceptual como es tener un estándar básico compartido en el diseño y seguridad de las redes, hasta implementación de instalaciones que cooperan y monitorean activamente las redes informáticas, con el objetivo de generar seguridad, protección y hasta capacidad ofensiva en la línea cibernética.

10 Ministerio de Defensa de Francia, *Le Livre Blanc sur la Défense et la Sécurité Nationale*, Ed. 2013.

11 CEEAG, *Observatorio,* Informe Mensual, Ciberdefensa-Situación a la fecha, septiembre 2016.

También ya se ha marcado la tendencia de separar aguas en lo que corresponde a la ciberseguridad y la ciberdefensa, misiones que les son propias, estableciendo actores específicos y dedicados a cada ámbito y ministerios con jurisdicción en cada uno de ellos, donde los requerimientos operacionales han tenido una mirada integral y multidisciplinaria, con atención puesta en las nuevas tecnologías, capacitación y preparación de personal técnico, como también la participación necesaria en conjunto del sector defensa (con visión conjunta), empresarial y académico para obtener resultados más eficientes y productivos.

UNASUR también ha continuado en el desarrollado de iniciativas en el ámbito de la ciberdefensa, manteniendo esfuerzos consignados en su Plan de Acción 2016 y tiene previsto, junto con el Consejo Suramericano de Infraestructura y Planeamiento de UNASUR (COSIPLAN), la realización de un Seminario concerniente a esta temática, bajo la responsabilidad directa o asociada de Chile, Ecuador, Perú, Argentina, Bolivia, Brasil y Uruguay.

Intercambio de información de ciberamenazas

En un mundo en el que las tecnologías evolucionan constantemente y los perímetros definidos y las zonas de confianza van desapareciendo poco a poco, los modelos tradicionales de seguridad están sometidos a una presión sin precedentes. Para ser eficaces, los modelos de seguridad deben adaptarse a la nueva realidad.

Ya existe una gran variedad de modelos para compartir inteligencia respecto de amenazas, y algunos llevan aplicándose más de 20 años[12]. Otros están evolucionando para adaptarse a los cambios en el panorama de las amenazas, y los hay que se encuentran en su fase inicial, mientras las fuerzas de seguridad, los proveedores de servicios de seguridad, el sector público y las empresas objetivo exploran métodos que permitan compartir la información y responder de manera eficaz a las modificaciones del marco normativo.

El intercambio de información acerca de amenazas ha sido un proceso lento y manual. Las empresas se han mostrado por lo general reticentes a compartir ni siquiera los más mínimos detalles de los ataques o los sistemas comprometidos, bien por miedo a demandas judiciales o al daño a su reputación, o simplemente para evitar divulgar vulnerabilidades no corregidas.

12 *Informe de McAfee Labs sobre amenazas*, abril de 2017.

Pese a ello, ha habido avances concretos en la conformación de los Centros ISAC, las ISAO y los CERT o CSIRT.

Los centros ISAC (Information Sharing and Analysis Centers) son organizaciones sin ánimo de lucro que actúan como puntos centralizados de intercambio y recopilación de inteligencia relativas a amenazas entre las agencias locales y nacionales, sectores verticales específicos y distintas infraestructuras críticas. Muchos de ellos comenzaron como resultado de una directiva presidencial de EE.UU. de 1998 destinada a promover el intercambio de inteligencia relacionada con amenazas y vulnerabilidades entre propietarios y operadores de infraestructuras críticas. Aunque en un primer momento se centraban en las infraestructuras estadounidenses, muchos centros ISAC han ampliado su cobertura para incluir miembros de todo el mundo. Se han creado igualmente centros ISAC también en sectores distintos de las infraestructuras críticas, como por ejemplo, los del automóvil, aviación, electricidad, comercio, servicios financieros, energía nuclear y abastecimiento de agua, entre otros.

Las organizaciones ISAO (Information Sharing and Analysis Organizations) tienen un campo de acción más amplio que los centros ISAC y constituyen un mecanismo suplementario para promover y apoyar el intercambio de información de amenazas. Su creación fue promovida por una ley estadounidense aprobada en 2015 cuyo objeto era limitar las responsabilidades legales por el intercambio de información pertinente a amenazas con otras empresas. Estas organizaciones pueden también ser privadas o sin ánimo de lucro, especializadas por tipo de amenaza o zona geográfica, y van de comunidades de interés a agencias gubernamentales, pasando por empresas de servicios.

Aplicación de la ciberguerra en un campo de batalla moderno

La ciberguerra puede aparentar ser una amenaza menor, pero se debe considerar que, a diferencia de la guerra convencional, para el desarrollo de sus acciones puede optarse por opciones que requieren reducidos recursos. Basta con contar con los conocimientos y menos de US$10.000 en equipos para convertirse en un "guerrero de la información"[13]. Es más, en un nivel básico de ciberguerra, el solo arriendo de una estación de trabajo en un

[13] Gregory Walters, *A new way of war in the information age*, Univesity of Otawa, Otawa, 1998, p. 3.

cibercafé, a un precio ínfimo, bastaría para generar un daño no menor en una red informática abierta a Internet, si se cuenta con los conocimientos para ello.

En respuesta a lo anterior, las organizaciones tienden a aumentar los recursos asignados para dar mayor seguridad a sus sistemas informáticos, pero la experiencia indica que los riesgos no desaparecen, sino que por el contrario, día a día se develan nuevas amenazas o debilidades que vienen a aumentar los incidentes, de origen interno y externo, existiendo una variedad de razones para ello, dentro de estos figuran[14]: el grado de conectividad se incrementa a niveles que sobrepasan la capacidad de control; la necesidad operacional de integrar elementos de *hardware* y *software* de mayor tecnología, lo antes posible y a menor costo, reducen la introducción de elementos de seguridad, o contramedidas que impiden que sean probados adecuadamente; la aplicación de medidas de seguridad nuevos a sistemas ya existentes es de alto costo y en algunos casos imposible, con serio impacto en su funcionamiento operativo.

Es conveniente señalar que todas las redes y sistemas informáticos, sin importar sus capacidades y cualidades, resguardos u otros, en alguna medida son vulnerables a la ciberguerra, por tanto, factibles de penetrar, destruir, modificar, etc., en función del factor tiempo, recursos y tecnología.

Por lo anterior, lo importante no es sencillamente lograr contar con una capacidad técnica que permita la aplicación o ejecución de acciones de ciberguerra, sino que se debe considerar una planificación que oriente la ejecución de acciones de ciberguerra al logro de determinados efectos, representados por la consecución de objetivos que permitan su materialización.

Se debe tener determinado previamente el momento de ejecución requerido, para así lograr el efecto con la debida oportunidad, previendo los tiempos necesarios para que ello ocurra.

La ciberguerra no obtiene efectos por sí sola, sino que debe asociarse al empleo de todos los recursos disponibles que permitan asegurar su éxito.

La aplicación de la ciberguerra en el campo de batalla moderno tiende a dos ejes bases, que son el asociado al proceso de manipulación del enemigo y sus capacidades para tomar decisiones, y por otra parte a la generación de una propia capacidad para obtención de inteligencia.

Para influir en las capacidades para tomar decisiones, la ciberguerra no puede actuar como compartimiento estanco y debe ser coordinada en sus

14 Anderson, Kent, *Intelligence-Based Threat Assesment for Information Networks and Infraestructures*, Global Tech Reserach Inc., marzo 1998, p. 2.

efectos, momento de aplicación y objetivos buscados por el C2 (combate por el Mando y Control), por tanto se deberá tender al empleo de dos o más de estos elementos, para así lograr un efecto de sinergia, lo que catalizará, potenciará, magnificará y asegurará el resultado.

Luego, su ejecución deberá ser enmarcada en una planificación que coordine adecuadamente la ejecución de operaciones psicológicas, operaciones de diversión (o demostración), operaciones de contrainteligencia, destrucción física y guerra electrónica[15].

Con esto se buscará afectar la capacidad de decisión del adversario, lo que en cuanto a ciberguerra puede orientarse a interferir su capacidad de obtención de información útil, degradar sus procesos de gestación de resoluciones y neutralizar sus medios de comunicación y enlace que le permitan direccionar el esfuerzo de búsqueda, tanto como usar o difundir la inteligencia obtenida.

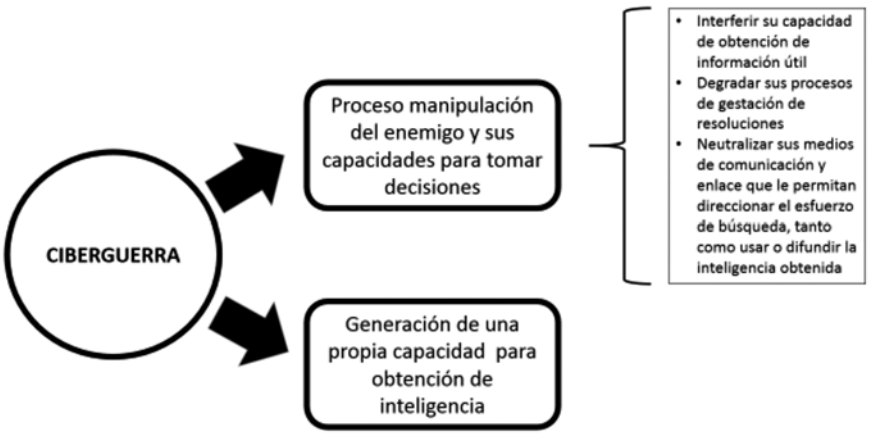
Luego, este proceso de manipulación del enemigo y sus capacidades para tomar decisiones mediante el empleo de la ciberguerra, como uno de sus elementos, podrá actuar en busca de los siguientes objetivos que son propios de lograr mediante la guerra de la información[16]:

- Seguridad informática: afectando la protección a la información y los sistemas informáticos, sus previsiones para el respaldo, restauración, detección y capacidad de reacción.
- Entorno informático: saturando, perturbando, degradando o interrumpiendo la interacción de individuos, organizaciones o sistemas de búsqueda, proceso o difusión de información.
- Superioridad informática: por medio de la negación de la capacidad del adversario de obtener, procesar y difundir información mediante un flujo ininterrumpido.
- Sistema informático: incidiendo en la eficacia de su infraestructura, organización, personal y componentes para degradar o neutralizar su capacidad de obtención, proceso, archivo, transmisión, proyección, difusión y acción.

15 Op. cit., Department of Defense, Ed. Feb. 2000, pág. A48 (Appendix A).

16 Departamento de Defensa de Estados Unidos, *DOD Directive S-3600.1, "Information Operations (IO)".*

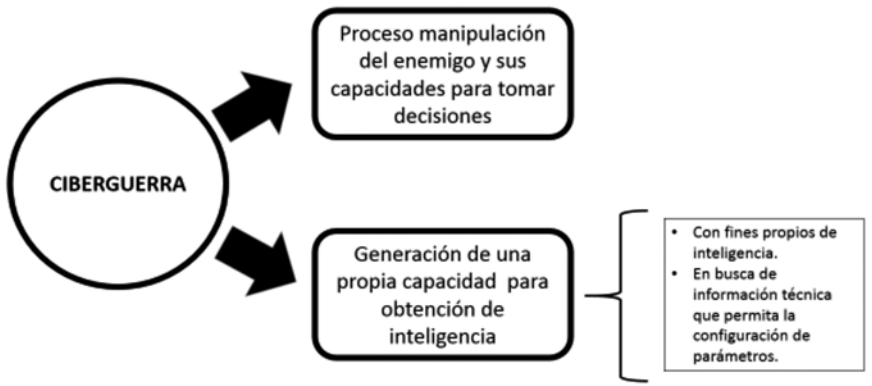
Figura 1
Ejes a los que tiende la aplicación de la ciberguerra



Fuente: Elaboración propia.

La ciberguerra puede ser empleada para la obtención de información con fines propios de inteligencia o en busca de información técnica que permita la configuración de parámetros para la ejecución de otras acciones de ciberguerra.

Figura 2
Ejes a los que tiende la aplicación de la ciberguerra



Fuente: Elaboración propia.

Para ello deberá orientar su acción bajo las normas que son propias de operaciones especiales, es decir, como una suma de acciones ocultas, que emplean para ello técnicas encubiertas, realizadas con medios especializados sobre un objetivo de inteligencia, dentro o fuera del territorio, en tiempo de paz o de guerra y cuyo logro no delata a quienes las inspiran, evitándose así los comprometimientos.

Al actuar en busca de información técnica que permita la configuración de parámetros para la ejecución de otras acciones de ciberguerra, tanto de obtención de información como de generar entrabamiento técnico de las redes objetivo, orientará su acción al logro de información referida principalmente a lo siguiente[17]:

En cuanto a aspectos cuantitativos

- Cantidad e identificación de los administradores de la red: verificar sus horarios de control y acciones rutinarias que permitan detectar vulnerabilidades.
- Número de alarmas activadas: con el fin de poder determinar la cantidad de ataques simultáneos que se requerirán.
- Usuarios detectados: para de esa forma suplantar usuarios y eventualmente generar intrusiones.
- Amenazas reconocidas por el sistema: para configurar medios de ataque que no sean reconocidos por los subsistemas de defensa, alerta y reacción.
- Sistemas de monitoreo: verificar los horarios en que la red se encuentra bajo control y bajo qué nivel de libertad de acción.
- Nodos protegidos: para centrar el ataque en aquellos nodos de mayor vulnerabilidad.
- Cantidad de ataques simultáneos que se requerirán: esta información será importante para la determinación de la cantidad de acciones requeridas simultáneamente, con el fin de generar ataques que atraigan respuestas de reacción y defensa del sistema víctima, distrayéndolo del ataque principal.

17 Myron Cramer, *New Methods of Intrusion detection using Control-Loop Measuremente*, Fourth Technology for Information Security Conference , Houston, Texas, mayo 1996, p. 2.

En cuanto a aspectos cualitativos

- Probabilidad de detección del ataque
- Índice de falsas alarmas
- Rango de detección de intrusión

En cuanto a aspectos de tiempo/oportunidad

- Tiempo de detección
- Tiempo de activación de la alarma
- Cantidad de información o *data* archivada
- Oportunidad de empleo de esa información (inmediato, corto, mediano, largo plazo)
- Históricamente, las acciones de ciberguerra se han desarrollado contra un número limitado de sistemas[18]. El motivo de estos ataques varía, pero los métodos y objetivos se limitaban al subsistema del computador como objetivo primario. Actualmente, un significativo cambio es experimentado al respecto, los avances tecnológicos, junto con intenciones que pasan a ser más criminales o delictuales, generan amenazas de ciberguerra para toda la infraestructura informática.

Una síntesis de su comportamiento nos indica que existen ataques a la infraestructura y otros orientados solo al sistema:

Ataques a la infraestructura

Buscan un significativo compromiso del funcionamiento de toda una infraestructura, más que el afectar sus componentes individuales. De ser exitosos, son capaces de mantener un compromiso del funcionamiento de la red en forma temporal.

Implican la ejecución de acciones contra los sistemas de respaldo y recuperación de archivos y elementos. Son difíciles de implementar, sustentar y lograr éxitos. Requieren una definición previa y precisa de sus objetivos, un ataque coordinado contra múltiples sistemas y puntos de control, en tiempo preciso, con el fin de comprometer los sistemas de redundancia o respaldo.

No todos los ataques de ciberguerra llegan a ser conocidos, ya que algunos no son divulgados por quienes han sido sus víctimas y otros nunca llegan a

[18] Op. cit. Kent Anderson, p. 8.

ser detectados. Un caso conocido contra una infraestructura fue el ejecutado por el Chaos Computer Club, en Alemania, en septiembre de 1995, quienes ejecutaron una acción en contra del sistema de comunicaciones francés, como una forma de protestar por las pruebas nucleares que Francia llevaba a cabo en el Pacífico. Este ataque tuvo pequeño o nada de impacto[19] en lo operacional del sistema, pero sí logró repercusión comunicacional.

Otro caso fue el del martes 27 de junio del 2017, donde algo que ya era esperable se hizo realidad. Una oleada de agresiones cibernéticas atacaba varios objetivos multinacionales. El agente agresor nuevamente se presentaba como un *malware* tipo *ransomware* (que genera una suerte de "secuestro virtual" de los archivos al capturarlos en su origen, encriptarlos y solo devolverlos a su normalidad previo pago de un rescate monetario). Esa agresión fue presumiblemente perpetrada mediante un virus denominado "Petrwrap", que corresponde a una variante "Ransomware Petya" usado en ataques anteriores, con una cercana similitud al "Wannacry", de triste memoria en su megabloqueo del 12 de mayo del 2017, en que afectó a más de 150 países, con efectos que no pudieron ser cuantificados en su totalidad.

Ataques a sistemas

Son acciones de ciberguerra orientadas a afectar sistemas individuales o centros de control, los que no generan la detención de la operación de toda la infraestructura u organización. Sin embargo, corresponde a una intrusión en la que se ve comprometida la integridad básica del sistema. Esto puede acarrear la pérdida de la confidencialidad de la información guardada, la integridad de los archivos o *data*, o afectar la disponibilidad de los recursos disponibles.

Ejemplos de este tipo de ataques con resultado exitoso son muy comunes de conocer, como las efectuadas contra la *web* de la VI Cumbre Iberoamerciana que se realizó en Santiago de Chile en 1996, la acción de *hackers* supuestamente brasileños contra la *web* de la Cámara de Diputados (www.cámara.cl) en el 2000, la intrusión a la *web* del Ministerio Secretaría General de Gobierno (www.segegob.cl) en febrero del 2000, entre otras[20].

Luego, el ataque a un sistema, con un objetivo bien determinado y un efecto perseguido que sea determinante, pasa a ser una de las acciones más rentables en la aplicación de ciberguerra. Por ello, es factible enunciar

19 Ibíd.

20 www.emol.cl *"Hackers atacaron la Web de la Cámara"*, http://hechos.com.do/article/88546/hackers-atacan-pagina-camara-diputados/.

características de los tipos de objetivos rentables a la aplicación de ciberguerra, los que al integrar las características de objetivos ya descritas, variarán de acuerdo con el fin perseguido, pudiendo presentar algunos rasgos comunes, pero serán diferenciables en su forma de explotación. Es así como se han determinado las siguientes:

Características comunes

El efecto buscado con el objetivo deberá ser compatible con otras formas de accionar, específicamente de combate por el C2, para así magnificar y asegurar el resultado.

Características de objetivos para manipular al enemigo

- Será fundamental mantener la acción en forma oculta por el máximo de tiempo que se pueda, no generando instancias de alarma o detección que puedan delatar el empleo de ciberguerra, de lo contrario el adversario buscará la reconfirmación de la información que está procesando, para luego alertarlo que está siendo víctima de medidas contra su sistema informático.
- Tenderán a ser compatibles con el desarrollo de acciones de combate por el C2 centradas en la diversión y en la guerra electrónica (decepción).
- Deberán servir a una historia de diversión.
- Su consecución tendrá un efecto de reducida permanencia, por lo que se requerirá planificar adecuadamente el instante y tiempo de ejecución y prever los lapsos necesarios para que se concrete el efecto con oportunidad.
- Parte del supuesto que las actividades reales son ocultadas mediante encubrimiento, para que así no se descubra que la situación que es presentada al adversario es falsa.
- Este tipo de objetivos requiere que se desplieguen medios de inteligencia que permitan detectar si se está causando el efecto deseado.

Para degradar la capacidad del enemigo de tomar decisiones

- Será difícil mantener la acción oculta, pues el adversario detectará, mediante sus procedimientos de control, que su sistema de mando y conducción se está viendo afectado.

- Su empleo puede considerar la saturación, obstaculización, deterioro, daño temporal o permanente de parte de sus sistemas informáticos de apoyo a la toma de decisiones o gestación de la resolución.
- Considerando que la víctima tenderá a contar con sistemas redundantes o respaldo, su efecto no podrá tener una gran permanencia, por lo que se requerirá planificar adecuadamente el instante y tiempo de ejecución y prever los lapsos necesarios para que se concrete el efecto con oportunidad.
- La rentabilidad del objetivo aumentará mientras mayor sea su conectividad a otros subsistemas o componentes y mientras mayor sea la necesidad del sistema de contar con ese punto para derivar informaciones hacia otros elementos informáticos.
- Este tipo de objetivos, al igual que el enunciado anteriormente, requiere que se desplieguen medios de inteligencia que permitan detectar si se está causando el efecto deseado.
- Su valor como objetivo será inversamente proporcional al grado de capacidad del sistema víctima para proceder a su redundancia, respaldo, restauración o reemplazo. Es decir, mientras menor sea la capacidad para reemplazar un componente del sistema, mayor será su valor como objetivo.
- El valor del objetivo aumentará mientras mayores sean las posibilidades de obtener el efecto por múltiples vías para así asegurar el éxito.

Para la obtención de inteligencia

- Aquellos subsistemas o componentes con baja capacidad de respuesta, detección o alarma a las intrusiones, representarán objetivos de alto valor.
- Los objetivos que tengan características de presentar un alto nivel de falsas alarmas requerirán previamente acciones que hagan perder la confianza de los operadores en ellos, para así retardar o anular sus reacciones. Normalmente este tipo de objetivos se emplearán como elementos secundarios que permitan amarrar la atención de quienes monitorean los sistemas, restando atención a la verdadera intrusión.
- La importancia del objetivo será directamente proporcional al acceso que permita a archivos de *data* de gran valor de uso y calidad. A su vez, la calidad de esa información se relacionará a la oportunidad y pertinencia para su empleo.

Bibliografía

A Strong Britain in an Age of Uncertainty: The National Security Strategy, Reino Unido, 2010.

Anabalón, Juan y Donders, Eric. Revisión de ciberdefensa de infraestructura crítica, Estudios Seguridad y Defensa Nº 3, ANEPE, Chile, 2014.

Acosta, Pastor, Pérez Rodríguez y otros, *Seguridad Nacional y Ciberdefensa*, ISDEFE-UPM, Cuadernos Cátedra Nº 6.

Adrianna Llongueras, Vicente. *La Ciberguerra; la guerra inexistente*, Tesina Doctorado en Paz y Seguridad Internacional, Instituto Universitario General Gutiérrez Mellado, 2011.

Amigo Tossi, Alejandro. Ciberdefensa en las Operaciones Militares, Seminario ACAPOMIL, Tendencias Tecnológicas Asociadas a la Ciberdefensa, agosto 2016.

Anderson, Kent. *Intelligence-Based Threat Assesment for Information Networks and Infraestructures*, Global Tech Reserach Inc., marzo 1998.

Arquilla, John. *Cyberwar and Netwar: New Modes, Old Concepts, of Conflict, Cyber War is Coming, Comparative Strategy*, vol. 12, RAND's home page.

Boid, John. *The School of Advanced Airpower Studies. The Paths of Heaven: The Evolution of Airpower Theory*, Alabama, USA: Air University Press, Maxwell Air Force Base, 1997.

Calduch Cervera, Rafael. *La Ocupación del Territorio Nacional y la Disuasión para su Defensa: La Cambiante Perspectiva Europea*, Universidad Complutense de Madrid.

Calvente Arturo M. *Resiliencia: un concepto clave para la sustentabilidad*, Universidad Abierta Interamericana, Centro de Altos Estudios Globales.

Cano, Jeimy J. *Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global*, Sistemas (Asociación Colombiana de Ingenieros de Sistemas), vol. 000, Nº 0119 (abr-jun. 2011).

Centro de Estudios Superiores de la Defensa Nacional (CESEDEN). El ciberespacio, nuevo escenario de confrontación, capacidades para defensa en el ciberespacio, España, 2012.

Development, Concepts and Doctrine Centre (DCDC), Cyber Primer, Second Edition, Ministry of Defensa, UK, 2016.

Departamento de Defensa de Estados Unidos, *DOD Directive S-3600.1, "Information Operations (IO)"*.

Ejército de EE.UU., Information Operations, FM34-1.

Koch, Sebastián. "La política de ciberdefensa en Chile", Columna de Opinión, (Documento en línea) http://www.losriosaldia.cl/?p=19065.

Le Livre blanc sur la défense et la sécurité nationale, Ministerio de Defensa de Francia, Ed., 2013.

Libicki, Martin. "The future of information Security", en *Institute for National Strategic Studies*, mayo de 2000.

Libro de la Defensa Nacional, MDN, Chile, Parte 2, Ed. 2010.

Lineamientos de Política para ciberseguridad y ciberdefensa, Consejo Nacional de Política Económica y Social, República de Colombia, Departamento Nacional de Planeación.

Mc Afee. *Informe de McAfee Labs sobre amenazas*, abril de 2017.

Myron Cramer. *New Methods of Intrusion detection using Control-Loop Measuremente*, Fourth Technology for Information Security Conference , Houston Texas, mayo 1996.

Observatorio, Informe Mensual, CEEAG, Ciberdefensa-Situación a la fecha, septiembre 2016.

Prandini, P. y Maggiore M., M. 2013. *Ciberdelito en América Latina y el Caribe*. Una visión desde la sociedad civil. Proyecto Amparo, Sección de Estudios. LACNIC Registro de Direcciones de Internet para América Latina y el Caribe.

Propuesta de Política Nacional de Ciberseguridad (PNCS) 2016-2022.

Hoecker Marcos Robledo. Subsecretario de Defensa Secretario Ejecutivo, Comité Interministerial sobre Ciberseguridad, PNCS 2017.

Ruiz Díaz, Joaquín. "Ciberamenazas: ¿El terrorismo del Futuro?", *en IEEE.ES*, Documento de Opinión 86/2016.

Saez Collantes, Luis. *La Ciberguerra en los Conflictos Modernos*, FACH, 2012.

Thauby García, Fernando. "Disuasión y Defensa", *Revista de Marina*, Armada de Chile, 1992.

Unión Internacional de Telecomunicaciones, referida en Alejandro Gómez Abutridy, "Ciberseguridad y Ciberdefensa, Dos elementos de la Ciberguerra", *Memorial del Ejército de Chile*, Nº 492, agosto 2014.

Walters, Gregory. *A New way of War in the Information Age, The Community of Rights in an Information Age*, Centre de Recherche et D'Enseignement, Universsité d'Otawa, mayo 2000.