

Principios Bélicos del Ciberespacio

CORONEL STEVEN E. CAHANIN, USAF

Introducción

A MEDIDA QUE LA Fuerza Aérea de EE.UU. desarrolla doctrina, formación y organización para el ciberespacio, necesitamos considerar los principios bélicos tradicionales y cómo/y si se aplican al ciberespacio, y en qué situaciones, de modo que podamos desarrollar una base conceptual para lograr una doctrina bélica eficaz del ciberespacio. Y lo que es más importante, debemos entender que el dominio del ciberespacio requiere una forma nueva y diferente de pensar en desarrollar las estructuras más útiles de doctrina, formación y organización. No debemos caer en la trampa de cambiar meramente las palabras de la doctrina existente del aire y del espacio simplemente reemplazando “aire” o “espacio” por “ciber”.

Generalmente hay dos tradiciones predominantes en los principios bélicos —el punto de vista occidental de Clausewitz y el punto de vista oriental de Sun Tzu. El mundo newtoniano occidental de Clausewitz conceptúa la guerra usando masa, objetivo y maniobra entre otros principios en una guerra cinética entre estados para lograr un objetivo político. No obstante, el mundo oriental de Sun Tzu conceptúa la guerra concentrándose en la transcendencia de la inteligencia, la decepción para superar la mente del enemigo, y saber que las relaciones entre cosas importan más en la estrategia bélica. Es fundamental examinar qué tradición es la mejor guía para desarrollar la ciberestrategia. ¿Es posible que necesitemos una combinación de ambas?

Al desarrollar principios bélicos para el ciberespacio, afirmo que debemos mirar a Clausewitz como guía cuando los efectos entre fuerzas cinéticas parecen ser necesarios, pero también nos fijamos en Sun Tzu como guía porque la inteligencia, la decepción y la relación entre cosas en el ciberespacio requieren una forma diferente de pensar; donde la fuerza contra fuerza es a menudo menos eficaz para lograr nuestro objetivo que los métodos no cinéticos apropiados. Los principios de Sun Tzu de estimaciones de inteligencia, decepción y disposición son guías importantes para las operaciones de un ciberespacio no cinético. Y lo que es más interesante, la interconexión y la integración de redes se producen como en la mente del comandante—incluidas cosas como los centros de fusión de inteligencia y soporte cibernético. ¿Qué mejor forma de atacar esta mente que reunir inteligencia mediante el uso de decepción en el ciberespacio?

La doctrina, la formación y las estructuras organizativas militares de EE.UU. están concentradas actualmente en la tradición bélica de Clausewitz. De hecho, la Fuerza Aérea ya no estudia los principios bélicos de Sun Tzu en la clase de estrategia del Air War College. Desgraciadamente, aunque Clausewitz puede aplicarse a ciertos aspectos de la ciberguerra, sus principios a veces muestran carencias, y cuando ocurre eso necesitamos pensar de forma diferente.

El pensamiento militar occidental tiende a considerar el mundo como si fuera una estructura newtoniana con leyes físicas claras, pero el ciberespacio es diferente; sí, tiene leyes físicas de electricidad y magnetismo, pero el dominio real puede ser mucho más—con aspectos virtuales y cognitivos no presentes en los otros dominios. Por lo tanto, la teoría y la doctrina bélicas del ciberespacio deben considerar la relación de las cosas, es decir, la red, y cómo han escogido las personas estructurar y usar el dominio del ciberespacio.

Las fuerzas militares de EE.UU. no han desarrollado aún una teoría bélica para el ciberespacio. Y aunque han publicado recientemente su primera doctrina del ciberespacio, Operaciones del ciberespacio AFDD 3-12, la Fuerza Aérea parece seguir concentrándose en las ideas de Clausewitz como lo hizo con la doctrina del aire y del espacio.

Por tanto hay temas fundamentales que examinar y preguntas que responder para contestar a medida que desarrollamos primero doctrina, formación y estructura organizativa del ciberes-

pacio. En primer lugar, tenemos que adueñarnos del dominio a nivel de concepto, es decir, ¿cómo vemos la guerra en un mundo donde “todo” puede conectarse con “todo”? Esto requiere entender si los principios bélicos tradicionales pueden aplicarse en este nuevo dominio, o tal vez ¿debemos seguir distintos principios? En segundo lugar, ¿requiere el ciberespacio un método diferente en la educación de los ciberguerreros? La complejidad del ciberespacio puede requerir una forma diferente de pensar sobre cómo formamos actualmente a los ciberguerreros. Necesitamos empezar a pensar de forma diferente en el ciberespacio, ya que si no lo hacemos, volveríamos al cómodo pensamiento occidental de Clausewitz, incluso cuando no favorezca nuestros propios intereses.

Suposiciones

Este análisis se basa en tres suposiciones básicas. Primero, el ciberespacio es un dominio artificial que debemos controlar para que las operaciones militares tengan éxito en los otros dominios de tierra, mar, aire y espacio. Hoy, con pocas excepciones, los demás dominios bélicos dependen del ciberespacio. Este artículo usa la definición del ciberespacio del Departamento de Defensa en la Publicación conjunta 1-02: “el ciberespacio es un dominio global dentro del entorno de información que consiste en la red interdependiente de infraestructuras de tecnología de información, incluida Internet, redes de telecomunicaciones, sistemas de computadoras y procesadores y controladores integrados”.² No obstante, estas interconexiones y capacidades conllevan la necesidad de abordar aspectos cognitivos de control y uso del dominio.

En segundo lugar, los objetivos ciberespaciales de hoy pueden ser penetrados o resultar dañados por un atacante con suficientemente determinación y/o recursos. Según el Dr. Kamal Jabbour, Científico Superior de la Fuerza Aérea para la Calidad de la Información, las políticas y los procedimientos de defensa de redes actuales han fracasado por lo general, y hay numerosos ejemplos de intrusiones en nuestras redes para proporcionar un apoyo suficiente para esta suposición.³

Por último, los avances en la tecnología ciberespacial seguirán cambiando rápidamente el dominio, lo que requiere que nos ajustemos rápidamente si vamos a mantener la libertad de acción en el ciberespacio, tanto defensiva como ofensiva.⁴ La nueva tecnología de la información está poniéndose continuamente a disposición de las fuerzas militares, del público y de nuestros oponentes. Cada nueva capacidad aporta sus propias fortalezas y vulnerabilidades. Los cambios de dominio de software y hardware usados para reparar vulnerabilidades también pueden crear vulnerabilidades. Debemos suponer que el dominio del ciberespacio seguirá cambiando y requieren capacidades de combate flexibles.

Culturas de estrategia y del ciberespacio

Para entender mejor las dos escuelas de estrategia necesitamos comparar sus culturas y formas de pensar. Podemos hacer esto comparando el pensamiento estratégico occidental y oriental de Clausewitz y Sun Tzu respectivamente y la aplicación del ciberespacio.

Ciberpensamiento clausewitziano

Los principios bélicos de Clausewitz se basan en un punto de vista newtoniano occidental del mundo. Clausewitz afirma que la guerra es un acto de fuerza para obligar a nuestro enemigo a hacer lo que queremos, se requiere el uso máximo de la fuerza, el objetivo es desarmar al enemigo, y el motivo de la guerra es el objetivo político.⁵

Es interesante poder ver la estrategia clausewitziana en nuestros juegos occidentales. Por ejemplo, el ajedrez es una batalla basada en la fuerza tratando de capturar al rey, el póquer requiere engaños y correr riesgos donde el ganador gana toda la batalla, y el fútbol americano se

asemeja de muchas formas a lo que Clausewitz y los generales americanos están muy acostumbrados. Estos son ejemplos excelentes del entorno estratégico altamente estructurado que refleja los principios bélicos clausewitzianos. Clausewitz trata adicionalmente los conceptos de probabilidad, suerte, coraje e inteligencia del general; pero con el tiempo, en resumidas cuentas, la guerra es una continuación de las relaciones políticas llevadas a cabo en lo que hoy llamamos fuerza cinética. Esta forma de pensar forma parte del pensamiento militar occidental moderno. La forma militar occidental tradicional de pensar ve una batalla campal donde el ganador se lleva todo.

Sin embargo, Clausewitz, tenía dificultades con la guerra irregular porque los métodos bélicos occidentales hasta el siglo XIX no experimentaban esto como algo frecuente.⁶ Clausewitz consideraba la guerra en un mundo de un estado contra otro estado, con fronteras claras, para obtener un objetivo político, pero eso no es así en el ciberespacio.⁷ El ciberespacio no tiene fronteras entre estados. El noventa por ciento de la estructura ciberespacial es propiedad privada y un gran número de centros de internet de todo el mundo residen físicamente en Estados Unidos.⁸ Un ciberatacante podría estar ubicado en cualquier parte del mundo, ya esté patrocinado por un estado o no, e incluso podría usar haberes ciberespaciales dentro de EE.UU. para atacarnos —aumentando los retos de atribución.⁹ Pero, nada de esto quiere decir que los principios de Clausewitz no sean apropiados al usar la fuerza cinética contra los haberes ciberespaciales del atacante como instalaciones de redes o computadoras, si se puede asignar la atribución. En esos casos, el uso de la fuerza cinética para destruir los haberes ciberespaciales físicos del adversario puede ser apropiado, y servirse mejor mediante los principios bélicos normales tradicionales clausewitzianos, no ciberbélicos.

Con el uso exclusivo del pensamiento de Clausewitz podríamos terminar relegando las operaciones en el dominio del ciberespacio para facilitar las operaciones centradas en la red en los otros dominios. Esto pondría los haberes cibernéticos en una función de apoyo de la guerra cinética—similar a la forma en que el poder aéreo se relegó primero a apoyar las fuerzas terrestres antes de que se descubriera que la guerra aérea tenía nuevos aspectos propios. Hoy hemos encontrado que el ciberespacio también tiene aspectos propios, aspectos que exigen nuevas formas de pensar. Los principios bélicos de Sun Tzu pueden ayudarnos en esta nueva forma de pensar y a menudo pueden demostrar ser un mejor modelo para el conflicto/competición en el ciberespacio.

Ciberpensamiento de Sun Tzu

Sun Tzu dijo, “Conseguir cien victorias en cien batallas no es el sumo de la habilidad. Someter al enemigo sin luchar es el sumo de la habilidad”.¹⁰ Solamente si se entiende esta forma de pensar se puede apreciar por completo a Sun Tzu, ya que de lo contrario sus escritos pueden parecer demasiado simplistas para el lector occidental. Una lectura apropiada de Sun Tzu requiere entender la cultura china y la palabra shi, que pueden significar muchas cosas incluida, “la realidad puede percibirse como un despliegue particular o una disposición de cosas en las que confiar y con las que trabajar para su propia ventaja”.¹¹ Para Sun Tzu, este concepto estaba muy claro, pero para los militares occidentales modernos tal vez no sea tan evidente. Los principios bélicos de Sun Tzu se fundamentan en los conceptos de que todas las guerras se basan en la decepción, que el general debe atacar la mente del enemigo, y que las armas cinéticas solamente se deben usar cuando no haya alternativa.¹² Estos conceptos pueden ser perfectos para el ciberespacio, donde un contrario puede ganar sin combates cinéticos.

Usando nuestra analogía de juegos, la forma de pensar de Sun Tzu es similar a la del juego de mesa más antiguo de la Tierra, go, que tiene sus orígenes en China hace más de 4000 años.¹³ Es más que probable que Sun Tzu conocía este juego en su época, y lo siguen jugando hoy niños y adultos en China. Go es un juego sencillo de dos jugadores que se juega en una cuadrícula de 19

x 19 con “piedras” blancas y negras, donde cada oponente coloca las piedras de una en una. Cada piedra no tiene más valor o poder que las otras, a diferencia de las piezas de ajedrez o las cartas de póquer. A medida que las piedras se relacionan entre sí representan “el yin y el yang penetrando territorios opuestos como el flujo del agua”.¹⁴ Este juego demuestra el uso de shi en una estrategia similar a Sun Tzu, ya que la relación de todas las piedras en el tablero se usa para poner al contrario en desventaja—la base de una estrategia con éxito en go.

Como ocurre a menudo en el caso de la guerra, en go es difícil o imposible ganar todo. El objetivo es conseguir más territorio que el oponente, y las reglas del juego son tales que las acciones demasiado agresivas a menudo fracasan.¹⁵ Sun Tzu entendía bien estos principios. Todos sus principios de inteligencia, decepción y la relación entre las cosas pueden aplicarse para tener éxito en go.

Los principios de Clausewitz de masa y maniobra se observan en juegos occidentales como el ajedrez, el póquer y el fútbol americano—y a menudo en la guerra. Pero el ciberespacio se asemeja frecuentemente a los aspectos fluidos y racionales de go—necesitando una visión estratégica más parecida a la de Sun Tzu. Necesitamos pensar de forma diferente sobre el ciberespacio para determinar qué principios bélicos aplicar y cuándo.

El yin y el yang en el ciberespacio

Podemos usar la idea de yin y yang para conceptualizar el flujo entre la aplicación de los principios de Sun Tzu y Clausewitz en el ciberespacio. Según la filosofía taoísta, el yin y el yang dependen uno del otro, no pueden existir por sí solos, y todo puede describirse como yin o yang.¹⁶ Sabemos que existe una interdependencia entre la guerra cinética y la no cinética. Por lo tanto Sun Tzu podría considerarse como el yin (es decir, guerra no cinética) en el ciberespacio mientras que Clausewitz es el yang (es decir, guerra cinética)—ambos dependen uno del otro, son incapaces de existir por sí solos. El reto a medida que desarrollamos la doctrina ciberespacial es determinar el uso apropiado de Sun Tzu y Clausewitz, y resistir la tentación de volver directamente al pensamiento occidental. Necesitamos que tanto Sun Tzu como Clausewitz funcionen como el yin y el yang a fin de entender cómo luchar para ganar en este nuevo dominio.

El yin cibernético

La doctrina ciberespacial es la que mejor utiliza los principios bélicos de Sun Tzu en el entorno de la guerra cibernética no cinética—particularmente la inteligencia y la decepción, y la importancia de la disposición de las cosas. No obstante, debemos empezar entendiendo cómo las diferentes culturas pueden pensar acerca del dominio cibernético. ¿Cómo operarían y lucharían en él? Los países tienen distintas doctrinas basadas en distintas culturas. Por ejemplo, las diferencias culturales entre China y EE.UU. son significativas, y entender esas diferencias es crucial. Según el modelo de dimensiones culturales de Geert Hofstede™, la cultura china tiene muy poco individualismo además de una perspectiva a muy largo plazo.¹⁷ ¿Cómo nos puede ayudar este conocimiento en el ciberespacio? Debemos considerar estas diferencias culturales al examinar cómo Sun Tzu puede hacernos avanzar usando el ciberespacio. Los taiwaneses nos ofrecen detalles de la perspectiva china, ya que son mucho más capaces de identificar el método de Sun Tzu que un analista occidental.¹⁸ El análisis taiwanés dice que los chinos están desarrollando operaciones ciberespaciales y una red en el contexto de Sun Tzu—pensando en la decepción, la guerra psicológica y el uso de estrategias en vez de fuerza.¹⁹ Por ejemplo, están desarrollando a largo plazo una capacidad bélica de red donde los ciudadanos chinos participarían junto a las fuerzas militares como “combatientes de la red”.²⁰ En el caso de que adopten correctamente esta doctrina, nos podrían forzar a una respuesta cinética o a ninguna respuesta dependiendo de nuestra voluntad de hacer que escale el conflicto. Una vez que entendamos que el ciberespacio requiere una

forma diferente de pensar, podemos examinar los principios de inteligencia y decepción de Sun Tzu, y cómo la disposición de las cosas importa en el ciberespacio.

La inteligencia y decepción son principios críticos de guerra en el ciberespacio, y deben integrarse en la doctrina y operaciones ciberespaciales. Hay ejemplos abundantes sobre cómo los actores estatales y no estatales usan estos principios. Se produjo un ejemplo de reunión de inteligencia con el sondeo de las redes militares de EE.UU. causada por la inserción de una miniunidad de disco en una computadora portátil militar en Oriente Próximo.²¹ Esta miniunidad insertó un código que “se propagó sin detectarse por sistemas clasificados y sin clasificar, estableciendo lo que equivalía a una cabeza de playa”.²² Un ejemplo de operación de decepción ciberespacial es la guerra entre Israel y Hezbolá de 2006, en la que Hezbolá usó la decepción con gran éxito.²³ Un fotógrafo independiente, partidario de Hezbolá, hizo fotos después de un ataque israelí y las modificó usando Photoshop para mostrar que se habían producido más daños. Aproximadamente 920 de sus fotos trucadas llegaron a la base de datos de Reuters y fueron usadas por los servicios de noticias globales antes de que se descubriera y el fotógrafo fuera despedido.²⁴ Es fácil ver que You Tube y otras capacidades del ciberespacio se pueden usar como una “Ofensiva Tet” donde el contrario pierde el apoyo del público aun cuando puedan estar ganando una guerra cinética. Por lo tanto, la inteligencia y la decepción deben ser los principios principales de la guerra en el ciberespacio.

El concepto de la disposición de las cosas también es crítico para el ciberespacio. Esta idea nos lleva al concepto de shi, y al potencial nacido de la disposición. El potencial nacido de la disposición significa que el “general debe tratar de explotar, para su propia ventaja y máximo efecto, las condiciones que encuentre”.²⁵ Esto significa que la disposición de las cosas dentro del dominio ciberespacial importan en diseño y gestión físicos. El diseño físico y el uso del ciberespacio en nuestra lucha bélica pueden darnos una eficacia alta o baja, e importa cómo usamos el dominio del ciberespacio. El pensamiento chino durante el período de los Reinos Combatientes, entre los siglos V y III AC, era que el desarrollo de la guerra podría predecirse lógicamente y por lo tanto gestionarse, de aquí que su pensamiento estratégico era que podían manejar la realidad²⁶ —algo que es curiosamente interesante para el ciberespacio. La realidad depende del color del cristal con que se mira, y puede gestionarse en el ciberespacio, como vemos arriba, no solo con operaciones de decepción, sino también cambiando el dominio como se trata a continuación.

El cambio de dominio significa que nuestros adversarios pueden establecer un dominio ciberespacial (ya que es artificial) completamente diferente a lo que los estados occidentales entienden y/o prefieren, y obtener una ventaja potencial significativa nacida de la disposición de las cosas en el ciberespacio. Esto nos conduce al concepto de “ciberterreno”. Los chinos, entre otros, han averiguado esto y están cambiando el ciberterreno para dificultar considerablemente el acceso.²⁷ Por ejemplo, los chinos han desarrollado un sistema de operación más seguro completamente diferente al mundo occidental con la esperanza de poder cambiar el ciberterreno y hacerlo impenetrable a las fuerzas militares o a la inteligencia de Estados Unidos—y han estado haciendo esto desde 2001.²⁸ No obstante, nosotros dependemos del ciberterreno actual en Estados Unidos y nuestros enemigos conocen muy bien ese terreno. Navegan por nuestro ciberterreno con facilidad aprovechándose de la propiedad extranjera de tecnologías de software y hardware y de nuestra cadena de suministro.²⁹

Sun Tzu escribe sobre las cinco distintas clases de terreno (atrapador, indeciso, limitado, precipitado y distante) y la capacidad de usar estos terrenos para su ventaja.³⁰ Creo que podemos usar este concepto en el ciberespacio. Sun Tzu advierte al comandante sobre cómo actuar en estos distintos entornos. Como nuestras operaciones están conectadas a través de muchos ciberterrenos (.com, .org, .edu, .mil, .smil, etc.), los guerreros ciberespaciales necesitan entender las diferencias de cada uno igual que un guerrero terrestre entiende terrenos diferentes. Una forma potencial de defender el ciberespacio es cambiar el ciberterreno para hacer que sea difícil o imposible para los enemigos que operen de la forma que necesitan.

Imagine si podemos cambiar las características físicas del aire de modo que nuestros adversarios no puedan usar los aviones existentes. Este es un ejemplo exagerado para el aire, pero no para el ciberespacio. La acción de cambiar el ciberterreno podría negar la capacidad de operar en el mismo. Si los chinos tienen éxito en esto, nos podrían obligar a invertir en las opciones cinéticas de Clausewitz que podrían no ser la mejor opción para nuestros objetivos políticos y podrían dejarnos sin opciones buenas. Aun así, hay veces que Clausewitz puede ser la mejor opción o la única.

El yang cibernético

La mejor forma en que la doctrina ciberespacial usa los principios bélicos de Clausewitz es en caso de guerra cinética. AFDD 3-12, Operaciones ciberespaciales, es una forma excelente de empezar a desarrollar esta doctrina, pero lo es exclusivamente desde el punto de vista del aviador y de Clausewitz. AFDD 3-12 indica, "Así como las operaciones aéreas crecieron desde su uso inicial como adjuntas a las operaciones superficiales, el espacio y el ciberespacio han crecido igualmente desde sus manifestaciones originales como capacidades de apoyo en arenas de combate por propio derecho".³¹ Además, AFDD 3-12 usa los principios de la fuerza aérea y de las operaciones conjuntas y las relaciona directamente con el ciberespacio.³² Todos los servicios desarrollan doctrina ciberespacial y algunos pueden retar las afirmaciones doctrinales de AFDD 3-12, especialmente las visiones céntricas del aviador. Además, la ciberguerra probablemente se luchará de forma conjunta en todos los dominios de combate.

Una ciberguerra a nivel estratégico es probable que se propague por otros dominios y por lo tanto requiere operaciones cinéticas clausewitzianas contra los haberes ciberespeciales. Raramente se lucha en un solo dominio—todos los dominios son interdependientes, y por lo tanto la nueva doctrina está obligada a ser pesada en el ciberespacio, en un papel de apoyo a la guerra cinética—de la misma forma que el poder aéreo desempeña a veces un papel de apoyo. No obstante, las medidas y los retos centrados en el ciberespacio son diferentes, y necesitamos abrir nuestras mentes a nuevas formas de luchar en el dominio ciberespacial así como lo hicieron los primeros teóricos para el dominio del aire.

Necesitamos considerar que la ciberguerra puede desarrollar características de coacción y disuasión estratégicas tradicionales contra Estados Unidos. Algunos teóricos ciberespaciales discuten que una ciberguerra estratégica puede combatirse exclusivamente en el ciberdominio y coacciona a un enemigo sin violencia.³³ No obstante, otros creen que el efecto de coacción haciendo uso de la ciberguerra estratégica exclusivamente en el ciberespacio es especulativo como mucho y que el ataque probablemente no causaría suficientes daños para forzar a un estado objetivo a admitir la derrota, y coaccionar a actores no estatales usando ciberataques es prácticamente imposible hoy debido a los retos con atribución.³⁴ Sea lo que sea, al considerar la coacción y la disuasión o la necesidad de usarlas, actualmente no hay ningún incentivo para los actores estatales para amenazar la ciberguerra estratégica contra Estados Unidos ya que los países importantes capaces de lanzar estos ataques necesitan el ciberdominio para seguir funcionando para sus propios usos, y por ello también resultarán dañados.³⁵

Como la guerra tiende a propagarse por dominios, hay pocas razones para creer que la futura guerra estratégica se limitará al dominio ciberespacial; por lo tanto, los principios bélicos de Clausewitz se aplicarán después en combinación con los de Sun Tzu.

Los principios bélicos cinéticos de Clausewitz en la doctrina ciberespacial deben tener en cuenta los impactos de destruir cinéticamente la infraestructura ciberespacial. Los haberes ciberespaciales del adversario, estén donde estén, podrían ser muy útiles. Por ejemplo, el Comandante de la Fuerza Conjunta podría requerir como objetivos un centro de comunicaciones, un puente, un edificio, etc., pero ¿cuáles serían los impactos en las operaciones de la ciberguerra? ¿Existe una necesidad crítica para ese puente debido a que lo atraviesa un cable de fibra óptica,

un cable necesario para comunicar el cese de las hostilidades para el uso en la etapa de recuperación más adelante? ¿Impactaría esta destrucción las ciberoperaciones críticas? ¿Quién defenderá la protección de estos objetivos cuando sea necesario? ¿Significa esto que necesitamos un Comandante de los Cibercomponentes de la Fuerza Conjunta? La doctrina de las operaciones ciberespaciales iniciales de la Fuerza Aérea sugiere que esta función se debe asignar al Comandante de los Componentes Aéreos de la Fuerza Conjunta ³⁶, pero ¿es esa la mejor solución? La armonización de objetivos en el ciberespacio es crítica en los casos en que podamos destruir una infraestructura clave cuya importancia cibernética no sea evidente para un comandante de un componente terrestre, marino o aéreo, no como un puente o un campo aéreo que saben que pueden necesitar—por lo que necesitamos corregir esto.

Recomendaciones

Este análisis me hace sugerir dos recomendaciones. Primero, debemos desarrollar una doctrina usando la combinación de Clausewitz y Sun Tzu para los efectos cinéticos y no cinéticos del ciberespacio, una especie de principios bélicos “ClauseTzu”. En segundo lugar, debido a la naturaleza compleja y siempre variable del dominio ciberespacial, debemos aspirar a un programa de educación riguroso del guerrero cibernético.

Doctrina cibernética ClauseTzu

Debemos desarrollar la doctrina ciberespacial usando una combinación de los principios bélicos de Sun Tzu para acciones no cinéticas, y de los principios bélicos cinéticos de Clausewitz para acciones cinéticas. AFDD 3-12 es un buen comienzo para traducir principios bélicos correspondientes de Clausewitz principalmente en una función de apoyo. No obstante, según se ha mostrado, los principios bélicos de Sun Tzu a menudo son fundamentales en el ciberespacio. No es demasiado tarde para desarrollar una doctrina ciberespacial que integre dichos principios bélicos orientales. AFDD 3-12 es la primera parte de doctrina ciberespacial, y generalmente ha vuelto a basarse en ideas occidentales tradicionales.

Debemos asegurarnos de que la doctrina ciberespacial tenga en cuenta los aspectos exclusivos del ciberespacio, teniendo cuidado de no adoptar simplemente en general de los otros dominios y simplemente reemplazar “aire” o “espacio” por “ciber”. Por lo tanto debemos integrar los principios de inteligencia, decepción y la disposición de las cosas de Sun Tzu en la doctrina ciberespacial ya que es así exactamente como se lucha en una guerra ciberespacial hoy en día, de forma predeterminada.

La doctrina ciberespacial debe incluir una guía para ejecutar operaciones en todo el dominio ciberespacial. Esto incluye cómo relacionarse con el ciberterreno fuera de las redes militares, ya que las operaciones militares dependen de todo el dominio ciberespacial. Esto requerirá un Comandante de Cibercomponentes de la Fuerza Conjunta para asegurar que las ciberoperaciones estén integradas en la lucha bélica—prestando atención especial a la armonización de objetivos (tanto entre objetivos cibernéticos como entre objetivos cibernéticos y cinéticos) y asuntos legales. Evidentemente, hay aspectos legales que deben tenerse en cuenta y cambiarse para que las fuerzas militares luchan de forma efectiva en todos los ciberterrenos, lo que afecta la implementación de los cambios necesarios. Desgraciadamente, las consideraciones/recomendaciones legales van más allá del alcance de este artículo.

Como la doctrina aérea tenía que desarrollarse por separado de la doctrina terrestre, la doctrina ciberespacial debe desarrollarse por separado de la doctrina aérea. La guerra cibernética ya ha empezado y se lucha usando decepción, inteligencia y la disposición de las cosas en todo el “ciberterreno” variable. Haríamos bien en integrar la mejor combinación de principios en nuestra doctrina ciberespacial.

Formación ciberespacial

Este análisis ha resaltado la complejidad de ciberespacio y el cambio continuo, y por lo tanto requiere una mejor formación además de capacitación. Esta formación trataría de entender la teoría cibernética compleja y cómo operar, combatir y ganar en el ciberespacio. Mientras desarrollamos la doctrina ciberespacial debemos acompañarla con un esfuerzo concertado para formar mejor a los guerreros ciberespaciales. Hoy en día, adiestramos a la mayoría del personal de comunicaciones de la Fuerza Aérea en la operación, el mantenimiento y el monitoreo del dominio ciberespacial. Esto necesita llevarse al siguiente nivel formando a los combatientes ciberespaciales, ya que la formación no es igual que la capacitación.

Una analogía de formación en vez de capacitación usando el poder en el ciberespacio es la comparación de un piloto con un mecánico de aviación. El piloto sabe cómo usar el avión en el dominio para el combate, mientras que el mecánico asegura que el avión esté a su disposición. En lo que se refiere al ciberespacio, en la actualidad estamos haciendo la mayor parte de nuestros esfuerzos formando a mecánicos de redes y abandonando la educación de nuestros guerreros cibernéticos.

El ciberespacio requiere una educación robusta para nuestros guerreros cibernéticos. El ciberespacio es un gran reto técnico, y está cambiando físicamente de forma continua (infraestructura, enlaces y espacios virtuales) mucho más rápida y extensamente que otros dominios de combate. Esta formación requiere una elevada inversión inicial que proporcionará un beneficio a largo plazo.³⁷ Educación significa adquirir conocimientos teóricos, capacidad de afrontar futuros inciertos, además de las destrezas de resolución de problemas necesarios para operar en el dominio ciberespacial.³⁸

- Crear un cuadro de oficiales ciberguerreros similar a pilotos y operadores espaciales calificados Debemos,
- Formarlos en ingeniería de computadoras, inteligencia y decepción
- Formarlos en la doctrina ciberespacial “ClauseTzu”

El empleo del poder ciberespacial requerirá ciberguerreros muy formados que entiendan completamente el ciberespacio y sus aspectos estratégicos y que sean capaces de adaptarse continuamente a medida que inevitablemente cambia el dominio.

Conclusión

La lucha en la siguiente guerra importante comprenderá ciertamente ataques asimétricos en el ciberespacio de Estados Unidos, ya que esto es actualmente nuestro talón de Aquiles—como estamos observando en los usos actuales del ciberespacio, especialmente en internet, por parte de nuestros enemigos que no son estados así como por parte de estados oponentes. Debemos entender la amenaza de la guerra cibernética. Actores que no sean estados o individuos pueden atacar a una nación en el ciberespacio debido al bajo costo de entrada así como a los retos de atribución. Los actores estatales siguen tratando de encontrar ventajas asimétricas usando el ciberespacio en futuros conflictos mediante operaciones de reunión de inteligencia y decepción así como ataques ciberespaciales físicos. Necesitamos prepararnos tanto para la defensa como para el ataque en el ciberespacio. Podemos defender y posiblemente reparar esta debilidad entendiendo que el ciberespacio es diferente. Nuestros adversarios potenciales saben esto. Esto requiere nuevas formas de pensar en la guerra.

Debemos entender el concepto de shi y que la disposición de las cosas en el ciberespacio es importante. Los principios bélicos descritos en el Arte de la Guerra de Sun Tzu pueden guiarnos en situaciones en las que no se apliquen los principios tradicionales de Clausewitz, o al menos no tan bien.

Por último, debemos educar un cuadro de ciberguerreros y organizarlos/prepararlos para luchar de forma efectiva en el ciberespacio. Estos serán nuestros guerreros en el ciberdominio así como nuestros pilotos lo son en el aire. En el dominio del aire, los primeros defensores del poder aéreo como Billy Mitchell aseguraron que el poder aéreo no se relegara a una función de apoyo—porque entendió que el dominio aéreo era diferente y añadió nuevas y exclusivas funciones y capacidades que tenían que dominarse y aprovecharse para poder luchar con eficacia. ¿Dónde está el Billy Mitchell del ciberespacio? Hasta que aparezca, nos podríamos preguntar, “¿Qué haría Sun Tzu?” □

Fuente: Este artículo fue desarrollado por el autor como un proyecto de investigación para su graduación del AirWar College de la Fuerza Aérea de EE.UU., 15 de enero 2011

Notas

1. Consulte AWC 2010-2011 Programa del curso de estrategia.
2. JP 1-02, Diccionario de Términos Militares y Asociados del Departamento de Defensa, 12 de abril de 2001 (incluidas las revisiones hasta el 30 de septiembre de 2010), 118.
3. Dr. Kamal Jabbour, ST (SES), Científico Superior para la Calidad de la Información de la Fuerza Aérea, “The Science and Technology of Cyber Warfare” (La ciencia y la tecnología de la ciberguerra) (conferencia, Army War College, Carlisle PA, 15 de julio de 2010).
4. Mike Lloyd, “The Silent Infiltrator” (El infiltrador silencioso), Armed Forces Journal, (Junio de 2010).
5. Carl von Clausewitz, De la guerra, editado y traducido por Michael Howard y Peter Paret (Princeton, NJ: Princeton University Press, 1976), 75-81.
6. Ibid., 479-483.
7. Greg Rattray, Strategic Warfare in Cyberspace (Guerra estratégica en el ciberespacio) (Cambridge, MA: The MIT Press, 2001), 15.
8. Rebecca Grant, Rise of Cyberwar (El ascenso de la guerra cibernética), Un estudio especial del Instituto Mitchell (Mitchell Institute Press, 2008), 13.
9. Martin C. Libicki, Cyberdeterrence and Cyberwar (Disuasión y guerra cibernéticas), (Santa Monica, CA: RAND, 2009), 41-52.
10. Sun Tzu, El arte de la guerra, traducido por Samuel B. Griffith, (Londres: Oxford University Press, 1963), 77.
11. Francios Jullien, The Propensity of Things: Toward a History of Efficacy in China (La propensión de las cosas: hacia una historia de la eficacia en China) (Nueva York, NY: Zone Books, 1995), 15.
12. Sun Tzu, El arte de la guerra, traducido por Samuel B. Griffith, (Londres: Oxford University Press, 1963), 40-41.
13. David Lai, Learning From the Stones: A Go Approach to Mastering China's Strategic Concepts (Aprender de las piedras: un método de go para dominar los conceptos estratégicos de China), Instituto de Estudios Estratégicos (Carlisle, PA: U.S. Army War College Press), Mayo de 2004), 2.
14. Ibid., 7.
15. Ibid., 12.
16. New World Encyclopedia, s.v. “Yin and Yang” (Yin y yang) http://www.newworldencyclopedia.org/entry/Yin_and_yang.
17. Modelos de Dimensiones Culturales de Geert Hofstede™, s.v. “Geert Hofstede,” http://www.geert-hofstede.com/hofstede_dimensions.php?culture1=95&culture2=18.
18. Timothy L. Thomas, Taiwan Examines Chinese Information Warfare (Taiwán examina la guerra de información china), High Frontier 5, no. 3 (Mayo de 2009): 26-35.
19. Ibid., 26-35.
20. Ibid., 26-35.
21. Ellen Nakashima, “Defense Official Discloses Cyberattack: Foreign agencies code on flash drive spread to Central Command” (Oficial de defensa descubre el ciberataque: las agencias extranjeras codifican la propagación de las unidades flash al Comando Central), Washington Post, 25 de agosto de 2010.
22. Ibid.
23. Timothy L. Thomas, “Hezbollah, Israel, and Cyber PSYOP” (Hezbolá, Israel y operaciones psicológicas en el ciberespacio), IO Sphere (Invierno de 2007).
24. Ibid.
25. Francios Jullien, The Propensity of Things: Toward a History of Efficacy in China (La propensión de las cosas: hacia una historia de la eficacia en China) (Nueva York, NY: Zone Books, 1995), 27.
26. Ibid., 25.

27. Centro de Estudios Estratégicos e Internacionales, Securing Cyberspace for the 44th Presidency (Cómo asegurar el ciberespacio para la cuadragésimo cuarta presidencia), (Washington, DC: CSIS Report, diciembre de 2008), 26.

28. Bill Gertz, "China Blocks U.S. From Cyber Warfare" (China bloquea a EE.UU. en la ciberguerra), Washington Times, 12 de mayo de 2009,

<http://www.washingtontimes.com/news/2009/may/12/china-bolsters-for-cyber-arms-race-with-us/>.

29. AFDD 3-12, Operaciones ciberespaciales, 15 de julio de 2010, 4-5.

30. Sun Tzu, El arte de la guerra, traducido por Samuel B. Griffith, (Londres: Oxford University Press, 1963), 124-129.

31. AFDD 3-12, Operaciones ciberespaciales, 15 de julio de 2010, 14.

32. Ibid., 16-19.

33. David J. Lonsdale, The Nature of War in the Information Age: Clausewitzian Future (La naturaleza de la guerra en la era de la información: futuro clausewitziano), (New York, NY: Frank Cass), 205-208.

34. Martin C. Libicki, Cyberdeterrence and Cyberwar (Disuasión y guerra cibernéticas), (Santa Monica, CA: RAND, 2009), 137.

35. Carolyn Duffy Marsan, "How Close is 3.0?" (¿Cuánto falta para 3.0?), Network World 24, no. 33 (Agosto de 2007): 4.

36. AFDD 3-12, Operaciones ciberespaciales, 15 de julio de 2010, 28.

37. Dr. Kama Jabbour, ST (SES), Científico superior para la calidad de la información de la Fuerza Aérea, "The Science and Technology of Cyber Warfare" (La ciencia y la tecnología de la ciberguerra) (conferencia, Army War College, Carlisle PA, 15 de julio de 2010).

38. Ibid.



El Coronel Steven E. Cahanin, USAF, ingresó en la Fuerza Aérea en 1982 como aviador básico, Base de la Fuerza Aérea de Lackland, Texas. Durante el servicio, fue un técnico en aviónica analógica y digital para aviones B-52H y B-1B. En 1987, ingresó en el Programa de Formación de Aviadores para el Cuerpo de Oficiales donde obtuvo su título de Meteorología de la Texas A&M University, y un nombramiento subsiguiente a través de la Escuela de Instrucción de Oficiales de la Base de la Fuerza Aérea Lackland, Anexo Medina en 1990. Desde su ingreso en el cuerpo de oficiales, ha sido Oficial Meteorológico de Escuadra Táctica de Aviones Caza, Comandante de Vuelo, Jefe de Ingeniería, Comandante de Destacamento, Monitor de Elementos de Programas para el Programa de Satélites Meteorológicos de Defensa, Director de Operaciones de Meteorología en el Centro de Control de Aviones Cisterna y Aerotransporte, un Director de Operaciones de Escuadrón Meteorológico, Comandante de los Escuadrones de Adiestramiento Militar Básico 321 y 326, y el Jefe de la División de Sistemas de Información del Servicio de Reclutamiento de la Fuerza Aérea donde es responsable del Sistema de Apoyo de Información de Reclutamiento de la Fuerza Aérea y apoyo de Tecnologías de Información de 3 grupos de reclutamiento y 24 escuadrones de reclutamiento mundiales. Tiene un master en Física de la Atmósfera Superior de Utah State University, y dos masters de la Air University en Arte y Ciencia Militares, y Estudios Estratégicos. El Coronel Cahanin es actualmente Comandante, 45 Escuadrón Meteorológico, asegurando operaciones de lanzamiento seguras y protección de recursos para veinte mil millones de dólares en haberes y veinticinco mil personas en la Base de la Fuerza Aérea Patrick, Cape Canaveral, y Centro Espacial Kennedy.