El uso del ciberpoder

Teniente Coronel Kevin L. Parker, Fuerza Aérea de EUA

El teniente coronel Kevin L. Parker, Fuerza Aérea de EUA, es el comandante del 100º Escuadrón de Ingeniería Civil en RAF Mildenhall, Reino Unido. Cuenta a su haber con una Licenciatura en Ingeniería civil de la Universidad de Texas A&M, una Maestría en Desarrollo de recursos humanos de la Universidad Webster, otra Maestría en Arte y ciencia militar operacional y otra en Estrategia militar de la Universidad del Aire. Se ha desplegado a Arabia Saudita, Kirguistán y dos veces a Irak.

Después de más de 50 años, la guerra de Corea no se ha acabado oficialmente, pero pocas veces se lanzan barreras de artillería a través de la zona desmilitarizada.[1] Las fuerzas militares de EUA continúan luchando en Afganistán después de más de 10 años, sin declaración formal de guerra.[2] Otro conflicto continúa hoy en día sin balas o declaraciones. En este conflicto, los adversarios de EUA realizan sondeos, ataques y asaltos diarios.[3] Las ofensivas son invisibles e inaudibles, pero no son menos reales que los proyectiles de artillería o dispositivos explosivos improvisados Este conflicto se lleva a cabo en el ciberespacio.

A fin de cumplir con el propósito de las Fuerzas Armadas de EUA de defender la nación y avanzar los intereses nacionales, el ambiente de seguridad complejo de hoy en día requiere la presencia incrementada en el ciberespacio.[4] Por consiguiente, el Departamento de Defensa (DoD, por sus siglas en inglés) ahora considera al ciberespacio un dominio operacional.[5] Parecido a los otros dominios, el ciberespacio tiene su propio conjunto de características distintivas. Estos atributos presentan ventajas singulares y limitaciones correspondientes. Mientras cambia el carácter de la guerra, comprender el uso del ciberpoder requiere una evaluación de las ventajas y limitaciones en los posibles contextos estratégicos.

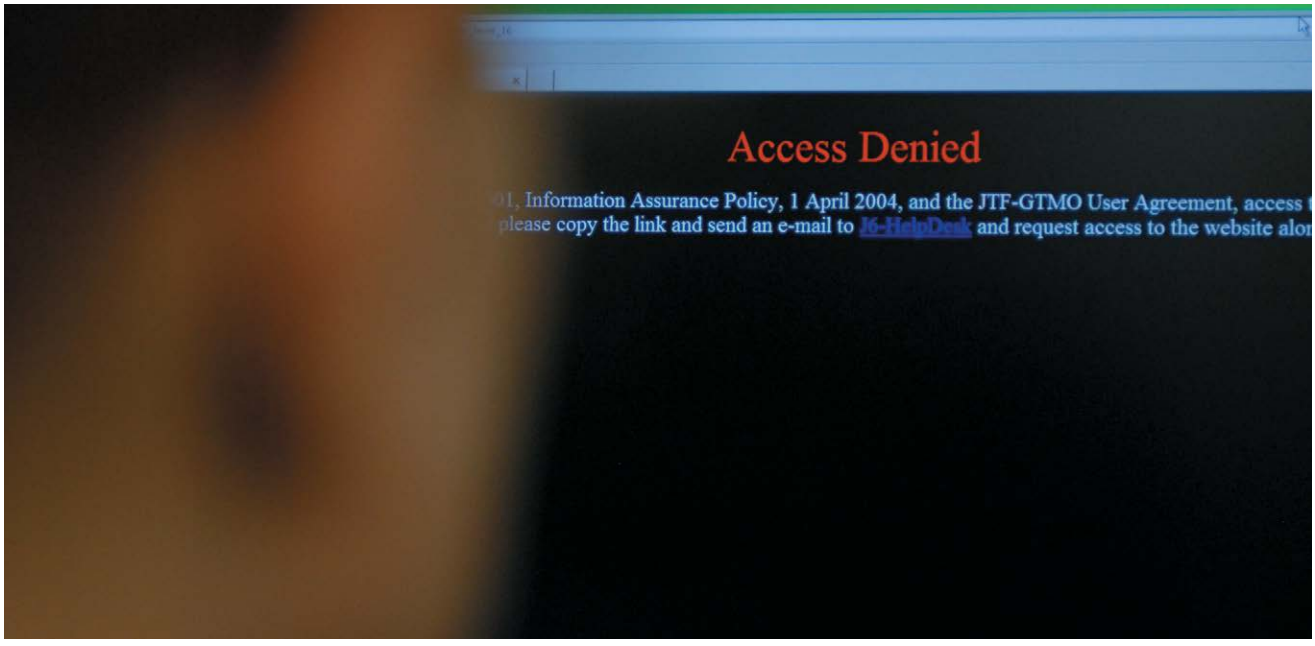
Cómo definir el ciberespacio y el ciberpoder

Hay una gama de definiciones del ciberespacio y ciberpoder, pero aún se debate la importancia de establecer las definiciones. Daniel Kuehl recopiló 14 definiciones diferentes del ciberespacio de diversas fuentes, solo para concluir que debía ofrecer su propia conclusión.[6] ¿Importan las definiciones exactas? En las organizaciones burocráticas, sí importan las definiciones porque facilitan una clara

división de roles y misiones a través de departamentos e instituciones militares. En el Departamento de Defensa, alguna duplicación de esfuerzos puede ser deseable pero ocurre a un costo elevado; por lo tanto, se necesitan definiciones para facilitar los análisis rigurosos a fin de establecer los límites y presupuestos organizacionales.[7] En la ejecución de roles asignados, importan mucho las definiciones para la comunicación y coordinación trans-organizacionales.

Sin importar cuán importante sea, es difícil encontrar las definiciones precisas que satisfagan todos los puntos de vista y contextos. Considere definir al mar como todos los océanos del mundo. Esta definición carece de la suficiente claridad para delimitar bahías o vías fluviales. Aparentemente irrelevante, la ambigüedad es de gran consecuencia para las organizaciones jurisdiccionalmente limitadas a la orilla del río. A diferencia de la presencia constante del mar por milenios, Internet es un fenómeno relativamente nuevo que continúa expandiéndose y evoluciona rápidamente. Puede ser fútil buscar definiciones singulares del ciberespacio y ciberpoder para eliminar toda pregunta. David Lonsdale sostiene que desde un punto de vista estratégico, las definiciones tienen poca importancia. En su opinión, "lo que en realidad más importa es percibir la esfera de información como un lugar que existe, comprender su naturaleza y considerarla como algo que puede ser manipulado y usado como una ventaja estratégica".[8] Las siguientes definiciones son consistentes con el punto de vista de Lonsdale y son suficientes para

El Comando Cibernético de EUA llevó a cabo un ejercicio conjunto de entrenamiento de ciberespacio en noviembre de 2011, llevado a cabo, principalmente, en la Instalación de Bandera Roja de la Fuerza Aérea en la base aérea Nellis, en el estado de Nevada. El ejercicio reunió a aproximadamente 300 profesionales de cibernética y tecnología de información, 2 de noviembre de 2011.
(Ejército de EUA)



¡Acceso negado! La Seguridad de Información de la sección J-6 (mando, control, comunicaciones y computadoras/cibernética) ejecutan proxies para proteger a los servidores de la Fuerza de Tarea Conjunta Guantánamo de sitios web malignos. La Seguridad de Información defiende los servidores de la fuerza de tarea conjunta de amenazas internas y externas mientras garantiza que se ajusten a las políticas y procedimientos de la Agencia de Sistemas de Información del Departamento de Defensa, el Ejército de EUA y el Comando Sur de EUA, en la Base Naval de Guantánamo, Cuba, 8 de julio de 2008.
(Armada de EUA)

satisfacer los propósitos de esta discusión, pero es poco probable que satisfagan a los profesionales que desean usarlas más allá de una perspectiva estratégica.

El ciberespacio: el dominio que existe para entrar, almacenar, transmitir y extraer información a través del uso del espectro electromagnético. Incluye todo el *hardware, software* y medios de transmisión usados, desde la entrada inicial (por ejemplo, los dedos pulsando las teclas, hablar en micrófonos o pasar documentos por escáneres) hasta la presentación de información para la cognición de usuarios (V.gr., imágenes en pantallas, sonido emitido de bocinas o reproducción de documentos) u otra acción (por ejemplo, guiar un vehículo no tripulado o cerrar válvulas).

El ciberpoder: El potencial para usar el ciberespacio a fin de lograr los resultados deseados.[9]

Las ventajas de manejar el ciberpoder

Al ser estas definiciones suficientes para esta discusión, considere las ventajas de las operaciones a través del ciberespacio.

El ciberespacio proporciona un alcance global. El número de personas, lugares y sistemas interconectados, a través del ciberespacio, está creciendo rápidamente.[10] Estas conexiones mejoran la capacidad de las Fuerzas Armadas de alcanzar a personas, lugares y sistemas militares en todas partes del mundo. El operar en el ciberespacio proporciona el acceso a áreas negadas en otros dominios. Los primeros defensores del poder aéreo alegaron que los aviones ofrecían una alternativa a las botas en el lugar para poder sobrevolar las defensas del enemigo para directamente atacar a los centros de poder.[11] Rápidamente se desarrollaron defensas antiaéreas sofisticadas, lo que incrementó los riesgos a los ataques aéreos y disminuyó su ventaja. A pesar de las actuales defensas cibernéticas que hay en la actualidad, el ciberespacio ofrece la ventaja de acceso a áreas en conflicto sin poner en peligro

a los operadores. Un ejemplo de cómo directamente alcanzar a los enemigos que toman decisiones a través del ciberespacio surge de un acontecimiento en 2003, antes de la invasión de Irak por Estados Unidos. Según se informa, el Comando Central de EUA envió un correo electrónico a los oficiales militares iraquíes en su red secreta que les avisó abandonar sus puestos.[12] Ningún otro dominio tenía tanto alcance con tan poco riesgo.

El ciberespacio permite la acción y concentración rápida. El ciberespacio no solo permite el alcance global, sino también su velocidad es sin paralelo. Con el reabastecimiento de combustible en vuelo, las fuerzas aéreas puede alcanzar casi todo punto en el mundo; sin embargo, llegar hasta allá puede tomar horas. El establecimiento de bases de vanguardia puede reducir a minutos los tiempos de reacción, pero la información se mueve, literalmente, a la velocidad de la luz en los cables ópticos. Los que inician los ciberataques pueden lograr la concentración mediante el uso de otras computadoras. Al distribuir discretamente un virus acondicionado para responder por mando, miles de computadoras botnet asimiladas pueden iniciar, instantáneamente, un ataque distribuido de negación de servicio. Estos actores también pueden instar a otros usuarios a unirse voluntariamente a la causa, como hicieron los "hackers patrióticos" rusos que participaron en los ataques con Estonia en 2007.[13] Con estas técnicas, grandes poblaciones interconectadas podrían movilizarse en una escala sin precedentes en masa, tiempo y concentración.[14]

El ciberespacio permite la anonimidad. Los diseñadores de Internet establecieron una alta prioridad en la descentralización y desarrollaron la estructura basada en la confianza mutua de sus pocos usuarios.[15] En las décadas desde de su comienzo, el número de usuarios de Internet ha crecido exponencialmente más allá de su concepción original.[16] El sistema resultante hace muy difícil seguir una ruta probatoria a cualquier usuario.[17] La anonimidad permite la libertad de acción con una atribución limitada.

El ciberespacio favorece la ofensiva. En la era de Clausewitz, la defensiva era más fuerte, pero el ciberespacio, debido a las ventajas antes mencionadas, actualmente favorece el ataque.[18] Históricamente, las ventajas de los avances tecnológicos erosionan con el tiempo.[19] Sin embargo, las circunstancias actuales contraponen defensores y rápidos ataques concentrados, apoyados por vulnerabilidades estructurales de seguridad que son inherentes en la arquitectura del ciberespacio.

El ciberespacio extiende el espectro de armas no letales. Joseph Nye describió una tendencia, especialmente en las democracias de antimilitarismo, lo que hace el uso de la fuerza "una opción políticamente peligrosa".[20] Frecuentemente, el deseo de limitar los daños colaterales ha pasado a primer plano en las operaciones en Afganistán, pero dicho deseo no se circunscribe a las contrainsurgencias.[21] Las municiones guiadas de precisión y bombas de pequeño diámetro son productos de los esfuerzos de mejorar las capacidades de ataque con un menor riesgo de daños colaterales. Los ciberataques ofrecen medios no letales de acción directa contra un adversario.[22] Las ventajas del ciberpoder pueden resultar atractivas a los formuladores de política, pero la comprensión de sus limitaciones debe templar dicho entusiasmo. La limitación más obvia es que el adversario puede usar todas las mismas ventajas en su contra. Otra limitación obvia es su mínima influencia en los adversarios no centrados en redes. En cambio, mientras más dependa una organización del ciberespacio, más vulnerable será en cuanto a los ciberataques. Tres limitaciones adicionales requieren más atención.

Los ataques en el ciberespacio dependen mucho de los efectos de segundo orden. En los términos de Thomas Schelling, no hay opciones de fuerza bruta en el ciberespacio, por lo tanto, las operaciones cibernéticas dependen de la coerción.[23] Los ejércitos continentales pueden ocupar terreno y tomar control de objetivos por medio de la fuerza bruta, pero el éxito en las operaciones en el ciberespacio, frecuentemente, depende de cómo reaccionan los adversarios ante la información suministrada, alterada o negada. Los ciberataques que crean efectos cinéticos, tales como mandos destructivos a los sistemas de control industriales, son posibles. Sin embargo, los raros incidentes de códigos malignos que ocasionan la explosión de un oleoducto ruso o el gusano *Stuxnet* que provoca un paro de procesos en una instalación nuclear iraní, no eran sus propósitos.[24] En este último caso, solo las decisiones de los líderes iraníes podrían realizar el abandono de la búsqueda de la tecnología nuclear. Parecido a la incapacidad del

bombardeo estratégico de romper el espíritu en la Segunda Guerra Mundial, los ciberataques frecuentemente dependen de efectos imprevisibles de segundo orden.[25] Si el contraalmirante Wylie tiene razón en cuanto a que la guerra es una cuestión de control y "su herramienta fundamental... es el hombre en el lugar con un arma", entonces las operaciones a través del ciberespacio solo pueden proporcionar una menor forma de control.[26] Evgeny Morozov en forma de broma dijo, "Sin duda alguna, los tweets no derrocan a los gobiernos; las personas lo hacen".[27]

Los ciberataques ponen en riego consecuencias involuntarias. Al igual que un ataque contra el sistema de alimentación de una instalación militar puede tener ramificaciones escalonadas sobre una población más grande, es difícil limitar los efectos a través del ciberespacio interconectado. Los instructores de tiro al blanco enseñan a los tiradores a considerar su alcance máximo y lo que se encuentra más allá de sus blancos. Sin mapas para todos los sistemas, es imposible identificar los alcances máximos y lo que se encuentra más allá de un blanco en el ciberespacio.

La defensa contra los ciberataques es posible. La ventaja ofensiva actual no hace inútil toda medida defensiva. Aún si las intrusiones de ataques complejos y persistentes son inevitables, las medidas defensivas específicas (por ejemplo, controles de seguridad física, limitar el acceso a los usuarios, *software* de filtración y antivirus y, paredes de protección (*firewalls*) ofrecen un nivel de protección. La redundancia y replica son estrategias de resiliencia que pueden disuadir a los presuntos agresores al hacer fútiles los ataques.[28] Las respuestas de represalia por medio del ciberespacio u otros medios también pueden mejorar la disuasión.[29] Actualmente, la defensiva está en desventaja, pero la ofensiva está libre de complicaciones en el ciberespacio.

Expectativas y Recomendaciones

Las ventajas y limitaciones del uso del ciberpoder informan las expectativas para el futuro y algunas recomendaciones para las Fuerzas Armadas.

No anticipe una política clara e integral a corto plazo.[30] El expresar una estrategia integral estadounidense para usar las armas nucleares retrasó, 15 años, su primer uso y el plazo para una política clara e integral de ciberespacio aún podría tomar más tiempo.[31] En el ciberespacio chocan múltiples intereses, lo cual obliga a los formuladores de política abordar los conceptos que, tradicionalmente, han sido difíciles de resolver en EUA. El ciberespacio, similar a la política exterior, expone la tensión entre volver al realismo en un sistema no gobernado y anárquico y aspirar al ideal liberal de seguridad a través del reconocimiento recíproco de derechos naturales. La política del ciberespacio requiere la adjudicación entre numerosas prioridades basada en valores estimados tales como los derechos de propiedad intelectual, el papel que desempeña el gobierno en asuntos de negocios, llevar a los criminales a la justicia, libertad de expresión, intereses de seguridad nacional y privacidad personal. Ninguno de estos asuntos es nuevo. El ciberespacio solo los entrelaza y los presenta desde ángulos extraños. Por ejemplo, es posible que el derecho de libre expresión no se extienda a falsamente gritar "fuego" en teatros llenos de gente, pero a través del ciberespacio se difunden todas las palabras a un teatro global lleno de personas.[32]

Más allá del frente interno, como mínimo, el acceso a Internet crea un gran dilema de política exterior. Si bien, dicho acceso puede ayudar a movilizar y habilitar a los disidentes bajo gobiernos opresivos, también puede proporcionar más herramientas de control de la población a los líderes autoritarios.[33] Es poco probable que desenredar estos conjuntos de asuntos superpuestos en nuevos contextos ocurra rápidamente. Es posible que se necesiten varias iteraciones y que esto solo pueda ocurrir en las crisis. Mientras tanto, las Fuerzas Armadas deben continuar el desarrollo de capacidades para operar en el ciberespacio según las políticas actuales.

La defensa en profundidad —las capas interiores. El lograr la resiliencia requiere una evaluación de dependencias y vulnerabilidades en todos los niveles. Comenzando dentro de la pared de protección y avanzando hacia fuera, la defensiva comienza en el nivel de unidad más inferior. Las organizaciones y funciones deben ser suficientemente resistentes para aguantar los ataques y continuar sus operaciones. En una era de presupuestos decrecientes, los elementos decisorios buscarán eficiencias a través del uso de la tecnología.[34] Por lo tanto, la prudencia requiere la reinversión de una parte de los ahorros para

El secretario del Ejército de EUA, John McHugh, recibe una presentación de actualización por parte de los integrantes del Comando Cibernético del Ejército de EUA en el Fuerte Belvoir, estado de Virginia, 2 de abril de 2012.
(Ejército de EUA)

evaluar y disminuir las vulnerabilidades creadas por las nuevas dependencias tecnológicas.[35] Los futuros juegos de guerra no solo deberán evaluar lo que pueden proporcionar las nuevas tecnologías, sino también deberán considerar cómo serían afectadas todas las capacidades si se negara el acceso al ciberespacio.

Más allá de las responsabilidades de los usuarios básicos, las fuerzas que proporcionan medidas defensivas contra los ciberataques requieren organizaciones y estructuras de comando según su función. Martin van Creveld delineó las evoluciones históricas de mando y avances tecnológicos. Conforme con su análisis, los líderes de defensa cibernética militar deben resistir el afán, habilitado por la tecnología, de centralizar y dominar toda la información disponible en el nivel más alto. En cambio, sus organizaciones deben actuar de manera semi-independiente, establecer bajos umbrales de decisión y reportaje de información regular, así como usar las comunicaciones formales e informales.[36] Estos métodos pueden mejorar el "constante aprendizaje mediante ensayo y error que es esencial para dar sentido a las sorpresas discapacitantes" y reducir los tiempos de reacción.[37] Las estructuras de redes pueden ser más adecuadas en este tipo de tarea que las estructuras militares jerárquicas tradicionales.[38] Cualquiera que sea la estructura, los líderes militares deben estar dispuestos a subordinar la tradición y organizar sus medidas defensivas según las tareas para lograr la eficacia contra los ciberataques.[39] A fin de cuentas, las armas "no triunfan en el combate; más bien, el éxito es producto de los sistemas de armamentos-hombres, sus servicios

de apoyo de todo tipo y la organización, doctrina y entrenamiento que los lanzan al combate".[40]

La defensa en profundidad —las capas exteriores. Se necesitan más que paredes de protección para defenderse contra los ciberataques. Una extensión de la defensa en profundidad requiere el uso creativo de influencia. El Departamento de Defensa no ejerce posesión o jurisdicción sobre los sectores civiles que operan la infraestructura de Internet o que desarrollan el *hardware* y *software*. Sin embargo, los sistemas del DoD son vulnerables a los ciberataques por medio de todos los caminos fuera de su control.[41] Richard Clarke recomendó la regulación federal comenzando con la red central de Internet como la mejor forma de superar las vulnerabilidades sistémicas.[42] Una reacción violenta contra la posible legislación para regular la actividad en Internet ilustra el carácter problemático de la regulación.[43] Por lo tanto, ¿cómo puede el DoD hacer cambios aparentemente fuera de su control? Se puede denominar el "poder blando" o "la conquista amistosa del ciberespacio", sin embargo, la respuesta yace en hacer uso de sus recursos.[44]

Uno de los recursos más importantes que el DoD puede usar es su poder adquisitivo. En 2011, el DoD gastó más de US$ 375 billones en contratos.[45] Sin lugar a dudas, las Fuerzas Armadas deben aprovechar su poder adquisitivo para destacar los rigurosos estándares de seguridad cuando compran *hardware* y *software*. Sin embargo, también pueden usar su proceso de adquisición para reducir las vulnerabilidades a través del uso de contratistas de defensa. Similares a

Oficiales de enlace en el Centro Conjunto de Control Cibernético durante la Operación *Deuce Lightning* reciben una presentación de atualización sobre la Lista de Sincronización de Tareas de la misión, Grafenwoehr, Alemania, 23 de febrero de 2011.
(Exército dos EUA, Lawrence Torres III)

los requerimientos de clasificación detallados, los contratos deben especificar los protocolos de seguridad en la red para toda empresa contratista así como sus suministradores, independientemente de los servicios proporcionados. El mantener protocolos de seguridad más rigurosos que las normas industriales llegaría a ser una condición de los contratos lucrativos. A través de sus contratos, aliados y posición como la fuente de empleo más grande de la Nación, el DoD puede afectar las preferencias para mejorar las defensas de la capa exterior.[46]

Desarrollar una defensa ofensiva. Aún en la guerra defensiva, Clausewitz reconoció la necesidad de la ofensiva para responder al fuego enemigo y lograr la victoria.[47] Las capacidades ofensivas robustas pueden mejorar la disuasión, lo cual afecta el cálculo de decisiones del adversario.[48] El DoD debe prepararse para las contingencias que exigen el apoyo ofensivo en otros dominios o la acción independiente a través del ciberespacio.

Las fuerzas armadas deben desarrollar capacidades ofensivas para posibles escenarios pero deben definir resueltamente sus preparaciones como medidas defensivas. Es importante comunicar una postura defensiva para evitar acelerar una carrera armamentista cibernética inspirada por un dilema de seguridad que posiblemente ya haya comenzado.[49] Según se informa, más de 20 naciones cuentan con alguna capacidad de ciberguerra.[50] Aunque sea demasiado tarde para frenar el desarrollo ofensivo de otros, sigue siendo importante controlar la narrativa.[51] De la misma manera que el nombre de Departamento de Defensa implica un mensaje distinto que su antiguo nombre de Departamento de Guerra —es decir, desarrollar las capacidades defensivas para bloquear las acciones de los atacantes cibernéticos autónomos parece significativamente mejor que desarrollar capacidades ofensivas que derrotan [al enemigo] en la primera ronda".[52]

No prevea cambios rápidos en el orden internacional o la naturaleza de la guerra. Sin duda alguna, el mundo está cambiando, pero el orden mundial no cambia de la noche a la mañana. Nye describió los cambios que han ocurrido debido a la globalización y la propagación de tecnologías de información, incluyendo la difusión del poder estadounidense a naciones en vías de desarrollo y actores no estatales. Sin embargo, sostuvo que esto no era una "narrativa de decadencia" y escribió, "Es poco probable que Estados Unidos decaiga como la Antigua Roma, o incluso, sea superado por otro estado".[53] Los Estados Unidos necesita adaptarse a las tendencias actuales, pero los cambios en el dominio estratégico no son tan radicales como sostienen algunos.

Similarmente, algunos aspectos de la guerra se adaptan a los tiempos mientras su carácter sigue constante. Clausewitz sugirió que la planificación debe tener en cuenta el carácter contemporáneo de la guerra.[54] Los avances en el ciberespacio cambian el carácter de la guerra, pero no completamente eclipsan los medios tradicionales. Sir John Slessor observó, "No hay una actitud más peligrosa que presumir el hecho de que una futura guerra será igual a la última guerra, y no podemos darnos el lujo de ignorar todas las lecciones de la última".[55] Además, Lonsdale sugirió aprovechar los avances en el ciberespacio, pero no "prever que estos cambios alteren la naturaleza de la guerra".[56] Las guerras continuarán siendo gobernadas por la política, influidas al azar y llevadas a cabo por personas, aunque sea por medio del ciberespacio.[57]

Esto no es muy prometedor. Los defensores del uso del ciberpoder deben refrenar suficientemente su entusiasmo para ver que su uso solo existe en el contexto estratégico. Colin Gray alegó que los entusiastas del poder aéreo "casi invitaron al gobierno y al público a plantear las preguntas incorrectas y tener una super-heroica consideración de la eficacia en el rendimiento de la Fuerza Aérea con estándares irrelevantes".[58] Al promocionar las capacidades decisivas, independientes y estratégicas, los defensores del poder aéreo frecuentemente no lograron tales expectativas exageradas en conflictos reales. Los contextos estratégicos hubieran ocurrido donde el poder aéreo, por sí solo, hubiera podido lograr los efectos estratégicos, pero con mucha frecuencia, el poder aéreo fué una de las muchas herramientas usadas.

Así es el ciberpoder. Gary alegó, "Si se analiza y debate una nueva forma de guerra, puede ser difícil convencer a los profetas que la posible eficacia no necesita ser conclusiva".[59] Los defensores del ciberpoder deben darse cuenta no solo de sus ventajas, sino también de sus limitaciones en el contexto estratégico.

Conclusión

Si el ciberpoder es la posibilidad de usar el ciberespacio para lograr resultados deseados, en consecuencia, el contexto estratégico es clave en la comprensión de su uso. A medida que cambia el carácter de la guerra y del ciberespacio, el combate se une lado a lado con otros dominios y los líderes militares deben tomar decisiones sensatas sobre lo que pueden aportar para lograr los resultados deseados. Los encargados de tomar decisiones deben sopesar las oportunidades y ventajas que presenta el ciberespacio contra las vulnerabilidades y limitaciones de las operaciones de dicho dominio. Sir Arthur Tedder restó importancia al debate sobre un arma u otra al ganar guerras por sí sola. Insistió que, "Las tres armas de defensa están inevitablemente involucradas, aunque el equilibrio correcto entre las mismas variaría".[60] Las guerras de hoy en día pueden implicar más armas, pero el concepto de Tedder de emplear una combinación de herramientas basadas en sus ventajas y limitaciones en el contexto estratégico sigue siendo un buen consejo.

Referencias Bibliográficas

1. Véase Harlan, Chico, "Korean DMZ troops exchange gunfire," *Washington Post*, 30 de octubre de 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/10/29/AR2010102906427.html. De vez en cuando, se lanzan balas a través de la zona desmilitarizada, pero las ocurrencias son poco comunes.

2. Véase *Authorization for Use of Military Force*, Public Law 107-40, 107° Congreso, 18 de septiembre de 2001, http://www.gpo.gov/fdsys/pkg/PLAW-107publ40/html/PLAW-107publ40.htm. El uso de fuerza militar en Afganistán era autorizado por el Congreso de EUA en 2001 a través de la Ley Pública 107-50, que no incluye una declaración de guerra.

3. "Usuarios no autorizados prueban a los sistemas del DOD aproximadamente 250.000 veces por hora, y más de 6 millones de veces por día." El general Keith Alexander, Director de la Agencia Nacional de Seguridad y Comandante del Comando Cibernético (comentarios presentados en el *Center for Strategic and International Studies Cybersecurity Policy Debate Series: US Cybersecurity Policy and the Role of US Cybercom*, Washington, DC, 3 de junio de 2010, 5), http://www.nsa.gov/public_info/_files/speeches_testimonies/100603_alexander_transcript.pdf.

4. "El propósito de este documento es proporcionar los medios y recursos necesarios con los cuales nuestras Fuerzas Armadas promoverán nuestros intereses nacionales duraderos... y lograrán los objetivos de defensa nacional en la *2010 Quadrennial Defense Review*". Junta de Jefes del Estado Mayor Conjunto, *The National Military Strategy of the United States of America, 2011: Redefining America's Military Leadership* (Washington, DC: United States Government Printing Office [GPO], 8 de febrero de 2011), i.

5. El Departamento de Defensa (DoD), *DOD Strategy for Operating in Cyberspace* (Washington, DC: GPO, julio de 2011), p. 5.

6. Kuehl, Daniel T., "From Cyberspace to Cyberpower: Defining the Problem," en *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr y Larry K. Wentz (Dulles, Virginia: Potomac Books, 2009): págs. 26-28.Defining the Problem," en *Cyberpower and National Security*, editores Franklin D. Kramer, Stuart H. Starr y Larry K. Wentz (Dulles, VA: Potomac Books, 2009): 26-28.

7. Staff Report to the Senate Committee on Armed Services, *Defense Organization: The Need for Change*, 99° Congreso, 1ª sesión, 1985, Committee Print, págs. 442-44.

8. Lonsdale, David J., *The Nature of War in the Information Age: Clausewitzian Future* (Londres: Frank Cass, 2004), p. 182.

9. Véase Nye, hijo, Joseph S., *The Future of Power* (Nueva York: PublicAffairs, 2011), p. 123. Esta definición es influenciada por el trabajo de Nye.

10. "Desde 2000 hasta 2010, el uso global de Internet incrementó de 360 millones a más de 2 billones de personas", *DOD Strategy for Operating in Cyberspace*, p. 1.

11. Douhet, Giulio, *The Command of the Air* (Tuscaloosa, Alabama: University of Alabama Press, 2009), p. 9.

12. Clarke, Richard A. y Knake, Robert K., *Cyber War: The Next Threat to National Security and What To Do About It* (Nueva York: HarperCollins Publisher, 2010), págs. 9-10.

13. Nye, p. 126.

14. Cronin, Audrey Kurth, "Cyber-Mobilization: The New *Levée en Masse*", *Parameters* (verano de 2006): págs. 77-87.

15. Clarke y Knake, págs. 81-84.

16. Véase Clarke y Knake, págs. 84-85. Las tendencias en el número de dispositivos conectados a Internet amenazan agotar todos los 4,29 billones de direcciones disponibles basadas en el sistema de numeración original de 32-bit.

17. Wilson, Clay, "Cyber Crime," en *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, Larry Wentz (Washington, DC: NDU Press, 2009), p. 428.

18. Carl von Clausewitz, *On War*, editores y traductores Michael Howard y Peter Paret (Princeton, Nueva Jersey: Princeton University Press, 1976), p. 357; Sheldon, John B., "Deciphering Cyberpower: Strategic Purpose in Peace and War," *Strategic Studies Quarterly* (Verano de 2011): p. 98.

19. Van Creveld, Martin, *Command in War* (Cambridge, Massachusetts: Harvard University Press, 1985), p. 231.

20. Nye, p. 30.

21. Filkins, Dexter, "US Tightens Airstrike Policy in Afghanistan," *New York Times*, 21 de junio de 2009, http://www.nytimes.com/2009/06/22/world/asia/22airstrikes.html.

22. "Mejoraremos nuestras capacidades de ciberespacio para que estas puedan frecuentemente lograr efectos significativos y conmensurados de una

manera más económica y un menor impacto de daños colaterales." Presidente del Estado Mayor Conjunto, *The National Military Strategy of the United States of America 2011: Redefining America's Military Leadership*, (Washington, DC: GPO, 2011), p. 19.

23. Schelling, Thomas C., *Arms and Influence* (New Haven, Connecticut: Yale University, 2008), págs. 2-4.

24. Véase Clarke y Knake, p. 93 para el oleoducto ruso; véase Nye, p. 127, para Stuxnet.

25. Lonsdale, págs. 143-45.

26. Contraalmirante Wylie, J.C., *Military Strategy: A General Theory of Power Control* (Annapolis, Maryland: Naval Institute Press, 1989), p. 74.

27. Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (Nueva York: PublicAffairs, 2011), p. 19.

28. Nye, p. 147.

29. Kugler, Richard L., "Deterrence of Cyber Attacks," *Cyberpower and National Security*, editores Franklin D. Kramer, Stuart H. Starr y Larry K. Wentz (Washington, DC: NDU Press, 2009), p. 320.

30. Véase United States Office of the President, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, mayo de 2011.

31. Véase Clarke y Knake, p. 155. La estrategia internacional para el ciberespacio aborda la diplomacia, defensa y desarrollo en el ciberespacio pero no delinea las prioridades relativas con intereses de política contrapuestos.

32. Los derechos de libre expresión y sus límites han sido un asunto contencioso por décadas. "Gritar ´ 'fuego' en un teatro lleno de gente" proviene de un caso en la Corte Suprema de EUA de 1919, Schenck v. Estados Unidos. El juez de la Corte Suprema Oliver Wendell Holmes estableció el contexto como relevante para limitar la libre expresión. En 1969 una prueba de "inminente acción ilegal" reemplazó su prueba de "peligro claro y presente", http://www.pbs.org/wnet/supremecourt/capitalism/landmark_schenck.html.

33. Morozov, p. 28.

34. "Las capacidades de tecnología de información de hoy en día han hecho posible esta visión [de la logística de precisión] y la demanda en el futuro por la eficiencia ha hecho urgente la necesidad". El general Norton Schwartz, Jefe de Estado Mayor de la Fuerza Aérea de Estados Unidos, "Toward More Efficient Military Logistics," discurso, 29 de marzo de 2011, ante la *27th Annual Logistics Conference and Exhibition*, Miami, Florida, http://www.af.mil/shared/media/document/AFD-110330-053.pdf .

35. Demchak, Chris C., *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens, Georgia: University of Georgia Press, 2011), p. 44.

36. Van Creveld, págs. 269-70.

37. Demchak, p. 73.

38. Bousquet, Antoine, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity* (Nueva York: Columbia University Press, 2009), págs. 228-29.

39. Véase Ratcliff, R.A., *Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers* (Cambridge, UK: Cambridge University Press, 2006), págs. 229-30. El criptoanálisis aliado del sistema Enigma en la Segunda Guerra Mundial ofrece un ejemplo exitoso de la organización de tarea creativa sin la jerarquía rígida.

40. Gray, Colin S., *Explorations in Strategy* (Westport, Connecticut: Praeger, 1996), p. 133.

41. *DOD Strategy for Operating in Cyberspace*, p. 8.

42. Clarke y Knake, p. 160.

43. Fowler, Geoffrey A., "Wikipedia, Google Go Black to Protest SOPA," *Wall Street Journal*, 18 de enero de 2012, http://online.wsj.com/article/SB10001424052970204555904577167873208040252.html?mod=WSJ_Tech_LEADTop; *Associated Press*, "White House objects to legislation that would undermine 'dynamic' Internet," *Washington Post*, 14 de enero de 2012, http://www.washingtonpost.com/politics/courts-law/white-house-objects-to-legislation-that-would-undermine-dynamicinternet/2012/01/14/gIQAJsFcyP_story.html.

44. "Poder blando", véase Nye, págs. 81-82; "conquista amistosa", véase Libicki, Martin C., *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge, Reino Unido: Cambridge University Press, 2007), p. 166.

45. Gobierno de EUA, sitio web oficial USASpending.gov, "Prime Award Spending Data," http://www.usaspending.gov/explore?carryfilters=on (18 de enero de 2012). "2011" refiere al año fiscal.

46. Sitio web del Departamento de Defensa, "About the Department of Defense," http://www.defense.gov/about (18 de enero de 2012). El DoD emplea 1,4 millones de personas de servicio activo, 1,1 millones de personas en la Guardia Nacional/Componente de Reserva y 718.000 civiles.

47. Clausewitz, p. 357.

48. Kugler, "Deterrence of Cyber Attacks," p. 335.

49. "Muchos observadores plantean que múltiples actores desarrollan capacidades expertas de ataque [cibernético]. *Ibíd*., p. 337.

50. Clarke y Knake, p. 144.

51. Las "narrativas son especialmente importantes para establecer el marco conceptual de los asuntos de manera convincente.". Nye, págs. 93-94.

52. Cita del general Robert Elder en calidad de comandante del Comando Cibernético de la Fuerza Aérea. Véase Clarke y Knake, p. 158; *Defense Tech*, "Chinese Cyberwar Alert!" 15 de junio de 2007, http://defensetech.org/2007/06/15/chinese-cyberwar-alert.

53. Nye, p. 234.

54. Clausewitz, p. 220.

55. Slessor, John Cotesworth, *Air Power and Armies* (Tuscaloosa, Alabama: University of Alabama Press, 2009), p. iv.

56. Lonsdale, p. 232.

57. Clausewitz, p. 89.

58. Gray, p. 58.

59. Gray, Colin S., *Modern Strategy* (Oxford, Reino Unido: Oxford University Press, 1999), p. 270.

60. Tedder, Arthur W., *Air Power in War*, (Tuscaloosa, Alabama: University of Alabama Press, 2010), p. 88.