C4ISR a través de webs oscuras

Un concepto alternativo para proteger información crítica en entornos ciberespaciales disputados

Capitán Kyle L. Bingman, USAF

El mundo está cada vez más conectado, tanto de forma física como metafórica, por la incesante propagación de redes como Internet y la multitud de dispositivos que obtienen la información que contienen. Aún más, los individuos, las organizaciones y las naciones estado están confiando cada vez más en este mundo interconectado para realizar actividades procedentes que van de lo mundano a lo crítico. Esta tendencia hacia una mayor conectividad es probable que continúe una espiral ascendente. Según la investigación efectuada por Cisco Systems, el tráfico de protocolos de internet globales en los últimos cinco años se ha quintuplicado y pasará el umbral de zettabyte (aproximadamente 1 billón de gigabytes o 10^{24} bytes) para fines de 2016.[1] No obstante, al mismo tiempo que se produce este desarrollo extraordinario y sus ventajas subsiguientes para la sociedad, han aumentado los incidentes de ciberseguridad. En 2015 se gastaron más de US$75billones en ciberseguridad en un intento de salvaguardar la información protegida contra una serie de actores maliciosos incluidos delincuentes y los que trabajan en naciones estado.[2] Estados Unidos hizo este gasto a pesar de reconocer que el método de ciberdefensa utilizado más a menudo, la defensa en profundidad, ha fracasado una y otra vez.[3]

Esta compleja y peligrosa realidad no afecta solamente al mundo civil sino también al militar. Es muy cierto que la Fuerza Aérea de EE.UU. no está exenta de esta situación. En vez de eso, debido a su dependencia en sistemas de comunicación y armas integrados para llevar a cabo misiones clave, es tal vez el servicio más de fiar en esta estructura increíblemente vulnerable de redes y dispositivos. Con los años, la Fuerza Aérea ha tratado de situarse de una manera que permita mantener la seguridad e integridad de sus redes de información usando el mismo método de defensa en profundidad de ciberseguridad que el sector comercial. Sin embargo, según se evidencia en los ataques exitosos contra muchas de las redes más críticas, este método se está convirtiendo en una causa perdida contra adversarios habilidosos que pueden superar el desarrollo de nuevas defensas.[4] Enfrentados con actores cibernéticos que son casi pares como China y Rusia, entre otros, así como con actores independientes y transnacionales muy diestros, la Fuerza Aérea debe encontrar una forma de asegurar la capacidad de acceso y uso de su información clave mediante un medio que se sale del statu quo. De lo contrario, debe aceptar un riesgo significativo durante futuras operaciones debido a las medidas adversarias tomadas en el ciberespacio. Este artículo detalla la naturaleza de esta realidad compleja y problemática, y ofrece una solución para el servicio para volver a obtener el control y la integridad de su información clave.

La situación

Las capacidades diseñadas para conectar nodos rápidamente y compartir información actúan como un multiplicador de fuerza debido a las ganancias de efectividad. El entorno interconectado permite a las fuerzas militares reabastecer, coordinar, cambiar de posición y compartir inteligencia a velocidades increíbles. No obstante, aunque estas capacidades abren posibilidades para la Fuerza Aérea, también exponen vulnerabilidades. Actores de todo el mundo, desde el nivel de nación estado a piratas informáticos, desde China y Rusia hasta Anonymous, también

reconocen esto. El ciberespacio es ahora el primer dominio de combate, y quizás más específicamente, el objetivo primero y primario, ya que la opción predeterminada significa iniciar hostilidades. Los líderes del Ejército de Liberación Popular de China, por ejemplo, han adoptado la idea de que un combate exitoso se basa en ejercer control sobre la información del adversario y la infraestructura asociada. Las evaluaciones indican que durante un conflicto, el ejército escogería como blancos la logística; el mando, el control, las comunicaciones, las computadoras, la inteligencia, la vigilancia y el reconocimiento (C4ISR); y otros sistemas críticos para las misiones a fin de demorar el flujo de la fuerza de EE.UU. a un teatro de operaciones y degradar las capacidades de combate.[5] En otros casos, los piratas individuales sin afiliar han expresado interés en sistemas militares o han llevado a cabo ataques que resaltaban vulnerabilidades significativas en redes relacionadas con los militares. Estos incluyen pirateos de satélites y sistemas asociados, ataques que causaban daños físicos por medio de códigos maliciosos, y ataques de negación de servicio distribuida que degradaban significativamente las redes a escala global.[6] Los ejemplos son innumerables, pero hay un tema común: la Fuerza Aérea se basa en sistemas de información para gestionar y operar una fuerza de alta tecnología, pero esos mismos sistemas están en el centro de muchos blancos de adversarios potenciales.

Muchas evaluaciones reconocen la probabilidad de que los ciberataques serán útiles para degradar la capacidad militar y reducir la capacidad. En el informe del Consejo Científico de Defensa de 2013 sobre la resistencia de los sistemas militares ante las amenazas cibernéticas avanzadas, los expertos observaron que "Estados Unidos no puede confiar en que nuestros sistemas de Tecnología de Información (IT) críticos den resultado bajo el ataque de un oponente refinado y con muchos recursos utilizando capacidades cibernéticas en combinación con todas sus capacidades militares y de inteligencia".[7] El informe continúa diciendo que, ente otros efectos, "es posible que las armas y otros sistemas de armas no funcionen según está previsto".[8] Otras evaluaciones son similarmente nefastas en sus pronunciamientos. Alan Shaffer, antiguo subsecretario de defensa de investigación e ingeniería, admitió que "se desafía al Departamento de Defensa en materias de superioridad tecnológica en formas que no se han visto durante muchos años", incluido el ciberespacio.[9] Añadió que los "sistemas cuyas capacidades pueden ser negadas por un ciberataque no ofrecen ninguna ventaja a Estados Unidos ".[10] En un testimonio subsiguiente al Congreso, el Sr. Shaffer dijo que "esto ha llevado a una situación donde . . . la superioridad de EE.UU. en muchos dominios bélicos estará en *riesgo*".[11] Es decir, no es probable que los futuros conflictos sean del tipo *Azul contra Rojo* de la forma en que normalmente conceptualizamos el conflicto de *Azules contra los límites de operación impuestos por un entorno de ciberespacio disputado según lo crean los Rojos.*[12] Esta estructura beneficia a cualquier actor con el deseo de crear una ventaja asimétrica para impedir que Estados Unidos actúe según sus máximas habilidades. Si EE.UU. tiene que luchar para presentar, suministrar y coordinar sus fuerzas, entonces la probabilidad de éxito es pequeña a medida que sus fuerzas luchan contra las limitaciones en vez de los recursos contra el adversario. Para superar esta situación, las fuerzas de EE.UU. deben encontrar una forma de actuar *más allá* de las limitaciones para llevar a cabo C4ISR de forma efectiva. No obstante, los métodos actuales, no habilitan este requisito.

Defensa en profundidad

Por el momento, el método utilizado para tratar esta situación y asegurar los sistemas críticos de la Fuerza Aérea son los medios tradicionales de defensa en profundidad de la ciberseguridad. La defensa en profundidad, desarrollada en los primeros días de Internet cuando la seguridad no era una preocupación importante, aplicó los principios de separación y distancia de forma muy efectiva para asegurar los haberes del mundo físico frente al creciente mundo cibernético. Lo hizo a pesar del hecho de que estas leyes físicas son irrelevantes en el dominio cibernético a

menos que se refieran a la infraestructura física sobre la que existe. Con la defensa en profundidad, las redes están protegidas al usar capas de mecanismos de detección y protección como cortafuegos, sistemas de intrusión y detección, software antivirus, seguridad física y una base de usuarios informada. Al igual que un ejército que asedia un castillo, la defensa en profundidad teóricamente fuerza a un atacante a gastar un gran número de recursos para tratar de encontrar una forma de llegar a una red objetivo. No obstante, sea cual sea la cantidad significativa de dinero y esfuerzo empleados en crear estos mecanismos de protección, han demostrado ser inefectivos en gran medida contra los atacantes más creativos y adiestrados. En vez de que los atacantes sean disuadidos por los costos de recursos requeridos para mantener un asedio, la situación se invirtió de modo que los defensores de las redes gastan cantidades masivas de recursos en un intento de resistir intrusiones casi constantes del adversario.

Estadísticas de años recientes pusieron al descubierto esta verdad desafortunada de forma bastante sencilla. En 2014, el número de incidentes de ciberseguridad informados en el mundo aumentó en un 48 por ciento; además, otra firma de ciberseguridad informó que no se detectan hasta el 71 por ciento de las situaciones arriesgadas.[13] Además, cuando se detectan situaciones arriesgadas, aproximadamente el 90 por ciento fueron activadas por malware determinado y diseñado específicamente para un cierto sistema, asegurando así que eludiría la detección o mitigación por parte de los mecanismos de defensa en profundidad usados comúnmente.[14] Con más de un millón de amenazas emitidas por día, no es de extrañar que la firma de ciberseguridad SANS se refiriera de forma perceptible a defensa en profundidad "insostenible"; de hecho, las amenazas avanzadas están desarrollándose más rápido que las defensas.[15] Al mismo tiempo, el Comité de Investigación e Ingeniería de Operaciones Cibernéticas Especiales de la Fundación Nacional de Ciencia enfáticamente indicó que la "defensa en profundidad no pudo proporcionar garantía de información contra todas las amenazas menos más las elementales, en el proceso de poner en riesgo funciones esenciales de las misiones".[16] El grupo pasó después a especular si la defensa en profundidad era realmente un medio de "postergar los daños en vez de un medio de seguridad".[17] Dicha especulación ha demostrado ser precisa; el status quo de defensa en profundidad no protegerá los sistemas clave y la información usada por la Fuerza Aérea para llevar a cabo operaciones de los atacantes más avanzados. Desgraciadamente, esta verdad sigue siendo desconocida en gran medida debido al paso involuntario cultural a una nueva modalidad de conceptualizar el mundo cibernético.

Seguir utilizando la defensa en profundidad como único mecanismo para la ciberseguridad es adherirse a una visión del mundo en la que el conflicto cinético era el único método de guerra. Esta perspectiva sigue ofreciendo soluciones viables para el mundo cinético, pero se hace menos relevante cuando el ciberespacio hizo que la distancia y la topografía ya no sean las preocupaciones que definen una defensa militar. Tratar de basarse solamente en defensa en profundidad para la ciberseguridad esencialmente equivale a tratar de proteger un mundo tridimensional contra adversarios con acceso a una cuarta dimensión. Siempre hay una forma para ellos de obtener acceso cuando puedan ver desde un punto de vista diferente. Como mencionó el General Stanley McChrystal, EE.UU., retirado, en una conversación reciente, la defensa en profundidad es efectivamente un método de ciberseguridad tipo "Línea Maginot".[18] Tiene éxito en mantener fuera de las redes a adversarios mucho menos capaces o innovadores, una ventaja asegurada, pero también resultará en que la habilidosa oposición encontrará una forma nueva y menos esperada de franquear la barrera. Las respuestas de defensa en profundidad estándar de aumentar la defensa en capas alrededor de las redes, e incluso iniciativas más nuevas como usar equipos cazadores como mecanismos de tipo defensa de puntos, no van a ser completamente efectivas cuando los adversarios hayan tenido años para preparar el acceso a redes bajo los ojos vigilantes de los defensores. Está claro que se necesitan cambios. Cualquier método de defensa que no sea verdaderamente efectivo en proteger información y sistemas clave necesarios para C4ISR, tam-

bién debe adoptar las características del ciberespacio de la forma en que verdaderamente existe en vez de tratar de hacer que se conforme a un entendimiento anticuado que sobrepasa y abarca.

Una solución

Aunque la perspectiva actual es deprimente, la situación puede mejorarse si el liderazgo de la Fuerza Aérea decide alterar radicalmente sus métodos actuales de llevar a cabo C4ISR en un entorno disputado. El servicio debe prepararse para implementar una estructura adicional, radicalmente diferente para C4ISR que contradiga cualquier método anterior o red anterior y, con toda probabilidad, que vaya notablemente contra la cultura común actual de compartir ampliamente información e imágenes de operación comunes. Solamente mediante este tipo de opción defensiva adicional puede la Fuerza Aérea aumentar las posibilidades de éxito operacional, mitigando así las probables acciones de un adversario habilidoso. Los pasos siguientes detallan los componentes principales de un sistema C4ISR verdaderamente viable para entornos disputados.

Prioridad de información y evaluación de riesgos

Antes del comienzo de un conflicto con un adversario que tenga suficiente capacidad para interrumpir los sistemas y las redes C4ISR actuales, la información debe ponerse por orden de prioridad en términos de su necesidad para crear efectos, así como la cantidad de riesgo que puede ser aceptada dentro de un conjunto de información debido a engaño. La información que sea menos necesaria o por la que se pueda anticipar o mitigar una cantidad de riesgo aceptable sin una dificultad notable debe continuar pasándose por medio de métodos primarios. Esto debe hacerse no solamente para limitar el alcance del método adicional de comunicación detallado abajo, sino también para asegurarse de que haya una disminución observable de tráfico que podría dar una pista a un adversario sobre este método.

Infraestructura no asociada

Durante un conflicto, la Fuerza Aérea no debe confiar exclusivamente en ninguna red o sistema utilizados previamente para pasar información clave o mantener una imagen de operación común. En vez de eso, debe cambiar a sistemas que no se hayan usado nunca y que se hayan verificado en origen para mitigar una cadena de suministro potencial o un malware colocado antes. Además, el servicio debe utilizar una red completamente no asociada con los medios actuales de permitir tráfico relacionado con los militares. La velocidad y la naturaleza encubiertas con la que se debe configurar esta nueva estructura limitará su tamaño y requerirá que solamente los participantes clave tengan acceso a ella. Solamente se permitirá el paso por esta red de información que se consideraba esencial. La información para la que la desinformación o degradación es un riesgo aceptable puede y debe seguir pasándose por métodos y sistemas actuales. Al hacer esto, no solamente se reducirá la escala requerida de la red necesaria para pasar información clave, sino que también asegurará que un declive significativo de tráfico en las redes actuales no se comporte como un indicador para el adversario. El desarrollo y las pruebas de esta red alternativa, así como sus demás componentes, tratados abajo, debe tener lugar fuera del proceso de adquisiciones estándar para garantizar su uso no anticipado.

Redes comerciales y webs oscuras

El tráfico debe circular completamente por redes comerciales, transitando idealmente por una web oscura y principalmente permaneciendo en ella, o por redes entre pares como el Proyecto de Internet Invisible o Freenet.[19] Como Internet es una red distribuida de redes que restablece conexiones constantemente entre sí en vez de en un solo sistema coordinado, puede curarse a sí

misma esencialmente y seguir estando disponible bajo ataque; las interrupciones en las rutas pueden ser temporales y subvertirse a menudo de forma rápida. La naturaleza global de Internet también aumenta su resistencia, ya que los efectos en una región pueden ser mitigados cambiando a rutas a través de otra. Las redes entre pares han demostrado ser aún más fuertes con esta capacidad, según se ve en sus numerosas y exitosas evasiones de los intentos policiales de cerrarlas.[20] Esta resistencia podría fortalecerse aumentando la diversidad de una posible infraestructura de conexiones de principalmente líneas de fibra óptica; no obstante, el estado actual de Internet sigue siendo fuerte. Dada la cantidad de tráfico que circula por Internet, así como el anonimato inherente de los usuarios de redes de la web oscura, se asegurarían datos clave debido a la oscuridad de ocultarse a plena vista en vez de basarse en mecanismos de defensa en profundidad como cortafuegos y sistemas de intrusión y detección alrededor de redes militares conocidas.

Datos constantemente variables

Los datos no deben almacenarse en el mismo lugar durante un tiempo significativo. El uso de tecnologías como computación central en la nube y la estructura entre pares sobre la que se construyen muchas redes de la web oscura, se debe cambiar cualquier almacenamiento grande de información de un lugar a otro de forma frecuente. Al hacer eso se ayudará a asegurar que, si un adversario detecta este método adicional de C4ISR, tendrá dificultades en actualizar los numerosos cambios y que, si el actor no los localiza, tendrá visibilidad solamente durante un período corto.

Rutas de datos múltiples y redundantes

Debe haber múltiples formas de introducir y extraer datos de este almacén de información basado en la web oscura. Se deben poder abandonar los enlaces con las rutas de información consideradas tradicionalmente "seguras" para la información más crucial en vista de la puesta en peligro potencial por parte de un oponente habilidoso. En vez de eso, se deben introducir y extraer datos clave del almacén de datos de la web oscura de modo subrepticio y transparente por múltiples métodos, utilizando nuevamente el principio de ocultar a plena vista. Cualquier fuente o ubicación podría introducir datos por métodos como anuncios automatizados de toda clase de sensores o incluso menos tradicionales como plataformas o foros de conversaciones. Al no depender de un solo método o fuente, la Fuerza Aérea no solamente gana en seguridad mediante la oscuridad sino también en flexibilidad y resistencia. Además, dada la naturaleza de las redes entre pares de la web oscura, la pérdida de una ruta de información no pondría al descubierto el almacén central ni pondría en peligro otras rutas de datos.

Reparto de información simultáneo

La fusión y el análisis de información deben producirse en escenarios no tradicionales que no estén asociados con centros tradicionales como los existentes en el sistema de base común distribuido (DCGS). Como este último es un sistema existente, uno debe asumir que se ha puesto en riesgo. La información, en vez de fluir de manera jerárquica hacia un grupo específico de analistas, debe moverse por sistemas de armas, analistas y planificadores por todo el mundo de manera simultánea para hacer uso completo de las capacidades de procesamiento, así como de los puntos de datos. Las fuentes de información "enviarían" pequeñas notificaciones de puntos de datos que pueden proporcionar mientras que se pueden "extraer" requisitos por parte de las fuentes según sea necesario, limitando así la cantidad de tráfico que circula por la red y ayudando a ocultar a plena vista. Como la estructura del DCGS ya ha colocado a analistas y requisitos asociados en todo el mundo, el personal está en posición. No obstante, deben trasladarse de

instalaciones militares conocidas a nuevos sitios equipados con las tecnologías requeridas. Cualquiera de estos sitios o todos ellos podrían llevar a cabo un análisis, pero la estructura podría cambiar esta situación en toda la operación, basándose en la viabilidad de las rutas de datos a ciertos sitios. Para que esta situación sea factible, habría que llevar a cabo un estudio completo de necesidades de personal para este "DCGS de todas las fuentes".

Hardware reemplazable

Estos sitios y otros unidos a esta nueva red C4ISR no deben basarse ni en infraestructura crítica a gran escala ni en métodos sencillos de conexión con Internet. A la luz de la naturaleza de posibles cortes de energía eléctrica y la oportunidad de correr riesgos, es esencial que cualquier sistema pueda ser autónomo y ser reemplazado con facilidad. En consecuencia, la Fuerza Aérea debe confiar en sistemas que reflejen mejor el ciberdominio actual, como computadoras portátiles y tabletas que pueden intercambiarse rápidamente y descartarse fácilmente. Además, el servicio debe utilizar múltiples puntos de acceso a Internet, desde conexiones de fibra tradicionales a medios más abiertos como redes de elementos o punto públicos de WiFi.

Defensa mediante engaño

La Fuerza Aérea debe desarrollar una capacidad de engaño para ayudar a ocultar la existencia de este método de comunicación adicional en caso de que sea descubierto. Al inundar Internet con tráfico realista pero engañoso, se puede forzar a un adversario a pasar una cantidad de tiempo considerable trabajando para discernir qué información es real y cuál no lo es.

Conclusión

Básicamente, estas son las tácticas de actores asimétricos como los insurgentes. Este medio propuesto de C4ISR se diferencia claramente de la cultura actual de la Fuerza Aérea de flujo de información y toma de decisiones jerárquicos, así como de su creencia en la defensa en profundidad como medio más efectivo de asegurar la información. La defensa en profundidad como medio de ciberseguridad no salvaguarda las redes contra amenazas de menor nivel y no se debe abandonar, pero no es una solución viable para asegurar la información más crítica durante un conflicto. La solución, una posible concepción de lo que se detalló arriba, es adoptar un mayor entendimiento de la seguridad que reconoce las verdaderas fortalezas del ciberespacio. Al utilizar las capacidades de la web oscura, aprovechándose de la relatividad geográfica del ciberespacio, y adoptar un flujo de información simultáneo, la Fuerza Aérea puede superar las limitaciones de C4ISR que un enemigo intentará poner en servicio durante un conflicto.

Adoptar dichos métodos no sería convencional. No obstante, no hacer esto es ignorar no solo el hecho de los dominios en los que se han ampliado las luchas de servicio, sino también que el ciberespacio es un dominio drásticamente diferente. Al utilizar solamente modelos como defensa en profundidad para asegurar su información en vez de aceptar el nuevo entorno de forma que también aproveche sus puntos fuertes, la Fuerza Aérea no está protegiendo su información clave de la mejor manera posible, sino facilitando la localización y el acceso a esos datos por parte de un adversario. Las operaciones ciberespaciales tienen el fuerte potencial de denegar la efectividad de las operaciones de servicio si el statu quo no cambia. Es hora de que la Fuerza Aérea acepte la verdadera naturaleza del ciberespacio y opere allí usando las capacidades diseñadas para triunfar en ese dominio. ❑

Notas

1. "La era de Zettabyte—Tendencias y análisis", Cisco, 2 de junio de 2016, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html.

2. "Gartner dice que los gastos de seguridad de información en todo el mundo crecieron casi el 4,7 por ciento hasta alcanzar $75.400 millones en 2015", Gartner, 23 de septiembre de 2015, http://www.gartner.com/newsroom/id/3135617.

3. *Defensa en profundidad* es un término amplio y puede significar, sin error, muchas cosas diferentes para diferentes personas. Este artículo usa el término solamente para referirse a una estructura defensiva en capas para una red que incluye elementos basados en tecnología como cortafuegos y sistemas de intrusión y detección, y prevención, elementos administrativos como políticas de contraseñas y prohibiciones en medios retirables, y elementos físicos como asegurar el acceso a componentes de hardware.

4. Se podrían citar aquí numerosos ejemplos de redes críticas. Un muestreo de las más importantes, después de Stuxnet, incluye Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid" (Dentro del pirateo ingenioso sin precedentes de la red energética de Ucrania), *Wired*, 3 de marzo de 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/; Dan Goodin, "Active Malware Operation Lets Attackers Sabotage US Energy Industry" (Operación de malware activa que permite a los atacantes sabotear la industria energética de EE.UU.), *Ars Technica*, 30 de junio de 2014, http://arstechnica.com/security/2014/06/active-malware-operation-let-attackers-sabotage-us-energy-industry/; Dan McWhorter, "Mandiant Exposes APT1—One of China's Cyber Espionage Units & Releases 3,000 Indicators" (Mandiant expone APT1, una de las unidades de espionaje cibernético de China y publica 3.000 indicadores), FireEye, 19 de febrero de 2013, https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionage-units.html; y Nicole Perlroth, "In Attack on Saudi Firm, U.S. Sees Iran Firing Back" (EE.UU. ve a Irán en un ataque a una firma saudita), *New York Times*, 23 de octubre 2012, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

5. Bryan Krekel, Patton Adams y George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage (Ocupación del terreno elevado: capacidades chinas para operaciones de redes de computadora y ciberespionaje)* (West Falls Church, VA: Northrop Grumman Corporation, 7 de marzo de 2012), http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-066.pdf; y Oficina del Secretario de Defensa, *Informe anual al Congreso: desarrollos militares y de seguridad en lo que se refiere a la República Popular China en 2015* (Washington, DC: Oficina del Secretario de Defensa, 7 abril de 2015), http://www.defense.gov/Portals/1/Documents/pubs/2015_China_Military_Power_Report.pdf.

6. Tony Capaccio y Jeff Bliss, "Chinese Military Suspected in Hacker Attacks on U.S. Satellites" (Fuerzas armadas chinas sospechosas de ataques de piratas a satélites de EE.UU.), Bloomberg Technology, 26 de octubre de 2011, http://www.bloomberg.com/news/articles/2011-10-27/chinese-military-suspected-in-hacker-attacks-on-u-s-satellites; y Kim Zetter, "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever" (Un ciberataque ha causado daños físicos confirmados por segunda vez), *Wired*, 8 de enero de 2015, https://www.wired.com/2015/01/german-steel-mill-hack-destruction/. El ejemplo de ataques de denegación de servicio distribuida no está claramente relacionado con la Fuerza Aérea, pero muestra cómo un pequeño grupo de actores técnicamente adiestrados puede producir efectos serios contra redes grandes. Acusados a menudo de "arruinar la Navidad" simplemente para enojar a las personas y haciendo poco para rebatir la afirmación, Lizard Squad es un ejemplo del tipo de actor gamberro que debe considerarse junto con más grupos organizados cuando se piensa en el conflicto del ciberespacio. Abby Ohlheiser, "Xbox Live Is Up, PlayStation's Network Still Recovering after Christmas Day Outage" (Xbox Live está conectada, la red de PlayStation sigue recuperándose después del corte de energía del día de Navidad), *Washington Post*, 26 de diciembre de 2014, https://www.washingtonpost.com/news/national/wp/2014/12/26/playstation-and-xboxs-networks-are-still-recovering-from-a-christmas-day-outage.

7. Departamento de Defensa, Consejo Científico de Defensa, *Informe de fuerza de tarea: sistemas militares resistentes y la amenaza cibernética avanzada* (Washington, DC: Departamento de Defensa, Consejo Científico de Defensa, enero de 2013), [ii], http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

8. Ibid., 28.

9. Senado, *Testimonio ante el Subcomité de Apropiaciones del Senado en Defensa, declaraciones del testigo del Honorable Frank Kendall, Subsecretario de Defensa para Adquisición, Tecnología y Defensa, Sr. Alan Shaffer, Subsecretario Principal de Defensa para Investigación e Ingeniería, Dr. Arati Prabhakar, Director, Agencia de Proyectos de Investigación Avanzada de Defensa*, 114º Congreso, primera sesión, 22 de abril de 2015, 12, http://www.defenseinnovationmarketplace.mil/resources/042215DoDInnovationResearch-JointTestimony-SAC-D.pdf.

10. Ibid., 7.

11. House, *Declaración testimonial del Sr. Alan R. Shaffer, Subsecretario Principal de Defensa para la Investigación e Ingeniería, ante el Comité sobre Servicios Armados de la Cámara de Representantes da la Cámara de Estados Unidos, Subcomité sobre Inteligencia, Amenazas y Capacidades Emergentes*, 113º Congreso, 2ª sesión, 26 de marzo de 2014, 9, http://www.acq.osd.mil/chieftechnologist/publications/docs/FY2015_TestimonyASD(RE)_ShafferA_20140326.pdf.

12. En situaciones militares, "Azul" se refiere típicamente a fuerzas amigas mientras que "Rojo" se refiere a fuerzas agresoras.

13. "El estado global de estudios de seguridad de información de 2015— Gestión de riesgos cibernéticos en un mundo interconectado", PWC, http://www.pwccn.com/home/eng/rcs_info_security_2015.html.

14. Rajendra Dodhiawala, "Why Protection Alone Won't Work Today" (Por qué la protección por sí sola no dará resultado hoy), CounterTack, 14 de diciembre de 2015, http://www.countertack.com/blog/why-protection-alone-wont-work-today.

15. Virginia Harrison y Jose Pagliery "Nearly 1 Million New Malware Threats Released Every Day" (Casi un millón de amenazas nuevas de malware publicadas todos los días), *CNN*, 14 de abril de 2015, http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security; y Prescott E. Small, *Defense in Depth: An Impractical Strategy for a Cyber World (Defensa en profundidad: una estrategia imparcial para un mundo cibernético)* (Bethesda MD: Instituto SANS, 14 de noviembre de 2011), http://www.sans.org/reading-room/whitepapers/warfare/defense-depth-impractical-strategy-cyber-world-33896.

16. "Assumption Buster Workshop: Defense-in-Depth Is a Smart Investment for Cyber Security" (Taller de eliminación de suposiciones: defensa en profundidad es una inversión inteligente), *Federal Register* 76, no. 8 (12 de enero de 2011), https://www.gpo.gov/fdsys/pkg/FR-2011-01-12/html/2011-522.htm.

17. Ibid.

18. Vídeo de "Stanley McChrystal", 4:15, Big Think, 2016, http://bigthink.com/videos/s-mcchrystal-cybersecurity.

19. Internet no es el único medio para compartir datos entre computadoras, sino simplemente el más común, así como el medio al que se tiene acceso con más facilidad porque está públicamente indexado. Por lo tanto, se refiere a la web "visible" o "superficial". Existen otras redes que sirven una finalidad similar pero que no están ni indexadas ni son accesibles sin un software especial. Estas redes son conocidas a menudo como una parte de la "web oscura" debido a su seguridad y anonimato. Muchas de ellas utilizan una estructura entre pares descentralizada que, junto a la encriptación, hace que sea difícil efectuar un análisis de tráfico en datos compartidos. Aunque estaría claro para un "observador" que alguien estaba usando un servicio como como el Proyecto de Internet Invisible, sería muy difícil determinar lo que se estaba haciendo o compartiendo.

20. George Dvorsky, "Could Someone Really Destroy the Whole Internet?" (¿Podría alguien destruir toda la internet?), *io9* (blog), 19 de septiembre de 2012, http://io9.gizmodo.com/5944558/could-someone-really-destroy-the-whole-internet.

Capitán Kyle L. Bingman, USAF (MA, Universidad Militar Estadounidense) lidera la inteligencia y los juegos de guerra del programa Horizontes Azules del Centro de Estrategia y Tecnología. Es responsable de dirigir los esfuerzos de inteligencia en apoyo del estudio estratégico más avanzado de la USAF, evaluando el impacto de tecnologías emergentes y disruptivas, así como de tendencias geoestratégicas sobe capacidades de defensa. Como oficial de inteligencia con unos conocimientos exclusivos del ciberespacio, la Capitán Bingman inició su carrera profesional como parte del Destacamento 2, 318º Grupo de Operaciones Ciberespaciales, donde trabajó para integrar operaciones ciberespaciales ofensivas y defensivas en ejercicios como eventos de Bandera Roja y Escuela de Armas de USAF. Después fue analista superior del 57º Escuadrón Agresor de Información, donde lideró los esfuerzos de investigación para asegurarse de que las ciberoperaciones del Equipo Rojo del escuadrón replicara tácticas realistas basadas en amenazadas. Antes de su asignación actual, la capitán Bingman fue instructora superior en un Colegio de Oficiales de Escuadrones.