

# Profesionales Cibernéticos en las Fuerzas Armadas y en la Industria—Asociación en Defensa de la Nación

Conversación entre la General de División Suzanne Vautrinot, USAF, Comandante, Veinticuatroava Fuerza Aérea, y el Sr. Charles Beard, Director de Información, Science Applications International Corporation

TRANSCRITO Y EDITADO POR EL CAPITÁN JEFFREY A. MARTÍNEZ, USAF,  
Y EL CAPITÁN MATTHEW R. KAYSER, USAF

UN DEBATE ESTRATÉGICO sobre cibernética ya no es un diálogo académico, y la tecnología asociada ya no es el dominio de los laboratorios de desarrollo de la industria o del gobierno. La “defensa” en el dominio cibernético es un imperativo nacional; los retos cada vez más complejos fuerzan a los ejecutivos superiores de la industria y del gobierno a ampliar los esfuerzos de colaboración para tratar estos retos. Las corporaciones de todo el mundo están aprovechando el dominio cibernético para suministrar bienes y servicios de forma más rápida y económica mientras equilibran la necesidad de proteger la información personal que les confían los clientes. Igualmente, los comandantes militares se basan cada vez más en las capacidades ciberintegradas para el mando y el control, y generar efectos en el campo de batalla, tanto cinéticos como no cinéticos. La clave para el éxito de la misión es salvaguardar los datos críticos, mientras se permite un acceso inmediato sin intercepción ni manipulación.

El 7 de noviembre de 2012, dos de nuestros ciberlíderes superiores de nuestra nación, la General de División Suzanne Vautrinot, comandante de la Veinticuatroava Fuerza Aérea y de las Ciberfuerzas Aéreas, y el Sr. Charles Beard, director de información y vicepresidente superior de Science Applications International Corporation (SAIC) se reunieron para tener una conversación. Durante esa conversación, el Sr. Beard narró una travesía de sus esfuerzos para reducir la superficie de ciberataque de su compañía y crear un entorno corporativo resultante en una solución de tecnología de información de una sola empresa, y la General de División Vautrinot no solamente articuló similitudes en la misión de la Fuerza Aérea de defender el país en el ciberespacio sino que también se concentró en cómo tanto la Fuerza Aérea como la industria pueden aplicar las lecciones aprendidas de éxitos como la migración de SAIC a medida que siguen avanzando hacia una postura de ciberseguridad más homogénea.

Con su consentimiento, nos gustaría compartir un diálogo privado entre colegas reconocidos y mutuamente respetados y socios en este dominio dinámico. Además, entrelazadas en esta conversación están las contribuciones de cada una de las escuadras ciberespaciales operacionales de la Veinticuatroava Fuerza Aérea, que explican puntos de debate clave y resaltan los esfuerzos actuales para poner en operación y normalizar el dominio ciberespacial.

\*\*\*\*\*

**Vautrinot:** No es sorprendente, sus esfuerzos tienen sentido, y existe una verdadera similitud de experiencia en esta área. Usted ha tomado lo que eran elementos significativamente diversos de una corporación y ha cambiado completamente la dinámica—primero desde el punto de vista organizativo y después tecnológicamente. Estoy interesado en qué cambios organizativos cree que fueron los más esenciales para ese éxito; me gustaría aprovechar esos cambios para nuestra responsabilidad compartida en este entorno global variable.

**Beard:** La responsabilidad compartida es algo correcto. Al observar la cibernética, reconocimos que el modelo del gobierno tenía que cambiar. Crecimos como 10.000 oficinas independientes, y aunque eso tiene sus ventajas desde un punto de vista de desarrollo de mercados y capacidad de respuesta del cliente, tiene sus desventajas desde un punto de vista de dirección de la tecnología de información y de la escala de una empresa. Necesitamos una agilidad estratégica para participar en múltiples mercados globales y en un entorno informático cada vez más hostil. El primer paso consistió en definir y estabilizar el entorno, y eso significó cambiar la manera de pensar sobre la tecnología de la información.

**Vautrinot:** En las fuerzas militares, los mandos importantes o las organizaciones funcionales podrían considerarse de la misma manera—todas muy talentosas pero muy discretas . . . la descripción “cilindros de excelencia” se nos viene a la mente. Desde un punto de vista de las operaciones militares, esto tiene sentido, pero presenta retos al tratar las amenazas y el riesgo desde el punto de vista del ciberespacio. Como la tecnología de información y las comunicaciones crecieron de forma descentralizada, existe una inercia aparente para conservar ese método descentralizado. No obstante, usted ha demostrado la necesidad de crear una solución de empresa para operar mejor lo que es ahora una ciberempresa.

**Beard:** El primer paso para nosotros fue establecer esa relación y asegurarnos de que teníamos un verdadero punto de vista de empresa acerca del entorno y empezamos a operarlo como un haber de la empresa—sin que importe cómo se originó. Como siguiente medida, empezamos a trabajar con el gobierno para hablar sobre la necesidad de compartir información sobre amenazas y mejorar nuestra postura respecto al ciberespacio. Nosotros [SAIC] operamos entornos de tecnología de información en nombre del gobierno. Tenemos información de clientes en nuestras redes, y asumimos la responsabilidad de su administración muy seriamente. No obstante, al mismo tiempo, somos una compañía que cotiza en bolsa y operamos de forma global. No pudimos simplemente adoptar un punto de vista centrado en EE.UU. sobre cómo íbamos a resolver este problema ya que la Fuerza Aérea tampoco podría adoptar dicha posición. Tuvimos que cambiar la referencia intelectual para muchas personas cuando nos referíamos al gobierno y lo que significaba realmente como corporación multinacional tratar este problema del ciberespacio.

**Vautrinot:** En los dominios aéreo y espacial, teníamos la ventaja de desarrollar sistemas exclusivos y a menudo superiores o especializados: transición de aviones de la quinta a la sexta generación y satélites de última tecnología . . . inherentemente únicos. Era siempre sobre sistemas militares. No obstante, el ciberespacio es un entorno interconectado global. Compartimos el mismo entorno artificial, y la industria utiliza esa “última tecnología”. Las fuerzas militares no pueden permitirse el lujo—técnica o financieramente—de responder de forma independiente. Necesitamos una responsabilidad compartida—industria, gobierno, organizaciones educativas, socios internacionales—para alterar el entorno para obtener una ventaja colectiva y responsabilizarnos mutuamente del éxito. En lenguaje militar, podemos cambiar el dominio para proporcionar libertad de movimiento a nuestros aliados a la vez que la negamos a nuestros adversarios. Todos estamos trabajando en el mismo espacio aunque quizás necesitemos calcular el riesgo y la respuesta a la misión de un modo un poco diferente.

**Beard:** Lo esencial es la gestión de los riesgos y las respuestas medidas. Vuelvo a mis días del Mando Aéreo Estratégico, donde operábamos en el dominio nuclear. Aunque la misión de disuasión estaba clara, la misión de ataque se entendía igualmente bien. La preparación para ambas estaba a la orden del día. A diferencia de los otros dominios dentro de las fuerzas armadas—tierra, aire, mar y espacio—la proyección de fuerzas y el control del dominio cibernético son muy difíciles. Estamos utilizando una infraestructura compartida de base global, y el adversario a menudo tiene una posición que es igual o mejor.

**Vautrinot:** Veo una dinámica global similar en nuestro apoyo a misiones de aviones pilotados por control remoto. Para garantizar la misión, teníamos que llevar a cabo una amplia investigación inicial para entender los diversos enlaces de Estados Unidos con el vuelo en el extranjero. El sistema estaba diseñado con aproximadamente 180 puntos de contacto, muchos de los cuales no están militarmente controlados, a través de diversas redes, incluidos sistemas extranjeros, lo que hacía que fuera crucial establecer relaciones con organizaciones y aliados comerciales. La seguridad y la garantía se convierten en una interdependencia tremenda, que también se puede ver en la industria.

**Beard:** En el dominio comercial, interdependencia equivale a continuidad de operaciones y gestión de riesgos. Hay una diferencia en la forma que consideramos la amenaza, pero la garantía de la misión para una compañía comercial es impulsada en gran medida por los mercados y geografías en las que opera y el tipo de operación que se está llevando a cabo. El hecho que esas operaciones se lleven a cabo en una infraestructura compartida a escala global es un contexto importante para ejecutivos de la corporación a fin de que entiendan al sopesar riesgos.

**Vautrinot:** Los comandantes que respaldamos han indicado un imperativo similar para el acceso ininterrumpido a datos de confianza y verificables. La garantía de la misión en el ciberdominio es tan básica para la misión que no podemos permitirnos el lujo de perder la capacidad de comunicación—es esencial para el mando y el control militares.

**Beard:** Exactamente. Una compañía puede disponer de las mayores capacidades del mundo, pero no puede operar en el dominio digital y si no puede sostener un acceso ininterrumpido a la infraestructura de energía y comunicaciones, es muy difícil tener un perfil de misión que sobreviva. Así pues, consideramos el mando y el control como muy parecidos en el contexto de las misiones militares y comerciales porque estamos tratando de llevar a cabo operaciones comerciales en todo el mundo. Si no puedo proporcionar acceso para disponer de unas comunicaciones limpias y una energía ininterrumpida, entonces se deteriora considerablemente la continuidad el negocio.

**Vautrinot:** A nivel de corporación, ustedes tenían que ir más allá de tener conciencia de lo que pasaba. Las personas tenían que apoyar, entender la codependencia y ver su ventaja para el individuo. Tener un debate a menor escala hace que el efecto sea tangible y el cambio aceptable. Un negocio con éxito puede aprovechar esto para mover la compañía en nuevos sentidos. ¿Fue la comprensión algo que estaba adaptado a cada individuo y a escala, o tuvo el liderazgo superior que impulsar la conciencia de la empresa a fin de cambiar la cultura de la organización?

**Beard:** En SAIC, tenemos suerte de disponer de personas en nuestra junta directiva que han recorrido los pasillos del gobierno y de la industria, que entienden que esta amenaza es real. Así pues, lo que empezamos a hacer fue trasladar ese riesgo al contexto de la empresa. Creo que lo que encontrará es que diversas industrias comerciales están más adelantadas en ese entendimiento, esa madurez. Ciertamente la industria de servicios financieros ha entendido esto durante muchos años. Disponen de comités de riesgo separados en sus juntas directivas, y es uno de los muchos riesgos que deben tener en cuenta. Tenemos otras industrias, como la energía, donde la conciencia va en aumento incluso más. Son testigos del cambio del vector de amenazas de una simple recopilación de inteligencia a la destrucción operacional, según se indicó en el caso de Saudi Aramco.<sup>1</sup> En la industria médica, una compañía podría pasarse una década y gas-

tar 10.000 millones de dólares de EE.UU. fabricando un producto o un medicamento nuevos, y ver cómo una copia exacta de ese producto se lanza al mercado en un país extranjero un año antes de recibir la aprobación de la Administración de Alimentos y Medicamentos (Food and Drug Administration) [FDA]. Toda su propiedad intelectual se ha esfumado, por lo que la corriente de ingresos anticipados por esa compañía para ese producto durante los 10 años siguientes se reduce significativamente. Los imperativos económicos se están convirtiendo en un peligro claro y presente para la economía nacional donde operan estas empresas, pero muchas compañías siguen sin entender las amenazas cibernéticas y sus posibles impactos, tanto físicos como económicos.

**Vautrinot:** Existe un reconocimiento similar referente a la dependencia cibernética. No obstante, no estoy seguro de que se conozca el nivel de dependencia, y nuestra capacidad para llevar cabo todas las misiones—volar, combatir y ganar en el aire, espacio y ciberespacio. Nuestro reto, a medida que avanzamos, es crear relaciones en todos los elementos de las misiones . . . el tejido operacional frente a los hilos de las misiones. A medida que ampliamos este enfoque, debemos saber cómo equilibrar estos esfuerzos operacionales con la capacidad de mantener y defender nuestras redes. Según la Veinticuatro Fuerza Aérea, la Escuadra de Comunicaciones de Combate 689 se especializa en mantener este equilibrio ampliando las capacidades cibernéticas al límite táctico en apoyo del combatiente mientras continúa proporcionando comunicaciones defendibles y de confianza en ese límite.<sup>2</sup>

**Beard:** El hecho de que el correo electrónico se envía a servidores fuera de las redes de su compañía y posiblemente de fronteras nacionales—quizás a países que tienen leyes de interceptación diferentes de las propias—es algo que el usuario fortuito simplemente no entiende. Hemos construido empresas completas que dependen del dominio cibernético, pero no entendemos realmente los retos de seguridad asociados con ese dominio. Resulta desalentador cuando se empieza a entender cuáles podrían ser los impactos, y esa es la razón por la que el liderazgo es tan crítico para sortear este reto, y la ampliación ilimitada de dependencia de la red.

**Vautrinot:** En el entorno del presupuesto actual, existe un factor de complicación: el compromiso de recursos esperado cierra realmente el espacio de diálogo y decisión antes de poder explorar opciones. La complejidad de esta transformación a nivel de empresa se convierte en su propia clase de inercia. Si la cibernética está actualmente desordenada, entonces estamos atrapados entre la “entropía” natural del dominio y la inercia de la decisión. ¿Luchó usted contra eso en la industria?

**Beard:** Recientemente oí a un abogado sugerir que los directores de la corporación no deben estar mejor informados sobre riesgos de ciberseguridad debido a que las leyes les protegen de cosas para los que no están formados. Creo que eso era una opinión falta de perspicacia. Creo que en el contexto de la industria comercial—por ejemplo, un banco, una compañía de servicios pública, una compañía de ciencias farmacéuticas o un contratista de defensa—la base de estas empresas es su reputación y confianza. Las juntas directivas de esas compañías, con prácticas de gestión de riesgo robustas, saben muy bien si están en una posición informada para adjudicar esos riesgos. Para nosotros, el riesgo cibernético puede ser el riesgo más dominante que creemos afrontar. No obstante, para un contratista de defensa, quizás el mayor riesgo al que nos estamos enfrentando es que tienen a personas en peligro. Una institución financiera puede enfrentarse a una crisis de liquidez. Una compañía farmacéutica puede preocuparse sobre lograr una aprobación de la FDA para cumplir con ciertos pronósticos de ventas y localizar las versiones falsificadas de productos que venden en todo el mundo. La cuestión es cómo está de bien articulado ese riesgo, y esta noción de que podemos simplemente construir una fortaleza alrededor del negocio con ciberdefensas estáticas es simplemente la versión digital de la Línea Maginot.

**Vautrinot:** De acuerdo, las defensas estáticas no dieron resultado en la SGM y no darán resultado en el entorno cibernético. Esa es la razón por la que en la Fuerza Aérea, nos hemos estado

concentrando en una postura defensiva proactiva. En vez de esperar hasta que un adversario penetre en nuestras redes para evaluar nuestras vulnerabilidades, hemos creado equipos especializados que investigan nuestras redes y buscan esas vulnerabilidades, preferiblemente antes de que sean explotadas. Nos concentramos en identificar y defender esas interconexiones que son esenciales para el éxito de la misión—el General Keith Alexander, comandante del Cibermando de EE.UU., llamaría a esta capacidad “reconocimiento/contrarreconocimiento”. Una faceta clave de este esfuerzo defensivo es identificar y concentrarse en una “lista de haberes defendidos” prioritarios del comandante, esas áreas críticas que deben poder operar mediante un entorno en contención o un ataque. Esto corresponde directamente a algo de lo que hablamos antes: unir nuestros esfuerzos a la misión de la operación. Podemos entrar en un entorno de redes y proporcionar al comandante que depende de ese sistema información sobre decisiones de forma puntual y precisa. Específicamente, ¿puede fiarse en el sistema de la red para lograr su misión con éxito?

Esta postura proactiva se ve reforzada por el vector de información y amenazas compartido entre la industria y el gobierno. Un ejemplo soberbio era la Ciberseguridad de Base Industrial de Defensa Voluntaria /Programa de Calidad de Información del Departamento de Defensa, un acuerdo en el que las compañías, incluidas muchas de las mayores corporaciones en este país, colaboró con el Departamento de Defensa (en la Fuerza Aérea, a través del Equipo de Respuesta de Emergencia Informática de la Fuerza Aérea bajo la Escuadra de Combate de Redes 67) y el Departamento de Seguridad Nacional para compartir información de amenazas sensible y por lo tanto mejorar la defensa ciberespacial colectiva.<sup>3</sup>

**Beard:** Lo que se está empezando a ver ahora en el lado comercial es la frustración de estar en una defensa estática. La economía básica de los ciberataques favorece actualmente al adversario así como los dispositivos explosivos improvisados favorecen a los insurgentes. Para contrarrestar ese modelo, nos hemos asociado con la industria y el gobierno para desarrollar plataformas de confianza que permiten defensas dinámicas a través de nuestros productos Cloudshield. De forma alternativa, algunas personas de los mercados comerciales creen que es hora de devolver los puñetazos. Este movimiento desde la perspectiva de las ciberoperaciones consiste en pasar de la defensa de redes informáticas al ataque de redes informáticas. Me preocupan realmente las compañías comerciales que emprenden un tipo de misión de ataque de redes informáticas, con consecuencias no intencionadas tanto para la agencia de ejecución de la ley como para otras agencias gubernamentales.

**Vautrinot:** Históricamente según la ley internacional, el concepto de ataque pertenecía al dominio de la nación-estado. No obstante, las fronteras geográficas ya no demarcan actores a la ofensiva; por ejemplo, hemos visto compañías que venden servicios que dicen responder a las intrusiones cibernéticas enviando comandos o desviando tráfico malicioso. La naturaleza cibernética es que las compañías pueden tener capacidad de llegar mucho más lejos. Al hacer eso, disputarán con la ley nacional así como con los estatutos donde están operando o causando efectos. Desgraciadamente, las políticas nacionales e internacionales actuales no han seguido el ritmo de avance en las capacidades cibernéticas; por lo tanto, existen pretextos y lagunas completas en el gobierno que pueden ser aprovechados por corporaciones audaces.

En la Fuerza Aérea, no estamos limitados simplemente por leyes nacionales sino también por política gubernamental. Por lo general, el Departamento de Seguridad Nacional es responsable de defender los haberes cibernéticos fuera de las redes del Departamento de Defensa, pero sea cual sea la organización que esté contemplando estas acciones, los problemas de atribuir definitivamente una intrusión a un atacante particular y las acciones de armonización del uso del espacio con otras entidades son particularmente difíciles. Eso resalta una vez más la necesidad de una estructura de reparto de información entre el gobierno y la industria que facilite la acción rápida a los eventos cibernéticos.

Los líderes superiores de la Fuerza Aérea son ciertamente conscientes de las vulnerabilidades de nuestros sistemas de redes, pero ahora hay un reconocimiento intenso de las oportunidades para permitir la defensa así como para facilitar el éxito de la misión. Un gran ejemplo ha sido nuestro trabajo con el Mando de Transporte y Mando de Movilidad Aérea de EE.UU. Sus dependencias no están limitadas al dominio .mil sino al .com y la capacidad para trabajar con los socios de la industria para asegurar un movimiento mundial. Como consecuencia, son muy conscientes, y el entendimiento hace que sean muy proactivos en términos de resolución. Sin embargo, en otros mandos, existe una resistencia y creencia de que sus redes son “privadas” o están separadas de la Internet global y por lo tanto son sus adversarios inherentes. En lo que respecta a sus oficinas independientes, ¿experimentó una variación similar?

**Beard:** Lo hicimos. Teníamos empleados, socios e incluso clientes que operaban en lo que creían que eran redes “cerradas”; por lo tanto, no sentían que tenían un problema. Simplemente no vieron la necesidad de añadir capas adicionales de protección o ejecución de políticas en sus actividades. Lo que llamaron burocracia es lo que llamamos garantía de misión en el contexto de ingeniería de sistemas.

**Vautrinot:** Claramente, una necesidad de unidad de esfuerzo y con ella una cadena clara de responsabilidad—mando y control. Ciertamente, ustedes estaban implementando una solución de empresa por razones adecuadas, y el campo de oficinas independientes se dio cuenta de la importancia. No obstante, hay resistencia a perder lo que algunos creen que es su autoactualización—su capacidad de control. ¿Qué les permitió a ustedes aunar esa resistencia natural en el campo e impulsar la implementación?

**Beard:** Diría que tres cosas. Una era el compromiso de liderazgo. Teníamos que tener la voluntad del liderazgo para decir, “Deseamos ir aquí”. En segundo lugar, empezamos a educar al liderazgo, a la gerencia y a grupos de empleados seleccionados. Eso era realmente importante para nosotros—aumentar la conciencia. Por último, teníamos que reflexionar el contexto de ciberseguridad. Necesitábamos entender qué es lo que realmente había que proteger y dónde estableceríamos la confianza. Los resultados de ese ejercicio cambiaron materialmente nuestra estrategia de defensa profunda.

**Vautrinot:** ¿Qué nivel de liderazgo fue necesario iniciar? En nuestro idioma vernáculo, serían los mandos importantes y las funciones clave que dicen, “de acuerdo, estamos todos de acuerdo. Reconocemos la amenaza, y todos vamos a movernos juntos en este sentido”. Después, sería nuestra responsabilidad ayudarles a entender la justificación para implementar o tomar medidas que puedan ser localmente restrictivas.

**Beard:** Correcto, no todo el mundo estaba de acuerdo. Se requirió un mandato a nivel de director ejecutivo/director de operaciones/director financiero combinado, y rompimos algún que otro cacharro.<sup>4</sup> Aunque la gente entendió la decisión de liderazgo y la necesidad de ejecución de políticas y supervisión, seguían queriendo autonomía, así pues desarrollamos herramientas para proporcionar autonomía mientras se preserva la postura de seguridad. Eso se hizo en el contexto de productividad y dando a la gente lo que quería. Lo que no entendimos hace 20 años, cuando las operaciones en el dominio digital empezaron a evolucionar, era este asunto de riesgo cibernético. El asunto del riesgo ha asomado ahora la cabeza, y no podemos ignorarlo, tenemos un conflicto. Deseo cuidarle como usuario final, como cliente, pero tengo esta otra responsabilidad que puede o no puede entender o apreciar, y trataré de ayudar a explicarlo. No puedo explicarlo simplemente a todos los usuarios finales porque no tengo los ciclos para hacer esto porque entonces no estoy haciendo mi trabajo. Eso, es parte del balance.

**Vautrinot:** Usted está protegiendo la viabilidad a largo plazo de la entidad corporativa, de la misma forma que estamos protegiendo la viabilidad a largo plazo de la misión y nuestro apoyo a la nación. Tiene que haber cierta libertad de acción, en toda la empresa, para permitir esa protección.

Creo que en la industria también tiene un requisito que reportar, no la ciberseguridad per se, sino su viabilidad como entidad corporativa en el dominio de la ciberseguridad. Si tuviera un informe similar, anticipo que no recibiríamos una nota de aprobado. No obstante, nos hemos movido hacia una estructura donde hay una gestión de nivel de haberes y empresas, pero solamente en las redes .mil y .smil. Cada una de las redes del sistema de misiones se define así mismo por separado y está provista y administrada de forma independiente. En su modelo, habría un “general” que sería designado para controlar la gestión de haberes de todas las interconexiones de redes de la Fuerza Aérea, desde los aperitivos hasta el postre—precisamente lo que se tenía que hacer en la industria. Es ciertamente necesario, pero he aprendido que la viabilidad operacional en este entorno en contención requiere un cambio fundamental en los haberes que gestionaríamos centralmente—requiere detectores para habilitar la conciencia y la respuesta proactiva a las amenazas dentro de la red. El primer paso, disponer de la gestión de haberes, por sí mismo es insuficiente, pero ser capaz de detectarlo—para obtener esa conciencia situacional y permitir que su sistema reaccione de modo automático—es el paso siguiente. ¿Cómo enfocó los cambios de nivel de ingeniería?

**Beard:** Eso formó parte de la segunda travesía en este proceso—instrumentalizar y hacer todo el análisis de vulnerabilidad de empresas y los escaneos con esa referencia. Esto permite preparar un monitoreo continuo. La razón por la que es importante es lo que compone la tercera travesía: tal vez desee cambiar mi red basándome en la misión comercial, la inteligencia de amenazas accionable y la intención de seleccionar adversarios que estén activos.

**Vautrinot:** Es aquí donde las operaciones del ciberespacio pueden facilitar las operaciones de la misión o dar alternativas de la misión. No necesitamos mandar y controlar la misión, sino que necesitamos tener una visibilidad completa de lo que ocurre en el [ciber]espacio y poder ajustarlo en tiempo real para desbaratar la posición del adversario. Hace que el conjunto de problemas del adversario sea mucho más difícil a la vez que se conserva la efectividad de la misión.

**Beard:** Exactamente. Porque si los adversarios entienden mejor su red que usted, usted tiene problemas, y si su infraestructura informática es tan rígida que no puede hacer asignaciones dinámicas, se van a aprovechar de eso, y una vez más las ventajas económicas y operacionales pasan al adversario. Esta es la razón por la que pasamos al modelo de nube híbrida—porque nos dio la oportunidad a nivel de aplicación y datos para mover cargas de trabajo de un lado a otro. Ahora puedo tomar una carga de trabajo que ha operado históricamente en servidores específicos en un centro de datos específico y asignar dinámicamente la carga de trabajo a máquinas virtuales que operan en centros de datos virtuales que pueden tener características geográficas diferentes. La información puede estar dentro de mi centro de datos, pero puedo moverla a lugares diferentes.

**Vautrinot:** En esa estructura, por ejemplo, la atención médica de los empleados no posee datos médicos, y el departamento de finanzas no poseería datos financieros. Mover y dar acceso a los datos deseados dentro de la empresa es la clave, y cada ramal de la empresa usa esos datos en vez de controlarlos como un elemento segregado. El objetivo no debe ser controlar sino tener datos de confianza accesibles en cualquier momento y en cualquier lugar. Nuestro reto es crear un entorno que sea constantemente ágil.

Los “ahorros” de eficiencia de tecnología de información parecen ser un término un poco desacertado. Al hablar con AT&T, Microsoft y socios de la industria como usted, la inversión inicial para hacer ese cambio no es solo una inversión de cultura y liderazgo corporativos sino también una inversión de capital significativa. No solo para ahorrar dinero en la operación a largo plazo de la tecnología de inversión sino una inversión financiera en ciberseguridad. ¿Cómo decidió su corporación la dinámica de inversiones para determinar que la compañía tenía el imperativo de poder permitirse la ciberseguridad? ¿Cuál fue el alcance de esa evaluación y ese diálogo?

**Beard:** No tratamos de ahorrar dinero al inicio. Tratamos de conseguir la agilidad estratégica y lo que eso significaba para nosotros como corporación global. Sabíamos que necesitábamos agilidad a nivel de empresa. Así pues, al hacer esta inversión, empezó a darnos la capacidad de empezar a ser flexibles. Considere esto no solo como usar esta tecnología para operar compañías sino en el contexto de cómo virtualizar compañías y recombinarlas. De hecho, SAIC está llevando a cabo una actividad así en este momento, y es interesante observar cómo la tecnología de información es un habilitador en vez de un obstáculo en el camino.

**Vautrinot:** La cibernética en este contexto que estamos describiendo—es una misión, y usted no es viable sin esta misión. A pesar de nuestra situación económica nacional actual, tenemos que hacer la transición del diálogo desde la reducción de costos hasta la defensa imperativa y por lo tanto merecedora de una inversión desde un punto de vista de estrategia nacional.

**Beard:** Eliminamos la cibernética por separado desde un punto de vista del presupuesto y la tratamos como si fuera una inversión estratégica. Si considera la tecnología de inversión como un centro de costos, perderá la oportunidad. Con el paso de los años he aconsejado a una serie de compañías que consideraban objetivos de reducción de costos en tecnología de información como una forma de cumplir con un objetivo de costo corporativo, pero el secreto es que adquieren deudas que no se muestran como un pasivo sin fondos ni en el balance general ni en el registro de riesgos de la empresa.

**Vautrinot:** Asimismo, mi “deuda técnica” es la falta de automatización y detección, que estoy superando manualmente—que en efecto es una fuerza laboral enorme que no es sostenible ni apropiada en un entorno cibernético dinámico. Impulsa respuestas de reacción ante problemas y excluye el suministro de detectores y soluciones automatizadas.

Nuestros esfuerzos para pasar de una red dispersa administrada por la instalación a una sola red homogénea administrada centralmente permitirá el seguimiento de detección y automatización necesario para liberar recursos y operaciones de red robustas a la escala requerida para una industria global, como la suya, u operaciones militares. Hasta entonces, esto impulsa un gran costo final.

**Beard:** Todos sabemos que la postura reactiva es más costosa. No haríamos nunca eso con un esfuerzo de desarrollo de sistemas de armas—tratamos de diseñar ingeniería firme en el inicio. Es mucho más económico a largo plazo hacerlo en ese orden.

**Vautrinot:** Se supone que las cosas que vemos, puede al menos tratarse, pero, ¿qué ocurre con las incógnitas desconocidas?

**Beard:** Las incógnitas desconocidas son inaceptables. Para fines de la Ley de Sarbanes-Oxley, por ejemplo, estamos obligados a tener listos controles preventivos.<sup>5</sup> Las incógnitas desconocidas obligan a pensar a la “izquierda del suceso”.<sup>6</sup> Pero eso le lleva a la conclusión de que no puede proteger todo. Así pues, llevemos a cabo un diálogo comercial o un diálogo militar sobre los haberes—podrían ser haberes de datos—que deseamos proteger.

**Vautrinot:** Es eso a lo que me refería como lista de haberes defendidos pero a un nivel discreto en vez de a un nivel de empresa. Hemos trabajado individualmente con el Centro de Control de Transporte Aéreo de Aviones Cisterna así como uno de los muchos centros de operaciones aéreas para demostrar esta dinámica. Pero no podemos aplicarla a un nivel de empresa porque no podemos “ver” o controlar los haberes cibernéticos en la empresa.

**Beard:** En mi función, puedo recibir una llamada telefónica donde se me diga, “Tengo este problema urgente de seguridad de información; ven y ayúdame”. Y las dos primeras preguntas son, “¿Cuándo se le hizo saber de un requisito para proteger este haber?” y “¿Cuándo supo que tenía este problema?” Si no estaba en la lista de haberes defendidos, no hice nada de forma proactiva para protegerlo, y si se ha exfiltrado o manipulado, no me ocupé específicamente de asegurarme de que se saliera de los límites o de preservar su referencia. Así pues, si la lista de haberes defendidos es incompleta, es muy difícil para mí desarrollar e implementar una política de ciber-

seguridad para proteger y defender esos haberes. Es un deporte de equipo, y hay una responsabilidad compartida para garantizar la misión que es increíblemente dinámica. Si usted compra simplemente un aparato de seguridad, para cuando lo despliegue, estará pasado de moda. Así pues, tiene una amenaza asimétrica, y usted está tratando de responder con un proceso anticuado tradicional. Es contraproducente, razón por la cual estamos tratando de cambiar las reglas del juego.

**Vautrinot:** Por supuesto, esa es la razón por la que estamos construyendo una plataforma que pueda ajustarse constantemente. Si estuviera usando una comparación de operaciones espaciales, definiría la interfaz entre la carga útil y la plataforma. Eso significa que necesito poseer la plataforma y la empresa y que puede hacer el ajuste en tiempo real. Por ejemplo, según el Coronel Paul Welch, comandante de la Escuadra de Operaciones de Información 688, desarrollamos la Plataforma de Operaciones de Información para proporcionar una estructura acreditada de arquitectura abierta para el despliegue rápido de aplicaciones de terceros.<sup>7</sup> Esta capacidad de intercambiar nuestras herramientas permite un despliegue acelerado de esas herramientas, que proporcionan operaciones dinámicas y de respuesta a las operaciones ciberespaciales de la Fuerza Aérea y del Departamento de Defensa. Esto proporciona flexibilidad—como un avión caza, que puede configurarse para una misión aire-tierra durante una salida y para una misión aire-aire durante la siguiente. La diferencia es que el avión caza se reconfigura en horas/días, mientras que en el espacio cibernético debe ser en segundos.

**Beard:** Digamos que mi sistema de detección de intrusión ha sido anulado y necesito algo nuevo. La base de software forma parte de una plataforma y no es negociable, por lo que la plataforma de hardware misma no cambia. Puedo desplegarlo ahora mismo. Es esta máquina encubierta con controles fuera de banda la que solamente vemos, pero puedo poner distintas cargas útiles en ella.<sup>8</sup> Las oficinas independientes pueden hacer lo que necesitan hacer, pero la empresa puede seguir dominando la red en su nombre. Ese es el truco—mando y control a nivel de empresa con ejecución descentralizada, un entorno dinámico que da a la empresa agilidad y “confianza” basadas en una plataforma que es muy configurable y le permite mirar a la “izquierda del suceso”.

**Vautrinot:** La intención, a medida que seguimos refinando nuestras destrezas en este dominio, es pasar de la postura reactiva a la proactiva y presentar objetivos ágiles detectables a nuestros adversarios. Todos nosotros, ya seamos del gobierno o de la industria, tenemos que fiarnos: debemos usar el capital intelectual disponible y las tecnologías emergentes para proteger nuestra información y sistemas a fin de evitar que pasen a formar parte de una cadena expansiva maliciosa [costo de remedio global de 2011 de 388.000 millones de dólares de EE.UU.].<sup>9</sup> La travesía cibernética de la nación es una responsabilidad compartida, y es personal—solamente a través de asociaciones de desarrollo podemos seguir defendiendo esta nación en el ciberespacio.

\*\*\*\*\*

El enorme alcance de este dominio es difícil de entender: en los próximos 60 segundos, se enviarán 168.000.000 de correos electrónicos; se anunciarán 695.000 actualizaciones en Facebook; y se llevarán a cabo 690.000 búsquedas en Google.<sup>10</sup> A medida que se siguen multiplicando las posibles oportunidades en este dominio, también lo hacen las vulnerabilidades. Aquellos de nosotros que estuvimos presentes en este debate salimos de la habitación no solo con un mayor entendimiento de los retos futuros en este dominio sino también con una mayor apreciación de los esfuerzos de colaboración que tienen lugar entre el gobierno y la industria para salvaguardar la información crítica en que se basan las corporaciones, los comandantes y el país. □

## Notas

1. En uno de los actos más destructivos de sabotaje informático al escribir esto, el 15 de agosto de 2012, un virus borró datos del 75% de las computadoras corporativas de Saudi Aramco, mostrando una bandera de EE.UU. en llamas en lugar de información. Debido al ataque, la compañía se vio obligada a reemplazar decenas de miles de discos duros.

2. La misión de la Escuadra de Comunicaciones de Combate 689 es capacitar, desplegar y suministrar comunicaciones expedicionarias y especializadas, control de tráfico aéreo, y sistemas de aterrizaje para operaciones de socorro humanitarias y operaciones de combate dominantes—en cualquier momento, en cualquier lugar. Para estar al día con el entorno estratégico rápidamente variable, los comunicadores de combates se basan en gran medida en la industria para proporcionar tecnología comercial, lo que les permite ampliar, operar y defender las capacidades ciberespaciales en los lugares más austeros y de la manera más efectiva posible.

3. Asegurar la defensa de información y sistemas militares—a través de la defensa de redes informáticas y ataques de redes informáticas—es un reto diario. La Escuadra de Combate de Redes 67 ejecuta operaciones de redes de la Fuerza Aérea, defensa, ataque y explotación para crear efectos ciberespaciales integrados en nombre de la Veinticuatro Fuerza Aérea y de los mandos combatientes. La escuadra opera dentro de las autoridades actuales del Departamento de Defensa para proteger la información y los sistemas de la Fuerza Aérea y del Departamento de Defensa y para asegurar la libertad de maniobra en el ciberdominio. El 67 incluye los operadores en la red responsables de la operación diaria de las redes de la Fuerza Aérea. La amplia colaboración entre el personal de la escuadra y otras organizaciones gubernamentales y civiles asegura el reparto continuo de información de amenazas cibernéticas a través de entidades públicas y privadas.

4. Al igual que “un toro en una cacharrería” rompe cacharros. En este caso, la introducción de los procesos de ciberseguridad rompió los procesos comerciales normales.

5. La Ley de Sarbanes-Oxley, una propuesta de ley del congreso promulgada en 2002, también conocida en el Senado como Ley de Reforma de Contabilidad de Compañías Públicas y Protección de Inversores, y en la Cámara de Representantes como la Ley de Rendimiento de Cuentas y Responsabilidad Corporativa y de Auditoría. La propuesta de ley se promulgó debido a un número de escándalos corporativos y contables importantes, incluidos los de Enron y WorldCom.

6. El término a la *izquierda del suceso* se refiere a una línea cronológica en la que cada incidente se marca con un suceso. Las actividades a la “derecha del suceso” son respuestas reactivas al incidente; esas acciones a la “izquierda del suceso” son acciones proactivas en preparación para dichos incidentes.

7. La Escuadra de Operaciones de Información 688 muestra estas operaciones de información y capacidades de infraestructura de ingeniería de funcionamiento demostrado integradas en los dominios del aire, espacio y ciberespacio. La escuadra ha desarrollado un proceso innovador de desarrollo de herramientas rápido acompañado por un programa de adquisición rápido que refleja métodos de sistemas inmediatos, intermedios y de largo plazo. La estructura de innovación comprende el Mando de Materiales de la Fuerza Aérea (AFMC) en colaboración con el Mando Espacial de la Fuerza Aérea para establecer un centro de innovación cibernética a fin de proporcionar capacidades ciberespaciales económicas, como la Plataforma de Operaciones de Información, en el intervalo apropiado para respaldar al combatiente conjunto.

La 688 amplía las innovaciones logradas por el tema de investigación de interés, organizadas por el Coronel Welch, asociándose localmente con expertos científicos y tecnológicos del Laboratorio de Investigación de la Fuerza Aérea y uniéndose simultáneamente con sus contrincantes de adquisición como el Coronel Chris Kinne, de AFMC en San Antonio, para ampliar la autoridad de adquisición local delegada de la Oficina del Secretario de la Fuerza Aérea para Adquisiciones. Se requiere un diverso conjunto de conocimientos colocalizados para complementar los conocimientos expertos de desarrollo cibernético residentes. El Teniente Coronel Jim Smith lidera la presencia del Centro de Pruebas y Evaluaciones Operacionales de la Fuerza Aérea en esta nueva organización a fin de probar y verificar la efectividad de las capacidades propuestas en un entorno operacional.

8. El control fuera de los límites pasa datos de control en una conexión separada de los datos principales.

9. *Norton Cybercrime Report 2011 (Informe Norton de delitos cibernéticos)*, Symantec Corporation, 7 septiembre de 2011, [http://www.symantec.com/content/en/us/home\\_homeoffice/html/cybercrimereport/](http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/).

10. “60 Seconds—Things That Happen On Internet Every Sixty Seconds” (60 segundos-Cosas que ocurren en Internet cada sesenta segundos), GO-Gulf.com, 1 de junio de 2011, <http://www.go-gulf.com/blog/60-seconds/>.



**La General de División Suzanne M. Vautrinot, USAF** (USAFA; MS, Universidad de Southern California) es la comandante de la Veinticuatro Fuerza Aérea, de las Fuerza Aéreas Cibernéticas y de las Operaciones de Redes de la Fuerza Aérea, Base de la Fuerza Aérea de Lackland, Texas. Ella es responsable de la fuerza aérea numerada de componentes de la Fuerza Aérea que proporciona a los comandantes combatientes fuerzas cibernéticas adiestradas y listas que planifican y llevan a cabo operaciones ciberespaciales. La General dirige las actividades de tres escuadras cibernéticas operacionales—dos con sede en Lackland y otra en la Base de la Fuerza Aérea Robins, Georgia—así como el Centro de Operaciones 624 de Lackland. La General Vautrinot ha servido en varias asignaciones, incluidas ciberoperaciones, planes y política, seguridad estratégica, operaciones espaciales y trabajo de estado mayor. Ha estado al mando a nivel de escuadrón, grupo y escuadra, así como en el Servicio de Reclutamiento de la Fuerza Aérea. La General ha servido en el Estado Mayor Conjunto, en los estados mayores de comandancias importantes, y en la comandancia de la Fuerza Aérea. Antes de asumir su posición actual, era la directora de planes y política, Cibercomando de EE.UU., Fort George G. Meade, Maryland, y la asistente especial al vicejefe de estado mayor de la Fuerza Aérea de EE.UU., Washington, DC. Asociado de Seguridad Nacional en la Escuela de Gobierno John F. Kennedy, Universidad de Harvard, el General Vautrinot es una graduada distinguida de la Escuela de Oficiales de Escuadrones, Colegio de Mando y Estado Mayor Aéreo (con honores), Escuela de Oficiales de Estado Mayor Conjunto y Combinado y Colegio de la Guerra Aérea (correspondencia).



**El Sr. Charles E. Beard Jr.** (BS, Universidad Texas A&M; MBA, Universidad de Montana) es el vicepresidente superior y oficial de información jefe para Science Applications International Corporation (SAIC) y gerente general de la Unidad Comercial de Giberseguridad de SAIC. En esta función doble, ha liderado el SAIC para convertirse primero en su industria a fin de efectuar la transición de la empresa a una infraestructura de cálculo de nube y tratar los retos de seguridad y control inherentes en esa travesía. Él es secretario de la Junta Fiduciaria de Inova Health Care Services y presidente de la Junta de Calidad en Inova Mount Vernon Hospital. Antes de incorporarse a SAIC, el Sr. Beard fue director de la división Oliver Wyman de Marsh & McLennan. En esta función, proporcionó servicios de recomendaciones estratégicas con transacciones y reestructuraciones corporativas y desarrollando estrategias de tecnología de información para lograr objetivos de diseño comercial. También sirvió como vicepresidente superior de Mercados de Transporte e Industrial Globales en KPMG Consulting (después BearingPoint), liderando la estrategia y los servicios de operaciones de la compañía para clientes comerciales globales, incluidas GE, Honeywell, United Technologies y Southwest Airlines. Ha completado una educación continuada en la Escuela de Negocios de Harvard y MIT Sloan. El Sr. Beard es un orador destacado.