David Eduardo Acosta R., CISA, CISM, CRISC, BS25999 LA, CCNA Security, CHFI Trainer, CISSP, PCI QSA, OPST, es consultor en seguridad de la información. Pertenece al cuerpo de Oficiales Profesionales de Reserva del Ejército Nacional de Colombia como Teniente. Trabaja actualmente con Internet Security Auditors en Barcelona (España). Puede ser contactado en *dacosta@ieee.org.*

"Posición Estratégica Defensiva" en el Campo de Seguridad de la Información

La invencibilidad es una cuestión de defensa, la vulnerabilidad, una cuestión de ataque.
—Sun Tzu

Also available in English
www.isaca.org/currentissue

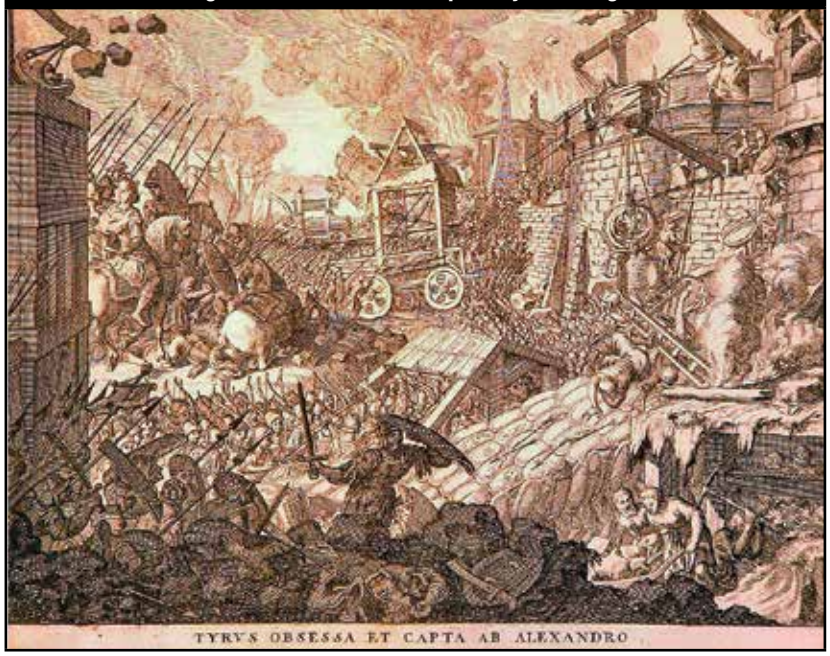
Mucho tiempo lleva hablándose de la aplicabilidad de los pensamientos militares en el ámbito de la seguridad de la información. Desde las teorías de Sun Tzu, pasando por la doctrina militar de Clausewitz, se han equiparado los conceptos militares de estrategia, operación y táctica con las actividades propias de la protección y gestión de riesgos de la información. Igualmente, estos conceptos han sido aplicados de forma efectiva en áreas tan diversas como la política, el mercadeo, la estrategia empresarial y en cualquier escenario donde se presente la necesidad de obtener ventaja entre actores con intereses enfrentados.

Desde una perspectiva de análisis de conflictos, cualquier situación que rompa un equilibrio de tranquilidad previo o *statu quo* (necesidades satisfechas) siempre tiene dos componentes: un componente ofensivo y un componente defensivo. Precisamente la estrategia militar nos indica cómo emplear el uno y el otro frente a determinadas situaciones con el fin lograr la consecución de los objetivos que motivaron dicha confrontación. En función de dichas estrategias y tácticas, así como de las capacidades defensivas y ofensivas de los actores involucrados, se pueden catalogar los diferentes conflictos desde un punto de vista militar: asedio, guerra de trincheras, guerra convencional, guerra asimétrica, terrorismo, guerra de desgaste, etc. (**figura 1**).

Figura 1, el asedio de Tiro por parte de Alejandro Magno (332 a.C.), mostrado en este dibujo de 1696, es un claro ejemplo del uso de estrategias de defensa y ataque por parte de ambos bandos.[1]

En este artículo se presentará una revisión al concepto de actitud estratégica defensiva en seguridad de la información en una organización. Bajo esta óptica, se explicará el por qué una organización siempre tendrá que asumir la figura defensiva al estar continuamente expuesta a potenciales ataques, debido a la limitante de no poder desarrollar acciones contraofensivas por cuestiones legales. Se replanteará el uso de los

Figura 1—El Asedio de Tiro por Alejandro Magno



controles defensivos actuales y su integración dentro de una estrategia corporativa, con el fin de poder reaccionar ante una potencial agresión de forma contundente.

DEFENSIVA Y OFENSIVA EN EL CONTEXTO DE SEGURIDAD DE LA INFORMACIÓN ORGANIZACIONAL

Tal como se ha descrito al inicio de este artículo, cualquier confrontación cuenta con un agente que actúa como ofensivo y otro que actúa como defensivo, pudiendo cambiar sus papeles a lo largo del desarrollo del conflicto. En una actitud ofensiva siempre se toma la iniciativa y se desarrollan acciones orientadas a atacar al otro, mientras que en la actitud defensiva se renuncia a la iniciativa y se espera al ataque para contenerlo y repelerlo. Cuando el actor defensivo encuentra la oportunidad de atacar, torna su estrategia en una *defensa activa*, mientras que el actor que ataca—al ser atacado—convierte su ofensiva en *ofensiva pasiva*. En palabras de Carl von Clausewitz, la defensiva es "la más fuerte, con objeto negativo," y la ofensiva, es "la más débil, con objeto positivo".[2] Aunque hay bastantes análisis respecto a cuál de las dos es más efectiva, lo que es cierto es que por lo general—y en función del escenario—los papeles van cambiando conforme con las necesidades.

En función de la estrategia, la operación y la táctica empleada por uno o por otro actor se puede llegar a cuatro estados finales en un conflicto: perder/ganar, perder/perder, ganar/ganar o negociar, en donde el factor motivante inicial juega un papel clave dentro de la resolución final del problema.

Estos conceptos son de fácil identificación en cualquier conflicto, en el cual las partes involucradas pueden (y por lo general deben) actuar combinando defensa y ataque de forma sincronizada, como se explicó anteriormente. Estas acciones no son ajenas en el campo de las tecnologías de la información a nivel de ciberseguridad nacional, por ejemplo. El hacking, el espionaje electrónico, el sabotaje informático, entre otros, son nuevos componentes adicionales que han entrado a formar parte del arsenal bélico empleado para proteger la infraestructura de una nación. Estos conceptos han promovido la creación de una nueva generación de guerra: La guerra informática (ciberguerra) o guerra de cuarta generación, que contempla el uso de InfoOps *(information operations)* que incluyen acciones cibernéticas e informáticas ofensivas y defensivas orientadas a debilitar y confundir al enemigo, así como a proteger los recursos propios de información, inclusive sin necesidad de un enfrentamiento frontal, como fue el caso del ataque cibernético sufrido por Estonia en 2007[3]. De hecho, la Casa Blanca en Estados Unidos publicó en Mayo de 2011 su *Estrategia Internacional para el Ciberespacio*[4] y la Unión Europea su *Estrategia de Ciberseguridad* en Febrero de 2013,[5] en las cuales se describen las acciones defensivas y ofensivas en caso de un potencial ataque informático.

Sin embargo, en el caso puntual de una organización, el escenario de reacción ante un potencial ataque es diferente. Con el auge de Internet, las organizaciones actuales han asumido este medio como canal básico para el intercambio de información con el exterior pero no tienen la certeza de cuándo ni cómo ni porqué podrán ser atacadas, con lo cual siempre estarán bajo una posición de *espera de ataque*. De hecho, muchos de los controles de seguridad informática siempre están basados en la premisa hipotética de *qué puede suceder y cómo se actuará*. Claramente, la estrategia siempre ha estado tácitamente orientada a la defensa. De hecho, en muchos lugares aún se tiende a confundir el término *seguridad* con *defensa*. Mientras el primero implica un estado de exención de peligros, daños o riesgos, el segundo se refiere a las acciones llevadas a cabo para protegerse de tales amenazas.[6]

En una empresa con presencia en una red de datos pública, el desarrollo por su parte de una acción ofensiva en el ámbito informático siempre se encontrará al margen de la ley y no será políticamente correcta, incluso si la acción es realizada como una *defensa activa*. Ante tales limitaciones, los conceptos tradicionales de ofensiva y defensiva dejan de ser válidos en el escenario de seguridad de la información en una organización y se plantea el reto de trabajar únicamente con una *defensa defensiva* en la cual siempre el objetivo será de resistencia, aspirando a conservar el *statu quo y* remitiendo la figura ofensiva al atacante por la fuerza misma de las circunstancias. No existirá una *contraofensiva*, no se iniciará de forma unilateral un ataque y el despliegue propio siempre será defensivo y dentro de las *fronteras* de la organización.

Dado que la limitante ofensiva de la organización es bien conocida por el potencial atacante informático, de antemano ya sabrá que su agresión no será respondida de forma activa y que las capacidades para responder ofensivamente serán mínimas o dependerán de un tercero (en este caso, un cuerpo de policía o una agencia de investigación), facilitando de cierta forma la agresión. Nunca un ataque informático contra una organización podrá ser respondido con las mismas técnicas

ofensivas empleadas por el atacante, dentro de los límites legales. Si esto llegase a suceder, la propia organización incurriría en los mismos delitos por los cuales se acusaría al atacante en caso de ser judicializado, lo cual no sería parte de una política corporativa bajo ningún criterio.

La actitud estratégica constituye la postura principal respecto a un objetivo estratégico específico. Tradicionalmente, el planeamiento militar opta entre dos actitudes estratégicas: una *actitud estratégica ofensiva* o una *actitud estratégica defensiva*. Dadas las consideraciones y variables descritas, una organización siempre debe plantear su estrategia de seguridad de la información como una *actitud estratégica defensiva* como se explicará a continuación.

LA POSICIÓN ESTRATÉGICA DEFENSIVA Y LA DEFENSA COOPERATIVA: SU APLICABILIDAD EN LA SEGURIDAD DE LA INFORMACIÓN ORGANIZACIONAL

El hecho de tener sistemas informáticos conectados a Internet ya plantea un reto para la seguridad de la propia empresa. En la práctica, esta posición sería equivalente a dejar una puerta abierta para que cualquier visitante malintencionado pueda atacar cuando quiera y donde quiera la infraestructura que soporta dichos servicios, dejando a la organización *a la espera* de un potencial ataque y a merced de múltiples amenazas sin posibilidad de desarrollar una contraofensiva que permita desestabilizar la agresión. Lamentablemente—y es aquí donde viene el problema fundamental—muchos encargados de seguridad interpretan esta posición como un escenario frustrante y negativo, dando a entender que cualquier inversión en controles defensivos no será efectiva. La expectación generada por la espera de un ataque en cualquier momento puede convertirse en agotadora y puede volver paranoico al más paciente de los directivos.

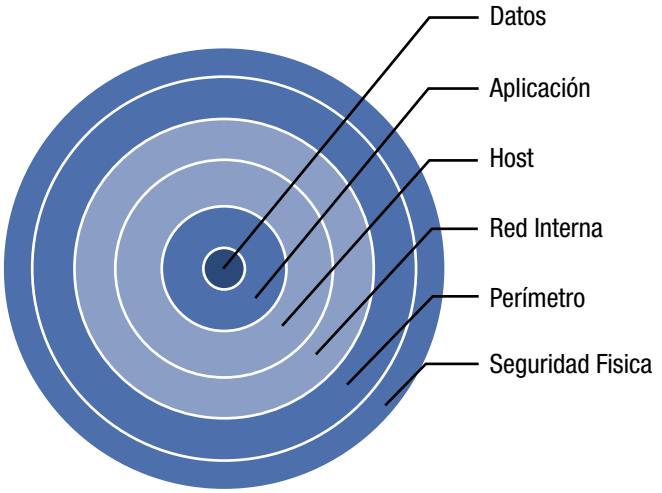
Los conceptos de *cortafuegos, sistema de detección de intrusos, sistema de prevención de intrusos, plan de recuperación de desastres*, entre otros, se cuentan entre los controles básicos en una postura de protección defensiva de la infraestructura de TI de la organización. Sin embargo, muchas veces—y por falta de concienciación y falta de una verdadera y sistemática estrategia de defensa integral—estos controles se despliegan de forma independiente y reactiva o simplemente sin estar alineados entre sí, por lo cual el valor real del conjunto no se percibe ni se puede estimar la capacidad de respuesta contundente ante un potencial ataque, y es precisamente éste el talón de Aquiles de un despliegue caótico de controles defensivos en una red de datos. En términos militares, se trata de un despliegue de controles tácticos sin una estrategia global conjunta.

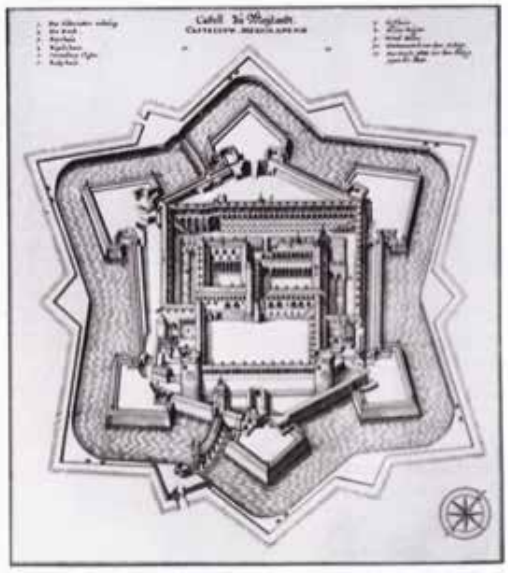
El planteamiento de una *actitud estratégica defensiva* como elemento clave en el desarrollo de una estrategia de seguridad de la información en una organización no se debe entender como una actitud pacifista o un desarme unilateral. Por el contrario: El modelo de implementación de controles defensivo debe ser planificado y desarrollado de tal manera que frente a cualquier ataque contra la organización el potencial atacante reciba una respuesta contundente que lo haga convencer que no podrá cumplir su objetivo y que su desgaste en el ataque será mucho mayor que el de la organización en la defensa. Por lo tanto, la inversión que la organización realizaría en controles ofensivos debería verse reflejada en una ampliación de los controles defensivos, organizados de forma táctica empleando el concepto de *defensa a fondo*, en el cual se cuenta con diversos anillos de seguridad en función de la información protegida, asimilando la estructura de un edificio fortificado o un castillo (**figura 2**).

De forma específica, se han desarrollado modelos de arquitectura segura de redes basados en la "defensa a en niveles de profundidad" como el modelo *Ultra-seguro (Ultra-secure network architecture)* de McGladrey[7] o el modelo de *Cero confianza (Zero Trust model)* de Forrester,[8] en donde se establecen directrices para la implementación de controles que trabajan conjuntamente empleando el mismo modelo de capas y de separación granular con base en confianza. Son un ejemplo claro de una estrategia de seguridad basada en defensa organizada. No se introducen componentes nuevos al sistema ni tecnologías desconocidas. Todo radica en su organización, gestión y topología, siendo éste último el factor diferencial.

Si se garantiza una capacidad defensiva eficiente y conjunta, se obtiene una ventaja potencial en el "conflicto". Carl Clausewitz daba una ventaja estimada relativa de tres a uno a favor de la defensa en un conflicto. Esto significa que una fuerza atacante requiere de tres unidades atacantes contra una de la defensa. En términos estratégicos, aplicando estas teorías, una actitud defensiva potencialmente tendría más ventaja en un conflicto que una actitud ofensiva. Bajo estos criterios, se garantiza la seguridad propia y se fortalece la seguridad de las redes a las cuales se encuentre conectada la organización.

Figure 2—El modelo de *defensa en niveles de profundidad* y el plano de una ciudad amurallada





Por otro lado, en el contexto de los ataques informáticos, la legislación y las entidades de defensa son locales y limitadas a las fronteras de cada país. No existe al día de hoy una entidad que permita gestionar una respuesta a nivel global dadas las características trasnacionales de Internet, con lo cual la organización debe depender en mayor medida de sí misma para su propia seguridad. Para apoyar y complementar dichas acciones se debe reforzar la creación de respuestas defensivas de apoyo mutuo, denominadas *defensa cooperativa*. Para que un modelo de seguridad de defensa cooperativa sea efectivo, hay que comenzar por tener una capacidad propia que sea creíble para luego poder presentarla a los *aliados*, entendiéndose como *aliados* a aquellas redes con las cuales la empresa está conectada (proveedores, clientes, filiales, etc.) y que pueden apoyar en un momento dado una maniobra defensiva.

DEFINICIÓN DE UNA EFECTIVA POSICIÓN ESTRATÉGICA DEFENSIVA

Una estrategia es un esquema desarrollado para intentar alcanzar los objetivos estratégicos que se han fijado. El objetivo de una estrategia defensiva en el contexto de la seguridad de la información es garantizar una existencia continua en la red. Este objetivo se convierte en un fundamento básico que influye en el comportamiento global de la organización y debe ser guiado por una política clara y completa, apoyada desde la dirección. Es importante tener en cuenta que la victoria en una guerra a la defensiva consiste en bloquear sistemáticamente los ataques del enemigo.

Una actitud estratégica defensiva se compone de dos acciones básicas: *la espera y la reacción*. Estas dos acciones no deben ser tratadas de forma independiente y son mutuamente complementarias. Una espera permite organizarse y prepararse de una manera eficaz. En la reacción, mientras que el actor ofensivo ejecuta sus ataques, paulatinamente presenta sus fortalezas y debilidades. Estos factores permiten retroalimentar la estrategia defensiva y prepararse para una nueva agresión de una forma más robusta.

Para la definición de una estrategia defensiva de seguridad de la información se pueden emplear las mismas variables que se tienen en cuenta en una guerra de guerrillas/guerra asimétrica/terrorismo, en donde se presentan elementos de agresión similares a los analizados en un ataque informático: sabotaje, hostigamiento al atacado en su propio terreno, uso de destacamentos irregulares con ataques rápidos y sorpresivos, clandestinidad, gran movilidad, bloqueos temporales de los canales básicos de comunicación y provisiones y secuestro/robo de activos.

En base a estas variables, pueden desarrollarse una serie de tácticas y maniobras defensivas como las contenidas en un plan de acción *anti-insurgencia*. Se emplea el término

anti-insurgencia y no *contrainsurgencia* (COIN), dado que éste último contiene elementos ofensivos, los cuales no son aplicables en un ámbito organizacional como el descrito en este artículo. Estos análisis claramente llevan a replantear la visión clásica de las teorías de la guerra en el ámbito informático: no hay contrincante claramente representado y la lucha no se desarrolla bajo ninguna norma o protocolo por el atacante pero si por el atacado.

Un plan de acción anti-insurgencia está conformado por cuatro componentes principales: prevención, disuasión, reacción y predicción. En un entorno informático, dado que los atacantes se apoyan en la clandestinidad para el desarrollo de sus acciones, la identificación de los mismos y la predicción son los elementos más complicados de obtener. Como resultado, para desarrollar una estrategia exitosa, es importante tener un conocimiento previo de los potenciales factores económicos, políticos, sociales, políticos, ideológicos y psicológicos que pueden motivar al atacante, empleando para ello unas acciones de inteligencia previas. Esta inteligencia es pieza fundamental para la identificación de amenazas, prevención, maniobras de manejo de crisis y tácticas y será la que podrá proveer información acerca de quién, dónde, qué, porqué, cómo y cuándo. Dado que acciones como penetración e infiltración por lo general no son prácticas para obtener información de un atacante informático (debido precisamente a su clandestinidad), debe estimarse esta información en base a datos que puedan obtenerse de actividades del pasado e información encontrada en fuentes abiertas, ya que por lo general algunas de estas actividades ofensivas dependen de publicidad y propaganda.

En la prevención se intentan minimizar las causas que los atacantes puedan explotar y se realiza un análisis de las amenazas. Estas causas no son únicamente tecnológicas, deben contemplar también componentes psicológicos, ideológicos, económicos, etc., que puedan motivar a un atacante a realizar una escalada ofensiva informática contra la organización. La efectividad de una buena prevención depende de la identificación oportuna de dichos problemas. Una herramienta indispensable en una fase de prevención es el análisis de información histórica y de incidentes pasados, que pueden arrojar luz acerca de las motivaciones, tácticas y maniobras a emplear por el atacante. En base a este análisis deberían definirse acciones disuasivas, de engaño, de desgaste (agotamiento), de despeje, etc.

En la disuasión son planificadas y desarrolladas las acciones operativas y tácticas que definan las maniobras defensivas y de contención de la organización en caso de un potencial ataque.

En la reacción, se pondrán en funcionamiento las tácticas y maniobras definidas previamente, en función del tipo de ataque sufrido. Algunas de las maniobras a desarrollar las podemos extraer de los escritos de André Beaufre:[9]

- **Guardarse:** Estar en una posición que permita cubrir a tiempo las potenciales vulnerabilidades que el atacante pueda aprovechar
- **Despejar:** Realizar acciones orientadas a atraer la ofensiva hacia vulnerabilidades protegidas
- **Parar:** Proteger una vulnerabilidad atacada
- **Esquivar/eludir:** Ubicar la vulnerabilidad objeto del ataque en una posición fuera del alcance del atacante
- **Romper/interrumpir:** Detenerse, abandonar una posición limitada

Uno de los objetivos principales de estas tácticas es lograr el desgaste moral y material del atacante, haciendo que deseche la idea de continuar con su ataque. Igualmente, en caso de que exista algún problema y una vulnerabilidad sea explotada satisfactoriamente por el atacante, no se debe entrar en el juego del insurgente. Este juego pretende desvirtuar y confundir la defensa ante una agresión haciendo que se responda de forma emocional y no racionalmente, con lo cual el problema se incrementa. Por esta razón, es importante establecer una gestión de crisis asociada a las situaciones excepcionales cuando se está bajo una ofensiva y controlar de forma calmada la información ofrecida a terceros relacionada con el ataque. Esto es así porque la propaganda y la publicidad solamente hacen más fuerte al agresor y puede ser uno de los factores que lo hayan motivado a perpetrar el ataque, con lo que habría logrado su objetivo aún sin culminar su ataque.

Finalmente, la interacción con terceros (proveedores, clientes y entidades de investigación) forman parte de una respuesta conjunta, lo que se conoce como seguridad de defensa cooperativa, explicada anteriormente. Bajo esta perspectiva, pueden desarrollarse acciones ofensivas coordinadas por entidades que están capacitadas y autorizadas para realizarlo.

La predicción es la fase de retroalimentación y permite que la estrategia siga siendo válida a lo largo del tiempo. Con base en el análisis de las acciones ofensivas recibidas y de nuevos

procesos de obtención de inteligencia, pueden preverse las acciones de un atacante para reforzar los puntos débiles y optimizar y adaptar las tácticas y maniobras.

Para garantizar que dichas estrategias pueden ser válidas en su conjunto frente a una potencial agresión, es importante desarrollar ejercicios periódicos de auto-ataque. Un auto-ataque es un juego de guerra desarrollado por la misma organización orientado a la evaluación de los controles defensivos implementados bajo un escenario controlado y con las mismas condiciones que podría tener un potencial atacante con el fin de detectar problemas y debilidades en los planteamientos teóricos definidos. De esta manera, el sistema se evalúa continuamente a sí mismo y permite incluir nuevos controles defensivos como respuesta a nuevas técnicas ofensivas.

LA "CARRERA ARMAMENTISTA" EN EL CONTEXTO DE POSICIÓN ESTRATÉGICA DEFENSIVA

En el ámbito militar, las armas en sí no son ni ofensivas ni defensivas. Todo depende de la actitud del que las utiliza. Igual sucede con la seguridad de la información: las herramientas están disponibles y dependiendo del uso y del objetivo con que se utilicen pueden ser empleadas para atacar o para defender. Cuando uno de los actores del conflicto incorpora a su arsenal defensivo u ofensivo una nueva arma, su contraparte debe actuar de forma similar para mantener el equilibrio.

La idea de mantener una posición defensiva no implica que la organización se mantenga al margen de una carrera armamentista. El hecho de definir una estrategia defensiva puede significar para el atacante una amenaza o una provocación. Es por esta razón que—al igual que para cualquier estrategia—se debe mantener el secreto y sigilo del mismo dentro de la organización. Las labores de inteligencia, de acciones de auto-ataque y la defensa cooperativa permitirán mantener el sistema y la estrategia actualizada conforme con los cambios que se presenten a nivel ofensivo por parte de los atacantes.

EL FUTURO DE LA ESTRATEGIA DEFENSIVA EN SEGURIDAD DE LA INFORMACIÓN Y NUEVOS RETOS

Como sucede con cualquier estrategia, el paso del tiempo obliga a replantear las acciones en menor y mayor escala y adaptarlas a los continuos cambios en el escenario. No hacerlo puede suponer el dejar de existir. En el ámbito de seguridad de la información, poco a poco las fronteras informáticas (ciberfronteras) de la organización empiezan a difuminarse por la propia dinámica de la tecnología. La llegada de la computación en la nube, los servicios gestionados, la interconexión con terceros, entre otros, obligan a empezar a diseñar estrategias defensivas comunes que involucren no solamente a la organización sino a los demás integrantes del ecosistema al que pertenece. Si cada uno de los elementos que integran este nuevo esquema es consciente de la necesidad de una actitud estratégica defensiva y procura mantener sus controles defensivos actualizados, la suma total de estos componentes constituirá un bloque defensivo efectivo. Esto es cierto particularmente recordando que las amenazas y vulnerabilidades de un componente pasarán automáticamente a ser amenazas de los demás con los que esté conectado, por lo que crece el alcance del ataque.

Una coordinación de políticas, estrategias, tácticas y maniobras en conjunto con el apoyo de entidades de investigación (maniobras externas) permitirán la definición de respuestas contundentes y disuasivas hacia los agresores.

Uno de los principales retos a nivel militar a los que se enfrenta una posición estratégica estrictamente defensiva como la descrita en este artículo es un asedio o sitio. Claramente, en un escenario de seguridad de la información dicha ofensiva podría encontrar similitud con un ataque de *denegación de servicio* (DoS) o *denegación de servicio distribuida* (DDoS), en el que la que el atacante intenta dejar fuera de servicio un sistema mediante una agresión masiva, agotando los controles defensivos del atacado y muchas veces confundiendo las posiciones sin poderle permitir distinguir entre un lo que es un ataque y una actuación autorizada.

Una de las soluciones a dicho problema es un sistema de seguridad de defensa cooperativo comentado anteriormente, en la que los diversos actores afectados por un ataque se coordinan para responder defensivamente y controlar hasta donde sea posible la agresión tratando de minimizar los daños. Así mismo, el factor multi-presencia es otro elemento a considerar. Esto implica la replicación de contenido y servicios en diferentes lugares lógicos y físicos, lo cual permite a la empresa mantener su presencia y operación en caso de ser atacado alguno de sus componentes.

CONCLUSIÓN

Los conceptos de *ofensiva y defensa* no pertenecen exclusivamente al ámbito militar. Se aplican desde hace mucho tiempo en el escenario de seguridad de la información (entre muchos otros) y son familiares (de forma consciente o inconsciente) a los encargados de seguridad de una organización debido a las continuas amenazas informáticas (ciberamenazas) a las que día a día se tienen que enfrentar. Sin embargo, una organización que recibe un ataque informático (ciberataque) no puede desarrollar una contra-ofensiva para repeler dicho ataque debido a limitaciones legales. Está limitada exclusivamente a defenderse, con lo cual, si no existe una estrategia definida, el elemento defensivo puede convertirse en contraproducente.

Por ello, la intención—y la labor a futuro—es dar un paso adelante en el nivel de controles y maniobras reactivas desplegado actualmente (de forma caótica la mayoría de veces) y establecer criterios estratégicos de defensa en la organización. Estos criterios permiten a la organización actuar de forma metódica y coordinada ante un eventual ataque empleando y fortaleciendo de forma paulatina sus propios controles defensivos e integrándose dentro de un esquema global de defensa cooperativa, objetivo clave a plantearse en el desarrollo de acciones orientadas a la supervivencia en la red.

REFERENCIAS

Aldao Zapiola, C.; *La negociación. Un enfoque transdisciplinario con específicas referencias a la negociación laboral*, OIT/Cinterfor, Uruguay, 2009

Amidor, Y.; *Winning Counterinsurgency War: The Israeli Experience. Strategic Perspectives From the Jerusalem Center for Public Affairs*, 2010, p. 1-5

Foro Aviación Argentina; *La defensa no provocativa*, 2010, *www.aviacionargentina.net/foros/temas-de-defensa-generales.11/1626-la-defensa-no-provocativa.html*

Department of the Army, *FMI 3-07.22 Contrainsurgency Operations*, USA, 2006

Tzu, S.; *El arte de la guerra*, D.F. Anaya Editores, México, 2007

NOTAS AL PIE

[1] Imagen obtenida en *http://commons.wikimedia.org/wiki/File:Tyre_besieged_and_captured_by_Alexander_(1696).jpg*

[2] Von Clausewitz; C. *De la guerra*. Madrid, España: Ediciones Ejército (1980)

[3] BBC News; *Estonia Hit by 'Moscow Cyber War, http://news.bbc.co.uk/2/hi/europe/6665145.stm (17 Mayo 2007)*

[4] The White House; *International Strategy for Cyberspace, www.whitehouse.gov*, 1 Julio 2011

[5] European Commission; *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security*, 7 Febrero 2013

[6] Vergara, E.; *Las diferencias conceptuales entre seguridad y defensa*, Instituto de estudios estratégicos de Buenos Aires, *www.ieeba.com.ar*, Febrero 2009

[7] McGladrey Consulting, *The Ultra-Secure Network Architecture, http://mcgladrey.com/Risk-Advisory-Services/The-UltraSecure-Network-Architecture*, 2013

[8] Forrester Research, *No More Chewy Centers: Introducing the Zero Trust Model of Information Security, www.forrester.com/rb/Research/no_more_chewy_centers_introducing_zero_trust/q/id/56682/t/2*, 17 Septiembre 2010

[9] Beaufre, A.; *Introduccción a la estrategia, 3a Edición*, Argentina, 1982

The *ISACA Journal* is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *ISACA Journal*.

Opinions expressed in the *ISACA Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this *Journal*. *ISACA Journal* does not attest to the originality of authors' content.