La nueva matriz de la guerra

Dependencia digital en entornos impugnados

Capitán Keith B. Nordquist, Fuerza Aérea de EE. UU.

¿Creen ustedes que el que yo sea más fuerte o más rápido tiene que ver con los músculos en este lugar?

—Morpheus (Laurence Fishburne), The Matrix

Sencillamente ser más fuerte o más rápido ya no es suficiente cuando las operaciones dependen de las capacidades cibernéticas, y esa dependencia revela vulnerabilidades. Desde el fin de la Guerra Fría, el Departamento de Defensa de los EE. UU (DOD por sus siglas en inglés) ha demostrado su ventaja estratégica a lo largo del espectro del conflicto en cantidad, calidad y apresto. Esta fortaleza cinética es en la que los aliados dependen y los enemigos temen, igualando el dominio estadounidense con la garantía de la misión.[1] En la era digital, el dominio cibernético respalda este dominio y conserva la capacidad para proyectar poder cinético mundialmente en todo momento.[2] Del mismo modo, los adversarios están comenzando a reconocer la dependencia de Estados Unidos en las herramientas digitales para preservar su ventaja estratégica. A medida que los adversarios crean aptitudes de interferencia digital sólidas, el conflicto se desplaza más allá de una competencia de fuerzas convencionales exclusivamente entre casi iguales y se convierte en una conglomeración exhaustiva de dominios impugnados. La famosa pregunta retórica planteada por Morfeo en la trilogía *The Matrix* capta la esencia de esta dependencia digital y y la reflexión que requiere; la fortaleza y la velocidad no importan dentro de la matriz.[3] Hoy en día, el significado de la pregunta es igualmente pertinente; cuando al proyectar fuerza militar se requieren herramientas digitales, los fracasos virtuales afectan la realidad.

El imperativo estratégico para una nueva matriz de la guerra es claro —las operaciones en el dominio cibernético son, en la actualidad, los cimientos de la fortaleza militar estadounidense y, por consiguiente, son su mayor responsabilidad para el mañana. En particular, esas ventajas competitivas del DOD entre casi iguales en el mando y control, despliegue y distribución y tecnología en el sistema de armamento existen debido a la naturaleza complementaria y habilitadora del ciberespacio.[4] Imaginen perseguir una operación a nivel táctico o estratégico sin herramientas cibernéticas que permitan la libertad de maniobra aunque sea por un día. Si un adversario trastorna, interrumpe o niega capacidades cibernéticas estadounidenses, la superioridad estadounidense ya no importa —el DOD no puede emplear su ventaja estratégica. Un día sin cibernética podría ser catastrófico si el impacto es una anulación de una capacidad para proyectar poder. Ejerciendo una evaluación holística de la vulnerabilidad, el dominio cibernético es esencial para la aplicación de poder cinético. Mediante la reflexión y el análisis, el DOD debe del mismo modo ajustarse para el riesgo mayor que enfrente cuando enlace la empresa militar con las herramientas digitales que necesita para funcionar.

El cargo implícito es comprender y contrarrestar el posible impacto estratégico de un ataque cibernético y apreciar la profundidad de las capacidades que hay en el ciberespacio. Al ajustar las asociaciones de planificación cognoscitiva de la planificación militar, a fin de apreciar la profundidad de las capacidades que hay en el ciberespacio, el DOD puede continuar garantizando el éxito de la misión, inclusive durante ataques cibernéticos y operaciones degradadas. Este cambio en la asociación cognoscitiva del DOD ilustraría cómo los efectos cinéticos son secundarios al dominio digital e informan soluciones estratégicas que disuaden y derrotan las amenazas al

dominio cibernético. El futuro exige que se cree una estrategia actualizada e integrada globalmente que reconozca que una fuerza superior atrae la interrupción digital. Considerar un día sin cibernética significa reconocer el riesgo a lo largo de los dominios y comprender que el conflicto transciende los campos de batalla físicos, especialmente a medida que el espacio de batalla se torna más transregional, multidimensional y multidominio.[5] La nueva matriz de la guerra en la era digital requiere una transformación concertada, para poder apreciar el cálculo actual del conflicto y reconocer el impacto estratégico de negar la entrega del efecto cinético.

Impacto estratégico

Los efectos disruptivos a las herramientas digitales en el dominio cibernético pasan por alto los entendimientos cinéticos tradicionales de la guerra convencional. En la actualidad, los planificadores militares tienden a enfocarse en dos suposiciones incompletas: (1) los entornos impugnados existen en el teatro del conflicto designado y (2) los militares ganan las guerras donde la fuerza cinética se enfrenta a una fuerza cinética.[6]

Suposiciones como estas no tratan adecuadamente las complejidades y conectividades de la nueva matriz de la guerra. Si los planificadores militares no aceptan que los adversarios pueden lograr resultados estratégicos sin el poder cinético, puede que Estados Unidos sea susceptible a un *impacto estratégico*.[7] El impacto estratégico es similar al principio de sorpresa y conmoción (*shock and awe*)en lugar de dominar la fuerza física de un adversario al punto de la parálisis, uno abruma estratégicamente su capacidad de orientarse a sí mismo en política o dirigir las fuerzas. En este contexto, el impacto estratégico es naturalmente cognoscitivo, abarcando las percepciones, experiencias y sicologías del opositor.[8] Por consiguiente, para inducir un impacto estratégico en un adversario, uno debe interrumpir esas asociaciones cognoscitivas.

La profundidad cognoscitiva del DOD está arraigada en sus capacidades cibernéticas, representando la base crucial de la ejecución de la milicia estadounidense. No obstante, los recursos y energías del DOD permanecen enfocadas en asociaciones cognoscitivas más institucionalizadas que tienen que ver con su empleo —fuerzas mejor administradas, capacidad de despliegue y tecnologías de armamento más avanzadas.[9] Comprender la necesidad de contar con un mayor enfoque en la seguridad del ámbito cibernético requiere una aceptación cognoscitiva de que la profundidad del DOD debe estar relacionada con sus herramientas digitales, no solamente su capacidad superior. En caso de que un adversario ataque la dependencia digital del DOD sin esta asociación, el potencial para un impacto estratégico es desastroso. Específicamente para la milicia, un adversario no necesita competir ni con la capacidad superior, ni la aptitud ni la disponibilidad superior del DOD —solo necesita degradar la capacidad de emplear sus ventajas para producir efectos estratégicos. En términos generales, un enemigo puede causar efectos superiores sobre una fuerza superior si interrumpe la profundidad cognoscitiva de su función. Una falta de asociación cognoscitiva a esa profundidad extiende la vulnerabilidad y exacerba el efecto. Esto amplía la apertura para comprender la mitigación de riesgo del DOD, y extiende la planificación desde la línea del frente hasta el punto de embarque y desde el sistema de armamento hasta su huella digital. En particular, esas capacidades estratégicas del DOD más susceptibles al impacto estratégico sin un cambio en la asociación cognoscitiva también son sus fortalezas de empleo —mando y control (C2), despliegue y distribución y tecnología del sistema de armamento. Cada una de esas fortalezas necesita soluciones estratégicas para disuadir y prevalecer en entornos impugnados.

Entornos impugnados

El dominio cibernético impugnado abarca un conflicto que ya no es exlcusivo a un campo de batalla tolerante en el exterior.[10] En cambio, las herramientas digitales extienden el conflicto a la patria y limitan el acceso de Estados Unidos; en la nueva matriz de la guerra uno tendrá que luchar para llegar a la contienda. El C2 es el elemento crítico que se necesita para guiar la proyección de poder desde la guarnición hasta una zona de conflicto. Un análisis del dominio cibernético necesario para entrar en el conflicto en un contexto multidominio y transregional abarca las herramientas utilizadas para la ejecución táctica, orientación operacional y la supervisión estratégica.[11] Hoy en día, los sistemas para comunicarse hacia arriba y hacia abajo de la cadena de mando son digitales, desde la planificación, a la asignación y ejecución. Ya sea a través de constelaciones de satélites o redes en el ciberespacio,[12] el C2 y las comunicaciones del DOD dependen de herramientas casi exclusivamente habilitadas a través del dominio cibernético para entrar en una acción. Concebidas para la ejecución descentralizada,[13] las exigencias en estas herramientas digitales requieren una conciencia global y un enfoque dedicado a preservar el acceso. Sin embargo, cada comando combatiente a menudo emplea herramientas C2 de forma aislada centralizando sus herramientas de ejecución, solicitando fuerzas y operando por separado de los socios geográficos y funcionales. Este modelo operacional representa la asociación cognoscitiva actual del DOD,[14] pero está limitada a dinámicas anticuadas y convencionales. En cambio, el DOD debe buscar una planificación globalmente integrada para sus funciones de C2 para adoptar las capacidades digitales exhaustivas de su organización. Mediante un conocimiento global de la situación, el DOD puede asociar cognoscitivamente el C2 con herramientas que trascienden designaciones y autoridades terrestres. Si no se tienen en cuenta, poner en vigor relaciones de C2 en zonas de responsabilidad geográficas incurren en mayor riesgo de un impacto estratégico.

Una utilidad crítica de un C2 competente es administrar el despliegue y distribución de la milicia, ofreciendo y sosteniendo una fuerza decisiva al lugar donde se necesite. Enlazar cognoscitivamente el campo de batalla a su red de distribución amplía el entorno impugnado e impulsa a la logística a desempeñar un papel de centro de gravedad precario y estratégico.[15] El DOD ya no podrá operar la red de distribución global con impunidad como la ha hecho durante los últimos 70 años. En la actualidad, la funcionalidad integral del sistema, desde la solicitud del comandante combatiente hasta el abastecimiento y entrega, depende casi completamente en herramientas digitales. El DOD debe realísticamente rendir cuenta por la posibilidad de negar acceso a esas herramientas de proyección de poder de manera que pueda dispersar la gravedad de su dependencia cibernética de la logística. A través de una perseverancia cibernética y estrategias de resistencia, el DOD debe luchar durante la degradación y conservar su capacidad de ofrecer opciones a los comandantes de la fuerza conjunta. Las asociaciones cognoscitivas canalizadas (stove-piped) de conflictos específicos del dominio ya no pueden apoyar el espacio de batalla global. Por consiguiente, la proyección de poder de la fuerza conjunta no puede ser solamente acerca de la capacidad de distribuir la fuerza eficaz y decisivamente; también debe de ser acerca de su red digital habilitadora. Esta visión mundial y de distintos niveles informa de manera más precisa las necesidades y los requerimientos, contrarrestando la amenaza de un impacto estratégico.

En un espacio de batalla integrado globalmente, los sistemas de armamento del DOD también dependen de tecnologías digitales para funcionar, y estas herramientas físicas son igual de susceptibles a las intromisiones cibernéticas. Dependiendo en el Sistema de Posicionamiento Global (GPS por sus siglas en inglés), software operativo y los procesos de adquisición de red no clasificados,[16] los sistemas de armamento están sujetos a posibles interrupciones desde su creación hasta su empleo. Además, esos mismos sistemas de armamento están sujetos al desgaste y complicaciones de movilización.[17] El no tomar en cuenta y planificar para la dependencia del

ámbito cibernético socava la supervivencia y movimiento de los sistemas de armamento del DOD, el equipo cinético necesario cuando se prosiguen las campañas. Sin tratar cómo el desgaste, la movilización y las vulnerabilidades cibernéticas coinciden, el DOD podría fracasar en contra de adversarios al mover recursos y emplear sistemas de armamento a la velocidad de la guerra. En el peor de los casos, el no asociar cognoscitivamente las amenazas cibernéticas con el desarrollo del sistema de armamento podría presagiar menos opciones disponibles para los comandantes de la fuerza conjunta, ocasionando que el DOD pierda potencia al proyectar poder y letalidad. En vista de que perder opciones cuesta resultados estratégicos, el DOD debe tratar la susceptibilidad del sistema de armamento para atacar cibernéticamente con el fin de evitar un impacto estratégico. De lo contrario, podría no estar preparado para contrarrestar las extensas responsabilidades del dominio cibernético.

Soluciones estratégicas

Con el fin de disuadir, negar, degradar o derrotar la amenaza de un impacto estratégico en el C2, despliegue y distribución y tecnología del sistema de armamento, el DOD debe tratar holísticamente la amenaza del ataque cibernético.[18] Esto requiere investigar dos conjuntos de problemas amplios con un enfoque coordinado: (1) cómo conservar la superioridad estadounidense en entornos cada vez más impugnados y (2) cómo elaborar una estrategia superior que proteja nuestra capacidad de proyección a lo largo de los ámbitos.

Estas áreas de enfoque toman en cuenta los impactos interdependientes de los problemas ciberespaciales como el marco estratégico para ocupar la nueva matriz de la guerra, ilustrando la necesidad para cambiar el paradigma. Equilibrando la cantidad, calidad y apresto superior de la fuerza con estrategia superior, el DOD puede justificar su dependencia digital, disuadir la acción agresiva y prevalecer cuando es interrumpido. Las soluciones estratégicas presentadas recalcan el cambio cognoscitivo requerido del DOD para entender su profundidad, cuando los efectos cinéticos superiores son secundarios a la postura superior con herramientas digitales. Sin básicamente cambiar su enfoque en la profundidad de su poder militar, podría fracasar para avanzar o inclusive conservar su ventaja estratégica.

La fuerza globalmente desplazable y dominante del DOD representa un blanco intrínseco para los adversarios en el ámbito cibernético.[19] Complicando este entorno impugnado, la fuerza está constantemente bajo tensión para balancear la cantidad, calidad y apresto superior. Aparentemente, los planificadores militares deben enfocarse en los tres —crear una capacidad orgánica robusta de las mejores tecnologías, listas para ser desplazadas al instante.[20] No obstante, las restricciones presupuestarias y las demandas variables hacen que esto sea difícil o casi imposible, creando una necesidad de introducir mayor agilidad y velocidad en los procesos de adquisición militar y en las operaciones.[21] Asociar cognoscitivamente una fuerza superior en entornos impugnados con el ámbito cibernético requiere la búsqueda explícita de ganancias en eficacia de la fuerza y la planificación globalmente integrada. Utilizando herramientas digitales avanzadas a través del ámbito cibernético, el DOD puede prepararse para el próximo conflicto superior aprovechándose expresamente de la cantidad, calidad y apresto de la fuerza existente para generar más capacidad. Específicamente, la optimización puede conservar una fuerza superior adelantando la eficacia en la asignación y ejecución con tecnologías evolutivas como la automatización, aprendizaje automático y análisis predictivo algorítmico.[22] Esta mentalidad regida por datos en administrar, mejorar y desplegar una fuerza superior aumenta la cantidad, calidad y apresto actual reduciendo el esfuerzo y el despilfarro. Al lograr que su equilibrio sea más fácil de administrar y mejorar en entornos impugnados y en los que los recursos están limitados, el DOD también le saca partido a su profundidad digital intrínseca.

Para poder disuadir y prevalecer contra los ataques cibernéticos en esta comunidad centrada en datos, el DOD debe negarle mejor el acceso al adversario y promover mayor redundancia.[23] Juntos, conservan las ventajas cibernéticas como estrategias de garantía cibernética. Si un enemigo no puede penetrar una red sólida, ya sea a través de una infraestructura segura basada en la nube del internet (*Cloud)* o protocolos de autenticación robustos de transacciones confiables o entrelazamiento cuántico, el DOD minimiza las vulnerabilidades.[24] Cuando el costo tecnológico de entrada aumenta, el grupo admisible de actores hostiles capaces se torna más pequeño, permitiendo una solución más a la medida y directa. No obstante, una barrera en la red que limite el acceso a esos adversarios más aptos no dispersa las vulnerabilidades ni protege el funcionamiento. Con el fin de que el DOD prevalezca y garantice la utilidad de su profundidad, debe cambiar de una dinámica de procesamiento cibernético de eslabón en una cadena a un modelo de porción de un todo.[25] Esparcir el riesgo en la red tanto física como virtual garantiza la capacidad de una fuerza superior al minimizar la exposición al riesgo y difundiendo la debilidad por una red. Un modelo de red le niega al adversario su capacidad de interrumpir totalmente las operaciones a través del alcance y nivel de esfuerzo necesario para afectarlas todas. Juntos, creando sinergias en un *firewall* (servidor de seguridad) con una presencia digital dispersada conserva la ventaja de la fuerza superior, especialmente si se le llama a la acción en entornos operacionales degradados cibernéticamente.

El modelo en evolución de entornos impugnados presenta una oportunidad singular para evaluar estratégicamente las suposiciones cibernéticas en la estrategia militar y reconocer cómo los enemigos buscan ventajas asimétricas o no convencionales.[26] En particular, crear una matriz de estrategia más amplia que reconozca cómo el mando y control, despliegue y distribución y las tecnologías del sistema de armamento son impugnadas a través del ámbito cibernético permite un entendimiento más global y exhaustivo de las operaciones militares. Una matriz de estrategia más amplia también contrarresta el potencial de un impacto estratégico afianzando las asociaciones cognoscitivas del DOD dentro de su dependencia digital. Con una mentalidad organizativa que se enfoca en la garantía de la misión en un entorno habilitado cibernéticamente y posiblemente degradado, el DOD no solo puede promover la evolución de las capacidades digitales sino también proteger de una desventaja las funciones cibernéticas críticas actuales. Está facultado para transformarse con el espacio de batalla evolucionado, nublando las líneas entre los ámbitos y los sistemas mediante la planificación estratégica para garantizar la misión.[27]

A medida que la cibernética se torna cada vez más multidominio en ejecución y función mediante la planificación global integrada, el DOD también debe tratar los roles y responsabilidades, autoridades y priorización dinámica con relación a la amenaza cibernética.[28] Específicamente, debe explorar modelos adicionales que apoyen su profundidad digital, sacándole provecho a las herramientas cibernéticas actuales y futuras para proteger las ventajas, negarle acceso al adversario y prevalecer contra una acción hostil. Además, esos modelos operacionales tienen que tratar la tensión cognoscitiva entre emplear ventajas cinéticas y habilitarlas. El DOD no puede aceptar perder capacidad o fuerzas en cifras inaceptables en esta conexión de empleo digital pero puede que sea susceptible a dichas pérdidas con la planificación restringida a resultados específicos al ámbito.

Con el fin de evitar el impacto estratégico de las asociaciones cognitivas aisladas**,** el riesgo estratégico debe continuamente tratar la posibilidad de interferencia en esas herramientas digitales que conectan al planificador militar con el guerrero, el hilo cibernético que conecta todos los niveles del DOD.[29] La milicia también debe evaluar el riesgo estratégico con una perspectiva global, para remediar las suposiciones geográficas permisivas que han penetrado el conflicto desde la Segunda Guerra Mundial, centradas en la creencia que Estados Unidos puede operar a su antojo. Los conflictos futuros no estarán limitados a un solo comando combatiente, de manera que las asociaciones cognoscitivas requieren ajustarse para mirar los efectos cinéticos como productos de una seguridad cibernética robusta y global. Además, los entornos impugnados

hacen que la relación binaria entre la paz y la guerra sea más turbia a causa de la acción adversaria persistente en el ámbito cibernético. Las herramientas digitales están en riesgo constantemente, por lo tanto, evitar un impacto estratégico requiere una defensa implacable. Al igual que conservar una fuerza superior, los planificadores del DOD deben enfocarse en cómo la organización militar es más resistente sin procesos enlazados o lineales, esparciendo recursos en una red para fomentar la supervivencia. La dependencia digital del DOD no puede prevalecer con un modelo de cadena consecutivo y puntos individuales de fracaso.

Una matriz nueva

Las amenazas del mañana al ámbito cibernético requieren que el impacto estratégico se comprenda hoy. Cabe señalar, la nueva matriz de la guerra no busca reemplazar o socavar la importancia de una fuerza superior, ya sea a través de su C2, despliegue y distribución o tecnología del sistema de armamento. En cambio, tan solo reconoce la dependencia digital del DOD para emplear esas ventajas, adoptando una asociación cognoscitiva entre la profundidad militar, la capacidad del ámbito cibernético y las vulnerabilidades del impacto cibernético. Muy similar a que el mítico Morfeo es el dios griego de los sueños, el personaje ficticio de *The Matrix* reta a los planificadores militares a contemplar la realidad de una manera diferente y apreciar las vulnerabilidades virtuales. La dependencia del DOD en las herramientas cibernéticas es como un sueño, ambos incorpóreos sin embargo sujetos a la influencia, manipulación e interrupción. Sin comprender cómo los adversarios buscan ventajas asimétricas contra las fuerzas superiores, el DOD no puede apreciar completamente el riesgo que acepta a través de su dependencia digital.

Proyectar poder hacia entornos impugnados requiere analizar continuamente la profundidad y razonamiento del DOD a través de la operación sin capacidades cibernéticas. Ahora el éxito requiere destacar funciones digitales clave, donde las vulnerabilidades cibernéticas necesitan un conocimiento táctico y estratégico de la permisividad y la libertad de maniobra. Facultada por una discusión exhaustiva de la integración global y la interconexión, la ventaja del poder cinético estadounidense es solamente parte de esta ecuación para los planificadores militares. El DOD debe entender, que la garantía de la misión para entrenar efectos cinéticos es un producto de operar de manera segura en el dominio cibernético. Despojar ambos es forzar una solución análoga a los problemas de la era digital, o como Morfeo diría, permanecer en el país de la maravillas. Estados Unidos no puede darse el lujo de vivir de falsas ilusiones y debe reconocer cómo los adversarios envalentonados tratarán de interrumpir nuestras ventajas, atacando la profundidad cibernética de la milicia y no necesariamente sus fuerzas convencionales para lograr efectos estratégicos. La fortaleza y la velocidad por sí solas no cuentan dentro de la nueva matriz de la guerra.

Se necesitan más discusión, investigación y directrices para ir más allá de las limitaciones de la asociación cognoscitiva actual. Para vencer la parálisis y prepararse para lo imprevisto de conflictos impugnados en el futuro, el DOD debe incansablemente buscar soluciones para disuadir las amenazas cibernéticas, prevalecerlas y evitar el sufrimiento del impacto estratégico. La nueva matriz requiere urgentemente una mejor integración global, seguridad y resistencia cibernética superior y un dominio optimizado con menos recursos, exigiendo más inversión en las herramientas digitales que promuevan la eficacia y menos enfoque en las autoridades geográficas. Por necesidad, el DOD puede ser el precursor de este futuro, pero solamente tan rápido como pueda aceptar cognoscitivamente su dependencia digital. Si Estados Unidos no asocia institucionalmente la proyección de poder con las herramientas digitales que requiere, puede que el DOD no prevalezca un día sin la cibernética. ❑

Notas

1. Michael O. Wheeler, "*The Changing Requirements of Assurance and Extended Deterrence*" (Los requerimientos cambiantes de garantía y la disuasión extendida), *Institute for Defense Analyses* (Instituto para el Análisis de la Defensa), julio de 2010, iii–iv, http://www.dtic.mil/docs/citations/ADA550264.

2. General de División Richard Weber, USAF, y Coronel Mark E. Ware, USAF, *"Cyberspace Mission Assurance: A New Paradigm for Operations in Cyberspace*" (Garantía de la misión ciberespacial: Un nuevo paradigma para las operaciones en el ciberespacio), *High Frontier* 6, no. 4, (agosto de 2010): 3–7, http://www.dtic.mil/docs/citations/ADA549792.

3. *Question Asked by Morpheus*" (Pregunta planteada por Morfeo), *The Matrix*, dirigida por Lana Wachowski y Lilly Wachowski (1999; Burbank, CA: Warner Home Video, 1999), DVD.

4. Coronel Clinton J. Ancker III, USA, Retirado, y Teniente Coronel Michael Flynn, USA, Retired, "*Exercising Command and Control in an Era of Persistent Conflict*", (Ejerciendo el mando y control en una era de conflicto persistente), *army.mil*, 3 de mayo de 2010, https://www.army.mil/article/38412/exercising-command-and-control-in-an-era-of-persistent-conflict/; Eric Peltz y Marc Robbins, "*Leveraging Complementary Distribution Channels for an Effective, Efficient Global Supply Chain*" (Sacándole provecho a los canales de distribución complementaria para una cadena de abastecimiento global eficaz y eficiente), *RAND Corporation*, 2007, vii–x, http://www.dtic.mil/docs/citations/ADA473027; *US Government Accountability Office* (Oficina Pública de Contabilidad del Gobierno de EE.UU. (GAO, por sus siglas en inglés), *Defense Acquisitions: Assessments of Selected Weapon Programs* (Adquisiciones para la defensa: Evaluaciones de programas de armamento seleccionados), *Report to Congressional Committees* (Informe a Comités del Congreso), (Washington, DC: US GAO, marzo de 2017), 5–6, http://www.dtic.mil/docs/citations/AD1032079; y Joshua T. Hartman, "*Exploring the Complementary Nature of Cyber and Space Operations*" (Explorando la naturaleza complementaria de las operaciones cibernéticas y espaciales), *High Frontier* 6, núm. 4 (agosto de 2010): 31–34, http://www.dtic.mil/docs/citations/ADA549792.

5. Jim Garamone, "*Dunford: Command, Control Must 'Keep Pace' in 21st Century*" (Dunford: Mando y control deben "mantener la paz" en el siglo XXI), *DoD News, Defense Media Activity*, 4 de enero de 2016, https://www.defense.gov/News/Article/Article/639844/dunford-command-control-must-keep-pace-in-21st-century/.

6. Estado Mayor Conjunto, "*The Joint Force in a Contested and Disordered World*" (La fuerza conjunta en un mundo impugnado y desordenado), *The Joint Operating Environment 2035*, 14 de julio de 2016, ii–iii, http://www.dtic.mil/docs/citations/AD1012885; y Mayor Paul J. Blakesley, Ejército Británico, "*Operational Shock and Complexity Theory*" (Impacto operacional y la teoría de la complejidad), monografía (Fort Leavenworth, KS: US Army Command and General Staff College School of Advanced Military Studies (Escuela de Comando y Estado Mayor General de Estudios Militares Avanzados del Ejército de EE.UU.), 26 de mayo de 2005), 69–71, http://www.dtic.mil/docs/citations/ADA437516.

7. Coronel Peter J. Lane, USA, "*Strategic Shock: Managing the Strategic Gap*" (Impacto estratégico: Administrando la brecha estratégica), Proyecto de Investigación sobre Estrategia), (Carlisle Barracks, PA: Army War College, March 2013), 1–5, http://www.dtic.mil/docs/citations/ADA589203.

8. Mayor Anthony L. Marston, USA, "*The Efficacy of Cognitive Shock*" (La eficacia del impacto cognoscitivo), monografía, (Fort Leavenworth, KS: US Army Command and General Staff College School of Advanced Military Studies, May 2015), 33–35, http://www.dtic.mil/get-tr-doc/pdf?AD=AD1001654.

9. Teniente Coronel Thomas M. Jordan, USA, "*Versatility and Balance: Maintaining a Full Spectrum Force for the 21st Century*" (Versatilidad y equilibrio: Manteniendo una fuerza de espectro total para el siglo XXI), esto se trata en el documento original Proyecto de Investigación sobre la Estrategia, (Carlisle Barracks, PA: Army War College, 6 de abril de 1998), 22–24, http://www.dtic.mil/docs/citations/ADA343362; Teniente Coronel Russell F. Miller, USA, "*Developing and Retaining Information Warriors: An Imperative to Achieve Information Superiority*" (Capacitando y reteniendo guerreros de informática: Un imperativo para lograr superioridad en la informática), Proyecto de Investigación sobre la Estrategia, (Carlisle Barracks, PA: Army War College, 29 de febrero de 2000), 2–3, http://www.dtic.mil/docs/citations/ADA377713; y Justin A. Thompson, "*Improving Department of Defense Global Distribution Performance Through Network Analysis*" (Mejorando el rendimiento de distribución global del DOD a través de análisis de la red), (tesis de maestría, Monterey, CA: Naval Postgraduate School (Escuela de Posgrado de la Armada), junio de 2016), 41–42, http://www.dtic.mil/docs/citations/AD1026843.

10. Peter C. Mastro, "*So Near and Yet So Far: Choices and Consequences of the Stand-In and Stand-Off Approach*" (Tan cerca y sin embargo tan lejos: Opciones y consecuencias del **método interino y del método seguro** (stand-in and stand-off approach) (tesis de Maestría, Fort Leavenworth, KS: US Army Command and General Staff College School of Advanced Military Studies, 1º de junio de 2015), 121–25, http://www.dtic.mil/docs/citations/AD1015800.

11. Capitán de Fragata Lawrence Rice, USN, "*Technology's Impact on Command and Control: How Much Does the Operational Commander Need?*" (Impacto de la tecnología en el mando y control: ¿Cuánto necesita el comandante operacional?), informe final (Monterey, CA: Escuela de Posgrado de la Armada, 19 de mayo de 1997), 13–14, http://www.dtic.mil/docs/citations/ADA328120.

12. Dan Shen, Genshe Chen, Jose B. Cruz Jr., Erik Blasch y Martin Kruger, "*Adapting C2 to the 21st Century: Game Theoretic Solutions to Cyber Attack and Network Defense Problems*" (Adaptando el C2 al siglo XXI: Soluciones teóricas del juego a los ataques cibernéticos y los problemas de defensa de la red), (Rockville, MD: Duodécimo Simposio Internacional de Investigación y Tecnología del Mando y Control, junio de 2007), 1–2, 16, http://www.dtic.mil/docs/citations

/ADA481265; y General de Brigada Kurt S. Story, USA, y Peter M. Stauffer, "*Delivering It to the Soldier*" (Entregándoselo al soldado), *High Frontier* 6, núm. 4 (agosto de 2010): 16–19, http://www.dtic.mil/docs/citations/ADA549792.

13. Teniente Coronel Robert C. Johnson, USA, "*Fighting with Fires: Decentralize Control to Increase Responsiveness*" (Luchando con fuegos: Control descentralizado para aumentar la reacción), monografía, (Fort Leavenworth, KS: US Army Command and General Staff College School of Advanced Military Studies, 2001), 37–41, http://www.dtic.mil/docs/citations/ADA403795.

14. Mayor Richard McGlamory, USAF, "*Defense or Diplomacy? Geographic Combatant Commands*" (¿Defensa o diplomacia? Comandos combatientes geográficos, (tesis de Maestría, Escuela de Estudios Avanzados Aéreos y Espaciales, Universidad del Aire, Maxwell, AFB, 1º de junio de 2011), 55–56, http://www.dtic.mil/docs/citations/AD1019397.

15. Thomas Lorenzen, "*The Edge of Chaos: Emergent Factors in the Information Environment*" *The Strategy Bridge* (El borde del caos: Factores emergentes en el entorno de la informática, El puente de la estrategia), 9 de mayo de 2017, https://thestrategybridge.org/the-bridge/2017/5/9/the-edge-of-chaos-emergent-factors-in-the-information-environment; y General de División Arnold Punaro, USMC, Retirado, Bill Phillips, John O'Connor, y Capitán de Navío Garrett Campbell, USN, "*Logistics as a Competitive War Advantage*" (La logística como una ventaja competitiva a la guerra), informe técnico (Washington, DC: Defense Business Board, 20 de octubre de 2016), 2–5, http://www.dtic.mil/docs/citations/AD1020304.

16. Marc A. Thibault, Jr., "*GPS: Public Utility or Software Platform?*, (GPS: ¿Utilidad pública o plataforma de software?), informe técnico (Monterey, CA: Naval Postgraduate School, 1º de septiembre de 2016), 57–62, http://www.dtic.mil/docs/citations/AD1030085; John B. Dickens y Dean R. Dukes, "*Innovative Decentralized Decision-Making Enabling Capability on Mobile Edge Devices*" (Innovadora toma de decisiones descentralizada permitiendo la capacidad en dispositivos móviles de vanguardia), informe técnico (Monterey, CA: Naval Postgraduate School, 1º de septiembre de 2015), 85–88, http://www.dtic.mil/docs/citations/AD1008918; y Coronel Robert L. Tremaine, USAF, Retirado, "*Demonstrating Cyberspace Superiority in an Acquisition World*" (Demostrando la superioridad ciberespacial en un mundo de adquisición), *High Frontier* 6, núm. 4 (agosto de 2010): 62–65, http://www.dtic.mil/docs/citations/ADA549792.

17. J. B. Bartholomess, Jr., "*The Issue of Attrition*" (El tema del desgaste), artículo de revista (Carlisle Barracks, PA: Army War College, Spring 2010), 17–18, http://www.dtic.mil/docs/citations/ADA522310; y Mayor Christopher G. Williams, USA, "*Fielding a Division Staff in the Modern Day*" (Poner en servicio al personal de una División en la vida contemporánea), informe técnico (Fort Leavenworth, KS: Army Command and General Staff College, 10 de junio de 2016, 58–61, http://www.dtic.mil/docs/citations/AD1020377.

18. Martin Libicki y Teniente General Robert Elder, USAF, Retirado, "*Mission Assurance in the Face of Cyber Attacks*" (Garantía de la misión ante ataques cibernéticos), *High Frontier* 6, núm. 4 (agosto de 2010): 24–27, http://www.dtic.mil/docs/citations/ADA549792.

19. Teniente Coronel William D. Bryant, USAF, "*Cyberspace Superiority: Dominating the Digital Frontier*" (Superioridad ciberespacial: Dominando la frontera digital), (tesis, Maxwell AFB, AL, School of Advanced Air and Space Studies: Enero de 2014), 47–48, http://www.dtic.mil/docs/citations/ADA622182.

20. Laura J. Junor, "*Managing Military Readiness*" (Administrando el apresto militar), *Strategic Perspectives*, 23 Institute for National Strategic Studies, (Washington, DC: National Defense University, February 2017), 1, http://www.dtic.mil/docs/citations/AD1030355.

21. Chad DeStefano, Kurt Lachevet y Joseph Carozzoni, "*Distributed Planning in a Mixed-Initiative Environment: Collaborative Technologies for Network Centric Operations*" (Planificación distribuida en un entorno de iniciativas mixtas: Tecnologías colaborativas para las operaciones centradas en la red), ponencia de conferencia (Rome, NY: Laboratorio de Investigaciones de la Fuera Aérea, octubre de 2007), 20, http://www.dtic.mil/docs/citations/ADA489219.

22. George K. Baah, Thomas Hobson, Hamad Okhravi, Shannon C. Roberts, William W. Streilein y Sophia C. Yuditskaya, "*A Study of Gaps in Cyber Defense Automation*" (Un estudio de las brechas en la automatización de la defensa cibernético), Informe Técnico Núm. 1194 (Lexington, MA: Massachusetts Institute of Technology, Lincoln Laboratory, 13 de octubre de 2016), 39–40, http://www.dtic.mil/docs/citations/AD1021685; Liang Xiong, "*On Learning from Collective Data*" (Aprendiendo de los datos colectivos), (tesis de doctorado, Carnegie Mellon University, Machine Learning Department, December 2013), 142–43, http://www.dtic.mil/docs/citations/ADA598234; y L. Richard Moore Jr., "*Cognitive Model Exploration and Optimization: A New Challenge for Computational Science*" (Exploración y optimización del modelo cognoscitivo: Un nuevo reto para la ciencia computacional), ponencia de conferencia (Mesa, AZ: Lockheed Martin Systems Management, Air Force Research Laboratory, Warfighter Readiness Research Laboratory, 24 de marzo de 2010), 160, http://www.dtic.mil/docs/citations/ADA553672.

23. Teniente Coronel Shane H. Connary, USAF, "*Computer Network Operations Command and Control: A New Perspective*" (Mando y control en las operaciones de la red de computadoras), informe final (Monterey, CA: *Naval War College*, 22 October 2009), 1–3, http://www.dtic.mil/docs/citations/ADA513948.

24. Matthew Presley, "*Beyond Data Services: Cloud Processing for Net-Centric Information Distribution*" (Más allá de los servicios de datos: Procesamiento en Cloud para la distribución de información centrada en la red), *High Frontier* 6, núm. 4, agosto de 2010: 57–61, http://www.dtic.mil/docs/citations/ADA549792; Andrew Miller y Rob Jansen, "*Shadow-Bitcoin: Scalable Simulation via Direct Execution of Multi-threaded Applications*" (Siguiendo de cerca el bitcoin: Simulación escalable vía ejecución directa de aplicaciones con múltiples subprocesos), informe de investigación (Monterey, CA: Naval Research Laboratory, 10 de agosto de 2015), 6, https://www.nrl.navy.mil/itd/chacs/sites/www.nrl.navy.mil.itd.chacs/files

/pdfs/15-1231-1593.pdf; y Rodney Van Meter, "*Security of Quantum Repeater Network Operation*" (Seguridad de operación en la red del repetidor cuántico), informe final (Fujsawa, Japan: Keio University, 3 de octubre de 2016), 3–5, http://www.dtic.mil/docs/citations/AD1019872.

25. Teniente General Charles Croom, USAF, Retirado, "*The Cyber Kill Chain: A Foundation for a New Cyber Security Strategy*" (La cadena de aniquilamiento cibernético: Base para una nueva estrategia de seguridad cibernético), *High Frontier* 6, núm. 4 (agosto de 2010): 52–56, http://www.dtic.mil/docs/citations/ADA549792.

26. Barry R. Schneider, "*Asymmetric Rivals: The Enemy Next Time*" (Rivales asimétricos: El enemigo la próxima vez), *The War Next Time: Countering Rogue States and Terrorist Armed with Chemical and Biological Weapons, 2nd edition,* (La guerra la próxima vez: Contrarrestando estados parias y terroristas armados con armas químicas y biológicas), editores Schneider y Jim A. Davis (Maxwell AFB, AL: USAF Counterproliferation Center, April 2004), 1, https://www.hsdl.org/?view&did=446550.

27. Teniente Coronel Patrick J. Obruba, USAF, "*Breaking Stovepipes: Bridging Gaps in Air Force Industrial Control Systems Management to Enable Multi-Domain Mission Assurance*" (Rompiendo los estancamientos: Uniendo las brechas en la gestión de sistemas de control industrial de la Fuerza Aérea para permitir la garantía de la misión en multidominios), informe técnico (Maxwell AFB, AL: Air War College, 16 de febrero de 2016), iv–1, http://www.dtic.mil/docs/citations/AD1037194.

28. Michael J. McNerney, "*Department of Defense and Security Cooperation: Improving Prioritization, Authorities, and Evaluations*" (El Departamento de Defensa y la cooperación en materia de seguridad: Mejorando la priorización, autoridades y evaluaciones), informe técnico (Santa Monica, CA: RAND Office of External Affairs, 9 de marzo de 2016), 3–4, http://www.dtic.mil/docs/citations/AD1014435.

29. Mayor Michael D. Pritchett, USAF, "*Cyber Mission Assurance: A Guide to Reducing the Uncertainties of Operating in a Contested Cyber Environment*" (Garantía de la misión cibernética: Una guía para disminuir las incertidumbres de operar en un entorno cibernético impugnado), (tesis de maestría, Wright Patterson AFB, OH: Air Force Institute of Technology, 14 de junio de 2012), 39–41, http://www.dtic.mil/docs/citations/ADA563712.

Capitán Keith B. Nordquist, Fuerza Aérea de EE.UU. (BA, USAFA; MA, Embry-Riddle Aeronautical University) obtuvo su nombramiento en el 2008 como egresado distinguido. Es un oficial especializado en iniciativas estratégicas con el Grupo de Acción del Comandante, Comando de Transporte de Estados Unidos en la Base Aérea Scott, Illinois. Antes de ocupar su puesto actual, el Capitán Nordquist completó dos asignaciones en calidad de instructor comandante de aeronave del C-5 y desempeñó puestos en entrenamiento, seguridad, inspección, comandante de vuelo y oficial ejecutivo a niveles de escuadrón, ala y comandos superiores.