¿Atacar o Defender? Manejando la información y equilibrando los riesgos en el ciberespacio

Coronel (jubilado) Dennis M. Murphy, Ejército de EUA

Cuando originalmente se escribió este artículo, la política del Departamento de Defensa (DOD) y los reglamentos militares restringieron el uso de Internet para fines de comunicación estratégica en pro de la seguridad. El 25 de febrero de 2010, el DOD publicó una política que adopta un enfoque equilibrado en este sentido, apoyando, de esta manera, la tesis original de este artículo. El autor ha actualizado el artículo, apropiadamente, para proveer una explicación más profunda sobre la decisión de emitir una política y para promover la adopción de sus principios.

LA HISTORIA DE Estados Unidos está repleta de ejemplos acerca de cómo prepararse para la siguiente guerra mediante el estudio de la última (o actual) guerra. Por consiguiente, a menudo nos involucramos en la guerra con doctrinas y procesos que se quedan rezagados en relación con la realidad actual. El resultado puede ser iniciativas de guerra prolongadas a un gran costo para el tesoro nacional, en término tanto fiscal como humano. El acosado desarrollo e implementación de la doctrina de contrainsurgencia, que dio lugar a la llamada "oleada" en medio de la campaña en Irak, es apenas uno de los muchos ejemplos.[1]

Sin embargo, la consideración introspectiva de guerras futuras a finales de los años 70 y principios de los años 80, es una excepción. Al usar la guerra árabe-israelí de 1973 como un presagio de guerra en que las armas de precisión y los adelantos tecnológicos ponen de manifiesto la importancia de maniobra, el Ejército pasó de una doctrina de "Defensa Activa" a "Combate Aeroterrestre". No obstante, esta doctrina no fue universalmente aceptada. En un ensayo *Landpower*, el General de Brigada Huba Wass de Czege recordó:

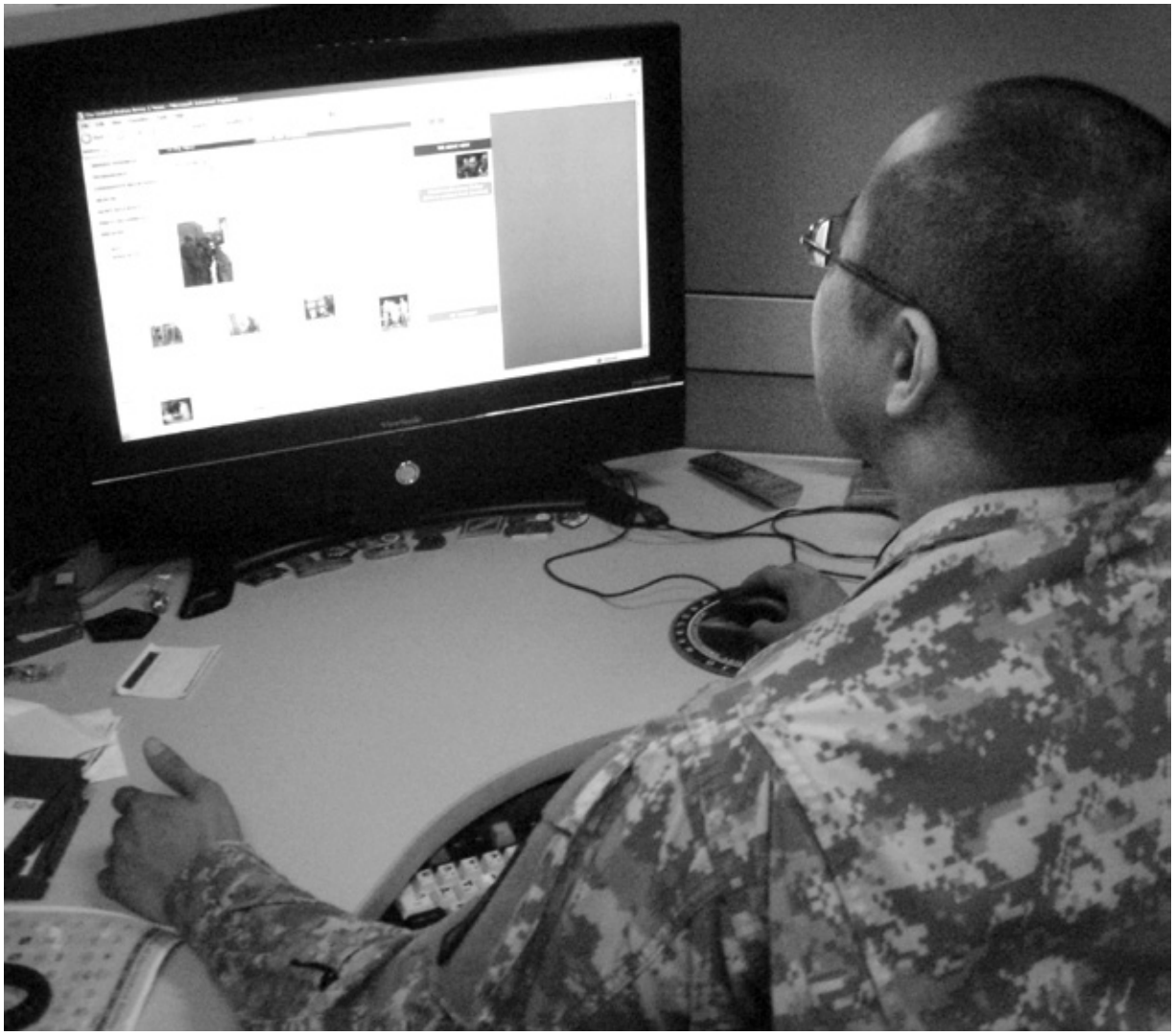
> Lo que se transformó en un intercambio sano, los *oficiales jóvenes* vieron las tácticas defensivas como un enfoque de "operaciones de retroceso realizadas en filas" que confundió, demoró y condujo a que los comandantes evitaran un enfrentamiento decisivo… Lo consideraron como reactivo, claudicando la iniciativa y dando como resultado un método arriesgado de defensa.[2]

La historia oficial de la Guerra del Golfo de 1991, describe el cambio a la doctrina de Combate Aeroterrestre como una decisión visionaria que fue la base de esa dramática victoria para los militares estadounidenses.[3]

Entonces, ¿cómo será la siguiente guerra? Nadie tiene una bola de cristal infalible para prever el futuro, sin embargo, una consideración superficial de futuros adversarios revela la importancia que tiene la información como un medio estratégico asimétrico para conducir la guerra. Según se informa, el ejército chino ha pirateado las redes militares del Pentágono. El gobierno ruso supuestamente ha llevado a cabo un ataque cibernético importante en la infraestructura estoniana.[5] No obstante, mientras los ataques a los sistemas de información están demostrando ser una amenaza, la dependencia de Internet para pelear contra la "guerra de ideas" va en aumento. Considere la llamada "segunda guerra del Líbano" entre Israel y Hezbolá en el verano de 2006. El Hezbolá utilizó la información para incidir en las opiniones como un medio de alcanzar la victoria estratégica, hasta

---

El Coronel (jubilado) Dennis M. Murphy, Ejército de EAU es el director de información del Grupo de Conducción de la Guerra en la Escuela Superior de Guerra del Ejército de EUA. El profesor Murphy imparte cursos electivos sobre operaciones de información y comunicación estratégica, y lleva a cabo talleres centrados en los elementos de información del poder nacional.



Ejército de EUA, David Vergun

Un soldado entra al ciberespacio.

el punto de colocar vallas publicitarias sobre los escombros de edificios en el sur de Líbano que decían "Hecho en EUA" (en inglés).[6]

Por supuesto que los militares estadounidenses reconocen esta amenaza, como lo demuestra la iniciativa de establecer un Comando Cibernético de EUA (*U.S. Cyber Command*). Sin embargo, hasta hace poco, la doctrina estaba rezagada. Las políticas anteriores favorecieron la "defensa activa" más que la "maniobra" en el ciberespacio. Y, si bien, un reciente cambio en la política apunta hacia un cambio potencialmente significativo en esa ecuación, surge la pregunta de si los militares adoptarán el cambio organizacional necesario para equilibrar la necesidad de proteger las redes mientras se encaminan hacia la ofensiva ideológica que han adoptado sus adversarios.

Al final de cuentas, los líderes deben sopesar los riesgos involucrados para lograr un equilibrio a fin de competir en el espacio de combate de información. ¿Elaborarán un "Combate Aeroterrestre" equivalente al ciberespacio, o esperarán hasta la siguiente guerra para conseguir un equilibrio a un coste potencialmente alto para nuestra Nación?

Cómo definir el problema

El mantenerse actualizado en lo que respecta a la definición del ciberespacio puede ser un trabajo a tiempo completo. Desde 2004, el gobierno de EUA ha presentado cuatro definiciones "oficiales" distintas. Actualmente, el Departamento de Defensa (DOD) define el ciberespacio de la siguiente manera:

> Un dominio global dentro del ambiente de información que consiste en una red interdependiente de infraestructura tecnológica de información, incluyendo a Internet, las redes de telecomunicaciones, los sistemas de informática y los procesadores y controladores integrados.[7]

Tal vez lo más importante del poder cibernético es, "la capacidad de utilizar el ciberespacio para crear ventajas e influenciar los eventos en todos los entornos operativos y a través de los instrumentos de poder".[8] Por lo tanto, de esa misma manera el poder terrestre, marítimo y aéreo, y el poder cibernético constituye un arma de guerra.

La definición que, acertadamente, le da el DOD al ciberespacio reconoce la importancia de Internet como un mecanismo de apoyo de ese dominio en el actual ambiente de información. La *World Wide Web* (red mundial de computadores), como un subconjunto de Internet está, fundamentalmente sin gobierno, proporcionando obvias libertades y riesgos. La *web* le proporciona al individuo una voz, a menudo, anónima y un público potencialmente vasto. Se puede fácilmente establecer, desmantelar y restablecer un sitio *web*. Este atributo lo hace valioso para los movimientos extremistas. Por otro lado, la misma capacidad que la *web* les confiere a nuestros adversarios nos la brinda a nosotros, si escogemos adoptarla. "La Estrategia Nacional para la Lucha Contra el Terrorismo" (The National Strategy for Combating Terrorism) observa que Internet les proporciona a los terroristas refugios cibernéticos seguros para "comunicar, reclutar, adiestrar, conseguir apoyo, persuadir y diseminar sus propaganda sin correr riesgo de contacto personal". Además, destaca la oportunidad que Internet ofrece para desacreditar esa misma propaganda.[9]

El efecto que surten las tecnologías de Internet en la Seguridad Nacional y de combate no sólo incrementará en el futuro, sino que lo hará de forma exponencial.[10] Considere a Internet como un medio significativo de conducir la "guerra de ideas". Los blogs, el *You Tube*, *Google Earth* y *Second Life* constituyen todos "nuevos medios sociales" —que les proveen tecnologías a nuestros adversarios para ganar ventaja asimétrica afectando las opiniones, actitudes, comportamientos y, en última instancia, creencias. Los sitios de medios sociales como *Facebook* y *Twitter* han ganado recientemente gran popularidad y han sido utilizados con fines que van mucho más allá de la interacción social que sugiere dicho medio. El *iPhone* puede parecer un teléfono, sin embargo, cuenta con todas las capacidades de una computadora de escritorio (y a veces más) en un dispositivo del tamaño de la palma de la mano.

No cabe duda de que la tecnología continuará haciéndose más rápida, más económica y más capaz. En este contexto, los nuevos medios rápidamente se convierten en medios "obsoletos". Y por lo tanto, una definición más atemporal considera a los nuevos medios como toda capacidad que le permita a una amplia variedad de actores (individuos a través de los estados-naciones) crear y difundir información en tiempo real o casi en tiempo real que puede afectar a un gran público (regional o mundial). Si bien previamente era una exclusividad al alcance de las naciones-estados y grandes corporaciones multinacionales, ahora los individuos pueden manejar información como un medio estratégico, una tendencia de importancia para los responsables de la toma de decisiones y los combatientes.

Los futuros desafíos de combate deben tomar en cuenta el uso casi seguro de Internet por parte de cualquier adversario futuro. Los analistas no deberían ganar una falsa sensación de seguridad basada en la penetración limitada de Internet en algunos de los lugares más contenciosos del mundo. Si bien África cuenta con sólo 6,8 por ciento de penetración de Internet basado en su población, el uso de Internet ha incrementado de 1.392% desde el 2000 hasta el 2009. En Asia, Oriente Medio y Latinoamérica se están dando dramáticas tasas de crecimiento similares.[11]

Los combatientes se dan cuenta de la necesidad de competir en el ciberespacio.

Los combatientes se dan cuenta de la necesidad de competir en el ciberespacio. Cada vez más, los líderes de alto grado y las unidades patrocinan las páginas de *Facebook* y envian "*tweets*" de manera rutinaria. El Comando Central de EUA se

interrelaciona con voces disidentes que participan en los blogs los cuales critican la guerra contra el terrorismo, señalando que "con la proliferación de información de hoy, si no se habla en estos foros, tampoco se le escuchará".[12] Los militares estadounidenses también se dan cuenta de la importancia de competir con el medio de video, usando *YouTube* para mostrar imágenes reales de las operaciones estadounidenses en los actuales teatros de guerra.[13]

Por otro lado, los militares estadounidenses dependen significativamente de Internet para llevar a cabo sus labores rutinarias y la comunicación crea una vulnerabilidad para el ataque cibernético. Sobran personas y organizaciones que ponen a prueba las redes estadounidenses. Si bien Estados Unidos repele estos ataques, los fracasos dejan entrever su impacto. El Ejército de Liberación Popular de China atacó a las computadoras del Pentágono en junio de 2007 aparentemente después de numerosos intentos y ocasionaron que deshabilitaran la red por más de una semana.[14] Los chinos se están transformando de una fuerza mecanizada a una "*informatizada*" y han declarado su intención de usar la guerra de información "como una herramienta de guerra o como una manera de lograr la victoria sin guerra".[15] El General jubilado Barry McCaffrey señala que esto no es una anomalía, sino que, de hecho, podría ser la norma. Además destaca que todo nuestros adversarios futuros, así como elementos facinerosos, llevan a cabo operaciones de reconocimiento de nuestro espectro electrónico en zonas críticas para la seguridad nacional de Estados Unidos.[16] De hecho, como promedio, los sistemas informáticos del gobierno de EUA son objetos de ataque cada 8 segundos.[17]

El caso de Estonia puede ser un precursor de lo que Estados Unidos puede esperar a medida que aumenta la dependencia de Internet en el gobierno y los militares. Estonia utiliza algunos de los más avanzados procesos gubernamentales electrónicos en el mundo. Los estonios realizan sus transacciones bancarias, sufragan y pagan impuestos en línea, y han enclavado sus tarjetas de identificación nacional con chips electrónicos, que son muy eficientes y, como se puede constatar, muy vulnerables. Por lo tanto, fue de gran importancia

Fort Leavenworth Lamp, Prudence Siebert

Estudiantes de la Escuela de Comando y Estado Mayor, Mayores Gary Belcher, Dexter Brookins y Troy Newman trabajan en el puesto de mando principal de la división durante el Ejercicio Guerrero Digital, Fuerte Leavenworth, Kansas, 14 de febrero de 2008.

cuando los piratas de computadora rusos atacaron en la primavera de 2007.[18] De hecho, algunos observadores consideraron ese ataque cibernético equivalente a un acto de guerra en el sentido Clausewitziano, con la intención de crear un pánico social generalizado.[19]

De ahí que, no debe sorprender que la protección de la red haya adquirido gran importancia en el Departamento de Defensa y es cada vez más importante usar la misma red para tomar medidas preventivas, comunicando mensajes positivos sobre EUA. Un cambio reciente de la política del Departamento de Defensa en lo que respecta a la información ha brindado la oportunidad de usar la Internet para contrarrestar la desinformación y para contar la historia de las fuerzas militares estadounidenses. Sin embargo, sólo el tiempo dirá si la cultura organizacional adoptará tal enfoque.

Defensa: cómo proteger la red

Se han emprendido grandes iniciativas y recursos para proteger los sistemas vinculados a Internet del Departamento de Defensa y otras organizaciones gubernamentales. El Departamento de Seguridad Nacional estableció un Centro Nacional de Seguridad Cibernética (*National Cybersecurity Center*), cuya misión es la de coordinar e integrar las informaciones necesarias para ayudar a proteger las redes y sistemas cibernéticos de EUA y promover la cooperación entre grupos cibernéticos federales"[20] El Departamento de Defensa codificó el proceso para proteger sus redes en un concepto llamado garantía de información. La garantía de información incluye lo siguiente:

> Medidas que protegen y defienden la información y los sistemas de información garantizando su disponibilidad, integridad, autenticación, confidencialidad y aceptación. Esto incluye proporcionar el restablecimiento de sistemas de información mediante la incorporación de capacidades de protección, detección y reacción…La garantía de información requiere un *enfoque de defensa en profundidad* [énfasis agregado por el autor].[21]

El Departamento de Defensa realiza operaciones computacionales sin clasificar dentro de un subconjunto de Internet conocido como *NIPRnet* (originalmente la red enrutadora de protocolo de Internet no clasificada). La *NIPRnet* aísla el acceso más amplio a Internet mediante el uso de un limitado número de portales y compuertas. Esta metodología hace la requerida "defensa en profundidad" fácil de manejar desde una perspectiva de recursos que reduce el número de rutas que vigilar en caso de ataques. La misma permite el acceso a Internet y facilita actividades eficientes de mando y control.[22] Sin embargo, los *firewalls* (sistema diseñado para prevenir el acceso ilegal a/o desde una red privada conectada a Internet) y filtros de contenido que bloquean el acceso a sitios externos específicos, a menudo, limitan el acceso a la *World Wide Web* (Sistema global de hipertexto que utiliza Internet como su mecanismo de transporte), a fin de fomentar la productividad en el trabajo, apoyar los requisitos de anchura de banda, proteger las operaciones de seguridad e impedir intrusiones y riesgos. No hace mucho, parecía que ese acceso externo sería aún más restrictivo. En julio de 2008, el Secretario adjunto de Defensa Gordon England solicitó al Congreso fondos para construir, por falta de mejor término, un "DODnet". Los recientes ataques de China a las redes y sistemas del Departamento de Defensa hicieron aún más urgente desarrollar sistemas cibernéticos impenetrables.[23] La tendencia era de aumentar la seguridad por medio del bloqueo del sistema, un enfoque que era incompatible con el de ganar la guerra de ideas.

Atacar: cómo difundir el mensaje

Los jefes militares enfatizan cada vez más la importancia de la "comunicación estratégica" para competir en el ambiente de información. El Departamento de Defensa define la comunicación estratégica como sigue:

> Procesos e iniciativas centrados en el gobierno estadounidense para comprender y atraer al público clave a fin de crear, fortalecer o, preservar las condiciones favorables para promover los intereses y objetivos nacionales a través del uso de información, temas, planes, programas y medidas coordinadas y sincronizadas con otros elementos del poder nacional.[24]

Por consiguiente, la comunicación estratégica es la integración de acciones, imágenes y palabras

para difundir un mensaje a fin de influenciar las opiniones, actitudes y comportamientos.[25] Las acciones transmiten un mensaje más fuerte, pero las imágenes y las palabras proveen contexto, y a menudo, tienen efectos significativos por sí solas. Si bien la comunicación estratégica se centra en la dimensión cognitiva del ambiente de información, depende del ambiente físico para difundir sus mensajes. A menudo, eso requiere el acceso fácil y rápido a Internet.

Cada vez más, los líderes señalan la importancia de usar nuevos medios e Internet para combatir de forma proactiva en el ciberespacio. Sin embargo, las pasadas evidencias empíricas revelan un conflicto entre defender las redes y usarlas para difundir activamente un mensaje. Las operaciones de EUA en Irak exhibidas en *YouTube* estuvieron entre los 10 videos más vistos por varias semanas después de su publicación, sin embargo, el Ejército las publicó sólo después de que los Generales de mayor antigüedad superaran considerables obstáculos burocráticos.[26] Las consideraciones de anchura de banda pudieron haber sido un motivo. Los blogs se han convertido rápidamente en el medio preferido no sólo para actividades recreativas sino para actividades militares y políticas más serias. Los blogs proveen un foro para contar la historia militar, a menudo por medio de fuentes con mayor credibilidad — por los mismos soldados, marineros, aerotécnicos e infantes— pero, a menudo, la aversión al riesgo impide la iniciativa. Las políticas militares pasadas en Irak han sido restrictivas y a menudo desalentaron los blogs en lugar de fomentarlos.[27] En mayo de 2008, los jefes del Teniente Matthew Gallagher eliminaron su blog "Kaboom" luego de que volviera a contar una conversación entre él y su comandante, sin mencionar nombres, no obstante, sin solicitar previa autorización. Antes de la eliminación de ese blog, el sitio recibió decenas de millares de visitas.[28] *MySpace* y *Facebook* reciben amplia cobertura de los medios acerca de su transparencia y el efecto perjudicial que tienen las revelaciones personales en las manos equivocadas. Por otro lado, desde un punto de vista militar, estos sitios de redes sociales proporcionan una oportunidad para contar una historia confiable y contextualizada de la vida en las barracas. Sin embargo, tanto los blogs como los medios sociales encaran problemas en cuanto a la seguridad operativa, por lo que los comandantes justamente se preocupan de mantener la confidencialidad de las operaciones, capacidades y vulnerabilidades militares.

Muchos líderes militares de mayor antigüedad reconocen la importancia de estas nuevas herramientas de medios como capacidades militares contemporáneas y fomentan la participación y el diálogo que ellos facilitan. Los ejemplos recientes apuntan hacia un clima de aversión al riesgo en los altos niveles que a su vez, perjudica el aprovechamiento del potencial de la red.[29] Por ejemplo, en marzo de 2008, el Centro de Armas Combinadas (CAC) del Ejército en el Fuerte Leavenworth, Kansas, presentó un memorando en el que solicitaba una "excepción de la política" a fin de permitir que sus oficiales participen en el blog del dominio público.[30] Cabe mencionar que el CAC es liderado por un General de tres estrellas. Además, el CAC es responsable de adiestrar y capacitar a los líderes del Ejército en el uso de este recurso.

El Departamento de Defensa también ha limitado el campo de autoridad para realizar actividades interactivas en Internet a nivel de General de cuatro estrellas y sólo permite a los funcionarios de asuntos públicos participar en actividades interactivas de Internet con periodistas.[31] Esta política no sólo compete a la *NIPRnet* sino que también limita el uso doméstico de Internet.

Sin embargo, lo que pareció ser un avance significativo se dio en febrero de 2010 con la publicación de un memorando del DOD titulado "Uso responsable y eficaz de recursos con base en Internet". Esta política general reduce significativamente las restricciones previas al dirigir explícitamente el acceso a la *NIPRnet* a una amplia gama de herramientas de colaboración y foros de discusión. (La política menciona, específicamente, a *YouTube*, *Facebook* y *Twitter* entre otras). Por otra parte, a los comandantes en todos los niveles, se les ha instruido defenderse contra actividades maliciosas y tomar las medidas necesarias para salvaguardar las misiones.[32] Aparentemente, esta reciente política tiene sentido desde una perspectiva de equilibrio. No obstante, también presenta un dilema para los líderes militares. Ellos son responsables de trabar una guerra de ideas en una época en la que deben

generar, rápidamente, mensajes preventivos y respuestas reactivas. Estos requisitos exigen un planteamiento descentralizado para la comunicación estratégica y el engranaje de información.[33] Los medios para alcanzar esa velocidad, Internet, es indispensable para la realización de todas las actividades diarias, sin embargo, está bajo permanente vigilancia y ataque, ocasionando que algunos líderes la coloquen bajo control centralizado. Este tema se inclina hacia un extremo y otro, basado en el nivel de riesgo que un comandante está dispuesto a correr en el ambiente de información y en la cultura organizacional militar en relación con el valor de competir en dicho ambiente.

Cómo abordar el dilema: Controlar el riesgo, lograr el equilibrio

El siguiente planteamiento de comando se centra en una "defensa en profundidad" para proteger a la *NIPRnet* y controlar el acceso y uso externo de Internet, mientras que, si bien es comprensible desde un planteamiento de análisis de amenaza, va en contra de los principios de buena estrategia y planificación militar:

> El pensamiento estratégico *es* un proceso intelectual sofisticado con miras a crear una síntesis de consenso, iniciativas y circunstancias para influir, favorablemente, el ambiente general, mientras controla los riesgos involucrados en la búsqueda de oportunidades o de cómo reaccionar ante amenazas.[34]

Por lo tanto, una estrategia con respecto a la utilización de Internet para influir el ambiente de información requiere controlar el riesgo de ataque, mientras se busca la oportunidad para competir. La definición antes citada del poder cibernético como la "capacidad de crear ventajas e influenciar los eventos" en el ciberespacio parece ofrecer un enfoque preventivo, una mentalidad ofensiva centrada en las actividades cibernéticas. La Estrategia Nacional para Combatir el Terrorismo anuncia la oportunidad que ofrece Internet para desacreditar la propaganda del enemigo. En junio de 2008, la Estrategia de Defensa Nacional planteó los requisitos para minimizar el riesgo — pero en términos de la habilidad para aprovechar las oportunidades.[35] Aún así, queda por verse si los comandantes tomarán el enfoque de aversión al riesgo en la nueva política del DOD mediante el establecimiento del control centralizado, poniendo hincapié en la defensa de la red.[36]

Las operaciones militares se basan en la planificación centralizada y ejecución descentralizada con un plan global sincronizado al cual organizaciones subalternas adhieren sus planes subordinados para lograr el fin deseado. La ejecución descentralizada fomenta la agilidad, velocidad y capacidad de respuesta en un ambiente fluido y en constante evolución. Por lo tanto, si la información constituye un componente clave de los ambientes operativos militares actuales y del futuro, se deduce que un plan centralizado con ejecución descentralizada funcionaría en el ciberespacio. Sin embargo, nuevamente, el énfasis de algunos comandos en relación con Internet puede restringir la ejecución descentralizada, obstaculizando la capacidad de ser preventivo, ágil y con capacidad de respuesta para trabar la guerra de ideas.

La pregunta es cómo aprovechar los recursos cibernéticos emergentes para influenciar las opiniones, actitudes y comportamientos al mismo tiempo que se controla el riesgo de vigilancia y ataque por medio de Internet. Resulta indispensable tener en cuenta las diversas razones dadas para limitar el acceso a los nuevos medios ya que las mismas influencian el razonamiento de esos comandantes propensos a restringir el acceso: a fin de fomentar la productividad, apoyar los requisitos de anchura de banda, mantener la seguridad operativa y evitar la intrusión y acceso no autorizado. Estos ejemplos están claramente estipulados en la nueva política del DOD. No obstante, esta expansión es necesaria para proveer un argumento razonado a favor del planteamiento equilibrado determinado por la política.

Productividad. Un argumento para el uso de la *NIPRnet* la cual contiene filtros que evitan el acceso de sitios con vínculos para subir videos (V.gr., *YouTube*), blogs y redes sociales es la presunción de que los soldados entrarán a los mismos para uso personal durante horas laborales, por consiguiente, mermando la productividad en el trabajo. Desde luego, ese potencial está latente. Sin embargo, la responsabilidad de administrar este asunto es responsabilidad de los líderes, simple y sencillamente, y deben tratarse

Fort Leavenworth Lamp, Prudence Siebert

Mayor Jason Wood y Mayor Lee Bokma, Fuerza Aérea de EUA, desempeñan papeles de comandantes de brigada, coordinando la inteligencia y fuegos en un ejercicio de Educación a Nivel Intermedio en la Escuela de Comando y Estado Mayor para la promoción de 2010-01, 25 de febrero de 2010.

con base en excepción. Los filtros de contenido establecidos en cualquier nivel de mando usurpan las responsabilidades de los líderes en las organizaciones subalternas.

Requisitos de anchura de banda. Otro argumento para restringir el acceso a los sitios con vínculos para subir videos es la necesidad de administrar los requisitos de anchura de banda. La anchura de banda es la "capacidad de mover la información".[37] Es un ítem de baja densidad y alta demanda en el suministro de las capacidades computarizadas de mando y control de las fuerzas armadas. Sin embargo, nuevamente, los líderes deciden cómo distribuir todo recurso valioso y limitado para apoyar los requisitos de la misión y llevar a cabo la misma.[38]

Seguridad de operación. La seguridad de operación "selecciona y ejecuta las medidas necesarias que eliminan o reducen a un nivel permisible las vulnerabilidades de acciones amistosas que puedan aprovechar los adversarios".[39] Algunos líderes se preocupan de que la participación de los militares en los blogs, redes sociales y sitios con vínculos para cargar videos, puedan revelar, potencialmente, los puntos vulnerables de las fuerzas militares. Este riesgo compete tanto a la *NIPRnet* como a Internet donde los militares pueden participar en los nuevos medios desde sus hogares. Sin duda, es un riesgo evidenciado por diversas violaciones significativas en los últimos años. Sin embargo, la *OPSEC* (Seguridad de Operación) es, y siempre ha sido un programa del comandante. Los comandantes controlan el ambiente *OPSEC* mediante el adiestramiento, capacitación y medidas punitivas por violaciones deliberadas. Los filtros de contenido y las políticas de mando establecidas a altos niveles para evitar violaciones de la *OPSEC* constituyen restricciones que disminuyen las capacidades de los comandantes de liderar y lograr los objetivos militares mediante el aprovechamiento de las capacidades de la red.

Las intrusiones y amenazas de acceso no autorizado de la red misma son, por otra parte, preocupaciones válidas y dignas de consideración. Los sistemas del DOD, según lo previamente señalado, están bajo permanente ataque de estados-naciones, actores no estatales, criminales y piratas

informáticos. En consecuencia, el departamento dio en el clavo al establecer un sistema que reduce los portales de Internet y permite la vigilancia prudente y continua para prevenir la descarga de software que podría albergar códigos maliciosos con consecuencias devastadoras para la red, y seguir evaluando maneras de reducir dicho riesgo. Cabe mencionar que tanto los adversarios como los criminales se adaptan continuamente a las actualizaciones y demás medidas defensivas.

La administración de riesgo, al mismo tiempo que ofrece la oportunidad de participar eficazmente y aprovechar las oportunidades que proporciona Internet, requiere un reajuste en cuanto a la filosofía de mando. Los líderes y comandantes cuentan con la autoridad y los recursos para, oportunamente, llevar a cabo comunicaciones estratégicas preventivas y sensibles. La productividad, la anchura de banda y los asuntos relacionados con la *OPSEC* son claramente responsabilidad de los líderes y los mismos deben vigilar a los subalternos y hacerlos responsables por violaciones a sus pautas. Este planteamiento descentralizado presenta riesgos. Los comandantes y líderes deben tomar los pasos necesarios para reducir este riesgo pero de manera equilibrada.

El Teniente General William Caldwell manifestó (curiosamente usando un blog como medio de su elección) lo siguiente: debemos incentivar a los soldados para que cuenten sus historias, potenciarlos al tolerar errores no intencionales, capacitarlos acerca de las posibles implicaciones estratégicas de tal participación y equiparlos para participar en el nuevo medio.[40] Si bien Caldwell se refiere, específicamente, al equipo físico, se podría razonablemente argumentar que igualmente, sino más importante, es equipar a los soldados con las pautas de mando adecuadas que les permita participar libremente en los nuevos medios y al mismo tiempo establecer los límites de la interacción. La nueva política del Departamento de Defensa, a medida que llega a los comandos subordinados, debe permitir la participación libre, siempre y cuando, los comandantes sean sensibles a las oportunidades y estén pendientes de las amenazas.

Conclusión

Aparentemente, en agosto de 2008, Rusia realizó ataques cibernéticos, pero esta vez contra Georgia, en una campaña cinética y no cinética coordinada y sincronizada.[41] Es muy posible que esto se convierta en la norma en las futuras guerras entre estados-naciones que pueden llevar a cabo tales incursiones complejas. El caso de Hezbolá, en el conflicto de 2006 con Israel, también sugiere el uso estratégico futuro de Internet y los nuevos medios para llegar al público doméstico e internacional.

El ambiente de información tiene tres dimensiones, a saber: física, los "medios" mediante el cual se envía un mensaje; informativa, el contenido del mensaje; y cognitiva, el efecto que surte el mensaje sobre las opiniones, actitudes y comportamientos del público blanco.[42] Puede decirse que la guerra del futuro incluirá, cada vez más, conflictos en el ciberespacio en las tres dimensiones mencionadas.

El aprovechar las oportunidades mientras se controlan los riesgos es el imperativo estratégico. Un plan militar eficaz, ya sea, en tierra, mar o aire, "protegerá a la fuerza" mientras que ataca al enemigo. Los líderes civiles y los comandantes sopesan el riesgo, implementan políticas y actúan para minimizar el riesgo, pero además, se concentran en lograr los objetivos políticos y militares. En el ciberespacio, esto significa tanto proteger a Internet y usarla como medio de participación.

Además, es importante considerar los efectos de segundo y tercer orden al tomar decisiones. Dada la amenaza constante de un ataque cibernético con éxito contra los sistemas del gobierno de EUA, los líderes pueden recurrir a la alternativa de no correr ningún o poco riesgo en fortalecer las paredes virtuales en torno a la *NIPRnet* a niveles impenetrables. Además, para evitar la violación futura de la seguridad de operación, podrían establecer políticas restrictivas en lo que toca al uso de Internet.

La administración de riesgo… [para] participar eficazmente… requiere un reajuste en cuanto a la filosofía de mando.

Actualmente, la estrategia del gobierno y de las fuerzas armadas de EUA es "convencer

o impresionar" en este sentido con evidencias alentadoras en cuanto a "practicar lo que se predica". El encauzamiento de los líderes de mayor antigüedad para interactuar con los distintos públicos mediante el uso de los nuevos medios promulga los inicios para la superación de las predisposiciones culturales presentes desde hace mucho tiempo contra el uso de Internet para compartir información importante. La nueva política del Departamento de Defensa brinda la oportunidad de lograr el equilibrio necesario tanto para aprovechar como para proteger la Internet. Los líderes y comandantes son responsables de conducir las guerras. Una *NIPRnet* más restrictiva no resolverá este dilema y, de hecho, puede tener efectos secundarios significativamente negativos. Ya es tiempo de romper algunas de las culturas de aversión al riesgo para darle cabida a la "maniobra" de manera que los líderes en todos los niveles puedan desempeñar su trabajo.***MR***

REFERENCIAS BIBLIOGRÁFICAS

1. El Ejército de EUA publicó su manual doctrinal sobre contrainsurgencia, Manual de Campaña 3-24 (Washington, DC: U.S. Government Printing Office [GPO], diciembre 2006). En el prólogo se observa que el Ejército no revisado su doctrina de contrainsurgencia en más de 20 años y cita las operaciones en curso en Irak y Afganistán como ímpetu para la iniciativa.

2. Wass de Czege, Huba, "Lessons from the Past: Making the Army's Doctrine 'Right Enough' Today," *Landpower Essay, Institute of Land Warfare*, no. 06-2 (September 2006): págs. 4, 5.

3. Scales, Robert H., *Certain Victory: The U.S. Army in the Gulf War* (Washington, DC: Brassey's, 1997), págs. 106-107.

4. Sevastopulo, Demitry y McGregor, Richard, "Chinese Military Hacked into Pentagon," *Financial Times*, (4 de septiembre de 2007).

5. Applebaum, Anne, "e-Stonia Under Attack," 22 de mayo de 2007, <www.slate.com/ id/2166716/> (18 agosto de 2008).

6. Kevin Peraino, "Winning Hearts and Minds," *Newsweek International*, 2 de octubre de 2006.

7. Presidente de la Junta de Estado Mayor Conjunto, "DOD Dictionary of Military Terms" según lo actualizado hasta el 30 de octubre de 2009.

8. Kuehl, Daniel "From Cyberspace to Cyberpower, Defining the Problem", in *Cyberpower and National Security* (Washington: National Defense University Press, 2009), p. 38.

9. *National Strategy for Combating Terrorism* (Washington, DC: GPO, septiembre de 2006) págs. 4, 17.

10. Cogan, Kevin J., y Delucio, Raymond G., "Network Centric Warfare Case Study, vol. II" (Carlisle Barracks, Pensilvania: U.S. Army War College, 2006), p. 4.

11. Deibert, Ronald, presentación, U.S. Army War College, Carlisle Barracks, Pensilvania, 10 de enero de 2008. Deibert cita <www.internetworldstats.com> como una fuente de documento para estas estos datos estadísticos. Actualizado hasta el 30 de marzo de 2009.

12. Levesque, William R., "Blogs are CENTCOM's New Target," *Saint Petersburg Times*, 12 de febrero de 2007.

13. Gleason, Carmen L., "Coalition Servicemembers Reach out to America via YouTube," *American Forces Press Service*, 14 de marzo de 2007.

14. Sevastopulo y McGregor, "Chinese Military Hacked into Pentagon."

15. Thomas, Timothy L., *DragonBytes: Chinese Information War Theory and Practice* (Foreign Military Studies Office: Fort Leavenworth, Kansas, 2004), p. 136.

16. Glebocki, Joseph "DOD Computer Network Operations: Time to Hit the Send Button" (Carlisle Barracks, Pensilvania: U.S. Department of the Army, 15 de marzo de 2008) p.4.

17. Blank, Stephen, "Web War I: Is Europe's First Information War a New Kind of War," *Comparative Strategy* 27, nro. 3 (mayo de 2008): p. 240.

18. Applebaum, "e-Stonia Under Attack."

19. Blank, p. 230.

20. Condon, Stephanie, "DHS Stays Mum on New 'Cyber Security' Center," 31 Julio de 2008, <http://news.cnet.com/8301-13578_3-10004266-38.htm> (4 de agosto de 2008).

21. Presidente de la Junta de Estado Mayor Conjunto, *Joint Publication* 3-13, *Information Operations*" (Washington, DC: GPO, septiembre, 2006, 13 de febrero de 2006), II-5, II-6.

22. El autor asistió a una conferencia sobre poder cibernético auspiciada por el Centro de Tecnología y Política de Seguridad Nacional en la Universidad de National Defense en Washington, D.C. en abril de 2008. Los comentarios a los cuales se les hace referencia reflejan las presentaciones de los panelistas. La conferencia se celebró bajo las reglas Chatham House permitiendo el dialogo libre y abierto y a la misma vez garantizando el anonimato de los oradores.

23. Capaccio, Tony, "Cyber Attacks from China Show Computers Insecure, Pentagon Says," 6 de agosto de 2008, <www.bloomberg.com/apps/news?pid=newsarchive&sid=aGqtPqPlSCt8> (18 de agosto de 2008).

24. Departamento de Defensa de EUA, *QDR Execution Roadmap for Strategic Communication* (Washington DC: U.S. Department of Defense, septiembre de 2006), p. 3.

25. Oficina del Subsecretario Asistente de Defensa para la Comunicación Conjunta (DASD (JC)), presentación, junio de 2008. DASD(JC) es la encargada de la capacitación y adiestramiento del Quadrennial Defense Review Strategic Communication Roadmap and Strategic Communication en el Departamento de Defensa.

26. Teniente General Caldwell, William, "Changing the Organizational Culture," 30 de enero de 2008, <http://smallwarsjournal.com/blog/2008/01/changing-the-organizational-cu-1/> (18 de agosto de 2008).

27. Robbins, Elizabeth, "Muddy Boots IO: The Rise of Soldier Blogs," *Military Review*, nro. 5 (septiembre-octubre de 2007), p. 116.

28. Londono, Ernesto, "Silent Posting," *Washington Post*, 24 de julio de 2008.

29. El autor ha asistido a numerosas presentaciones en la Escuela Superior de Guerra del Ejército de EUA en donde líderes de mayor antigüedad (oficiales a nivel de general y civiles de alto rango del Ejército) abogaron por el uso activo de los nuevos medios para transmitir mensajes positivos acerca de nuestras tropas. Un memo emitido en abril de 2008 co-firmado por el Jefe de Estado Mayor del Ejército y el Secretario del Ejército instó una iniciativa significativa para contar la historia de apoyo de las familias del Ejército mediante el empleo del nuevo medio tal como blogs como medios eficaces para transmitir el mensaje.

30. Centro de Armas Combinadas, Comandante, Teniente General William Caldwell, "Request for Exception to Policy for Publishing to a Publically Accessible Website," memorandum for Commander, U.S. Army Training and Doctrine Command et al., p. 27, marzo de 2008.

31. Asistente del Secretario de Defensa de EUA, Gordon England, "Policy for Department of Defense (DOD) Interactive Internet Activities," memorandum for Secretaries of the Military Departments et al., 8 de junio de 2007.

32. Asistente del Secretario de Defensa de EUA, William Lynn, "Responsible and Effective use of Internet-based Capabilities," memorandum for Secretaries of the Military Departments et al., 25 de febrero de 2010.

33. El Manual de Campaña sobre operaciones (febrero de 2008), dedica un capítulo al tema de la información como capacidades para trabar guerra. Destaca la necesidad de la "participación de información" a nivel de cada soldado. Además, trata acerca de los requisitos para superar la cultura de aversión a riesgos para poder participar eficazmente. Véase el capítulo 7.

34. Yarger, Harry R., *Strategic Theory for the 21st Century: The Little Book on Big Strategy* (Carlisle Barracks, Pensilvania: Strategic Studies Institute, 2006), p. 36.

35. U.S. Department of Defense, *National Defense Strategy* (Washington, DC: U.S. Department of Defense, junio de 2008). Véase el "Strategic Framework."

36. Hace poco el autor no pudo entrar a *Facebook* en una visita reciente al Centro de Armas Combinadas, Fuerte Leavenworth, Kansas, donde tenía la intención de demostrar a los estudiantes su efecto capacitador militar.

37. Wu, Tim, "OPEC 2.0," *New York Times*, 30 de julio de 2008.

38. Tisserand, John B., "Network Centric Warfare Case Study, Volumen I" (Carlisle Barracks, Pensilvania: U.S. Army War College, 2006), 53.

39. Presidente de la Junta de Estado Mayor Conjunto "DOD Dictionary of Military Terms," según lo actualizado hasta el 31 de octubre de 2009.

40. Caldwell, "Changing the Organizational Culture."

41. Markoff, John, "Before the Gunfire, Cyberattacks," *New York Times*, p. 13, agosto de 2008.

42. *Joint Publication* 3-13, *Information Operations*, I-1-I-2.