Cómo conseguir el dominio ciberespacial

Dr. Martin R. Stytz, PhD, Teniente Coronel USAF-Retirado
Dra. Sheila B. Banks, PhD

No es lo que no sepa lo que le puede matar; es lo que sabe con seguridad que no es cierto.

—Mark Twain

Lograr la superioridad ciberespacial global o el control ciberespacial global por parte de cualquier organización ya no es técnicamente posible. En vez de eso, el propio objetivo predominante debe ser el dominio de uno o más de los elementos del ciberespacio de máxima importancia para la organización en un tiempo dado.[1] El éxito de la nación es lograr y mantener un dominio estratégico y táctico en sus elementos críticos del ciberespacio cuando sea necesario.[2] Dos preguntas importantes relacionadas con los aspectos estratégicos del conflicto ciberespacial son: ¿cuáles deben ser los bloques de formación tecnológica para la defensa ciberespacial estratégica a fin de asegurar el dominio de los propios elementos críticos del ciberespacio, y cuáles son las clases de objetivos de datos estratégicos que debe proteger la defensa ciberespacial estratégica?

El conflicto ciberespacial estratégico permite sorprender, impactar y confundir a un adversario en el momento elegido por el atacante, del modo escogido por el atacante y de forma que aproveche las tendencias de toma de decisiones de los adversarios. *El dominio ciberespacial ofensivo estratégico* explota las tendencias del adversario mediante una combinación de exfiltración y manipulación de datos para forzar a los adversarios a tomar las decisiones que queremos que tomen. Socava la toma de decisiones efectiva y el mando de la misión de los contrarios. La determinación de objetivos de la ofensiva ciberespacial estratégica debe basarse en los efectos deseados en los datos y procesos de decisión del oponente y no en los daños materiales que pueden causar o no. Por el contrario, el *dominio ciberespacial defensivo estratégico* permite tomar decisiones efectivas para el bando propio. Asegura datos precisos, fiables y pertinentes para los encargados de tomar decisiones amigas. La gran cantidad de publicaciones de ataques ciberespaciales de código abierto demuestra que no existe ninguna combinación de tecnologías de defensa ciberespacial táctica que sea impenetrable. Por lo tanto, los sistemas y encargados de tomar decisiones propios deben estar preparados tecnológica y sicológicamente para desarrollar su función a pesar de los ataques ciberespaciales estratégicos diseñados para socavar la consciencia situacional, la capacidad de tomar decisiones y el mando de la misión al atacar sus datos y otros elementos del ciberespacio.

El dominio de la defensa ciberespacial estratégica surge de una combinación de tecnologías defensivas ciberespaciales tácticas, una arquitectura de sistemas de defensa ciberespacial flexible y resistente, y la preparación de los encargados de tomar decisiones para afrontar los efectos sicológicos de un ataque ciberespacial estratégico. Tecnológicamente, una defensa ciberespacial estratégica flexible y resistente debe basarse en una defensa ciberespacial estratificada dinámica (DLCD) activa. La preparación de la defensa ciberespacial estratégica requiere el adiestramiento de los encargados de tomar decisiones por medio de la exposición a los efectos de los ataques ciberespaciales de modo que puedan sobreponerse a los retos planteados por un ataque ciberespacial estratégico. Debido a los peligros evidentes planteados por el adiestramiento usando ataques ciberespaciales en el mundo real, el lugar de adiestramiento de los encargados de tomar

*Este artículo fue previamente publicado en la revista SSQ en Primavera 2014.

decisiones debe ser un entorno de simulación. La DLCD, la consciencia situacional y el método de apoyo de decisiones que describimos complementa el entorno de información conjunto (JIE) o las arquitecturas de flujo de datos similares y sus defensas ciberespaciales.

Este artículo trata del dominio ciberespacial estratégico, con un enfoque en la defensa ciberespacial estratégica. Contiene un debate de fondo sobre el ciberespacio estratégico y la consciencia situacional mientras se examina el concepto de DLCD activa.[3] El artículo también presenta un método de adiestramiento y simulación de defensa ciberespacial estratégica para preparar a los encargados de tomar decisiones frente a las incertidumbres y la confusión de datos que se producirán en un conflicto ciberespacial.

El ciberespacio estratégico y táctico

La guerra ciberespacial estratégica es una disputa para el acceso, el control, el uso y la manipulación de los datos de los oponentes junto con la protección y el uso fiable de sus propios datos. Por el contrario, el nivel táctico ofensivo de la guerra ciberespacial comprende las tecnologías usadas parar penetrar las defensas ciberespaciales de los oponentes y las tecnologías para exfiltrar, alterar o manipular sus datos. Entre otros ejemplos de tecnologías de guerra ciberespacial ofensiva táctica podemos mencionar los gusanos, los virus, las redes de robots informáticos, los escaners de puertos, los troyanos, las puertas traseras y los ataques de ingeniería social (como phishing o suplantación de identidades). Usamos el término *software malicioso* para describir todas las tecnologías bélicas ciberespaciales tácticas ofensivas. El nivel táctico defensivo de la guerra ciberespacial se relaciona con las tecnologías usadas para proteger los sistemas y datos propios. Entre otros ejemplos de tecnologías usadas para fines de guerra ciberespacial táctica defensiva están el cifrado, los cortafuegos, el enrutamiento de cebolla o comunicaciones anónimas en una red de computadoras, el aislamiento de redes seguras frente a redes inseguras, la conexión biométrica y la distribución aleatoria de espacio de direcciones. Diferenciamos entre las operaciones ciberespaciales tácticas y estratégicas para resaltar la diferencia entre la lucha táctica para controlar el acceso a sistemas y sus datos, y la lucha para acceder y controlar elementos ciberespaciales a fin de lograr objetivos estratégicos. El conflicto ciberespacial táctico está dominado por consideraciones tecnológicas; el conflicto ciberespacial estratégico está dominado por datos, consciencia situacional y consideraciones de toma de decisiones. Afirmamos que cualquier efecto físico de las actividades ciberespaciales a nivel táctico, aunque sea importante, es también irrelevantes al nivel de guerra ciberespacial estratégica.

El conflicto ciberespacial es diferente de las operaciones de información. Las operaciones de información pueden ser ejecutadas por un número de tecnologías, incluso por seres humanos, mientras que las alteraciones de datos que se pueden lograr en un conflicto ciberespacial son únicas, de mayor alcance, adaptables y más rápidas que en las operaciones de información. Por lo tanto, consideramos que la tecnología ciberespacial es una capacidad distinta de las operaciones de información. Según se observó antes, los retos a los que se enfrenta un defensor ciberespacial estratégico van en aumento, y existen pocas expectativas de lograr la confianza total para cualquier parte del ciberespacio del defensor que no sea el aislamiento completo de Internet (que evidentemente anular la utilidad de ese conjunto de sistemas ciberespaciales del defensor).[4] Hay varias causas claras de la importancia y del alcance del reto de la defensa ciberespacial táctica. En primer lugar, los ataques ciberespaciales tácticos mixtos se está haciendo más comunes y son de esperar. Los ataques ciberespaciales tácticos emplean comúnmente componentes de diversos canales, dominios y funciones, por lo que aumentan significativamente la complejidad del ataque ciberespacial táctico y la dificultad de detectar o defenderse contra él. En segundo lugar, mientras que las defensas contra los ataques ciberespaciales conocidos son necesarias, no son suficientes para asegurar una defensa ciberespacial táctica satisfactoria, ya que las

nuevas tecnologías de ataque están siempre en desarrollo. Como consecuencia, no se puede esperar que las defensas ciberespaciales tácticas repelan o mitiguen todos los ataques. El problema se complica debido a la existencia de un número desconocido de ataques de cero días. En tercer lugar, los recursos ciberespaciales de los adversarios van en aumento debido a la participación de naciones estado y de delincuentes, lo que acelera la velocidad de avance en tecnologías de ataque ciberespaciales. En cuarto lugar, los avances de las tecnologías de computadoras y redes ha favorecido tradicionalmente el ataque ciberespacial táctico, lo que socava la capacidad de las defensas ciberespaciales para repeler o mitigar un ataque de esa clase. Por último, el cumplimiento de normas ciberespaciales tácticas no garantiza la seguridad ciberespacial ni siquiera una defensa ciberespacial táctica efectiva pero no aumenta sus costos. Por estas razones, los defensores ciberespaciales deben esperar que se abran brechas en sus defensas tácticas, y que sean cada vez más difíciles de detectar, y prepararse para operar bien a pesar de que las brechas tengan éxito mientras se recuperan al mismo tiempo de las brechas y las sellan.

A pesar de los retos planteados por los objetivos de los ataques ciberespaciales estratégicos y los ataques ciberespaciales tácticos del adversario, la defensa ciberespacial estratégica debe esforzarse en asegurar los elementos ciberespaciales vitales para el contexto actual de toma de decisiones. El método usado para asegurar estos elementos es la estrategia de la defensa ciberespacial; típicamente una estrategia de la defensa ciberespacial es estática o cambia lentamente en una escala de tiempo humana. Una disminución de la confianza o una demora en el suministro de un elemento o un componente de elemento cruciales del ciberespacio es una "pérdida" de defensa ciberespacial estratégica. Específicamente, la defensa ciberespacial estratégica pierde si el atacante puede (1) demorar el suministro de elementos o componentes ciberespaciales necesarios para las decisiones críticas, (2) reducir la velocidad del flujo de datos en los sistemas ciberespaciales del defensor, (3) forzar el uso de equipos o sistemas anticuados/pasados de moda para asegurar elementos o componentes ciberespaciales, (4) impedir el intercambio de los elementos o componentes ciberespaciales entre los defensores o (5) demorar mejoras o la adopción de tecnologías ciberespaciales. Claramente, los atacantes ciberespaciales tratarán de aumentar sus capacidades en las cinco áreas. Es de importancia crítica durante un ataque ciberespacial es que no todos los elementos del ciberespacio o los componentes de cada elemento son de igual valor *y* el valor de cada elemento o componente varía con el tiempo debido a cambios en el contexto de las decisiones. El contexto de las decisiones por sí solo determina la importancia de los elementos. Como varía el valor del elemento, la cuestión clave para el defensor ciberespacial estratégico es cuáles de las cinco áreas son cruciales para el éxito estratégico del atacante y que son cruciales para la defensa ciberespacial estratégica. Las prioridades de los elementos ciberespaciales, y por lo tanto la asignación de recursos de defensa ciberespacial, deben cambiar a medida que cambian las circunstancias y el contexto de las decisiones. Afirmamos que la estrategia de defensa ciberespacial también debe cambiar tan rápidamente.

Para responder rápidamente a los cambios en las prioridades de los elementos ciberespaciales, las defensas ciberespaciales estratégicas deben poder cambiar de forma dinámica, uniforme y encubierta para mejorar las defensas de los elementos y componentes ciberespaciales que tienen un valor y una importancia máximos en cualquier momento dado. Sin embargo, los cambios en la estrategia o las tácticas defensivas emprendidas para aumentar la protección de los elementos o componentes cruciales no debe sacrificar elementos o componentes de menor valor (evidentemente, el valor de un elemento puede aumentar en el siguiente contexto de decisión). En vez de eso, se deben proporcionar elementos o componentes de mayor valor con protecciones adicionales mientras se preserva el valor de componentes y elementos que no están siendo atacados o de menor importancia en el contexto de las decisiones actuales. Los cimientos de estas capacidades se basan en la DLCD y su capacidad para apoyar cambios rápidos en la estrategia y las tácticas de la defensa ciberespacial.

La ejecución de un ataque ciberespacial estratégico sobre un objetivo estratégico y táctico importante no es una empresa tecnológicamente sencilla. Un ataque ciberespacial estratégico o táctico con éxito requiere un elevado nivel de complejidad de alto nivel, paciencia y un entendimiento profundo y completo de las tecnologías informáticas, del conocimiento humano, de la toma de decisiones y del desarrollo de la consciencia situacional individual y de grupo. Lo malo es que los atacantes ciberespaciales no necesitan poseer estas capacidades tecnológicas, ya que pueden comprarse a personas que las tengan. Sin que importe cómo se han adquirido, los avances tecnológicos permiten ataques que antes no eran posibles además de aumentar la posibilidad de éxito de tipos conocidos de ataques ciberespaciales tácticos, lo que ha resultado en una mayor capacidad para fijar como objetivos elementos específicos del ciberespacio.[5] Los retos planteados por un software malicioso cada vez más potente se agravan y compensan a la vez debido al amplio uso de la máquina virtual (VM) y de tecnologías informáticas en la nube.[6] Los atacantes ciberespaciales tienen, y probablemente retendrán, la ventaja técnica táctica y la iniciativa que requieren que supongamos que todos los elementos ciberespaciales corren riesgo. Durante los últimos desarrollos tecnológicos demostrados por los ataques ciberespaciales tácticos de Stuxnet, Bluepill, Flame y Conficker se indica el carácter probable de futuros ataques así como sus consecuencias probables sobre los encargados de tomar decisiones.

Stuxnet resaltó los retos afrontados por la defensa ciberespacial estratégica. Aparentemente solamente se activó si el sistema infiltrado era uno de sus objetivos. En un sistema fijado como objetivo, pasó a alterar el software en el objetivo y buscar nuevos objetivos desde el interior del sistema. LA campaña de Stuxnet no fue dirigida ni gestionada por seres humanos o sistemas de computadoras. En vez de eso, el software Stuxnet llevó a cabo de forma autónoma el ataque ciberespacial. Se debe esperar que tenga lugar el mismo nivel de autonomía en el futuro. Es de gran importancia la primacía de los elementos ciberespaciales, especialmente los datos, sobre los sistemas físicos según se indica en el ataque de Stuxnet. Tácticamente, Stuxnet alteró el rendimiento de las centrífugas fijadas como objetivos; no obstante, su éxito fue críticamente dependiente de su capacidad de alteración de los datos. Stuxnet alteró los datos de rendimiento de las centrífugas a disposición de los encargados humanos de tomar decisiones; los operadores humanos creyeron que el rendimiento de las centrífugas era correcto. Sin esta capacidad de manipulación de los elementos ciberespaciales clave, el ataque ciberespacial de Stuxnet se habría detectado fácilmente y habría fracasado.

Claramente, los ataques ciberespaciales futuros fijarán objetivos de sistemas de una manera más refinada que Stuxnet o Flame. Transmitirán datos de los objetivos o modificarán sutilmente los datos para corromperlos de forma maliciosa pero no de una maneta inmediatamente aparente. Esperamos que los futuros ataques ciberespaciales se estructuren para introducir información falsa, fijar individuos específicos como objetivos así como sistemas para la degradación de la información, y para corromper precisamente la información que llega a los encargados de tomar decisiones dentro de las campañas ciberespaciales en curso de significado táctico y estratégico. Los ataques ciberespaciales se coordinarán y se montarán en campañas diseñadas para maximizar la confusión y explotar al máximo de forma automática los éxitos tácticos y estratégicos.

Como demostró Conficker, la tecnología existe parar crear un arma ciberespacial consistente en millones de sistemas de computadoras y mantener el mando y el control de esa arma a pesar de cambios en las defensas ciberespaciales tácticas durante un ataque ciberespacial táctico. Stuxnet demostró que la tecnología de un arma ciberespacial que se comporta como una "munición inteligente" debido a su capacidad de alterar, dañar o destruir datos específicos de sistemas físicos específicos. Con el tiempo, las naciones poseerán arsenales ciberespaciales que contendrán una variedad de estas y otras clases de armas ciberespaciales de precisión controladas así como armas para amplios ataques ciberespaciales. Debemos esperar que las campañas ciberespaciales emplearán una amplia variedad de software malicioso que opera de forma cooperativa y estratégica para desorientar y confundir a los encargados de tomar decisiones, demorar sus decisiones

y hacerles llegar a conclusiones incorrectas y malas decisiones sin ser conscientes de que la información que está usando es corrupta. A pesar de la clara amenaza ciberespacial, que es cada vez mayor, se ha dedicado muy poca atención al adiestramiento de toma de decisiones o defensa ciberespacial estratégica durante un ataque ciberespacial cuando se hayan puesto en riesgo partes críticas de las decisiones del ciberespacio. Podemos prepararnos y prevenir hasta cierto punto la perturbación causada por un ataque ciberespacial estratégico al exponer a los encargados de tomar decisiones a ataques ciberespaciales estratégicos simulados así como a seguir nuevas tecnologías defensivas estratégicas con la intención de mejorar la consciencia situacional del encargado de tomar decisiones durante los ataques ciberespaciales.

Consciencia situacional

El único peligro planteado por los ataques ciberespaciales surge del uso de tecnologías de información, entre las que se incluyen computadoras, software, redes y sensores en el paradigma de guerra centrada en la red (NCW)/guerra centrada en los datos (DCW).[7] La NCW/DCW aprovecha los datos y otros elementos del ciberespacio para mejorar el rendimiento y los resultados operacionales. Las mejoras de la consciencia situacional compartida y la toma de decisiones en grupo proporcionadas por las capacidades de la NCW/DCW reducen la incertidumbre de la información entre las personas encargadas de tomar decisiones.[8] Estas dos ventajas significativas proporcionan un conocimiento compuesto, detallado y compartido del estado del conflicto. Los elementos del ciberespacio que apoyan la NCW/DCW son la única manera de lograr las decisiones oportunas y precisas necesarias en conflictos ciberespaciales actuales y futuros. Un ataque ciberespacial estratégico socava los datos y otros elementos ciberespaciales usados para la toma de decisiones y deteriora el desarrollo de una consciencia situacional individual y de grupo. Las vulnerabilidades explotadas por un ataque ciberespacial táctico en apoyo de un ataque ciberespacial estratégico son inherentes a las tecnologías usadas para lograr las ventajas proporcionadas por tecnologías ciberespaciales modernas. Las ventajas ofrecidas por las tecnologías ciberespaciales las convierte en objetivos rentables. Un ataque ciberespacial estratégico puede prevenir que haya datos valiosos que lleguen a los encargados de tomar decisiones, corrompan datos pertinentes para las decisiones, corrompan sistemas de apoyo de decisiones y corrompan los otros elementos del ciberespacio. No obstante, lo que nos preocupa no es la corrupción de los elementos ciberespaciales sino la corrupción de la toma de decisiones. La aparición de tecnologías de computadoras y redes modernas han dado lugar a la expectativa de que la consciencia situacional individual y compartida correcta desarrollará y facilitará la toma de decisiones. La adquisición rápida de una consciencia situacional individual y de grupo puede permitir una respuesta más rápida y coherente ante las circunstancias en evolución. Un ataque ciberespacial estratégico afecta negativamente la consciencia situacional de grupo e individual.

La consciencia situacional es consecuencia de un proceso dinámico para percibir y comprender eventos en un entorno.[9] Permite proyecciones razonables de cómo el entorno puede cambiar y predicciones relacionadas con futuras circunstancias y resultados. El proceso (vea la fig.1) se asemeja algo a la formulación del bucle de observación, orientación, decisión y actuación (OODA) del Coronel John Boyd para la consciencia situacional.[10] Los componentes del proceso no son etapas, sino ciclos enclavados que avanzan en relación entre sí usando un esquema de avance de acciones. Los factores que promocionan la consciencia situacional individual son estructurales y situacionales. Entre los factores estructurales se incluyen antecedentes, adiestramiento, experiencia, personalidad, intereses y destreza. Entre los factores situacionales se incluye la misión que se efectúa y las circunstancias en el momento de la misión. La estructura y los factores situacionales afectan la consciencia situacional según se indica en la figura 2.

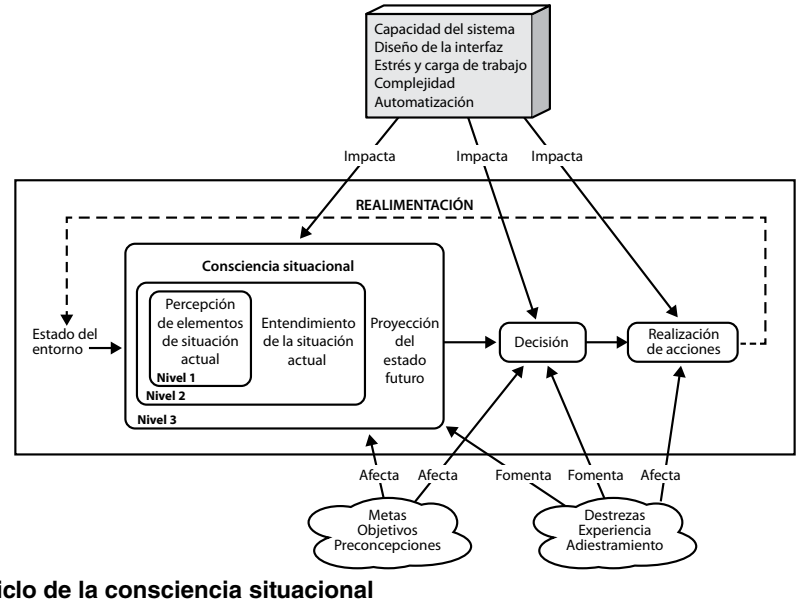

Figura 1. El ciclo de la consciencia situacional
Adaptado de **Mica Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems" (Hacia una teoría de consciencia situacional en sistemas dinámicos),** *Human Factors* **37, no. 1 (1995)**

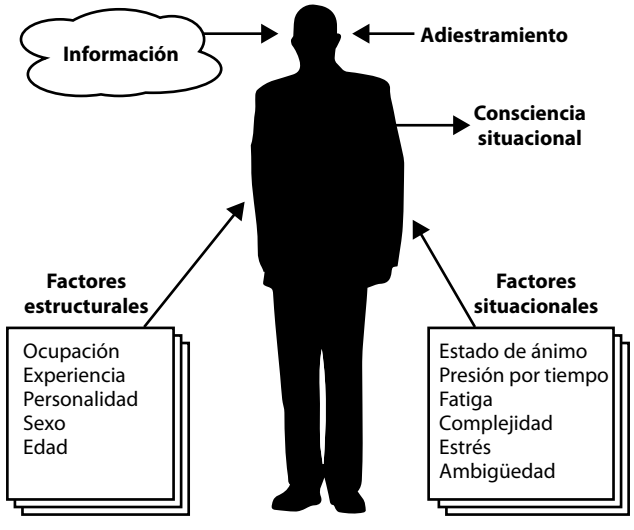

Figura 2. Formación de la consciencia situacional

La consciencia situacional compartida (o de grupo) puede definirse como un modelo mental pertinente común de un entorno o como el nivel al que la percepción de un individuo del entorno refleja la misma situación que la percibida por otros en el grupo. Tanto el logro de ventajas de la consciencia situacional compartida del dominio del ciberespacio como una representación de información interoperable exigen una defensa ciberespacial estratégica y táctica efectiva. La consciencia situacional de grupo asegura que los líderes poseen a todos los niveles una imagen

clara y precisa, común, pertinente de la situación. La consciencia situacional compartida requiere una comprensión común de la política y la estrategia pertinentes así como el estado de operaciones, tecnología, logística, táctica, planes, estructura de mando, personalidades y postura de preparación.

Hay muchos factores que se sabe que degradan la consciencia situacional compartida en un grupo: (1) mentalidad de grupo falsa, (2) mentalidad de "seguir adelante pase lo que pase" (permitiendo que el logro de la misión afecte la evaluación del objetivo), (3) niveles de adiestramiento/destrezas variables insuficientes, (4) destrezas de comunicaciones personales deficientes, (5) conflictos de percepción, (6) cambios frecuentes de personal, (7) condiciones de operación degradadas, (8) carencia de un conjunto común de información en un grupo y (9) la ausencia de pistas no verbales. En general, los trabajadores distribuidos físicamente tienen una consciencia situacional compartida más deficiente que los trabajadores colocados a lado a lado, un problema que se acrecienta debido a la rara tendencia a debatir información contextual entre trabajadores distribuidos.[11] Un ataque ciberespacial moderno bien planificado seguramente fijará objetivos y socavará tanto la consciencia situacional individual como la compartida aumentando el impacto de uno o más factores que degradan ambas. A la luz de estos y otros desarrollos previsibles en capacidades tácticas de ataque ciberespaciales, sugerimos que la mejor práctica de una *defensa estática exhaustiva* para la defensa ciberespacial táctica está pasando de moda y no es viable frente a las capacidades de ataques ciberespaciales tácticos previsibles. Para activar una defensa ciberespacial estratégica efectiva y flexible, es necesaria una transición a una defensa ciberespacial táctica basada en una *defensa ciberespacial exhaustiva estratificada dinámica que sea activa.*

Disminución de la eficacia de un ataque ciberespacial mediante una DLCD

La defensa ciberespacial exhaustiva estratificada dinámica requiere una defensa ciberespacial táctica activa de datos y otros elementos ciberespaciales de manera que proporcione una respuesta rápida y robusta a un ataque ciberespacial aislando los sistemas infectados a medida que se detectan y aumentan la defensa ciberespacial táctica de sistemas sin infectar para impedir la propagación de la infestación del software malicioso y preservar el valor de los elementos del ciberespacio. La clave para desplegar una defensa exhaustiva activa y dinámica efectiva de apoyo mutuo y coherente se basa en un análisis continuo rápido del estado y de la calidad de la protección de los elementos y sistemas del ciberespacio y en el uso de la evaluación resultante para alterar y mejorar inmediatamente las defensas ciberespaciales tácticas para los datos y sistemas fijados como objetivos. Sin embargo, como puede haber y habrá sin duda múltiples infestaciones y múltiples campañas de ataques ciberespaciales emprendidas al mismo tiempo, se necesitará una capacidad de aislar satisfactoriamente infestaciones múltiples y desplegar anillos defensivos múltiples e independientes alrededor de elementos (y componentes) ciberespaciales sin infestar. La valoración de datos y categorización de los ataques ciberespaciales son esenciales para el éxito de este método porque la valoración de los datos amenazados debe determinar los recursos dedicados dinámicamente a la defensa del elemento ciberespacial.

Fundamentalmente, cada ataque ciberespacial tiene como objetivo principal el control de los elementos ciberespaciales del defensor (típicamente datos) ya sea mediante la ejecución de las instrucciones de la computadora del atacante en los recursos informáticos del defensor o mediante la ejecución de instrucciones de alto privilegio del defensor en los recursos informáticos del defensor usando parámetros escogidos por el atacante ciberespacial. Podemos volver a declarar estos objetivos ya sea ejecutando las instrucciones del atacante sobre las computadoras físicas del defensor o ejecutando comandos privilegiados del sistema del defensor usando los valores de

entrada del atacante. Lógicamente, el objetivo principal de la defensa ciberespacial táctica debe ser impedir que se consigan ambos objetivos. En la práctica esto ha sido difícil para la defensa ciberespacial táctica debido al énfasis tradicional puesto en la capacidad y eficiencia de procesamiento de las computadoras, y la dependencia resultante en las defensas ciberespaciales tácticas del perímetro. El énfasis se ha convertido en contraproducente, ya que permite el éxito del ataque ciberespacial táctico, promociona el éxito del ataque ciberespacial, y deja al defensor vulnerable ante una consciencia situacional deficiente y las sorpresas inevitables que esto acarrea.

La defensa ciberespacial estratégica debe tener como objetivos impedir la penetración de las defensas ciberespaciales tácticas, y en el caso de que se produzca, impedir al atacante que determine el terreno ciberespacial, impidiendo que se ejecute el software malicioso del atacante, y si se ejecuta el software malicioso, impidiendo que tenga acceso a su objetivo o que se comunique. Mientras que se tratan de lograr estos objetivos de alguna manera en tecnologías de defensa ciberespacial tácticas, el primer objetivo indicado recibe el máximo énfasis, y una penetración con éxito resulta normalmente en un ataque ciberespacial con éxito. La necesidad de una defensiva ciberespacial estratégica es aumentar considerablemente la capacidad de lograr estos objetivos mientras se mantiene la flexibilidad y la robustez como respuesta a un ataque ciberespacial.

Debido a que se puede invalidar cualquier defensa ciberespacial táctica estratificada estática, una DLCD debe poder cambiar cualquier aspecto de su configuración en cualquier momento. Al hacer eso, una DLCD (1) dificulta la anulación de una configuración de defensa ciberespacial táctica tanto como sea posible, (2) proporciona a los defensores ciberespaciales un entorno defensivo ciberespacial táctico cuyas defensas pueden alterarse dinámicamente, (3) proporciona a los defensores ciberespaciales herramientas para la detección rápida de ataques ciberespaciales tácticos, (4) permite a los defensores ciberespaciales operar con éxito a pesar de una brecha en las defensas ciberespaciales tácticas, (5) proporciona un entorno que permite la recuperación rápida de la penetración e intrusión ciberespaciales tácticas y (6) elimina cualquier ventaja que pueda tener un atacante ciberespacial táctico debido a los conocimientos transitorios de algún aspecto de las defensas ciberespaciales tácticas.[12] Para complementar estos objetivos, nos basamos en principios de seguridad ciberespacial,[13] empleamos tecnologías avanzadas de seguridad ciberespacial táctica, y requerimos un medio de identificar, modelar y establecer una prioridad de los componentes clave de cada elemento ciberespacial en cualquier contexto de decisiones.

Las tecnologías de defensa ciberespaciales estratégicas y tácticas actuales dan al defensor el control del terreno ciberespacial, permitiendo que la defensa ciberespacial determine las condiciones de enfrentamiento en un ataque ciberespacial. Algunas tecnologías de defensa ciberespacial tácticas actuales, como control de aplicaciones y distribución aleatoria de espacio de direcciones, pueden ser efectivas para impedir que se ejecuten algunas aplicaciones no autorizadas y prevenir el acceso a algunas URL peligrosas, pero las tecnologías de defensa ciberespacial táctica actuales son estáticas y no completamente efectivas. La DLCD parece ser más prometedora y efectiva. Al usar la DLCD, el defensor ciberespacial puede formar un laberinto continuamente variable de defensas ciberespaciales tácticas basadas en máquinas virtuales, cada una de ellas con una combinación diferente de propiedades y características operacionales que sirven para complicar el reto de los atacantes ciberespaciales tácticos. Entre otros ejemplos de control de los defensores ciberespaciales tácticos se incluyen entre otros detener procesos de computación, migrar procesos de computación desde un entorno de computación vulnerado hasta otro seguro, cambiando puertos y direcciones de comunicaciones de redes, cambiando códigos de autenticación de M2M y códigos de cifrado, cambiando la configuración y el anidado de máquinas virtuales, purgando software, enfrentándose a cortafuegos adicionales, alterando propiedades de cortafuegos, alterando aplicaciones, alterando protocolos de autenticación o desconectando partes del sistema defendido desde la Internet. El reto planteado al atacante ciberespacial táctico puede complicarse adicionalmente si el defensor ciberespacial da información falsa referente al estado del ataque ciberespacial táctico al atacante ciberespacial, lo que puede ser muy efectivo

porque el atacante ciberespacial casi siempre carece de un canal de información no ciberespacial para averiguar la precisión de la información.

No obstante, al escribir esto, los cambios defensivos ciberespaciales tácticos deben implementarse antes, no durante el enfrentamiento ciberespacial, desechando así una ventaja tremenda poseída por la defensa ciberespacial táctica. La alteración de la defensa ciberespacial táctica durante el ataque así como el control de la información del ataque ciberespacial táctico recibida por el atacante amplificaría las ventajas de la defensa ciberespacial táctica y disminuiría la efectividad del ataque ciberespacial táctico, que es la razón por la que se use la DLCD. Los estratos de la DLCD no corresponden a los estratos de seguridad sino a estratos de máquinas virtuales independientes por las que debe navegar un atacante para penetrar en un sistema y aprovechar un ataque ciberespacial táctico exitoso. La disminución de la efectividad y facilidad de los ataques ciberespaciales tácticos minimiza la oportunidad de sorpresa, minimiza el aprovechamiento de la sorpresa y mejora la protección y el empleo de los cuatro elementos del ciberespacio por parte de la defensa ciberespacial. La alteración del terreno ciberespacial usando la DLCD complica la capacidad de los atacantes ciberespaciales tácticos para evaluar el avance del ataque y disminuye su capacidad para lograr objetivos de ataque. Al aumentar la velocidad a la que cambia el terreno ciberespacial usando la DLCD, la defensa ciberespacial táctica podría forzar al atacante a adaptarse tan frecuentemente y a tener tanta incertidumbre de la información procedente que las posibilidades de éxito del ataque ciberespacial táctico disminuyen significativamente. En la sección siguiente hablaremos con más detalle de la operación de la DLCD.

Defensa ciberespacial activa

Tradicionalmente, los principios para asegurar los sistemas ciberespaciales incluyen (1) el sistema debe ser sustancialmente indescifrable, (2) el sistema no debe requerir confidencialidad y el enemigo puede robarlo sin causar problemas, (3) el sistema debe ser fácil de cambiar o modificar a discreción de los interlocutores, y (4) el sistema debe ser fácil de usar y no debe forzar la mente ni requerir el conocimiento de una larga serie de reglas. Estos principios se han empleado hasta cierto punto desde las primeras investigaciones en seguridad de computadoras.[14] En el contexto de sistemas de seguridad ciberespacial, estos principios exigen (1) al atacante ciberespacial táctico que no pueda determinar las defensas ciberespaciales tácticas antes o durante el ataque ciberespacial, (2) posesión de un sistema que implemente las defensas ciberespaciales tácticas no proporciona detalles sobre las configuraciones de defensa ciberespacial táctica de sistemas similares, (3) las defensas ciberespaciales tácticas deben ser fáciles de cambiar en cualquier momento y (4) las defensas ciberespaciales tácticas son esencialmente invisibles para las personas que no tengan responsabilidades de seguridad ciberespacial. La necesidad de una mejora considerable en puntos de defensa ciberespacial táctica apunta a la necesidad de DLCD. La DLCD implementa los principios al ser construida y diseñada para aislar infestaciones de software malicioso, complicar la perspectiva del atacante ciberespacial táctico del terreno ciberespacial, y mantener elementos ciberespaciales suficientes, exactos y fiables a pesar del ataque. Este método difiere de los intentos de defensa ciberespacial táctica actuales por su gran énfasis en los cuatro principios como la propiedad y el requisito ante todo del sistema ciberespacial sin tener en cuenta su impacto en el rendimiento del sistema.

La DLCD también hace énfasis en la importancia de las tres propiedades deseables adicionales de un sistema ciberespacial: maximizar la velocidad de la información dentro del sistema cuando sea atacado, maximizar las razones del objetivo para la confianza del usuario del sistema y sus datos, y maximizar la capacidad del sistema ciberespacial para modificar las defensas ciberespaciales tácticas aumentando o disminuyendo su complejidad y propiedades de seguridad. El cambio de propiedades se basa en la importancia de la información que procesa el sistema con

relación al contexto de toma de decisiones actual. Al fijar la prioridad de la seguridad del sistema ciberespacial, permitimos la consecución de estas propiedades adicionales.

En la DLCD, la capa más externa de la defensa ciberespacial táctica tiene acceso a los equipos de computación; cada estrato anidado adicional aísla más los equipos del componente ciberespacial y viceversa. El estrato más interno de la defensa de la DLCD encierra el componente. Como se usa software sonda para instrumentar la operación y el rendimiento de cada estrato, la DLCD puede dar a los encargados de tomar decisiones tiempo e información suficientes para reconocer y contrarrestar un ataque ciberespacial. La DLCD también permite a los defensores ciberespaciales alterar la complejidad y configuración de defensa ciberespacial táctica en cualquier momento, lo que complica más los retos planteados a un atacante. Afirmamos que la supervisión y el juicio humanos son cruciales para la operación de la DLCD y asegurar que un atacante ciberespacial no active las respuestas de defensa ciberespacial táctica que malgastan recursos. En consecuencia, aunque algunas respuestas de la defensa ciberespacial táctica deben ser automáticas, los encargados humanos de tomar decisiones proporcionan una guía y una gestión generales de la defensa. La Figura 3 muestra la esencia del método de la DLCD para un solo elemento del ciberespacio. La Figura 4 muestra su uso para la protección de la aplicación.

La clave para la DLCD es la protección de cada elemento del ciberespacio por una o más máquinas virtuales anidadas del Tipo 1, cada una de ellas operada por su propio monitor de máquinas virtuales (VMM) usando distintas configuraciones.[15] Cada máquina virtual proporciona un estrato de protección de defensa ciberespacial, que tiene su propio conjunto de propiedades de máquinas virtuales y defensas ciberespaciales tácticas tradicionales, según se indica en la figura 3. Se añaden máquinas virtuales a la protección de estratos según lo justifique la amenaza e importancia del componente en el contexto de decisiones actual. La seguridad completa dentro del entorno de DLCD se logra según las líneas descritas por Cricket Liu y Paul Ablitz en *DNS y BIND*.[16] Por ejemplo, la comunicación entre las máquinas virtuales debe ser segura y fiable. Por lo tanto, los datos se cifran antes de su transmisión entre máquinas virtuales o entre aplicaciones. La comunicación segura mejora usando la tecnología de redes privadas virtuales (VPN) a fin de asegurar la comunicación entre procesos dentro del sistema de computadoras. Al proporcionar máquinas virtuales y aplicaciones autorizadas, la presencia de un certificado digital para la autenticación proporciona una seguridad adicional. La seguridad ciberespacial defensiva táctica mejora aún más usando DNSSEC e IPSEC para la comunicación dentro y entre estratos y direcciones IPv6 para identificar aplicaciones individuales y máquinas virtuales (las direcciones IPv6 no se comparten ni se heredan).[17] La combinación de máquinas virtuales con otras tecnologías de defensa ciberespacial táctica permite una alteración segura y dinámica del terreno ciberespacial defensivo que el atacante debe superar para lograr los objetivos del ataque ciberespacial.

Al usar múltiples máquinas virtuales anidadas y otras tecnologías de defensa ciberespacial para proteger los elementos del ciberespacio, la DLCD es compatible con la asignación dinámica de recursos de defensa ciberespacial táctica permitiendo la adición de máquinas virtuales a los estratos de protección de un elemento o componente, alterando la mezcla de tipos y configuraciones de máquinas virtuales, o cambiando los sistemas de detección de ataques ciberespaciales tácticos dentro de cada máquina virtual sin alterar ni influir en las otras máquinas virtuales o elementos ciberespaciales dentro de un sistema. Usando la DLCD, el terreno ciberespacial defensivo puede alterarse de una manera significativa, útil e impredecible que no puede ser detectada ni prevenida por el atacante ciberespacial o por software malicioso que haya abierto una brecha en las defensas del sistema. La DLCD presenta a los atacantes ciberespaciales tácticos un laberinto reconfigurable que deben resolver de forma continua para penetrar en el ciberespacio defensivo y aprovechar una penetración. Observe que por cada estrato de máquinas virtuales añadido para proteger un componente o un elemento, cuanto peor es el rendimiento del elemento o componente encerrados, lo que inevitablemente degrada la utilidad del elemento o

componente del ciberespacio para un logro más amplio de la misión. Por lo tanto es vital que los encargados de tomar decisiones alteren la protección solamente en respuesta a las amenazas reales contra los recursos ciberespaciales; de lo contrario el rendimiento de los elementos y componentes puede degradarse a tal nivel que pierdan utilidad para un encargado de tomar decisiones. La complejidad de las ventajas y desventajas entre seguridad y puntualidad de los elementos es la base de nuestra afirmación de que los seres humanos deben gestionar las defensas ciberespaciales tácticas aun cuando las respuestas rápidas deben ser ejecutadas por sistemas inteligentes.

Al usar un método de máquinas virtuales anidadas de múltiples estratos (fig. 3 y 4), como base de la DLCD, la defensa ciberespacial táctica puede responder a un ataque ciberespacial táctico mientras el ataque sigue su curso. Una defensa ciberespacial táctica estratificado dinámica basada en tecnologías de máquinas virtuales anidadas puede proteger de forma efectiva los cuatro elementos ciberespaciales.

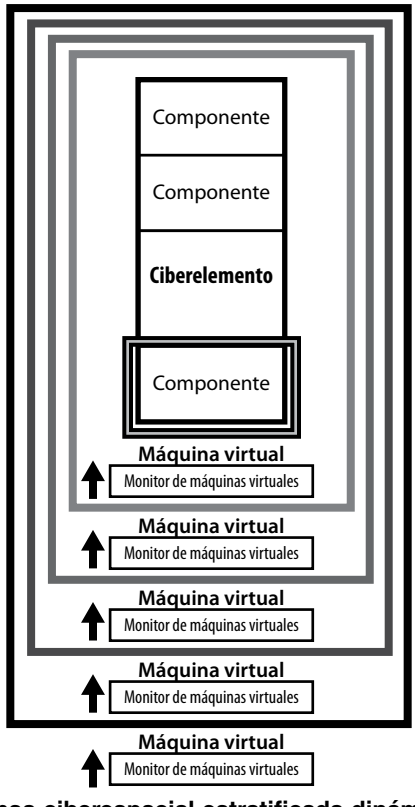

Figura 3. Arquitectura de defensa ciberespacial estratificada dinámica nominal para un elemento que muestra la colocación del VMM

No se puede exagerar la importancia de un suministro puntual y preciso de elementos ciberespaciales para el éxito de la toma de decisiones.[18] La demora hace que no se obtenga ni se mantenga la consciencia situacional, fracase la toma de decisiones y se produzcan decisiones incorrectas. La necesidad de compartir algunas porciones de cada elemento ciberespacial para desarrollar y mantener la consciencia situacional del grupo complica aún más el reto de un suministro oportuno y preciso, porque en un conflicto moderno generalmente hay muchos encargados de tomar decisiones involucrados en el proceso de evaluación y decisión por cada deci-

sión, según se prevé en el JIE. Mientras que los elementos ciberespaciales aumentan de valor cuando se comparten, el proceso de reparto aumenta también la vulnerabilidad del elemento y del proceso de toma de decisiones. En consecuencia, cuando los encargados de tomar decisiones están evaluando métodos de defensa ciberespacial táctica, no deben considerar solamente cuál es la mejor manera de protegerse contra los elementos que son cruciales para el contexto de decisiones actuales, sino también cómo proteger los elementos y componentes suministrados a las demás personas involucradas en la misma decisión. El reto de la defensa ciberespacial táctica aumenta debido a la variabilidad en los elementos y componentes del ciberespacio en decisiones diferentes, a la variabilidad en la capacidad de un elemento o componente ciberespacial para disminuir la incertidumbre, a las diferencias de tolerancia de los elementos, componentes y encargados de la toma de decisiones para arriesgar, y variando las percepciones de la importancia de cada decisión dentro de una situación en evolución.

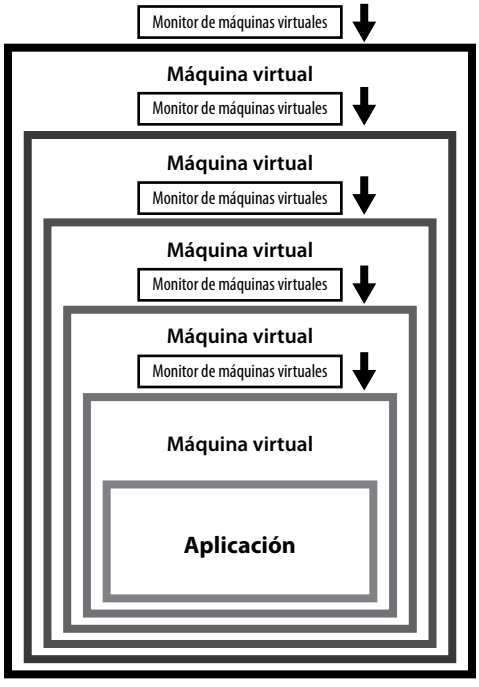

Figura 4: Uso de máquinas virtuales anidadas para proteger una aplicación en la DLCD

La bien conocida dificultad de evaluación de valores de elementos ciberespaciales, especialmente los datos, aumenta cuando aumenta el número de encargados de tomar decisiones que usan los mismos elementos. La solución clara del problema es evaluar el valor de los elementos y componentes del ciberespacio en una variedad de situaciones y usar estas evaluaciones como guías a una acción de defensa ciberespacial durante los ataques. Podemos llevar a cabo evaluaciones de valores de elementos y componentes ciberespaciales supervisando las opciones de protección y de usos de elementos ciberespaciales escogidas durante el proceso de toma de decisiones en un entorno de simulación. Para hacer la evaluación, suponemos que los elementos y componentes ciberespaciales pertinentes empleados para la decisión son importantes y que los otros elementos y componentes ciberespaciales no considerados no son tan importantes en esa circunstancia particular. No obstante, los elementos y componentes ciberespaciales no emplea-

dos en una decisión deben protegerse hasta cierto nivel. La participación humana es crucial para fijar y revisar prioridades de elementos y componentes para la defensa ciberespacial táctica debido a las complejidades involucradas al hacer evaluaciones de prioridad. Las prioridades derivadas de la simulación pueden usarse para guiar las opciones de defensa ciberespacial tácticas de elementos y componentes ciberespaciales del encargado de tomar decisiones durante los ataques ciberespaciales del mundo real.

Adiestramiento de defensa ciberespacial

A medida que los ataques ciberespaciales aumentan su refinamiento técnico puede aumentar su capacidad de fijar objetivos de información, datos y recursos físicos específicos, lo que puede ser desorientador. Incluso un ataque que no desoriente a los usuarios puede seguir produciendo confusión, lo que a su vez disminuye la consciencia situacional del grupo, la consciencia situacional individual y la calidad de la toma de decisiones. El resultado inevitable de un mayor refinamiento técnico por parte de los atacantes ciberespaciales es la mejora de su capacidad de enturbiar la consciencia situacional, perturbar la diseminación de decisiones e impedir información de respuesta exacta. La preparación para la toma de decisiones durante un ataque ciberespacial requiere adiestramiento para preparar retos sicológicos, de consciencia situacional y de toma de decisiones del atacante ciberespacial junto con las herramientas de análisis y gestión de información necesarios para ayudar a los encargados de tomar decisiones a evaluar la información a su disposición, evaluar la fiabilidad de la información y desarrollar una consciencia situacional. La búsqueda de la consciencia situacional ciberespacial es crucial para asegurar el ciberespacio y lograr la consciencia situacional en otras partes del conflicto —aire, tierra, mar o espacio. Debido a que la consciencia situacional del ciberespacio para individuos y grupos de encargados de tomar decisiones es vital, es esencial desarrollar entornos de adiestramiento para encargados de toma de decisiones y defensores ciberespaciales estratégicos a fin de proporcionar experiencia y conocimientos expertos para tratar los ataques ciberespaciales y sus intentos de socavar la consciencia situacional. Las necesidades del defensor ciberespacial estratégico son claras: estrategias que protegen los elementos y sus componentes cuando sufran un ataque ciberespacial mientras se asegura a los encargados de la toma decisiones que tengan los componentes de los elementos ciberespaciales que necesitan.

A la luz de estos requisitos complementarios, el adiestramiento de los defensores ciberespaciales y encargados de tomar decisiones estratégicas debe tratar dos necesidades. *Primero*, preparar a los defensores y encargados de tomar decisiones para los elementos ciberespaciales confusos, contradictorios y engañosos presentes durante un ataque ciberespacial. El adiestramiento puede prepararlos para hacer frente a las tensiones sicológicas causadas por las variaciones de disponibilidad y calidad de los elementos ciberespaciales. Un aspecto clave de este adiestramiento debe ser aprender a evaluar el valor de los elementos ciberespaciales, tanto en lo que se relaciona con el valor (importancia) de los elementos disponibles en relación a decisiones actuales así como en relación con el valor de los elementos vulnerados. Los encargados de tomar decisiones deben aprender que el valor del elemento ciberespacial no está correlacionado con la clasificación de seguridad. Los defensores también necesitan evaluar la efectividad de varias estrategias para contrarrestar ataques ciberespaciales y campañas. La *segunda* necesidad es preparar a los encargados de tomar decisiones para que exploten el dominio del ciberespacio por medio del empleo de efectivo de análisis/comprensión de datos fiables (como el análisis basado en datos grandes) y tecnologías de interacción/gestión de datos. El análisis, la comprensión y la interacción deben realizarse, en parte, automáticamente debido al volumen de los datos disponibles. No obstante, los encargados de tomar decisiones deben aprender a navegar por el ciberes-

pacio, cómo usar visualizaciones como visores en partes críticas del ciberespacio, cómo comparar y componer visualizaciones para proporcionar los detalles necesarios, cómo identificar y explotar datos clave, y cómo coordinar su navegación, análisis y esfuerzos de comprensión a pesar de ataques ciberespaciales diseñados para socavar estos esfuerzos.

Los retos planteados para una defensa ciberespacial estratégica al tratar estas dos necesidades son significativas, porque lograr y mantener un dominio ciberespacial defensivo de amplio espectro es cada vez más difícil y poco de fiar debido a las mejoras en las tecnologías de ataques ciberespaciales tácticos. El reto crucial en la defensa ciberespacial estratégica radica en determinar qué defensa emplear a la luz de qué elementos requieren mejorar la defensa ciberespacial táctica y qué elementos se defiende de forma adecuada en el contexto de toma de decisiones actual. Debido al volumen de datos que debe considerarse y al ritmo rápido de actividad, el defensor ciberespacial estratégico así como el encargado de tomar decisiones deben estar preparados para las circunstancias de información confusas y noveles que se encuentren. La exposición a ataques ciberespaciales simulados puede preparar al defensor ciberespacial estratégico para lograr una evaluación apropiada de circunstancias ciberespaciales y seleccionar las respuestas de defensa ciberespacial estratégicas y tácticas más ventajosas para los ataques ciberespaciales.

La preparación de los defensores ciberespaciales estratégicos es crítica porque los comportamientos instintivos mostrados frente a la incertidumbre son invariablemente incorrectos y contraproducentes. En condiciones de estrés, se adoptan comportamientos instintivos. Los comportamientos inducidos por estrés hacen que use una tendencia emocional para tomar decisiones (tomar la decisión que permita a la personas *sentir* que es probable obtener un resultado más positivo), a una tendencia de expectativa (la expectativa de que ocurrirán las cosas que *quiere* ocurra la persona), a una aversión de pérdidas/riesgo (la tendencia a opciones de valores que *parecen* minimizar el riesgo y las pérdidas a pesar de cualquier evidencia o datos de lo contrario), a la adopción de la falacia de un costo irrecuperable (donde la tendencia es *continuar* una acción porque el encargado de tomar decisiones cree que la situación no empeorará o porque el encargado de tomar decisiones tiene un interés creado emocional y egoísta de seguir el mismo curso de acción). Por último, los comportamientos instintivos también pueden conducir a una fijación del pasado (la tendencia a tomar decisiones basada en la expectativa de que las condiciones que existían en el pasado *recurrirán* a pesar del hecho de que nunca pueden recurrir). Contrarrestar comportamientos instintivos contraproducentes es difícil y debe ser una de las preocupaciones principales de adiestramiento de defensa ciberespacial estratégica por medio de la simulación.

Las herramientas y el adiestramiento requeridos por los defensores ciberespaciales estratégicos y encargados de tomar decisiones para prepararlos para los retos del conflicto ciberespacial deben tratar tres clases de situaciones ciberespaciales: operaciones en condiciones normales, operaciones durante un ataque ciberespacial y operaciones después de un ataque ciberespacial.[19] El adiestramiento, las técnicas y las herramientas que son vitales en estas tres circunstancias pueden desarrollarse usando entornos de simulación diseñados para proporcionar las capacidades siguientes: (1) mejorar el entendimiento de los retos planteados durante un ataque ciberespacial, (2) probar y evaluar herramientas, técnicas y adiestramiento de defensa ciberespacial, (3) practicar el uso de herramientas y técnicas de defensa ciberespacial para adquirir conocimientos expertos y (4) evaluar el valor del elemento ciberespacial durante una amplia variedad de circunstancias para determinar cuál es la mejor forma de desplegar las defensas cibernéticas. Las herramientas, las técnicas y el adiestramiento deben ser amplios y flexibles de modo que puedan alterarse inmediatamente para tratar nuevas amenazas cibernéticas y ataques cibernéticos tácticas a medida que surgen o se hacen posibles.[20]

Adiestramiento de la defensa ciberespacial mediante simulación

La simulación de ataques ciberespaciales es el único medio de preparar a los encargados de tomar decisiones para la complejidad de los ataques inevitables sobre elementos ciberespaciales. Es el mejor medio disponible para determinar las estrategias que se deben usar para asegurar los elementos críticos del ciberespacio en apoyo de las necesidades de los encargados de tomar decisiones.

La simulación proporciona una forma segura y flexible para preparar defensores ciberespaciales estratégicos y encargados de tomar decisiones para los retos enfrentados en un ataque ciberespacial así como evaluar las técnicas de protección de elementos y estrategias ciberespaciales. La simulación del ataque ciberespacial puede proporcionar un entorno que permite a los encargados de tomar decisiones y defensores ciberespaciales estratégicos practicar de modo que sus decisiones y actividades del mundo real produzcan una defensa ciberespacial estratégica efectiva, una conciencia situacional adecuada y decisiones efectivas. Para cambiar las dimensiones a medida que evolucionan las tecnologías, la simulación de ataques ciberespaciales debe representar las acciones de ataque y defensa de manera que corresponda a cómo son percibidas estas acciones por los seres humanos, incluso a medida que el ataque sigue y las defensas triunfan o fracasan en el entorno de simulación. Para lograr estos objetivos, el entorno de simulación ciberespacial debe capturar y representar las actividades de los encargados de tomar decisiones y defensores ciberespaciales estratégicos, los objetivos del atacante y defensor, la secuencia de operaciones que ejecutará el atacante, las actividades de la defensa ciberespacial táctica, la ubicación de datos lógicos y físicos, y las respuestas potenciales de los atacantes y defensores a las acciones recíprocas. En trabajos anteriores, describimos las técnicas de simulación de ataques ciberespaciales que pueden usarse para modelar las operaciones ciberespaciales, sus componentes y las posibles respuestas a las acciones defensivas.[21]

La simulación de los ataques ciberespaciales presenta una serie de análisis y retos de evaluación, todos los cuales se refieren a la determinación del estado y de la importancia de los elementos ciberespaciales a disposición de los encargados de tomar decisiones. Se pueden usar estudios anteriores sobre la importancia de los datos en la toma de decisiones así como en los retos planteados por datos contradictorios o confusos como base para determinar cómo alterar los elementos ciberespaciales y sus componentes como respuesta a un ataque ciberespacial simulado. Para simular un ataque ciberespacial, necesitamos afectar solamente los elementos ciberespaciales a disposición de los usuarios; no necesitamos infectar o corromper computadores o su software. Para una simulación realista, los estímulos y los elementos ciberespaciales proporcionados a los encargados de tomar decisiones deben contener el ruido, las discontinuidades y los errores del tipo que serían causados por la actividad ciberespacial real de modo que el encargado de tomar decisiones y los defensores ciberespaciales se habitúen a ataques ciberespaciales como los que podrían desarrollarse en el mundo real. Se puede usar el mismo entorno de simulación para evaluar el valor de los elementos del ciberespacio y desarrollar procedimientos para continuar las operaciones en vista de los ataques ciberespaciales.

Son necesarios cuatro objetivos de simulación para preparar a los encargados de tomar decisiones y a los defensores ciberespaciales para los ataques ciberespaciales. *Primero*, enseñarles cómo determinar los objetivos de los ataques ciberespaciales. En *segundo lugar*, enseñarles las técnicas y tácticas que probablemente se usarán en los objetivos. En *tercer lugar*, enseñar a los encargados de tomar decisiones y a los defensores ciberespaciales los efectos de cada tipo de ataque y las técnicas y herramientas que deben usarse para contrarrestar cada tipo de ataque ciberespacial. En *cuarto lugar*, enseñarles los medios para evaluar explícitamente el valor de los elementos ciberespaciales y desplegar una defensa ciberespacial para proteger información de máximo valor. Una consideración adicional para los defensores es explorar estrategias y tácticas a fin de evaluar su utilidad. La simulación ciberespacial puede lograr estos objetivos. Para mini-

mizar el costo de desarrollo de los entornos de simulación, los sistemas de simulación actuales pueden acoplarse con los sistemas de simulación ciberespacial, según se indica en la figura 5. Las situaciones que se van a ejecutar en la simulación ciberespacial se describen usando el Lenguaje de Modelación Unificado (UML).[22] Para crear entornos de simulación ciberespacial realista, los componentes del entorno de simulación ciberespacial deben intercambiar información sobre el ataque y la defensa ciberespaciales, el estado del evento ciberespacial, y representar los resultados del ataque ciberespacial y las respuestas defensivas.

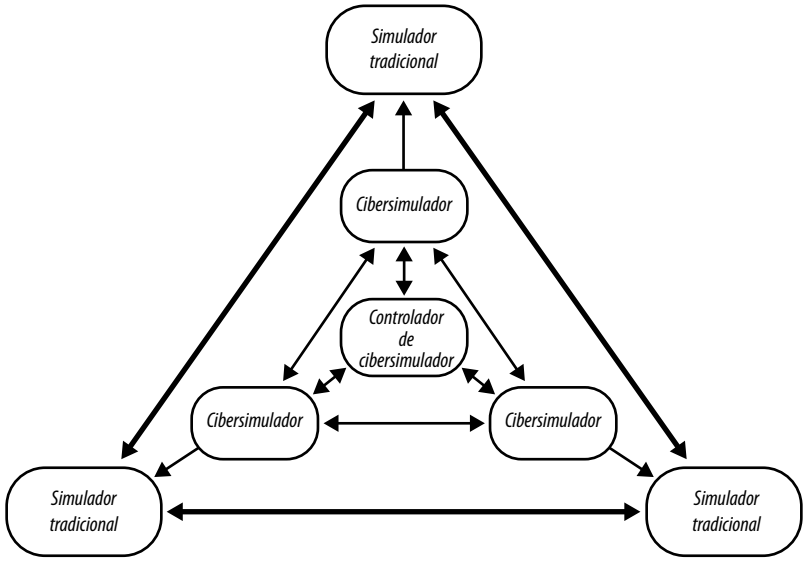

Figura 5. Entorno de simulación ciberespacial conceptual

La clave para este método es reconocer que simular un ataque ciberespacial solamente requiere afectar la información presentada a los usuarios en el entorno de simulación. Por lo tanto, para prepararse para la conciencia situacional y los retos de toma de decisiones enfrentados durante un ataque ciberespacial, solamente se debe alterar la presentación de los elementos ciberespaciales; no es necesario alterar los elementos "verdaderos" y sus valores. Se dispone de tres métodos para afectar la presentación de elementos: aumentar la cantidad de información presentada por medio de un elemento, bloquear la información requerida por un usuario que es proporcionada por un elemento, y reemplazar la información real por información falsa presentada por medio de un elemento. Por ejemplo, se puede dar una cantidad de datos abrumadora a un usuario, negar datos o dar una mezcla de datos exactos y falsos. Otras técnicas que se pueden usar para simular un ataque ciberespacial son: dar instrucciones a todos los anfitriones de simulación para replicar todos los mensajes recibidos en el anfitrión pero con el número de mensajes recibidos cambiados por una cantidad aleatoria pero pequeña, dar instrucciones a cada anfitrión de simulación para que se duplique la misma información en numerosas ventanas, o dar instrucciones de cada anfitrión de simulación para eliminar palabras aleatorias de cada mensaje. Los efectos de estas medidas simples pueden complicarse si se repiten mensajes falsos en intervalos aleatorios después de recibir el primer mensaje.

Un entorno de simulación de adiestramiento ciberespacial (vea la fig. 5) debe lograr tres tareas para conseguir sus objetivos de adiestramiento: determinar si un ataque ciberespacial simulado tiene éxito, determinar el efecto del ataque ciberespacial simulado en cada anfitrión y sus

datos, y representar respuestas defensivas ciberespaciales simuladas al ataque simulado. En el método ilustrado, cada anfitrión tiene un simulador ciberespacial que efectúa el servicio del anfitrión y proporciona estas tres capacidades. El simulador ciberespacial proporciona a cada anfitrión los datos de entrada necesarios para representar los efectos de ataques simulados y respuestas defensivas. Los sistemas de simulación se comunican entre sí usando una red de simulaciones ciberespaciales lógicamente separadas para lograr un estado ciberespacial uniforme en todo el entorno de simulación.

En cada paso del ataque ciberespacial y de la respuesta defensiva ciberespacial, el entorno de simulación debe proporcionar indicaciones apropiadas y realistas del estado del ataque y estado/valores de elementos ciberespaciales de modo que reflejen las demoras y alteraciones que ocurrirían en el ataque ciberespacial del mundo real correspondiente. Por ejemplo, los cambios en la defensa ciberespacial táctica que aumentan o disminuyen la profundidad de la defensa se reflejarían en mayores o menores demoras en el transporte de datos. La arquitectura de simulación permite a los defensores ciberespaciales alterar los tipos y las configuraciones de la defensa ciberespacial táctica en cualquier momento. Como consecuencia de la exposición a una defensa ciberespacial realista y un entorno de ataque, el defensor y el encargado de tomar decisiones pueden experimentar los efectos de sus opciones defensivas y experimentar técnicas dinámicas.

Una situación de ejemplo ilustra cómo se puede usar el entorno de simulación ciberespacial para preparar a los encargados de tomar decisiones y a los defensores ciberespaciales estratégicos para los ataques. Se podría asignar al entorno de simulación ciberespacial la tarea de proporcionar experiencia en el uso de tecnologías de análisis de información y navegación para detectar la presencia de una red de robots informáticos. Los métodos de detección de redes de robots informáticos introducidos podrían incluir un análisis de redes específico o flujos de tráfico en la nube, análisis de red agregada o datos de tráfico de la nube, variaciones en volumen de datos, variaciones en orígenes y destinos de tráfico de redes, y otros comportamientos atípicos. El entorno de adiestramiento prepararía a los encargados de tomar decisiones y a los defensores para el mundo real donde un indicador de infección no es suficiente. En la práctica, la confirmación de una infección de una red de robots informáticos requiere múltiples indicadores para lograr robustez de confirmación proporcionando tanto la capacidad de corroborar datos de fiabilidad dudosa o variable y minimizar el índice de alarmas falsas.

En la figura 6, se usan anillos de "protección" o "valor" para establecer prioridades de los cuatro componentes de elementos ciberespaciales. Los anillos corresponden al valor y a las prioridades asignadas a la protección de cada elemento ciberespacial. Para el defensor ciberespacial estratégico, el modelo de anillos se puede usar para guiar la asignación de recursos así como para tomar decisiones con el fin de aislar sistemas o subsistemas que están en riesgo. En el método de modelos de anillos, cuanto más cerca del centro estén los anillos, mayor será el valor, la importancia y la utilidad (de ese elemento ciberespacial) en el contexto de las decisiones. El número de anillos y el contenido de cada anillo se determinan mediante el contexto de toma de decisiones. En consecuencia, el número y el contenido de anillos para cada elemento varía dinámicamente. Usamos un conjunto de anillos por cada uno de los cuatro elementos. Cada anillo de elementos ciberespaciales contiene componentes de aproximadamente la misma importancia para ese elemento en un contexto de toma de decisiones. El modelo de anillos sirve también para simplificar el reto de simulación de ataques ciberespaciales. Para simular un ataque dentro de un contexto de toma de decisiones, afectamos los elementos y componentes requeridos en el contexto de decisiones simulando la modificación del contenido de los anillos específicos para esos elementos del ciberespacio defensivo vulnerables. La decisión, el tipo de ataque ciberespacial, las defensas ciberespaciales tácticas, los conocimientos expertos del encargado de tomar decisiones y los resultados de aprendizaje para el ejercicio de simulación determinan el número de anillos afectados para cada elemento y los componentes del elemento que se alteran.

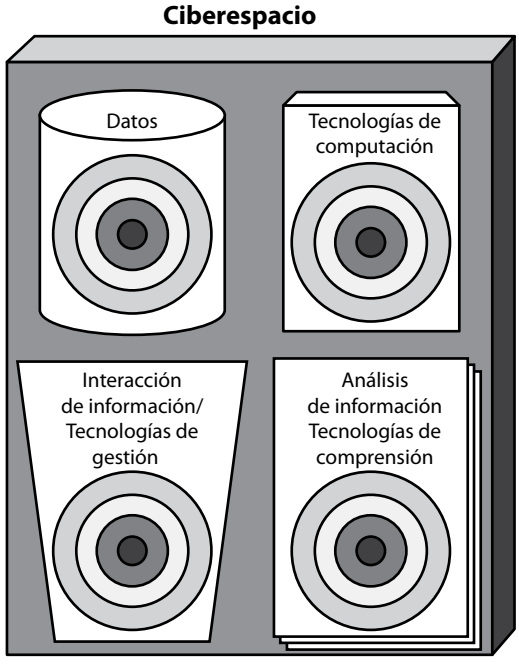

Figura 6. Estructura para modelar la importancia relativa de los componentes de los elementos ciberespaciales

Un entorno de adiestramiento de simulación ciberespacial puede preparar a los encargados de tomar decisiones para alterar de forma proactiva las defensas ciberespaciales tácticas, establecer las prioridades de datos, establecer la prioridad de los elementos del ciberespacio y operar durante un ataque ciberespacial estratégico donde algunos de los elementos y componentes ciberespaciales son vulnerables hasta un nivel incierto.

El método de simulación descrito arriba nos permite tratar las cuatro consideraciones de adiestramiento del encargado de tomar decisiones y defensor ciberespacial con un riesgo mínimo para el ciberespacio del mundo real junto con la alta fidelidad en el entorno de simulación ciberespacial. El problema de simulación que sigue es determinar las métricas ciberespaciales para evaluar tanto el estado del ciberespacio simulado y del mundo real y desarrollar la consciencia situacional. Las métricas ciberespaciales deben proporcionar detalles en el estado ciberespacial, intentos de ataques ciberespaciales, objetivos de ataques ciberespaciales, el nivel de éxito de un ataque ciberespacial y la eficacia de las defensas ciberespaciales desplegadas a niveles de elementos y componentes.[23]

Resumen y asuntos abiertos

El dominio ciberespacial tiene un objetivo, el mando de los elementos ciberespaciales. Mientras que los encargados de tomar decisiones esperan implícitamente el dominio ciberespacial, no está asegurado a la luz de las tecnologías de ataques ciberespaciales tácticos actuales y tecnologías de defensa ciberespacial tácticas. Lograr el dominio ciberespacial no garantizará la victoria para una fuerza centrada en los datos; no obstante, la falta de dominio ciberespacial casi ciertamente asegurará su derrota. Cualquier método de dominio ciberespacial debe poseer dos

rasgos cruciales: el método debe mejorar la seguridad ciberespacial defensiva y mantener la fiabilidad del sistema durante el ataque ciberespacial. El método descrito arriba para lograr el dominio defensivo ciberespacial requiere una DLCD junto con el adiestramiento de simulación para asistir a los encargados de tomar decisiones y defensores ciberespaciales estratégicos. Puede proporcionar la experiencia necesaria para permitir a los encargados de tomar decisiones que operen dentro de un entorno defensivo ciberespacial arriesgado e identificar, analizar y predecir los objetivos y la presencia de ataques ciberespaciales. El mismo método permite también el desarrollo y la evaluación de opciones de defensa ciberespacial estratégica para emplearla contra diversos ataques y campañas ciberespaciales. El método complementa el JIE o arquitecturas de flujo de datos similares y sus tecnologías de defensa ciberespacial táctica.

A medida que mejoran las tecnologías ciberespaciales, aumentarán los retos para lograr el dominio ciberespacial. Además, aumentará la complejidad de futuros sistemas ciberespaciales y del ciberespacio, según lo atestigua el desarrollo de tecnologías de nubes de nubes, tecnologías de "redes inteligentes" para el control remoto y la gestión de infraestructura del mundo real (sistemas SCADA),[24] el despliegue de IPv6 y la "Internet de cosas".[25] Esperamos que la mayor eficacia de las tecnologías de computación y la mayor complejidad de los ataques ciberespaciales tácticos y estratégicos aumentarán las dificultades planteadas al defensor ciberespacial y crearán nuevas rutas para ejecutar los ataque ciberespaciales.

La preparación para futuros ataques ciberespaciales requiere el desarrollo de sistemas de adiestramiento que imparten la experiencia y los conocimientos expertos necesarios para hacer posible una defensa ciberespacial estratégica y táctica efectiva. Aunque ahora se pueden desplegar los sistemas de adiestramiento requeridos, antes de poder desplegar un entorno de simulación ciberespacial completamente inclusivo para fines de adiestramiento, se debe llevar a cabo una investigación y un desarrollo adicionales para avanzar en el entendimiento de las batallas ciberespaciales, los modelos de comportamiento humano, las inferencias de intenciones, la visualización de información, la extracción de datos y la toma de decisiones durante el conflicto ciberespacial y la defensa ciberespacial estratégica. Un área adicional importante de investigación consiste en entender mejor la toma de decisiones y la consciencia situacional dentro de entornos de datos a gran escala y alto volumen que tienen ruido e incertidumbre inherentes a los datos así como debido a los ataques ciberespaciales. La investigación requerida en un entorno de alto volumen de datos radica en la intersección de programación de la máquina, extracción de datos, teoría de juegos, análisis de datos a gran escala y tecnologías de desarrollo de consciencia situacional. Un área final de investigación adicional es la evaluación de la efectividad de opciones de defensa ciberespacial táctica más apropiadas para lograr cada una de las estrategias de defensa ciberespacial apropiadas.

Aunque las operaciones de decepción y rechazo de información son tan antiguas como la guerra misma, los ataques ciberespaciales técnicamente refinados permiten, por primera vez, un ataque a gran escala, persistente y prácticamente no detectable en los datos, las herramientas y otros elementos del ciberespacio que emplea rutinariamente un encargado de tomar decisiones. El ataque ciberespacial técnicamente refinado del futuro destruirá o corromperá datos, sorprenderá a los encargados de tomar decisiones, generará confusión, demorará la respuesta y aumentará considerablemente lo que Clausewitz llama "niebla y fricción" en la guerra. Como habrá una lucha en el ciberespacio, los encargados de tomar decisiones deben estar preparados para ataques ciberespaciales estratégicos diseñados para socavar su capacidad de toma de decisiones. No estar preparado para los efectos de un ataque ciberespacial estratégico es correr un peligro innecesario. En el futuro, tratar el reto del ataque ciberespacial estratégico se hará más crítico para el éxito, no menos.[26] ❑

Glosario

computación en la nube —modelo para permitir un acceso ubicuo de la red a petición a un grupo compartido de recursos de computación configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden aprovisionarse y emitirse rápidamente con un esfuerzo de gestión o una interacción con los proveedores de servicios mínimos.

métricas a nivel de componentes —miden el rendimiento de las características específicas de un componente ciberespacial. Entre otros ejemplos de componentes se incluyen (1) el número de intercambios de páginas por intervalo de tiempo en cada máquina virtual, (2) el tiempo transcurrido promedio antes de intercambiar una página en una máquina virtual, (3) el tiempo transcurrido promedio para migrar una máquina virtual de un anfitrión a otro, y (4) el tiempo promedio para ejecutar un cifrado de RC4 un número fijo de veces en una entrada de texto especificada clara entre máquinas virtuales diferentes y otras.[27]

ataque ciberespacial —una aplicación de tecnologías de seguridad ciberespacial dentro del ciberespacio con la intención de degradar los datos, las tecnologías de computación, el análisis y la comprensión de información o la capacidad de interacción/gestión de información de un adversario para ventaja propia.

defensa ciberespacial —la aplicación de tecnologías de seguridad ciberespacial para proteger la parte propia del ciberespacio a fin de asegurar los datos y las tecnologías de computación así como para proteger el análisis y la comprensión de información y las capacidades de interacción/gestión de información.

tecnologías de seguridad ciberespacial —subconjunto de tecnologías de computación usado para proteger los datos propios, las tecnologías de análisis y compresión de información, las tecnologías de computación y las tecnologías de interacción/gestión de información o para socavar las de un adversario.

ciberespacio —se compone de cuatro elementos: (1) datos, (2) tecnologías de computación (como computadoras, software, redes/infraestructura de computadoras, protocolos de redes, virtualización y computación en la nube), (3) tecnologías de análisis y comprensión de información (incluida la visualización de información, la inteligencia artificial, la colaboración, las tecnologías de extracción de datos y las tecnologías de datos grandes), y (4) tecnologías interaction/gestión de información (incluida la interacción entre seres humanos y computadoras, los agentes inteligentes, las inferencias de intención humana y las tecnologías de bases de datos).

certificado digital —clave pública firmada. Una autoridad fiable firma el certificado digital antes de que se emita.

DNSSEC (Convención de Extensiones de Seguridad del Sistema de Nombres de Dominios)—conjunto de especificaciones de fuerza de tarea de ingeniería de Internet (IETF) para asegurar ciertas clases de información proporcionadas por el Sistema de Nombres de Dominios (DNS) en redes de protocolo de Internet (IP). Un servidor de nombres de dominios gestiona el depósito de nombres de dominios y proporciona la resolución de nombres para una zona de Internet. Las especificaciones de DNSSEC están cubiertas por Solicitud de Comentarios (RFC) 4033, 4034, 4035 y 3833 en http://www.ietf.org/rfc.html.

exploit —software que ataca una vulnerabilidad de seguridad ciberespacial.

inferencias de intención (humanas) —técnica basada en inteligencia artificial usada para proporcionar una interfaz de usuario inteligente en la que los objetivos del usuario se deducen basándose en un historial de acciones de usuario y una representación computable de la misión actual.[28]

corriente de información —ruta lógica por la arquitectura desde una fuente de información a un sumidero de información diseñado.

IPSEC (Seguridad de Protocolo de Internet)-conjunto de protocolos para asegurar las comunicaciones de IP en el estrato de la red, estrato 3 del modelo de OSI, autenticando o cifrando

cada paquete de IP en una corriente de datos. IPSEC incluye protocolos para el establecimiento de claves criptográficas.

nube de nubes —modelo para computar basado en una nube compuesta por nubes de computación.

software malicioso —software usado para alterar la operación de la computadora, recopilar información sensible u obtener acceso a un sistema de computadoras privado. Incluye virus de computadora, ransomware o software de rescate, puertas traseras, gusanos, troyanos, rootkits, programas espía, software bandido, y otros programas de software maliciosos. El tipo de software malicioso se clasifica según se ejecuta, cómo se propaga y lo que hace. Un **virus** es software malicioso que se puede ejecutar por sí mismo colocando su propio código en la ruta de ejecución de otro programa y puede reproducirse remplazando los archivos de computadora existentes por copias de sí mismo. Un **troyano** es un programa oculto que pasa por una aplicación inofensiva. Un **gusano** no requiere un programa anfitrión para propagarse sino que se introduce en una computadora por una brecha en las defensas del sistema de computadoras y se propaga usando defectos de seguridad de tráfico de la red. Una **puerta trasera** es software que permite el acceso al sistema de la computadora pasando por alto los procedimientos de autenticación normales.

rootkit —software que oculta rastros de un ataque, instala troyanos y puertas traseras, proporciona al atacante un control de la raíz del sistema, y permite actividades maliciosas adicionales.

consciencia situacional (SA) —"la percepción de los elementos en el entorno dentro de un volumen de espacio y tiempo, la comprensión de su significado, la proyección de su estado en el futuro próximo, y la predicción de cómo las diversas acciones afectarán la satisfacción de sus propios objetivos".[29] Endsley identifica cuatro componentes de consciencia situacional: **percepción** (cuáles son los datos), **comprensión** (entender los hechos), **proyección** (anticipación basada en entendimiento) y **predicción** (evaluación de cómo las fuerzas exteriores pueden actuar sobre la situación para afectar sus proyecciones). Estas etapas son similares pero no idénticas a la estructura de bucle de observar, orientar decidir y actuar (OODA) de Boyd.[30]

red inteligente —emplea un control remoto basado en computadoras y automatización de todos los elementos de suministro de corriente eléctrica para optimizar la generación y la distribución de corriente eléctrica.

software indicador—software que convierte los datos recopilados por un software sonda en una medida que es significativa para un sistema particular con el fin de afinar el rendimiento, asegurar la información, validar las funciones, ser compatible o evaluar la corrección operacional.

software sonda —software que se relaciona con un sistema de operación, aplicación operacional o subconjunto de una aplicación para recopilar datos para indicadores.

virtualización —técnica para emular un recurso de computación y ocultar las características físicas de recursos de computación de los sistemas, las aplicaciones o los usuarios finales que se relacionan con esos recursos. La virtualización explota las tecnologías de máquinas virtuales. Las tecnologías de virtualización proporcionan seis ventajas clave: (1) uso eficiente de recursos de computación, que reducen la infraestructura de tecnologías de información y los requisitos medioambientales (corriente, enfriamiento y bienes raíces); (2) aislamiento de fallas en las que un error de aplicación, una caída del sistema de operación o un error de usuario en una máquina virtual no afectará el uso de otras máquinas virtuales en el mismo sistema; (3) mayor seguridad donde puedan contenerse y ponerse en cuarentena las vulnerabilidades o exploits en una sola máquina virtual sin afectar todo el sistema; (4) aprovisionamiento rápido mediante copia de archivos o clonación de volumen usado para crear rápidamente nuevas máquinas virtuales; (5) flexibilidad para gestionar cambios con el fin de incluir la capacidad de redimensionar según la demanda de servicios, sistemas de operación únicos y aprovisionamiento de servicios; y (6) portabilidad mediante la abstracción de dispositivos combinada con la encapsulación de datos virtuales en discos virtuales. La virtualización es una tecnología clave para la computación en la nube.

Se dispone de definiciones adicionales en http://www.sans.org/security-resources/glossary-of-terms/and http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf.

Notas

1. Para nuestros fines, los cuatro elementos (o aspectos) del ciberespacio son (1) datos, (2) tecnologías de computación, (3) tecnologías de interacción y gestión de información y (4) tecnologías de análisis y comprensión de información.

2. Chris Buckley, "China PLA Officers Call Internet Key Battleground" (Los oficiales del Ejército de Liberación Popular de China llaman a Internet el campo de batalla clave), Reuters, 3 de junio de 2011. El Coronal Superior Ye Zheng y su colega Zhao Baoxian, hacen énfasis en *China Youth Daily* en la importancia de las capacidades bélicas ciberespaciales de China, llegando a la conclusión de que "así como la guerra nuclear fue la guerra estratégica de la era industrial, la guerra ciberespacial se ha convertido en la guerra estratégica de la era de la información, y esta se ha convertido en una *forma de batalla que es masivamente destructora y concierne a la vida y muerte de las naciones*". Vea también R. A. Clarke y R. Knake, *Cyber War: The Next Threat to National Security and What to Do about It (La guerra ciberespacial: la siguiente amenaza para la seguridad nacional y qué hacer con esto),* (New York: HarperCollins, 2010); A. F. Krepinevich, *Cyber Warfare: A Nuclear Option? (La guerra ciberespacial: ¿una opción nuclear?),* (Washington: Center for Strategic and Budgetary Assessments, 2012); General Keith Alexander, *Testimonio ante el Comité de Servicios Armados de la Cámara de Representantes*, 23 de septiembre de 2010; D. E. Geer y J. Archer, "Stand Your Ground" (No ceda terreno), *IEE Security and Privacy* 10, Nº 4 (2012): 96; "Panetta Warns of Dire Threat of Cyberattack on U.S." (Panetta nos advierte de las peligrosas amenazas de los ataques ciberespaciales en EUA.), *New York Times*, 11 de octubre de 2012; y B. H. Liddell Hart, *The Revolution in Warfare (La revolución en la guerra)* (New Haven, CT: Yale University Press, 1932), 121.

3. Este y otros términos se tratan en un glosario al final del artículo.

4. Val Smith y Chris, "Why Black Hats Always Win" (¿Por qué ganan siempre los piratas de sombrero negro?), *Blackhat.com*, enero de 2010; Joanna Rutkowska, "Subverting Vista Kernel for Fun and Profit" (Subversión del núcleo de Vista por motivos de diversión y beneficios), Black Hat USA, julio de 2006; J. Levine, J. Grizzard y H. Owen, "Detecting and Categorizing Kernel-Level Rootkits to aid Future Detection" (Detección y categorización de rotkits de nivel de núcleo para contribuir a una detección futura), *IEEE Security and Privacy* 4, Nº 1 (enero/febrero de 2006): 24–32; Rutkowska, "Rootkit Hunting vs. Compromise Detection" (Búsqueda de rootkits y detección de riesgos), Black Hat Federal 2006, Washington, DC, 25 de enero de 2006; A. Lakhotia, "Analysis of Adversarial Code: Problems, Challenges, and Results" (Análisis de código del adversario: problemas, retos y resultados), Black Hat Federal 2006; William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy" (Defensa de un nuevo dominio: la estrategia ciberespacial del Pentágono), *Foreign Affairs* 89, no. 5 (septiembre/octubre de 2010); A. Acquisti y J. Grossklacs, "Privacy and Rationality in Individual Decision Making" (Privacidad y racionalidad en la toma de decisiones individual), *IEE Security and Privacy* 3, Nº 1 (2005): 26–33; I. P. Cook y Pfleeger, "Security Decision Support: Challenges in Data Collection and Use" (Apoyo de decisiones de seguridad; retos de recopilación y uso de datos), *IEE Security and Privacy* 8, Nº 3 (2010): 28–35; J. Giffin, "The Next Malware Battleground: Recovery after Unknown Infection" (El siguiente campo de batalla de software malicioso: recuperación después de una infección desconocida), ibid., 77–82; K. J. Hole y L. Netland, "Toward Risk Assessment of Large-Impact and Rare Events" (Hacia la evaluación de riesgos de eventos de gran impacto y raros) ibid., 21–27; J. R. Kenney y C. Robinson, "Embedded Software Assurance for Configuring Secure Hardware" (Seguro de software integrado para configurar equipos seguros), *IEE Security and Privacy* 8, no. 5 (2010): 20–26; M. E. Johnson y Pfleger, "Addressing Information Risk in Turbulent Times" (Cómo tratar el riesgo de la información en tiempos turbulentos), *IEE Security and Privacy* 9, Nº 1 (2011): 49–58; J. Schiffman y otros, "Network-Based Root of Trust for Installation" (Raíz basada en la red de confianza para la instalación), ibid., 40–48; B. Stone-Grosset y otros, "Analysis of a Botnet Takeover" (Análisis de una toma de una red de robots informáticos), ibid., 64–72; P. Ning, Y. Cui y D. S. Reeves, "Intrusion Detection: Constructing Attack Scenarios through Correlation of Intrusion Alerts" (Detección de intrusiones: construcción de situaciones de ataque mediante la correlación de alertas e intrusiones). *Minuta del 9º Congreso de ACM sobre Seguridad y Comunicación de Computadoras*, noviembre de 2002; M. M. Pillai, J. H. P. Eloff, y H. S. Venter, "An Approach to Implement a Network Intrusion Detection System Using Genetic Algorithms" (Método para implementar un sistema de detección de intrusión de redes usado algoritmos genéticos), *Minuta del Congreso de Investigación Anual de 2004 del Instituto Sudafricano de Científicos Informáticos y Tecnologías de Información en Investigación de IT en Países en Vías de Desarrollo*, octubre de 2004; E. Skoudis y L. Zeltser, *Malware: Fighting Malicious Code (Software malicioso: lucha contra el código malicioso)* (Upper Saddle River, NJ: Prentice Hall, 2003); C. C. Zou, W. Gong y D. Towsley, "Formation and Simulation: Worm Propagation Modeling and Analysis under Dynamic Quarantine Defense" (Formación y simulación: modelos de propagación de gusanos y análisis bajo defensa de cuarentena dinámica), *Minuta del Taller sobre Código Malicioso Rápido de ACM de 2003*, octubre de 2003; R. Graham y D. Maynor, "SCADA Security and Terrorism: We're Not Crying Wolf" (Seguridad y terrorismo de SCADA: no son alarmas falsas), Black Hat Federal 2006; M. Jakobson y Z. Tamzan, *Crimeware: Understanding New Attacks and Defenses (Delitos informáticos; cómo entender los ataques y las defensas nuevos)* (Upper Saddle River: Addison-Wesley, 2008); J. V. Antrosio y E. W. Flup, "Malware Defense Using Network Security Authentication" (Defensa de software malicioso usando autenticación de seguridad de redes), *Minuta del 3º Taller Internacional sobre Seguridad de Información (IWIA'05) del IEEE*, marzo de 2005; J. Aycock y K. Barker, "Viruses 101" (Virus 101) *Boletín de ACM SIGCSE: Minuta del 36º Simposio Técnico de SIGCSE sobre Educación de Ciencias Informáticas* 37, no. 1 (febrero de 2005); D. Ellis, "Formation and Simulation:

Worm Anatomy and Model" (Formación y simulación: anatomía y modelo de gusanos) *Minuta del Taller sobre Código Malicioso Rápido de ACM de 2003*, octubre de 2003; D. M. Kienzle y M. C. Elder, "Internet WORMS: Past, Present, and Future: Recent Worms: A Survey And Trends" (GUSANOS de Internet: pasado, presente y futuro: gusanos recientes: estudio y tendencias), ibid.; J. Nazaro, *Defense and Detection Strategies against Internet Worms (Estrategias de defensa y detección contra los gusanos de Internet)* (Boston: Artech House, 2004); S. T. King y P. M. Chen, "Backtracking Intrusions" (Identificación de intrusiones) *ACM Transactions on Computer Systems (TOCS)* 23, Nº 1, enero de 2005; C. Kruegel, W. Robertson y G. Vigna, "Detecting Kernel-Level Rootkits through Binary Analysis" (Detección de rootkits a nivel de núcleo mediante un análisis binario), *Minuta del 20º Congreso Anual de Aplicaciones de Seguridad Informática*, diciembre de 2004; C. P. Pfleeger y S. L. Pfleeger, *Analyzing Computer Security: A Threat, Vulnerability, Countermeasure Approach (Análisis de seguridad de computadoras: método de amenaza, vulnerabilidad y contramedidas),* (Upper Saddle River: Prentice Hall, 2012); Pfleeger y Pfleeger, *Security in Computing (Seguridad en computación)*, 4ª edición (Upper Saddle River: Prentice Hall, 2007); R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems (Ingeniería de seguridad: guía para construir sistemas distribuidor fiables)*, 2ª edición (Indianapolis: Wiley, 2008); y M. Maras, *Computer Forensics: Cybercriminals, Laws, and Evidence (Informática forense; delincuentes ciberespaciales, leyes y evidencia)* (Burlington, MA: Jones & Bartlett, 2012).

5. Ibid.

6. J. M. Graaido, R. Schlesinger y K. Hoganson, *Principles of Modern Operating Systems (Principios de sistemas de operación modernos)*, segunda edición (Burlington, MA: Jones & Bartlett, 2013); P. A. Karger y D. R. Safford, "I/O for Virtual Machine Monitors: Security and Performance Issues" (E/S para monitores de máquinas virtuales), *IEE Security and Privacy* 6, Nº 5, (2008): 16–23; H. Takabi, J. B. D. Joshi y G. Ahn, "Security and Privacy Challenges in Cloud Computing Environments" (Retos de seguridad y privacidad en entornos de computación en la nube), *IEE Security and Privacy* 8, Nº 6, (2010): 24–31; Qian Liu y otros, "An In-VM Measuring Framework for Increasing Virtual Machine Security in Clouds" (Una estructura de medición en máquina virtual para aumentar la seguridad de la máquina virtual en nubes), *IEE Security and Privacy* 8, Nº 6, (2010): 56–62; R. L. Krutz y R. D. Vines, *Cloud Security: A Comprehensive Guide to Secure Cloud Computing (Seguridad en la nube: una guía completa para asegurar la computación en la nube)* (Indianapolis: Wiley, 2010); A. Belapurkar y otros, *Distributed Systems Security: Issues, Processes, and Solutions (Seguridad de sistemas distribuidos: temas, procesos y soluciones),* (Indianapolis: Wiley, 2009); C. Cachin y M. Schunter, "A Cloud You Can Trust" (Una nube en la que puede confiar), *Espectro del IEEE* 48, Nº 12 (2011): 28–51; y K. Jamsa, *Cloud Computing (Computación en la nube)* (Burlington, MA: Jones & Bartlett, 2013).

7. D. S. Alberts y otros, *Understanding Information Age Warfare (Cómo entender la guerra de la era de la información),* (Washington: CCRP Press, 2001); y Alberts y R. E. Hayes, *Power to the Edge (Poder al límite)* (Washington: CCRP Press, 2003)

8. Ibid.

9. Mica Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems" (Hacia una teoría de consciencia situacional en sistemas dinámicos), *Human Factors* 37, Nº 1 (1995): 35–64.

10. Frans Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd (Ciencia, estrategia y guerra; la teoría estratégica de John Boyd),* (Abingdon, UK: Routledge, 2005).

11. L. Ying, L. Bingyang y W. Huiqiang, "Dynamic Awareness of Network Security Situation Based on Stochastic Game Theory" (Consciencia dinámica de situación de seguridad de redes basada en la teoría de juegos estocástica), 2º Congreso Internacional sobre Ingeniería de Software y Extracción de Datos (2010), 101–5; K. Smith y P. A. Hancock, "Situation Awareness is Adaptive, Externally Directed Consciousness" (La consciencia situacional es una consciencia de adaptación dirigida externamente), *Factores humanos* 37, Nº 1 (1995): 137; VADM A. K. Cebrowski, "Network-Centric Warfare: An Emerging Military Response to the Information Age" (Guerra centrada en redes: una respuesta militar emergente para la edad de la información), Simposio de Investigación y Tecnología de Mando y Control de 1999, 29 de junio de 1999, http: //www.nwc.navy.mil/press/speeches/ccrp2htm; y P. Hinds, *Perspective Taking among Distributed Workers: The Effect of Distance on Shared Mental Models of Work (Perspectiva adoptada entre los trabajadores distribuidos: el efecto de la distancia en modelos de trabajo mental compartido)*, Artículo de trabajo de la World Trade Organization 7 (Stanford, CA: Centro de Trabajo, Tecnología y Organización, 1999).

12. Lynn, "Defending a New Domain" (Defensa de un nuevo dominio).

13. J. H. Saltzer y M. D. Schroeder, "The Protection of Information in Computer Systems" (La protección de la información en sistemas informáticos), *Minuta del IEEE* 63, Nº 9, (1975): 1278–1308; Saltzer y M. F. Kaashoek, *Principles of Computer System Design (Principios de diseño de sistemas informáticos)* (Indianapolis: Wiley, 2009); R. E. Smith, *Elementary Information Security (Seguridad de información elemental)* (Burlington, MA: Jones & Bartlett, 2013); A. Kerckhoffs, "La Cryptographie Militare" (La criptografía militar), *Journal Sciences Militaires* 9 (febrero de 1883): 161–91; B. Schneier, "Secrecy, Security, and Obscurity" (Confidencialidad, seguridad y oscuridad), *Noticiero de criptogramas*, 15 de mayo de 2002, http: //www.schneier.com/crypto-gram-0205.html; C. E. Shannon, "Communication Theory of Secrecy Systems" (Teoría de comunicación de sistemas confidenciales), *Bell System Technical Journal*, octubre de 1949, 656–715; D. E. Denning, "A Lattice Model of Secure Information Flow" (Un modelo reticular de flujo de información seguro). *Comunicaciones del ACM* 19, Nº 5 (1976): 236–43; DoD 5200.28-STD, *Criterios de evaluación de sistemas de computadoras fiables del Departamento de Defensa*, 26 de diciembre de 1985; P. A. Karger y R. R. Schell, *Multics Security Evaluation: Vulnerability Analysis (Evaluación de seguridad de Multics; análisis de vulnerabilidad)*, ESD-TR-74-193, tomo II, División de Sistemas Electrónicos de HQ, junio de 1974; K. Thompson, "Reflections on Trusting Trust" (Reflexiones sobre confiar en la confianza), *Comunicaciones del ACM* 27, no. 8 (1984): 761–63; R. E. Smith, "A Contemporary Look at Saltzer and Schroeder's 1975 Design Principles"

(Vistazo contemporáneo de los principios de diseño de Saltzer y Schroeder de 1975), *IEE Security and Privacy* 10, Nº 6, (2012): 20–25; R. Smith, *Elementary System Security (Seguridad de sistemas elementales)* (Burlington, MA: Jones & Bartlett, 2013); S. Smith y J. Marchesini, *The Craft of System Security (El arte de la seguridad de sistemas),* (Upper Saddle River: Addison-Wesley, 2008); S. Lipner, T. Jaeger y M. E. Zurko, "Lessons from VAX/SVS for High-Assurance VM Systems" (Lecciones de VAX/SVS para sistemas de máquinas virtuales de alta seguridad), *IEE Security and Privacy* 10, Nº 6 (2012): 26–35; J. C. Wray, "An Analysis of Covert Timing Channels" (Análisis de canales de temporización encubiertos), *Minuta del Simposio sobre Seguridad y Privacidad del IEEE,* (1991): 52–61; L. J. Fraim, "SCOMP: A Solution to the Multilevel Security Problem" (SCOMP, solución al problema de seguridad de múltiples niveles), *IEEE Computer* 16, no. 7 (1983): 26–34; C. Larman, *Agile and Iterative Development: A Manager's Guide (Desarrollo ágil e iterativo: guía del gerente)* (Boston: Pearson Education, 2004); H. Shrobe y D. Adams, "Suppose We Got a Do-Over: A Revolution for Secure Computing" (Supongamos que partimos de cero otra vez: revolución para una computación segura), *IEEE Security and Privacy* 10, Nº 6 (2012): 36–39; R. J. Feiertag yP. G. Neumann, "The Foundations of a Provably Secure Operating System" (Los cimientos de un sistema de operación seguro demostrable), *Minuta del Congreso Nacional de Computadoras,* 1979, 329–34; y W. H. Ware, *Security Controls for Computer Systems: Report of the Defense Science Board Task Force on Computer Security (Controles de seguridad para sistemas de computadoras: informe de la fuerza de tarea de la junta de ciencias de defensa sobre seguridad de computadoras)* (Santa Monica, CA: RAND, 1970).

14. Ibid.

15. R. J. Adair y otros, "A Virtual Machine System for the 360/40" (Un sistema de máquinas virtuales para el 360/40), Informe del Centro Científico de Cambridge 320, IBM, mayo de 1966; G. M. Amdahl, G. A. Blaauw y F. P. Brooks, "Architecture of the IBM System/360" (Arquitectura del sistema IBM/360), *IBM Journal of Research and Development* 8, Nº 2 (1964): 87–101; Paul Barham y otros, "Xen and the Art of Virtualization" (Xen y el arte de la virtualización), *Minuta del 19º Simposio de ACM sobre Principios de Sistemas de Operación (SOSP),* Bolton Landing, NY, October 2003, 164–77; A. Bieniusa, J. Eickhold y T. Fuhrman, "The Architecture of the Decent VM: Towards a Decentralized Virtual Machine for Many-Core Computing" (La arquitectura de la máquina virtual decente: hacia una máquina virtual descentralizada para computación de muchos elementos), Virtual Machines and Intermediate Languages (Systems Programming Languages and Applications: Software for Humanity) (Máquinas virtuales y lenguajes intermedios (lenguajes y aplicaciones de programación de sistemas)), Reno, NV, 17–21 de octubre de 2010; Sean Campbell y Michael Jeronimo, *Applied Virtualization Technology: Usage Models for IT Professionals and Software Developers (Tecnología de virtualización aplicada: modelos de uso para profesionales de IT y desarrolladores de software),* (Santa Clara, CA: Intel Press, 2006), cap. 9; R. P. Case y A. Padegs, "Architecture of the IBM System/370" (Arquitectura del sistema IBM/370), *Communications of the ACM* 21, Nº 1 (enero de 1978): 73–96; R. J. Creasy, "The Origin of the VM/370 Time Sharing System" (El origen de la máquina virtual/sistema de reparto de tiempo 370), *IBM Journal of R&D* 25, Nº 5 (septiembre de 1981): 483–90; R. W. Doran, "Amdahl Multiple-Domain Architecture" (Arquitectura de dominios múltiples de Amdahl), *Computer,* octubre de 1988, 20–28; R. C. Daley y J. B. Dennis, "Virtual Memory, Processes, and Sharing in MULTICS" (Memoria virtual, procesos y reparto en MULTICS), *Communications of the ACM* 11, Nº 5 (mayo de 1968): 306–12; T. Egawa, N. Nishimura y K. Kourai, "Dependable and Secure Remote Management in IaaS Clouds" (Gestión remota fiable y segura en nubes de IaaS), 4º Congreso Internacional de IEEE de 2012 sobre Tecnología y Ciencia de Computación en la Nube, 3–6 de diciembre de 2012, Taipei, Taiwán, 411–18; D. Gifford y A. Spector, "Case Study: IBM's System 360-370 Architecture" (Estudio práctico: arquitectura del sistema 360-370 de IBM), *Communications of the ACM* 30, Nº 4 (abril de 1987): 291–307; P. H. Gum, "System/370 Extended Architecture: Facilities for Virtual Machines*" (Arquitectura ampliada de sistema/370: instalaciones para máquinas virtuales), IBM Journal of Research and Development* 27, Nº 6 (1983): 530; K. Hwang y D. Li, "Trusted Cloud Computing with Secure Resources and Data Coloring" (Computación en la nube fiable con recursos seguros y colores de datos), *Computación de Internet del IEEE* 14, Nº 5 (septiembre/octubre de 2010): 14–22; A. S. Lett y W. L. Konigsford, "TSS/360: A Time-Shared Operating System" (TSS/360: sistema de operación repartido en el tiempo), *Minuta del Congreso de Informática Conjunto de Otoño,* AFIPS, tomo 33, parte 1 (1968): 15–28; A. Mann, "The Pros and Cons of Virtualization" (Ventajas y desventajas de la virtualización), *Business Trends Quarterly,* Primero trimestre de 2007; R. A. Meyer y L. H. Seawright, "A Virtual Machine Time-Sharing System" (Sistema de reparto de tiempo de máquinas virtuales), *IBM Systems Journal* 9, Nº 3 (1970): 199–218; Seawright y R. A. McKinnon, "VM/370–A Study of Multiplicity and Usefulness" (VM/370-Estudio de multiplicidad y utilidad), *IBM Systems Journal* 18, no. 1 (1979): 4–17; A. V. Anderson y otros, "Intel Virtualization Technology" (Tecnología de virtualización de Intel), *Computadora de IEEE* 38, no. 5,(2005): 48–56; B. Yee y otros, "Native Client: A Sandbox for Portable, Untrusted x86 Native Code" (Cliente nativo: área de pruebas de código nativo portátil y no fiable x86), 30º Simposio sobre Seguridad y Privacidad del IEEE de 2009, Oakland, CA, 17–20 de mayo de 2009, 79–93; e Y. Wen y K. Du, "Pollux VMM: A Virtual Machine Monitor for Executing Untrusted Code" (VMM Pollux: monitor de máquinas virtuales para ejecutar un código no fiable), 1º Congreso Internacional sobre Ciencia e Ingeniería de Información (ICISE2009), Nanjing, China, 28–29 de diciembre 2009, 1785–1788.

16. Cricket Liu y Paul Ablitz, *DNS and BIND (DNS y BIND),* quinta edición (Sebastopol, CA: O'Reilly & Associates, 2006).

17. A. Karasidis, *DNS Security (Seguridad de DNS,* (New York: Springer, 2012); y N. Doraswamy y D. Harkins, *IPSEC: The New Security Standard for the Internet, Intranets, and Virtual Private Networks (IPSEC: la nueva norma de seguridad para la Internet, las redes internas y las redes privadas virtuales),* (Upper Saddle River: Prentice Hall, 2003.

18. D. L. Rulke y J. Galaskiewicz, "Distributed Knowledge, Group Network Structure, and Group Performance" (Conocimientos distribuidos, estructura de redes de grupos y rendimiento de grupos), *Management Science* 46, Nº 5 (mayo de 2000): 612–22; M. R. Stytz y S. B. Banks, "Metrics for Assessing Command, Control, and Communications Capabilities" (Métricas para evaluar las capacidades de mando, control y comunicación), 11º Simposio Internacional de Investigación y Tecnología de Mando y Control, San Diego, CA, 20–26 de junio de 2006; P. Barton, "What Happens to Value of Information Measures as the Number of Decision Options Increases?" (¿Qué pasa con el valor de las medidas de información a medida que aumentan las opciones de las decisiones?), *Health Economics* 20 (2011): 853–63; D. Bellin, "The Economic Value of Information" (El valor económico de la información), *Science Communication* 15, Nº 2 (1993): 233–40; A. Cleveland, "Harvesting the Value of Information" (Cómo cosechar el valor de la información), *Journal of Management and Engineering* 15, Nº 4 (1999): 37–42; P. Delquié, "The Value of Information and Intensity of Preference" (El valor de la información y la intensidad de preferencia), *Análisis de decisiones* 5, Nº 3 (2008): 129–39, 169; R. Glazer, "Measuring the Value of Information: The Information-Intensive Organization" (Medición del valor de la información: la organización intensiva de información), *IBM Systems Journal* 32, Nº 1 (1993): 99; T. Hulme, "Unlocking the Business Value of Information: Information on Demand" (Resolución del valor comercial de información; información a petición), *Business Information Review* 26, Nº 3 (2009): 170–81; M. E. Johnson y S. L. Pfleger, "Addressing Information Risk in Turbulent Times" (Trato del riesgo de información en tiempos turbulentos), *IEE Security and Privacy* 9, Nº 1 (2011): 49–58; A. Kangas, "Measuring the Value of Information in Multicriteria Decision Making" (Medición del valor de información en toma de decisiones de criterios múltiples), *Forest Science* 26, Nº 6 (2010): 558–66; C. Oppenheim y otros, "Studies on Information as an Asset I: Definitions" (Estudios sobre información como haber 1: definiciones), *Journal of Information Science*, vol. 29, Nº 3, (2003): 159–66; Oppenheim y otros, "Studies on Information as an Asset II: Repertory Grid" (Estudios sobre información como haber II: red de repertorio), *Journal of Information Science* 29, Nº 5 (2003): 419–32; Oppenheim y otros, "Studies on Information as an Asset III: Views of Information Professionals" (Estudios sobre información como haber III: opiniones de profesionales de la información), *Journal of Information Science* 30, Nº 2 (2003): 181–90; Oppenheim y otros, "The Attributes of Information as an Asset" (Los atributos de información como un haber), *New Library World* 102, Nº 11/12 (2001): 458–63; R. Fattahi y E. Afshar, "Added Value of Information and Information Systems: A Conceptual Approach" (Valor añadido de información y sistemas de información: método conceptual), *Library Review* 55, Nº 1–2 (2006): 132–47; A. Repo, "The Dual Approach to the Value of Information: An Appraisal of Use and Exchange Values" (El método doble del valor de información; una evaluación de valores de uso e intercambio), *Information Processing & Management* 22, Nº 5 (1986): 373–83; A. Shepanski, "The Value of Information in Decision Making" (El valor de la información en la toma de decisiones), *Journal of Economic Psychology* 5, Nº 2 (1984): 177–94; y J. Sillince, "A Stochastic Approach of Information Value" (Método estocástico de valor de la información), *Information Processing & Management* 31, Nº 4 (1995): 543–54.

19. M. R. Stytz y S. B. Banks, "Toward Improved Software Security Training Using a Cyber Warfare Opposing Force (CW OPFOR): The Knowledge Base Design" (Hacia un adiestramiento mejorado de la seguridad de software usando una fuerza de oposición de la guerra ciberespacial (CW POFOR), *Minuta del Congreso de SPIE sobre Extracción de Datos, Detección de Intrusión, Seguridad de Información y Redes de Datos 2005* 5812, no. 28–29 (marzo de 2005): 130–41; Stytz y Banks, "Metrics to Assess Command, Control, and Communications (C3) Performance within a Network-Centric Warfare Simulation" (Métricas para evaluar el rendimiento de mando, control y comunicaciones (C3) dentro de una simulación de guerra centrada en una red), *Minuta del Congreso de SPIE sobre cómo Habilitar la Ciencia de Simulación X*, tomo 6227 (abril de 2006): 17–21; Stytz y Banks, "Requirements and Issues in Cyberwarfare Simulation" (Requisitos y problemas en la simulación de la guerra ciberespacial), *Minuta del Taller de Interoperabilidad de Simulación de Otoño de 2000*, Orlando, FL, 17–22 de septiembre de 2000, 1–10; Stytz y Banks, "Toward Computer Generated Actors As Cyberspace Opposing Forces Used In Network Centric Warfare Simulations" (Hacia actores generados por computadora como fuerzas opositoras ciberespaciales usadas en simulaciones de guerra centradas en la red), *Minuta del Taller de Interoperabilidad de Simulación de la Primavera de 2004*, Washington, DC; 18–23 de abril de 2004, 84–95.

20. Se trata de un método que no usa simulación para la preparación de usuarios en caso de ataques ciberespaciales de S. L. Garfinkel y G. Dinout, "Operations and Degraded Security" (Operaciones y seguridad degradada), *Seguridad y privacidad del IEEE* 9, no. 6 (2011): 43–48.

21. Ibid.; y Stytz y Banks, "Metrics for Assessing Command, Control, and Communications Capabilities" (Métricas para evaluar las capacidades de mando, control y comunicaciones), 11º Simposio Internacional de Investigación y Tecnología de Mando y Control, 20–26 de junio de 2006, San Diego, CA.

22. G. Booch, J. Rumbaugh, e I. Jacobson, *The Unified Modeling Language User Guide (Guía del usuario de lenguajes de modelación unificados*) (Reading, MA: Addison-Wesley, 1999)

23. Nuestros primeros esfuerzos hacia el desarrollo de herramientas para métricas de rendimiento ciberespacial se tratan en referencias citadas anteriormente. Las métricas son similares a los algoritmos en línea de una pasada usados en comercio de alta frecuencia y se derivan de un procesamiento de señales digitales.

24. *ommunications of the ACM* 55, Nº 4: ejemplar especial sobre tecnología.

25. *IEEE Computer* 46, no. 2: ejemplar especial en la "Internet de las cosas".

26. J. Carr y otros Project Grey Goose Report on Critical Infrastructure: Attacks, Actors, and Emerging threats (Proyecto Grey Goose: información sobre infraestructura crítica: ataques, actores y amenazas emergentes) McLean, VA: Grey Logic, 2010),12 .

27. A. Jaquith, *Security Metrics: Replacing Fear, Uncertainty, and Doubt (Métricas de seguridad: cómo reemplazar el temor, la incertiudumbre y la duda),* (Upper Saddle River: Addison-Wesley, 2007)

28. S. Banks y C. Lizza, "Pilot's Associate: A Cooperative, Knowledge-Based System Application" (Socio del piloto: aplicación cooperativa de sistemas basados en conocimientos), *IEEE Expert* 6, no. 3 (1991): 18–29.

29. Mica Endsley, "Situation Awareness Global Assessment Technique (SAGAT)" (Técnica de Evaluación Global de Consciencia Situacional (SAGAT)), *Minuta del Congreso Nacional Aeroespacial y de Electrónica del IEEE de 1988*, 789–95.

30. singa, *Science Strategy and War (Estrategia de ciencia y guerra).*

Dr. Martin R. Stytz, **PhD**, Teniente Coronel USAF-Retirado; es profesor catedrático de seguridad ciberespacial de la Universidad de Maryland y profesor de investigación de la Universidad de Georgetown. Recibió un título de BS de la Academia de la Fuerza Aérea en 1975, un título de MA de la Universidad de Central Missouri, un título de MS de la Universidad de Michigan, y un doctorado en ciencias e ingeniería de computación de la Universidad de Michigan en 1989. Sus intereses de investigación incluyen simulación distribuida, protección de software y seguridad ciberespacial.

Dra. Sheila B. Banks, PhD, es presidente de Calculated Insight. Recibió su título de BS de la Universidad de Miami en 1984, un título de BSEE y un título de MS de ingeniería eléctrica e informática en 1987 de North Carolina State, y su doctorado de ingeniería informática (inteligencia artificial) de la Universidad Clemson en 1995. Entre sus temas de investigación se incluyen inteligencia artificial, comportamiento humano y modelación cognitiva, y seguridad ciberespacial.