Capítulo 3

La lógica de la ciberguerra y su relación compleja con la disuasión

René Leiva Villagra[*]

Introducción

En la línea de seguir desarrollando la visualización de impactos de la ciberguerra, caemos en la disuasión, como elemento constitutivo de la estrategia moderna, donde nos indica Torres Soriano que se considera que todos los actores estatales tratan de disuadir a sus potenciales enemigos desarrollando capacidades de respuesta que les permitan sobrevivir y responder militarmente a una agresión previa. Así, por ejemplo, la capacidad de infligir un daño similar o mayor al sufrido neutralizaba el atractivo que algunos contendientes podían encontrar en lanzar un primer ataque.

Este convencimiento fue la base sobre la que, durante décadas, se construyó la estrategia nuclear y que hizo posible que ninguno de los países dotados de estas armas decidiese recurrir a ellas contra otro actor nuclear. Sin embargo, para que dicho equilibro disuasorio sea posible no solo es necesario poseer los medios para el ataque, sino también ser vulnerable a la represalia del enemigo.

* René Leiva es General de Brigada (R) del Ejército de Chile. Oficial de Estado Mayor, Licenciado en Ciencias Militares y Magíster en Ciencias Militares con mención en Planificación y Gestión Estratégica en la Academia de Guerra del Ejército de Chile. Diplomado de la Pontificia Universidad Católica de Chile en Gestión en Educación. Especialista en Inteligencia y Guerra Electrónica. Investigador del Centro de Estudios Estratégicos de la Academia de Guerra del Ejército de Chile en el área de ciberguerra. En el ámbito privado se desempeña como consultor en ciberdefensa para empresas nacionales y extranjeras. rene.leiva@acague.cl; leivarene@yahoo.com

Por ello, ir a una respuesta de la interrogante de cómo se relaciona la ciberguerra con la disuasión pasa a ser una necesidad como aporte al pensamiento estratégico. Acá, como buscará demostrarse, existe una línea relacionada entre estos elementos, que pasa por la vía del entendimiento de las amenazas, para de esa forma ir conjugando ideas de acción respecto de la base del concepto de articular el arte de la estrategia con la tecnología de lo cibernético y sus consideraciones que para con el área de defensa implica.

Es aquí[1] donde empiezan a surgir los problemas cuando hablamos de ciberguerra. Por ello, en el ámbito estratégico surge la pregunta de cómo generar disuasión en el ciberespacio, donde la sorpresa y el secreto son claves, pero donde el requerimiento de exteriorizar en forma creíble y real esa capacidad se da como una situación necesaria y funcional, como factor previo imprescindible al efecto de *deterrence*.

Las ciberarmas son dispositivos de un solo uso, continúa Torres Soriano. La posibilidad de infiltrarse y desbaratar la infraestructura informática del adversario descansa generalmente en el descubrimiento de vulnerabilidades en el diseño de sus sistemas y el *software* que lo mantiene activo. Su utilidad depende directamente de que el potencial atacado desconozca la existencia de estas brechas en su seguridad. Queda, por tanto, descartada la posibilidad de que un actor estatal decidiese hacer una demostración de sus capacidades de ciberguerra con una finalidad exclusivamente disuasoria.

La implementación de un pequeño ataque deja tras de sí un rastro digital, que puede ser estudiado y que permite crear los parches para evitar un nuevo ataque utilizando el mismo procedimiento. De igual modo, las ciberarmas tienen una caducidad muy rápida. Las vulnerabilidades en los sistemas enemigos desaparecen como consecuencia de la continua evolución tecnológica y de programación de unos sistemas en continua actualización.

Hacia una disuasión ciberaplicable

La teoría de la disuasión se basaba en una aplicación creíble y lograble de represalia, que buscaba prevenir que el oponente ataque, porque de hacerlo recibiría castigo por una acción ofensiva que lo destruiría o al menos le generaría un enorme daño.

Esto le plantea a los ciberguerreros el dilema de si deben hacer uso de esta ventaja sobre su adversario antes de que esta desaparezca, sobre todo,

[1] Manuel Ricardo Torres Soriano, *Los Dilemas Estratégicos de la Ciberguerra*, Revista Ejército, España, Nº 839, marzo 2011, pp. 14-19.

si no existe la seguridad de que en el futuro vuelva a poseer esta ventana de oportunidad.

El carácter necesariamente secreto de estas armas, junto con su atractivo para actores incapaces de desafiar convencionalmente a sus adversarios, hace tremendamente difícil que se pueda alcanzar un tratado de control y limitación de ciberarmas. De hecho, la lógica de la ciberguerra no solo hace compleja la disuasión, sino que también beneficia al contendiente que decide tomar la iniciativa y lanzar el primer ataque. El tiempo transcurrido entre la decisión de llevar a cabo el ataque y sus efectos es prácticamente imperceptible, lo que dificulta la existencia de un sistema de alerta temprana y anticipación. Esto crea un entorno estratégico tremendamente inestable, con una elevada posibilidad de iniciar un ciberconflicto como consecuencia de un error, una mala interpretación de las acciones del adversario, o una incorrecta atribución de responsabilidades.

Al analizar la teoría de la disuasión, que en su conjunto estableció el fundamento de las relaciones y estrategias que dieron forma a la Guerra Fría, en esencia se está frente a una capacidad de represalia creíble que puede impedir que los adversarios ataquen, ya que saben que si lo hacen serán destruidos. En ello, Howard define la estrategia de la disuasión como el intento de persuadir a un adversario por medio de la amenaza de una represión, implicando que los costes (para el agresor) de utilizar la fuerza militar para resolver un conflicto político sobrepasarán los beneficios que pudieran obtenerse[2]. En la actualidad se tiende a aplicar la disuasión clásica a la esfera cibernética[3], pero hay mucha confusión acerca de cómo la disuasión funcionaría en ese dominio.

El ámbito de acción de la disuasión no es una panacea y no impide totalmente que adversarios cibernéticos penetren en nuestras redes e infraestructuras. El éxito de la disuasión se reduce a nuestra capacidad de convencer a los adversarios que sus intrusiones cibernéticas implicarán un costo demasiado alto para ellos, pero cuando los objetivos que nos pueden ser batidos son de un alto valor y el agresor no posee mucho que perder, la ecuación costo-beneficio se torna muy favorable para el atacante y le da una condición asimétrica crítica, generando un atractivo índice neto de rentabilidad.

En la llamada guerra asimétrica se miden bandos con fuerzas muy dispares. Es claro que, debido al carácter mortífero del conflicto armado, cada parte buscará la máxima superioridad o asimetría. Más que un término asociado a la desigualdad, o a la incapacidad de un bando débil frente a uno de fuerzas

2 M. Howard Reasurance and Deterrence, *Western Defense in the 1980's*, Foreign Affaires, 61 (winter 1982-1983), p. 315.

3 Rhea Siers, *Mitos de la Ciber Disuasión*, The Cipherbrief.

abrumadoras, la opción asimétrica busca la conformación de desequilibrios mediante recursos que exceden lo convencional e incluso llegan a lo clandestino. Por ello, un enfrentamiento asimétrico[4] a lo que hace referencia es a batallas que tienen lugar entre fuerzas disimilares que utilizan determinados factores o estrategias para alterar el escenario del enfrentamiento y así obtener una ventaja sobre el oponente. Esos factores pueden ser el engaño, la sorpresa, la velocidad, el movimiento, el uso de armas de forma inesperada.

La ventaja (y la voluntad de aprovecharla) es lo que permite a un ejército prevalecer sobre otro. La guerra asimétrica es también un medio con que fuerzas militares inferiores ganan ventaja sobre oponentes más poderosos, o al menos con más recursos. Términos como "no tradicional" o "no convencional" son también utilizados a la hora de definir la guerra asimétrica porque en esta se emplean métodos que no encajan con las imágenes más extendidas de la guerra. También puede ser entendido como guerra asimétrica el uso de nueva tecnología con que una fuerza militar superior derrota a otra fuerza militar inferior. Todos estos elementos podrían combinarse para conseguir una completa definición de la guerra de este tipo (asimétrica), pero tal vez lo más relevante es que lo asimétrico abarcaría todo aquello que altera el campo de batalla, de tal manera que se niega la ventaja del oponente.

El problema fundamental para la Defensa es el cambio que las nuevas tecnologías han producido. Si en el pasado era suficiente con aprovecharse de las nuevas capacidades de los sistemas de información y del ciberespacio para mejorar la eficacia operacional de las Fuerzas Armadas, ahora es necesario poder combatir, y ganar, en el ciberespacio.

La Defensa requiere asegurar las capacidades en el ciberespacio para poder garantizar la efectividad en las operaciones tradicionales. Se ha dicho del ciberespacio que es el campo de batalla del futuro. Este cambio obliga a modificar los conceptos y doctrinas que se aplican a la confrontación clásica, que deben ser adaptados a las exigencias de un escenario virtual. Este proceso adaptativo debe ser el punto de partida para la definición sólida y la creación ordenada de una capacidad de ciberdefensa.

La protección y la defensa del ciberespacio se han convertido en uno de los retos fundamentales para las Fuerzas Armadas de la mayoría de los países, de ahí la necesidad de disponer de ellas adaptadas a un entorno con continuos avances tecnológicos y dentro de un presupuesto cada vez más restrictivo. El riesgo omnipresente de ataques desde el ciberespacio hace prever que en los futuros conflictos las primeras acciones tengan lugar en el ciberespacio.

[4] César Pintado Rodríguez, *De la Guerra (Asimétrica)*, Boletín 55/2014, 19 mayo de 2014, Instituto Español de Estudios Estratégicos.

En lo anterior, el efecto de la ciberguerra tiene una potencialidad de aplicación enorme. A causa de que la ciberguerra va a operar en un escenario de dimensión distinta, que es el ciberespacio, como entorno virtual que contiene los sistemas de redes informáticas, donde se utilizan medios físicos y el espectro electromagnético para interconectarse y realizar el funcionamiento del procesamiento, almacenamiento y difusión de la información requerida por el Sistema de Mando y Control, su dominio puede llegar a constituir un factor multiplicador de las fuerzas, por tanto será un factor que coadyuvará en la concreción del anhelado desequilibrio.

Existen actores en el ciberespacio que poseen capacidad técnica para provocar muchos estragos en un amplio espectro[5]. Muy pocos pueden hacer mucho daño y, por tanto, la ciberguerra es el paradigma de la guerra asimétrica. Cubeiro considera también que, en este ámbito, el esfuerzo del defensor es mayor que el que pueda realizar el agresor. La ciberdefensa es mucho más cara y compleja que el ciberataque. Además, cuanto más técnico-dependiente es una nación, una organización o un ejército, más vulnerables serán a este tipo de agresiones. Más adelante, aseguró que existe un considerable vacío legal en el ciberespacio. Esta ausencia de autoridad favorece al agresor y hace que la trazabilidad del ataque y su origen sean muy difíciles de controlar.

Las fuerzas convencionales, al ser enfrentadas a este tipo de conflicto asimétrico, requieren necesariamente una reconfiguración de sus estructuras, procedimientos, entrenamiento e incluso equipamiento. Por lógica ese tipo de fuerzas estarán conformadas para actuar contra ejércitos de características similares, regulares y convencionales. Al ser el escenario enrarecido por un accionar de medios opositores que agreden desde una dimensión distinta, como lo es el ciberespacio, una fuerza convencional, por grande que sea, podrá hacer poco o nada ante ello. Esto implica que la capacidad de ciberguerra, en sus componentes defensivos, ofensivos y exploratorios, debe ser desarrollada, mantenida y sostenida con antelación, porque de no hacerlo se estará en riesgo real y concreto de ser víctima del desequilibrio que el conflicto asimétrico busque.

Desde que Estonia fue víctima de un ataque cibernético a gran escala en 2007, los países se han vuelto vulnerables a ataques de este tipo, porque la sociedad, la economía y la vida cotidiana son cada vez más dependientes del

5 Enrique Cubeiro, Capitán de Navío, Jefe de Operaciones del Mando Conjunto de Ciberdefensa, *Conciencia nacional de ciberdefensa*, Centro Superior Estudios de la Defensa Nacional (CESEDEN), Jornadas Construyendo la Ciberdefensa en España, http://www.defensa.gob.es/Galerias/gabinete/red/2014/red-306-ciberdefensa.pdf

ciberespacio. Las complejidades y amenazas a la seguridad internacional que vemos diariamente están inmigrando al ciberespacio[6].

Volvemos entonces a la teoría de la disuasión, que sintéticamente es la degradación de una intención agresora sobre la base de la amenaza e imposición de un castigo, lo que opera a lo largo de un conjunto continuo.

Esta relación de poderes opera sobre una base en que es necesaria una línea lógica, donde la racionalidad está presente, donde hay intereses definidos y principales. En ello entonces se actúa para sacar el máximo provecho y reducir al mínimo las posibles consecuencias negativas[7].

Esta teoría entonces depende en buena parte de actores que evalúan las consecuencias a favor y en contra, basándose en la consideración de las acciones y reacciones posibles de cada uno.

La complejidad en ello aparece cuando la racionalidad está ausente y toma protagonismo el arrebato o la intención de daño en ausencia de fortaleza o estructura crítica propia que pueda ser afectada, permitiendo al agresor ser aún más arriesgado en su operación. El ciberterrorismo, usado en la crisis o en el conflicto, como herramienta de ciberguerra será un ejemplo de ello. También lo será el uso de ciberagresión en guerra asimétrica, donde logra una alta relación en la ecuación de beneficio para el que es más débil. Así definido ello, si el agresor tiene poco (como reducidas infraestructura crítica dependiente del ciberespacio, por ejemplo), arriesga poco al ofender, pero es atraído e impulsado a ello por el daño que puede inferir, junto con la dificultad eventual en ser identificado como fuente de la acción agresiva.

Por ello la disuasión nuclear no aplica necesariamente como un referente para la estrategia de ciberguerra. Hay ciertas diferencias significativas entre el poder nuclear y cibernético. Por ejemplo, el "club" cibernético es mucho más amplio que el club nuclear, además de contener un sinnúmero de actores que no son estatales, englobando el ámbito privado, académico, industrial, comercial e incluso individual. Muchos actores, de diferente raigambre, están permanentemente en la línea de defensa contra intrusiones y ataques cibernéticos. Por ello, la disuasión cibernética necesariamente debe contener en su estrategia una respuesta multiparticipativa privada-pública.

Parte de la disuasión será basada en la resiliencia de la red cibernética. Para ello se debe ser capaz de demostrar que hay procesos y recursos para responder a los ataques cibernéticos y contener las interrupciones, con

6 Edgardo Riveros, Subsecretario de Relaciones Exteriores, Seminario Internacional "Ciberseguridad y Ciberdefensa en Chile", 27 de noviembre de 2015, Aula Magna, Facultad de Derecho, Universidad de Chile.

7 Alan Dershowitz, *Por qué aumenta el Terrorismo*, Ediciones Encuentro, Madrid.

respaldos versátiles y robustos, para así desalentar a algunos actores si creen que sus acciones serán menos impactantes de lo previsto.

Las demás condiciones, componentes o requisitos de la disuasión dependen del disuasor. Es pues su responsabilidad que la disuasión funcione. Es decir, que exista. Pues hablar de fallos de la disuasión no es más que una manera impropia de expresarse. Si se produce la agresión es que no se cumplía alguna de las condiciones que crean la disuasión. Entre estas podemos identificar una de carácter físico y varias de carácter psicológico, ya que la disuasión es ante todo un fenómeno psicológico La disuasión está en la mente del disuadido. El disuasor trata de actuar sobre la mente de su enemigo, modificar su cálculo coste-beneficios para que le resulte negativo. El elemento físico es la fuerza disuasora, la capacidad bélica con la que amenazar al potencial agresor y con la que llevar a cabo la réplica o la resistencia si el ataque se produce. Esa fuerza debe ser de tal naturaleza y magnitud que haga la réplica (o resistencia) segura y eleve los costos de la aventura agresora por encima de los posibles beneficios. La probabilidad de la réplica y la cuantía probable de los daños son dos elementos esenciales del cálculo del agresor.

La especulación acerca de cuál es el castigo adecuado para disuadir y qué fuerzas son necesarias para ejecutarlo constituye una parte importante de los estudios acerca de la disuasión, precisamente aquella parte que tiene una mayor incidencia práctica en el diseño de una política de seguridad nacional. Pero lo que disuade es algo contingente. Depende de la evolución de la tecnología militar, de la naturaleza política del potencial agresor, de la correlación o balance de fuerzas y de la situación internacional. Depende, pues, de circunstancias cambiantes[8].

Ciberdefensa y ciberseguridad, conceptualizando

En un paso previo a visualizar algunos esbozos de enfrentamiento o mitigación a la amenaza, se hace necesario conceptualizar la ciberdefensa y la ciberseguridad, que muchas veces son confundidos, pero que tienen segmentos de interpenetración, lo que tiene impacto en sus jurisdicciones, estructuras, potencialidades y rangos de acción.

El concepto de defensa dice relación con la acción y efecto de conservar la posesión de un bien o de mantener un grado suficiente de libertad de acción para alcanzarlo. Entonces, la Defensa Nacional es el conjunto de medios materiales, humanos y morales que una nación puede oponer a las amenazas

8 Manuel Coma, *¿Qué es disuasión?*, Revista de Occidente número 78, noviembre 1987.

de un adversario en contra de sus intereses. Luego, la orientación de empleo de medios para la conformación de una capacidad de ciberdefensa debe ir necesariamente asociado a lo que el concepto de defensa nacional impone, es decir, la consecución de un grado de libertad de acción en el uso del ciberespacio, como también una capacidad de oposición a la ciberamenaza.

Pero en el entendimiento del diseño y alcances de esa capacidad de ciberdefensa se generan confusiones que, más que ser conceptuales o semánticas, tienen impactos en la operacionalización de las acciones y recursos a emplear. Nace entonces la interrogante de la delimitación de la disyuntiva entre ciberdefensa y ciberseguridad.

Ciberdefensa

La ciberdefensa[9] es una connotación sistémica y sistemática que deben desarrollar los gobiernos y sus entes subordinados o asociados, para comprender sus responsabilidades de Estado, en el contexto de un ciudadano y las fronteras nacionales electrónicas o digitales. Un concepto estratégico de los gobiernos que requiere la comprensión de variables como, las vulnerabilidades en la infraestructura crítica de una nación; las garantías y derechos de los ciudadanos en el mundo *online*; la renovación de la administración de justicia en el entorno digital; y la evolución de la inseguridad de la información en el contexto tecnológico y operacional.

Contempla la capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional[10]. Por ello, la ciberdefensa[11] se relaciona con el desarrollo y aseguramiento de capacidades, preocupándose de sus recursos, actividades, tácticas y procedimientos para preservar la seguridad de los sistemas y la información que manejan, así como permitir la explotación y respuesta sobre los sistemas necesarios para garantizar el libre acceso al ciberespacio.

Como realidad complementaria de la ciberdefensa, se materializa el concepto de defensa nacional digital, en un conjunto de variables claves, en las que son necesarias el desarrollo de prácticas primordiales para darle sentido y real dimensión a la seguridad de una nación, en el contexto de

9 Jeimy Cano 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), pp. 4-7.

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

11 Jeimy Cano, *Ciberdefensa y Ciberseguridad, desafíos emergentes para los profesionales de Gobierno*, CFE, ECOPETROL.

una realidad digital y de información instantánea. Por ello, la ciberdefensa contendrá un conjunto de acciones de defensa activas, pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al adversario en oposición.

Correlaciona entonces "un dominio global y dinámico dentro del entorno de la información, compuesto por una infraestructura de redes, de tecnologías de información y telecomunicaciones interdependientes, que incluye Internet, los sistemas de información y los controladores y procesadores integrados, junto con sus usuarios y operadores". Es de notar que incluye a usuarios y operadores, en realidad redundante, pues los sistemas por definición ya incluyen a las personas y los procedimientos.

Por ello, la ciberdefensa va notoriamente ligada al desarrollo y aseguramiento de capacidades.

Enfocándose en la conceptualización de ciberdefensa para el ámbito de la Defensa Nacional, estas son puntualizadas como "el conjunto de acciones en contra de ataques al Estado en el ciberespacio que se orientan a la defensa y supervivencia de sistemas militares"[12], materializándose mediante ciberoperaciones que otorgan la capacidad para operar militarmente en el ciberespacio donde la presencia en lo específico de ciberamenazas pueden afectar los sistemas C4I, redes de datos, nodos de comunicación, centros de procesamiento y lugares de almacenamiento de información, por lo que cumplen con los propósitos de seguridad (protección), inteligencia (recolección de información de la amenaza) y de respuesta (operaciones).

Por este motivo, las ciberoperaciones pueden ser ofensivas o defensivas, donde las primeras son acciones de respuesta sobre sistemas de información y comunicaciones adversarias, y las segundas corresponden a medidas preventivas, reactivas y de gestión de riesgo para dar protección a los sistemas, servicios y datos propios. De esta forma, el objetivo de estas operaciones será aportar a la solución del problema con una intencionalidad y un efecto deseado.

Ciberseguridad

Por su parte la ciberseguridad[13] puede ser entendida como el conjunto de actividades dirigidas a proteger el ciberspacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan. Entonces, asegura el uso de las redes propia y niega su empleo a terceros.

12 Santiago Aguayo, *Operaciones de Ciberdefensa*, Tesis ACAGUE, 2017.
13 Op. cit. Jeimy Cano.

A mayor abundamiento, el concepto de ciberseguridad es descrito[14] como "El conjunto de herramientas, políticas, conceptos de seguridad, directrices, métodos de gestión, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de una organización y a los usuarios en el ciberentorno". Por ello, comporta un conjunto de acciones de carácter preventivo que tienen por objeto asegurar el uso de las redes propias y negarlo a terceros[15].

La UIT (Unión Internacional de Telecomunicaciones) dice que la ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos, cuales son amenazas de seguridad correspondientes en el ciberentorno. Luego, entendiendo que la problemática de la ciberseguridad requiere un esfuerzo colectivo y coordinado entre los diferentes países, establece cinco elementos fundamentales para desarrollar una estrategia de ciberseguridad, acorde con la realidad de cada una de las naciones: desarrollo de un marco legal para la acción, desarrollo y aplicación de medidas técnicas y procedimentales, diseño y aplicación de estructuras organizacionales requeridas, desarrollo y aplicación de una cultura de ciberseguridad y la cooperación internacional.

Figura 1
Elementos de una estrategia de ciberseguridad

Fuente: Elaboración propia.

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

15 http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf

La ciberseguridad consta de tres elementos fundamentales que forman parte de los objetivos que intentan afectar los potenciales atacantes. Estos son la confidencialidad, la integridad y la disponibilidad de los recursos, CIA (Confidentiality-Integrity-Availability).

Sintéticamente entonces, la ciberseguridad puede ser definida como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética[16].

Por ello, la ciberseguridad va notoriamente ligada al desarrollo y aseguramiento de prácticas.

Debido a lo indicado, podemos concluir que la ciberseguridad tiende a ser un objetivo y la ciberdefensa apunta a ser un medio para su concreción.

En una analogía de los conceptos de Seguridad Nacional y Defensa Nacional, que sabemos se encuentran férreamente relacionados; también la ciberseguridad y la ciberdefensa en términos generales están estrechamente vinculados, la diferencia consiste en que la segunda tiene como propósito preservar la ciberseguridad, haciendo frente a un conjunto particular de riesgos y amenazas, los que identificados, controlados, neutralizados o contenidos darán paso a una condición de ciberseguridad.

Por ello, esa separación de aguas no es tan simple de delimitar, porque en la acción de la ciberdefensa de dar cabida a la condición de ciberseguridad, existirán espacios de interpenetración o traslapo, con áreas comunes donde ambos elementos se interrelacionan.

Acá es bueno traer a referencia a Feliú, quien acota que la ciberseguridad resulta ser un componente o aspecto muy importante de la Seguridad Nacional: Si no se controla adecuadamente el ciberespacio, desde allí una nación puede ver amenazada su libertad de acción y su Seguridad, no solo su ciberseguridad sino toda la Seguridad Nacional. El ciberespacio es pues un espacio estratégico a considerar al establecer la Estrategia de Seguridad y, como consecuencia, al planear la correspondiente Defensa Nacional, por lo que habrá que definir en ella los objetivos a alcanzar y las medidas de prevención, disuasión, protección y reacción de la ciberdefensa.

También la ciberseguridad y la ciberdefensa tienen puntos de encuentro en la forma cómo impulsan, aglutinan y coordinan los diferentes estamentos del Estado (incluidas sus Fuerzas Armadas y Policía), privados y académicos para generar un uso con libertad de acción del ciberespacio. Independiente de quién lidere estos esfuerzos, lo importante es que exista el concepto de empleo interagencial o multiactores, porque los esfuerzos de compartimientos

16 Op. cit. Consejo Nacional de Política Económica y Social de Colombia.

estancos poco o nada podrán hacer contra una amenaza que se presentará asimétrica, artera y sorpresiva.

Por ello se insiste que la ciberdefensa camina de la mano del desarrollo de las capacidades y la ciberseguridad del aseguramiento de las prácticas.

Infraestructuras de información de Defensa

Es entendida como un sistema interconectado de computadores/ordenadores, comunicaciones, aplicaciones de *data*, seguridad, personal, entrenamiento y otras estructuras que sirven a un sistema de defensa.

Luego, este proceso de manipulación por parte de un agresor 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[17]:

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.

La seguridad de las infraestructuras críticas

Las infraestructuras críticas, por definición, son sistemas físicos y basados en sistemas computacionales complejos que forman parte importante en una sociedad moderna y su funcionamiento fiable y seguro es de suma importancia para la vida económica y la Seguridad Nacional[18]. Si llegase a ocurrir un

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

18 TEN, Chee-Wooi and LIU, Chen-Ching. *Cybersecurity for Critical Infrastructures: Attack and Defense Modeling*. IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans. July 2010. Vol. 40, no. 4, pp. 853-865. DOI 10.1109/TSMCA.2010.2048028.

incidente de seguridad en estos sistemas podría tener incluso conmoción a nivel nacional[19], consecuencias en los sistemas físicos que dependen de tales sistemas y mucha conmoción en la vida de los ciudadanos.

La seguridad física de la infraestructura de las plantas estratégicas es muy importante para evitar actos vandálicos comunes en subestaciones o plantas de gas. Sin embargo, la seguridad en redes es tan importante como la seguridad física, debido al impacto potencial que se puede alcanzar al manipular maliciosamente, por ejemplo, los sistemas remotos (SCADA o PLC-Programmable Logic Controller) de una planta eléctrica, de agua, gas, petróleo, cobre u otro tipo.

En seguridad informática, una vulnerabilidad implica que existen puntos débiles en la infraestructura tecnológica, políticas o de procedimientos, por lo que un atacante puede utilizar un conjunto de aplicaciones o métodos para romper la seguridad y explotar los puntos débiles en las redes y comprometer los sistemas. Por ello, la seguridad como tal está conformada por la confluencia de tres características[20], una tríada, que la configuran como tal, siendo estas: confidencialidad (*confidentiality*), integridad (*integrity*) y disponibilidad (*availability*).

La confidencialidad se refiere a mantener la *data* fuera de manos no autorizadas para su uso, empleo o conocimiento.

La integridad se orienta a la modificación no autorizada de *data* o funciones del sistema.

La disponibilidad corresponde a la capacidad de acceder a determinada *data* cuando ello es necesario.

Una de las actividades extendidas en ambientes de redes IT, para poder aplicar contramedidas a estas vulnerabilidades, consiste en adelantarse a las acciones maliciosas y realizar una intensiva búsqueda de brechas antes que un atacante real las descubra primero.

Un análisis de vulnerabilidades o *Ethical Hacking* es un buen comienzo para descubrir problemas de seguridad en redes y sistemas SCADA y pueden ser aplicados sin mayor inversión. Este tipo de actividad se puede transformar en el primer paso de un programa de seguridad informático con un enfoque holístico y de proceso para la administración de la infraestructura crítica.

En cuanto a infraestructuras críticas, y su definición de infraestructura de la información, es conformada por las personas, procesos, procedimientos,

[19] Juan Anabalón y Eric Donders, *Una Revisión de Ciberdefensa de Infraestructura Crítica*, Trabajo de titulación para obtener el grado de Magíster en Seguridad, Peritaje y Auditoría en Procesos Informáticos de la Universidad de Santiago de Chile.

[20] J. Andress (2011). Cyber Warfare, Techniques, Tactics and Tools for Security Practitioners, Estados Unidos, Syngress.

Figura 2
Triada de la seguridad

Fuente: Cyber Warfare, Techniques, Tactics and Tools for Security Practitioners.

herramientas, instalaciones y tecnologías que soportan la creación, uso, transporte, almacenamiento y destrucción de la información. Dentro de las infraestructuras de la información, existe un conjunto especialmente relevante para la marcha del país, las denominadas infraestructuras críticas de la información (ICI), que comprende las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación, interrupción o destrucción pueden tener una repercusión importante en la seguridad, la salud, el bienestar de los ciudadanos y el efectivo funcionamiento del Estado y del sector privado. Las ICI se deberán robustecer, resguardar y diseñar para que sean seguras y resilientes frente a eventos que las puedan inhabilitar, adaptándose a cambios en el medio ambiente, a intervenciones humanas o interferencias informáticas, como incidentes involuntarios o ciberataques.

En cuanto a la identificación y jerarquización de las infraestructuras críticas de la información, aporta que los sectores que componen la clasificación de ICI son muy similares y se repiten en varias clasificaciones a nivel internacional. Luego, en una visión particular, esta determina que la infraestructura de la información de los siguientes sectores sea considerada como crítica: energía, telecomunicaciones, agua, salud, servicios financieros, seguridad pública, transporte, administración pública, protección civil y defensa, entre otras. Entonces, en algunos Estados ya existe una definición oficial para lo que es contenido bajo la categorización de infraestructura crítica de información,

determinada por las 10 áreas que enuncia, aun cuando queda abierta a "otras".

Al hablar de infraestructura crítica, como vemos, surge repetitivamente el concepto SCADA, que corresponde a *Supervisory Control and Data Acquisition*. Obedece a un concepto que mediante un *software* para ordenadores permite controlar y supervisar procesos industriales remotamente. Su diseño tiene la ventaja de entregar retroalimentación en tiempo real con los dispositivos desplegados en la instalación o terreno (sensores y actuadores), y controla el proceso automáticamente. Provee de toda la información que se genera en el proceso productivo (supervisión, control de calidad, control de producción, almacenamiento de datos, etc.) y permite su gestión e intervención.

Entre los procedimientos de acción remota están HMI (interfaz hombre-máquina) y SCADA, los que están relacionados entre sí en la medida en que uno o varios HMI son subconjuntos o componentes de un sistema SCADA[21]. Además, un DCS o Sistema de Control Distribuido es muy similar a un sistema SCADA, y también puede utilizar uno o más HMI también. Todos estos componentes son clases de, o describen partes de, un ICS o Sistema de Control, que es la descripción general de la automatización. En los sistemas de control modernos hay una gran cantidad de tecnología y funcionalidad entre estas dos clases de ICS.

Un sistema SCADA involucra control directo o comunicarse con uno o más de los siguientes:

Redes de automatización industrial y máquinas
Telemetría y control remoto utilizando comunicaciones continuas o ráfaga
Sistemas de control de procesos y control de procesos estadísticos
Sistemas de adquisición de datos (DAQ)
Históricos y servidores de almacenamiento de datos
Sistemas de control industrial utilizando PLC y RTU
Sistemas del entorno empresarial, como sistemas ERP y MES
Entorno de computación de nube industrial
Sistemas de seguridad y procesos
Seguridad de máquina local
Seguridad y control de procesos
Conectividad empresarial o global que implica LDAP y otros.

Un sistema SCADA puede estar conectado continuamente a todos los componentes en el ICS, o puede estar intermitentemente conectado a

21 Schneider Electric, ¿Cuál es la diferencia entre SCADA y HMI?

algunos o todos, y se actualiza con una ráfaga de comunicación por medio de módems de radio o celular (tecnologías 2G, 3G o 4G, CDMA y GSM, otras) a los dispositivos y equipos de campo. Así el SCADA suele tener uno o más servidores que contienen una aplicación que se está comunicando con una ejecución en conjunto con componentes inteligentes, independientemente del sistema SCADA.

Un Sistema de Control Industrial como se describe pueden conectarse entre sí mediante (uno o más de los siguientes) conexiones en serie, redes propietarias y/o Ethernet, LAN, WAN y/o la nube y puede incluir componentes externos ampliamente dispersos y/o instalaciones; incluir procesos tales como sistemas MES y ERP, Control de procesos y datos de historiadores, JIT y otros fabricantes de conectividad aguas arriba/aguas abajo, etcétera.

Debido a que los HMI, SCADA y sistemas de control son usados en muchos tipos de infraestructura que es crítica, su ventana de conectividad pasa a ser un blanco susceptible de una ciberagresión. La intrusión buscará penetrar los puertos de proceso directo y control de máquinas, automatización, seguridad, almacenamiento y análisis de datos, servicios de explotación indirectos, como el control de entrada / salida, comunicaciones y video, y conectividad a una variedad de funciones dentro del sistema de producción o servicio.

La seguridad en los sistemas SCADA anteriormente se mantenía físicamente, es decir, solo las personas con permisos de acceso a las instalaciones podían obtener los datos, por tanto la seguridad computacional no era preocupante.

La convergencia de las redes de datos industriales con las redes de datos de TI ha proporcionado nuevas vías de acceso a estos sistemas, lo que implica a su vez que los riesgos de seguridad asociados históricamente a las redes IT ahora también son de preocupación de las redes operacionales (OT)[22].

El problema fundamental de los sistemas SCADA, ampliamente utilizados en infraestructuras críticas, es que nunca fueron pensados ni diseñados con sistemas de seguridad informática, ni tampoco se han elaborado con la mentalidad de seguridad desde el proceso mismo de desarrollo de *software*, algo que incluso aún no se considera completamente en el proceso de diseño de programas para sistemas que no son de la naturaleza de los sistemas de control industrial[23]. Muchos sistemas SCADA utilizan sistemas de autenticación muy básicos, sin protocolos de cifrado de datos e infraestructura con muchos *bugs* de seguridad y totalmente desactualizada, este escenario se agrava por

[22] Op. cit. Juan Anabalón y Eric Donders.

[23] Daniel Mellado, Eduardo Fernández-Medina, and Mario Piattini,. Security requirements engineering framework for software product lines. Information and Software Technology. October 2010. Vol. 52, no. 10, p. 1094-1117. DOI 10.1016/j.infsof.2010.05.007.

el hecho de que la actualización de una plataforma muchas veces implica la actualización de sistemas relacionados, lo que para la industria energética y otra infraestructura crítica es casi imposible desarrollar sin detener los servicios que provee[24].

En Chile se han desarrollado algunos estudios de infraestructura crítica a nivel gubernamental por distintas secretarías de Estado. En el caso de la infraestructura crítica de telecomunicaciones se refiere a "aquellas redes cuya interrupción o destrucción podría producir un serio impacto en la salud, seguridad o bienestar de la población o producir un serio impacto en el funcionamiento del gobierno o de la economía del país"[25].

En este sector, los elementos de red más críticos corresponden a las redes de transporte de la señal de comunicaciones, ya que están seriamente expuestos a amenazas de tipo físico debido a que sus componentes están emplazados en espacios no controlados. Estas redes cuentan con respaldos de otros operadores, sin embargo la cercanía que existe entre sí, en ciertos tramos, reducen la efectividad esperada. Además, existen sitios (edificios) de los distintos operadores altamente concentrados en cuanto a redes y nodos, que los transforman en importantes puntos de falla en caso de amenazas. Sin embargo, los operadores de telecomunicaciones trabajan cooperativamente y se respaldan mutuamente y cada operador cuenta con los sistemas de protección en sus redes y nodos que permiten proveer servicios con alto nivel de disponibilidad.

En este actuar, estudio, diseño, planificación, conducción y evaluación concurren no solo militares sino que también civiles, participando como unidades u organizaciones estructuradas (no necesariamente reconocidas), pasando por células aisladas pero orientadas desde un nivel coordinador superior, hasta el ciberguerrero aislado (*broken arrow*).

Amenazas en el ciberespacio

La amenaza es definida[26] como "la percepción de la capacidad que un potencial adversario posee para infligir un daño o perjuicio, especialmente si

[24] Op. cit. Juan Anabalón y Eric Donders.

[25] Zagreb, Consultores Ltda., Subsecretaría de Telecomunicaciones y Ministerio de Transporte y Telecomunicaciones. Estudio para la definición e identificación de infraestructura crítica de la información en Chile. Diciembre 2008.

[26] Op. cit. Santiago Aguayo, Operaciones de Ciberdefensa.

no se actúa como él desea"[27]. Complementa esto Timothy K. Buennemeyer[28] al aportar una definición que logra relacionar ciberespacio y amenaza, estableciendo que "El ciberespacio se ha transformado rápidamente en un ambiente volátil, incierto, complejo y ambiguo, donde los gobiernos, empresarios e individuos requieren un balance de información que contemple la trilogía de confidencialidad, disponibilidad e integridad, en orden a establecer un modelo de seguridad de la información estable". Agrega que "la confidencialidad es el término usado para describir la prevención de difusión de información a individuos o sistemas no autorizados". Continúa aportando que en seguridad de la información, integridad implica que la *data* no puede ser modificada sin que ello sea detectado. Del análisis de esta expresión se deduce que existe una caracterización del ciberespacio y su entorno, como también las actividades que se deben realizar para impedir su afectación por parte de las amenazas, que considerará ciertas acciones destinadas a impedir la divulgación de información virtual a las personas o sistemas no autorizados, pese a que no se entrega una definición de cuáles son.

Así pues, el desarrollo del ciberespacio ha facilitado enormemente el impulso de toda clase de actividades, incluyendo interacciones comerciales, sociales y gubernamentales[29], constituyendo una dimensión importante para los Estados, organizaciones y las personas y, por consiguiente, la seguridad del ciberespacio ha crecido en importancia frente a las amenazas. "Debido a que la sociedad actual depende ampliamente de las tecnologías de la información (TI), esto conlleva la irrupción de nuevas amenazas desconocidas en el pasado. En virtud del carácter global de las redes, los incidentes de seguridad de las TI que les afecten, pueden ocasionar interrupciones o fallos permanentes en la infraestructura de información del país"[30]. Esto deja en evidencia la vinculación de la información que circula por medio de las redes respecto de potenciales amenazas en este escenario virtual, que asociándolos al entorno en que se originan entran en la definición de "ciberamenazas".

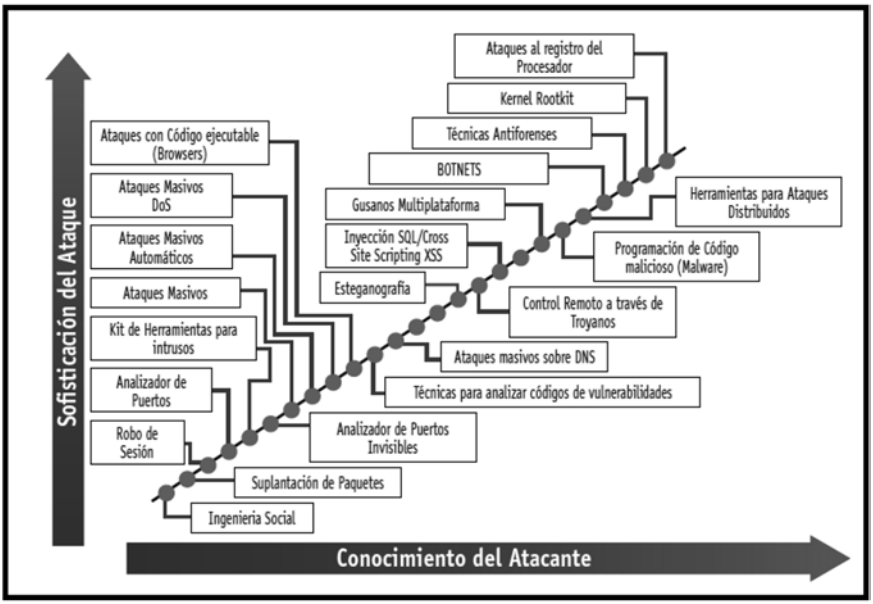
27 Luis Feliú Ortega. "La Ciberseguridad y La Ciberdefensa". En Monografías del CESEDEN Nº 126. El Ciberespacio. Nuevo Escenario de Confrontación, de Centro Superior de Estudios de la Defensa Nacional. Madrid: Imprenta del Ministerio de Defensa, 2012, p. 40.

28 Timothy K. Buennemeyer, "A Strategic Approach to Network Defense: Framing the Cloud". Parameters 45, no. 3 (Autumn, 2011) ProQuest Military Collection p. 45.

29 José L. González Cussac, "Estrategias legales frente a las Ciberamenazas", en *Cuaderno de Estrategia* Nº 149 Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio, de Instituto Español de Estudios Estratégicos, Madrid: Imprenta del Ministerio de Defensa, 2010, pp. 259-322.

30 P. Acosta, "Seguridad nacional y ciberdefensa" (2009). http://catedraisdefe.etsit.upm.es/wp-content/uploads/2010/07/CUADERNO-N%C2%BA-6.pdf.

Figura 3
Conocimiento del atacante vs. sofisticación del ataque



Fuente: "Ciberdefensa y ciberseguridad: dos elementos de la Ciberguerra" (Memorial del Ejército de Chile, agosto, 2014).

En este contexto y considerando la tipología de las amenazas que pueden afectar a los sistemas[31], estas pueden ser agrupadas en:

- Desastres naturales.
- Amenazas de origen industrial.
- Errores o fallos no intencionados.
- Ataques deliberados.

No obstante las amenazas asociadas a desastres naturales, las de origen natural y las relacionadas con errores o fallos no intencionados siempre estarán presentes, es necesario profundizar en los ataques deliberados, porque su sofisticación, precisión y posible impacto está en continua evolución y elevan el nivel de riesgo al que están sometidos los sistemas.

Dependiendo de la motivación de dichos ataques, estas amenazas pueden ser agrupadas en los siguientes tipos:

31 Op. cit. Ricardo Mesa Illés, archivo CEEAG, 2016.

- **Cibercrimen**: centradas en la obtención de beneficios económicos mediante la realización de acciones ilegales.
- **Ciberespionaje**: centradas en la obtención de información, sea para beneficio propio o para obtener un beneficio monetario posterior a su venta.
- **Ciberterrorismo**: donde se busca un impacto significativo mediante la destrucción física. Así las infraestructuras críticas pueden ser uno de los objetivos más probables de ser atacados.
- **Ciberguerra**: la lucha o el conflicto entre dos o más naciones o diferentes bandos dentro de una nación, donde el ciberespacio es el campo de batalla.
- **Hacktivismo**[32] **o ciberactivismo**: que también podría ser considerado como un campo de acción de la ciberamenaza (Escuela de Altos Estudios de la Defensa, 2014).

Asimismo, tomando en consideración las motivaciones de las fuentes de dichas amenazas y su probabilidad de ocurrencia, es que estas se pueden clasificar en:

- Cibercriminales.
- Espías industriales.
- Hacktivistas.
- Terroristas.
- Naciones.
- Hackers.
- Personal interno.

Por otra parte, las motivaciones, que pueden ser independientes del origen de la amenaza, podrían clasificarse en:

- **Beneficios económicos**: es la más usual en el ciberespacio y consiste en la realización de actos fraudulentos, robo y venta de información o la ejecución de ataques.
- **Ventaja táctica o competitiva**: una forma de llevarla a cabo es mediante el robo de información de una nación en medio de un conflicto y que

[32] El hacktivismo es la piratería motivada políticamente llevada a cabo por grupos como Anonymous o LulzSec. Se trata de ataques que tienen como objetivos interrumpir la actividad normal de las instituciones públicas y aquellos organismos contrarios a los valores defendidos por estas agrupaciones de personas. http://www.pcworld.com.mx/Articulos/23891.htm.

puede dar una ventaja táctica al enemigo. Las naciones y los espías son los agentes con más probabilidad de tener esta motivación.
- **Motivaciones políticas**: diferentes organizaciones podrían atacar o realizar acciones perjudiciales contra los gobiernos u organizaciones públicas.
- **Destrucción o daño**: esta motivación puede ser asociada a terroristas, ya que pueden buscar la ejecución de ataques que tengan este efecto. Las naciones en conflicto también podrían estar dentro de este grupo.
- **Fama o venganza**: principalmente ligada a los *hackers*[33] que buscan reconocimiento dentro de sus comunidades. Su objetivo no es causar daño, aunque podrían acceder a información sensible.

La Organización del Tratado del Atlántico Norte (OTAN) a partir del 2010, consciente del riesgo de las ciberamenazas, creó un plan estratégico que consideraba que los ciberataques estaban entre las tres amenazas más probables a la Alianza. Lo anterior se basa en la tendencia general que establece que a mayor desarrollo de un país existirán una mayor cantidad de elementos vulnerables que afecten a su seguridad, aumentando proporcionalmente la exposición frente a estas amenazas, concibiéndose algunas acciones para defenderlas, lo que es inclusivo para los sistemas C4I de cualquier nivel, ya que son altamente dependientes del ciberespacio, no tan solo en el ámbito militar, sino además como parte de las denominadas infraestructuras críticas de una Nación.

Concordemente, esta perspectiva ya se encuentra estipulado en las Tendencias estratégicas globales del Ministerio de Defensa de Gran Bretaña hacia el 2045 publicadas en el 2014, donde se aprecia una declaración al respecto y que orienta una visión estratégica en esta política sectorial, al establecerse que "existirá un incremento en la amenaza de ciberataques provenientes de criminales y terroristas, toda vez que la infraestructura crítica nacional se vuelve más integrada a las plataformas de información y comunicación[34]".

De modo que, de acuerdo con lo expresado por González Cussac[35], la concepción de ciberamenazas estará conformada por los ataques perpetrados

[33] Un *hacker* es aquella persona experta en alguna rama de la tecnología, a menudo informática, que se dedica a intervenir o realizar alteraciones técnicas con buenas o malas intenciones sobre un producto o dispositivo. http://www.definicionabc.com/tecnologia/hacker-2.php. (último acceso: 18 de diciembre de 2015).

[34] United Kingdom's Ministry of Defence, "Strategic Trends Programme Global Strategic Trends-Out to 2045" (en línea) [fecha de consulta 20.08.2016] https://www.gov.uk/government/publications/global-strategic-trends-out-to-2045.

[35] José L. González Cussac, "Estrategias legales frente a las Ciberamenazas", en *Cuaderno de Estrategia* Nº 149 Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio,

o patrocinados por Estados (ataques a infraestructuras críticas), ataques cometidos por grupos terroristas o por cualquier otra manifestación de extremismos, ya sean políticos, ideológicos o religiosos. Al respecto, surgen los ataques de la delincuencia organizada denominado "cibercrimen" y, por último, los ataques de bajo perfil, los que por su naturaleza muy heterogénea afectan transversalmente a las personas incluyendo desde intromisiones en la información personal hasta pequeños fraudes.

En síntesis, el ciberespacio es la expresión de un espacio virtual y vital para que exista la transmisión de la información, razón por lo que se desarrollarán sucesivas acciones de amplia variedad para ejercer el control y la protección de las redes informáticas, originando por consecuencia la necesidad de asegurar el funcionamiento de estos sistemas frente a diversas amenazas, definidas como ciberamenazas; cuyos efectos son traslapados desde lo virtual a lo físico generando en los Estados y sus habitantes múltiples e insospechadas consecuencias que afectan los derechos de las personas, las infraestructuras críticas de la información y, por esta razón, los intereses vitales de Chile a nivel nacional e internacional.

Respecto de la clasificación y estratificación de amenazas, el CARI (Consejo Argentino para las Relaciones Internacionales) genera un muy completo trabajo académico que es traído como referencia. En su caracterización de las amenazas[36] da cuenta de una estructuración de acuerdo con diferentes elementos distintivos, como sigue:

Amenazas por el origen

El hecho de conectar una red a un entorno externo nos da la posibilidad de que algún atacante pueda entrar en ella, con esto se puede hacer robo de información o alterar el funcionamiento de la red. Sin embargo el hecho de que la red no esté conectada a un entorno externo, como Internet, no nos garantiza la seguridad de la misma. De acuerdo con el Computer Security Institute (CSI) de San Francisco, aproximadamente entre el 60 y 80 por ciento de los incidentes de red son causados desde dentro de la misma. Basado en el origen del ataque podemos decir que existen dos tipos de amenazas:

de Instituto Español de Estudios Estratégicos. Madrid: Imprenta del Ministerio de Defensa, 2010, p. 93.

36 Ciberdefensa-Ciberseguridad Riesgos y Amenazas CARI. Noviembre 2013.

Amenazas externas y amenazas internas

***Amenazas internas**:* generalmente estas amenazas pueden ser más serias que las externas. Los usuarios o personal técnico conocen la red y saben cómo es su funcionamiento, ubicación de la información, datos de interés, etc. Además tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo, lo que les permite unos mínimos movimientos. Los sistemas de prevención de intrusos o IPS, y *firewalls* son mecanismos no efectivos en amenazas internas, porque habitualmente no están orientados al tráfico interno.

***Amenazas externas**:* se originan fuera de la red local. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos. Para clasificarlo como externo debe ser exclusivamente por personas ajenas a la red, podría ser por vulnerabilidades que permiten acceder a la red: rosetas, *switches* o *Hubs* accesibles, redes inalámbricas desprotegidas, equipos sin vigilancia, etcétera.

Amenazas por el efecto: el tipo de amenazas por el efecto que causan a quien recibe los ataques podría clasificarse en robo de información, destrucción de información, anulación del funcionamiento de los sistemas o efectos que tiendan a ello, suplantación de la identidad, publicidad de datos personales o confidenciales, cambio de información, venta de datos personales, etc. robo de dinero, estafas, otras.

Amenazas por el medio utilizado: se pueden clasificar por el *modus operandi* del atacante, si bien el efecto puede ser distinto para un mismo tipo de ataque. En esta clasificación tienen cabida los virus informático o *malware*, que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus habitualmente reemplazan archivos ejecutables por otros infectados con el código de este, así pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos (*Worms*, *BOTs*, *Adware*, *Cookies*, *Phishing*, etc.).

Los atacantes pueden tener a su favor el tiempo de preparación, prácticamente sin límite. Sus campañas, que con frecuencia aprovechan las vulnerabilidades conocidas que las organizaciones y los usuarios finales pueden tener –y deberían conocer y abordar– permanecen activas e inadvertidas durante días, meses o incluso más tiempo. Los defensores, mientras tanto se esfuerzan para obtener visibilidad de la actividad en torno a las amenazas y por reducir el tiempo de detección (TTD) de las amenazas nuevas y conocidas[37].

[37] http://www.cisco.com/c/dam/m/es_mx/offers/assets/pdfs/cisco_2016_mcr_es-xl.pdf

Las principales ciberamenazas[38]

Ataque DDoS	Saturar un servidor haciendo más conexiones de las que puede soportar. En 2014, una compañía energética española fue víctima de un ataque mediante ordenadores zombis, infectados por un troyano. Duró tres horas y se recibieron 119 millones de conexiones que tumbaron el servicio.
Troyanos	Como el caballo de Troya, entran subrepticiamente en un sistema. Aprovechan una puerta trasera para ejecutar programas sin permiso.
Gusanos	Virus capaces de duplicarse por sí mismos y de hacer que las máquinas que los hospedan sean cada vez más lentas.
Keyloggers, stealers	Programas para robar datos.
Botnets	Redes de ordenadores infectados o zombis. Pueden, por ejemplo, hacer millones de clics en un *banner* haciendo creer al cliente que su promoción está teniendo éxito, cuando no es así.
Amenaza avanzada persistente	Conjunto de procesos informáticos sigilosos y continuos, dirigidos sobre todo a romper la seguridad informática de una empresa para realizar espionaje industrial o encontrar vulnerabilidades de seguridad.
Backdoor	Puerta trasera, entrada en un PC sin ser detectado, generalmente para someterlo a un acceso remoto.
Drive by downloads	Sitios que instalan códigos (*spyware*) que dan información de los equipos sin que se percate el usuario.
Ransomware	Programas que hacen inaccesibles archivos. Cifran, por ejemplo, el disco duro. El ciberagresor pide un rescate para que el afectado pueda recuperar la información.
Ataque de día cero	Es un ataque contra una aplicación o sistema que ejecuta código malicioso gracias al conocimiento de vulnerabilidades que son desconocidas para la gente y el fabricante del producto. Esto supone que aún no se conocen antivirus o herramientas para repararlas.

[38] http://www.xlsemanal.com/conocer/20150719/cuartel-general-antihackers-8672.html

Reflexiones finales

El ciberespacio ha pasado a constituir un factor estratégico que requiere la imperiosa atención permanente del ámbito de la defensa, orientando a ser incorporada y mantenida dentro de la estrategia de seguridad de todo Estado, llamando así a definir en ella objetivos por alcanzar medidas de prevención, disuasión, protección y reacción de la ciberdefensa, que generen un centinela estructural que vele por amenazas dinámicas que se caracterizan por su sofisticación, precisión y grado de impacto, lo que está en continua evolución y elevan el nivel de riesgo al que están sometidos los sistemas.

La ciberdisuasión impone una visión moderna de aplicación, porque es inviable hacer una demostración de capacidades de ciberguerra con una finalidad exclusivamente intimidatoria, desafiante o de potencial coacción. Así, la lógica de la ciberguerra entrega ventajas comparativas al contendiente que decide tomar la iniciativa y lanzar el primer ataque, porque técnica y estratégicamente la existencia de un sistema de alerta temprana y anticipación es muy difícil, como también el concepto de "profundidad estratégica", en su vertiente clásica, está ausente. Esto crea un entorno estratégico marcado por la incertidumbre, tremendamente inestable, donde el éxito de la disuasión se potenciará por nuestra capacidad de convencer a los adversarios que sus intrusiones cibernéticas implicarán un costo demasiado alto para ellos, evento ante el cual aún podremos seguir operando por contar con un grado de resiliencia, pese a que esta sea local, parcial, temporal e imperfecta.

De no haber optado por la iniciativa, en su analogía de dar el primer cibergolpe, uno de los cursos de acción a considerar es la respuesta en masa, concatenada en el máximo de medios simultáneos, sobre efectos vinculados y orientados principalmente a infraestructura crítica, solución que debemos tener en vista tanto para un enfoque ofensivo como defensivo del problema estratégico.

Bibliografía

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

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.

Aguayo Santiago. *Operaciones de Ciberdefensa*, Tesis ACAGUE, 2017.