Ataque Conjunto Inteligente en el Ciberespacio

Mayor Steven J. Smart, USAF

A diario, Estados Unidos depende de nuestra infraestructura digital y proteger este recurso estratégico es una prioridad de seguridad nacional.

—Presidente Barack Obama, 2010

LA SEGURIDAD en el ciberespacio es una prioridad nacional evidente pero el papel que la milicia estadounidense desempeña en este ámbito nuevo no es tan claro. Con la activación en el 2010 del Comando Cibernético de Estados Unidos, el debate con respecto a la militarización del ciberespacio y la conducción de la "guerra" cibernética ha adquirido un papel protagónico entre los encargados de formular la política en el gobierno de EE.UU.[1] Complicando el asunto tenemos la práctica incierta del comportamiento del gobierno en el ciberespacio imponiendo pautas internas legales y políticas al igual que tratados internacionales con base en la guerra cinética.[2] A pesar de esta incertidumbre, la política del Departamento de Defensa (DOD, por sus siglas en inglés) exige que los componentes del DOD "cumplan con el derecho de guerra durante todos los conflictos armados, indistintamente de cómo se caractericen esos conflictos, y en todas las demás operaciones militares".[3] Aunque aún queda por ver cuáles roles y responsabilidades los encargados de formular la política en Washington, DC, harán para la milicia, el personal del DOD debe prepararse para llevar a cabo operaciones militares en el ámbito cibernético. Para hacerlo eficazmente, el Departamento debe aplicarles, con ligeras modificaciones, a las operaciones militares en el ciberespacio principios de ataque conjunto que han dado resultado anteriormente.[4] En este artículo se analiza la eficacia de la *Joint Publication (JP) 3-60, Joint Targeting* (Publicación Conjunta (JP) 3-60, Selección conjunta de blancos), según aplica a las operaciones militares en el ciberespacio y propone recomendaciones para una doctrina conjunta de selección de blancos para el ciberespacio.[5]

Principios fundamentales de la selección conjunta de blancos

Antes de abordar la conveniencia de aplicar la JP 3-60 a la selección de blancos cibernética, debemos comprender sus principios fundamentales, la razón de aplicarlas y la relación entre la doctrina y la ley. "La doctrina conjunta presenta principios fundamentales que guían el empleo de las fuerzas militares estadounidenses", y "(los comandantes) a todos los niveles deben garantizar que sus fuerzas operan según el 'derecho de guerra'," la cual es obligatoria para Estados Unidos."[6] La doctrina conjunta incorpora lo que Estados Unidos ha acordado acatar en el derecho internacional al igual que las mejores prácticas operacionales. El "derecho de guerra" consta del derecho internacional convencional (tratados y acuerdos entre naciones estados) y el derecho internacional consuetudinario (basado en la práctica estatal).[7] Este último surge de la práctica estatal, principalmente la conducta gubernamental oficial reflejada en una variedad de actos, inclusive la doctrina publicada. Por lo tanto, la doctrina conjunta no solo reafirma los compromisos legales obligatorios sino también fomenta el desarrollo del derecho internacional consuetudinario.

Para simplificar, los cánones principales que establecen la base para el derecho de guerra moderno están divididos entre reglas para la *conducción* de la guerra y el *trato* de las partes en el conflicto y sus testigos: las convenciones de la Haya y de Ginebra, respectivamente.[8] Además, en

la Carta de las Naciones Unidas se esbozan las obligaciones de los estados miembros de la organización con respecto al "uso de la fuerza" contra otros estados.[9] El derecho interno (los estatutos federales y las decisiones judiciales), las directrices del gobierno de EE.UU., la doctrina conjunta y de los servicios, al igual que las reglas de enfrentamiento (ROE, por sus siglas in inglés) especifican cómo las fuerzas militares estadounidenses cumplirán con esas obligaciones internacionales. Debemos comprender que ni la doctrina militar ni las ROE, ya sean permanentes o específicas a una misión, ni reemplazan ni sustituyen las leyes de guerra. Más bien, representan la puesta en vigor por parte de Estados Unidos de principios internacionales acordados a una situación específica.

Podemos sintetizar este conjunto de normas, regulaciones y doctrina en cinco principios sencillos que aplican a cualquier situación específica. Primero, el uso de la fuerza presupone la existencia de la *necesidad militar* (una razón militar válida para emplear la fuerza necesaria para llevar a cabo la misión).[10] Segundo, el empleo de la fuerza propuesto no le debe ocasionar *sufrimiento innecesario* ni a la población civil ni a la fuerza enemiga objetivo.[11] Los comandantes deben implementar este principio—la base para convenciones futuras que prohíben el uso de ciertos tipos de armas y municiones (por ejemplo, armas químicas)—no solo a posibles "daños colaterales" (pérdida fortuita de vida civil o daño a la propiedad civil) sino también al objetivo propuesto del ataque. Tercero, el empleo de la fuerza debe discernir o distinguir entre combatientes y no combatientes al igual que evitar ataques intencionales contra las poblaciones civiles que no participan directamente en las hostilidades.[12] En pocas palabras, el operador debe usar un arma capaz de ser apuntada y debe distinguir entre civiles y adversarios—el principio subyacente que guía el análisis de la selección conjunta de blancos, la cual se explora más a fondo a continuación. Cuarto, la operación militar propuesta tiene que ser *proporcional*—es decir, debe evitar daños colaterales excesivos en virtud de la ventaja militar prevista.[13] Por último las partes en el conflicto armado deben mantener el código de caballería o una "cierta cantidad de equidad… y un grado de respeto y confianza mutua".[14] Aplicar esos principios guía el empleo de la fuerza en general y las decisiones del ataque individual en particular.

En los círculos militares, el término *selección de blancos* a menudo describe una acción de una fuerza militar atacando, o preparándose para atacar, un adversario. Oficialmente, la doctrina conjunta define la selección de blancos como "el proceso de seleccionar y priorizar blancos y equiparar la respuesta correcta a ellos, tomando en cuenta los requerimientos y capacidades operacionales".[15] Esta definición, específicamente el proceso de seleccionar el blanco y equiparar la respuesta correcta al mismo, implican más directamente las obligaciones bajo el derecho de guerra. La selección de blancos es la premisa principal sobre la cual radica el principio de discriminación. Los *objetos* militares son blancos legítimos, pero las fuerzas no deben atacar a civiles intencionalmente y los deben salvar de efectos colaterales tanto como sea posible.[16] Por lo tanto, el derecho de guerra responsabiliza tanto al comandante militar como al operador por identificar, caracterizar funcionalmente y atribuirle a un no combatiente, tan correctamente como sea práctico, la intención de una operación militar propuesta.

En la doctrina militar se establecen principios para guiar a las fuerzas en la conducción de sus obligaciones de discriminación. En la JP 3-60 se encuentran los principios globales de selección de blancos para llevar a cabo las operaciones combinadas o conjuntas. La doctrina del servicio militar, tales como el *Air Force Doctrine Document (AFDD) 2-1.9, Targeting* (Documento de Doctrina de la Fuerza Aérea (AFDD) 2-1.9, Selección de blancos), complementa la doctrina conjunta con principios diseñados específicamente para la responsabilidad principal del servicio individual.[17] Esos principios emanan de las mejores prácticas, recurriendo a la experiencia colectiva de la milicia estadounidense y sus aliados durante campañas y operaciones militares anteriores. En vista de que ningún servicio militar tiene la responsabilidad primaria del ámbito ciberespacial y en vista de que hay pocas mejores prácticas colectivas, de haberlas, para las operaciones militares en el ciberespacio, la doctrina actual para otros ámbitos bélicos determina la planificación de la

operación ciberespacial e informa las decisiones de selección de blancos ciberespaciales.[18] Por lo tanto, la JP 3-60 es *por omisión* la publicación fundamental actual sobre la selección conjunta de blancos en el ciberespacio.

Aplicación al ciberespacio

Aplicar la doctrina militar existente (específicamente, selección de blancos y principios del derecho de guerra) a las operaciones en el ciberespacio es fácil en teoría pero puede resultar extremadamente difícil en práctica. La ciberguerra difiere fundamentalmente del conflicto armado tradicional. A diferencia de la conducción de la guerra en el pasado, los opositores (inclusive actores estatales, criminales, terroristas y *hackers* [piratas informáticos]) pueden librar una ciberguerra desde lugares apartados en el globo rápida, económica, anónima y devastadoramente. La doctrina militar actual analiza las experiencias y teorías de la guerra *cinética* entre las naciones estados en espacios de batalla que existen casi exclusivamente en una zona físicamente reconocible y comprensible (aire, tierra, mar y espacio). Por el contrario, la guerra cibernética ocurre en "un ámbito ubicado simultáneamente en capas lógicas y físicas que cruzan actividades en, a través y que tienen que ver con el espectro electromagnético que cruza ininterrumpidamente otros ámbitos al igual que fronteras geográficas y políticamente reconocidas".[19]

El punto hasta el cual la ciberguerra difiere de la guerra cinética y representa un cambio de paradigma en los asuntos militares modernos es un tema polémico más apropiado para los historiadores académicos. Sin embargo, hay diferencias entre los actores y los métodos del conflicto armado en el mundo físico y sus homólogos relacionados con los conflictos en el ciberespacio. Esas variaciones ilustran los retos complejos de aplicar la ley, política y doctrina militar vigentes a golpes de teclado y clics de ratón.

Primero, la participación en la ciberguerra no está limitada a los agentes de la nación estado. A diferencia del ataque militar convencional, llevar a cabo un ataque en el ciberespacio no requiere el patrocino del gobierno.[20] Segundo, el agresor no necesita sistemas de armamento tradicionales costosos, solamente una computadora, una conexión a la *Internet* y experiencia cibernética básica.[21] Tercero, a diferencia de atribuir un ataque en el mundo cinético, identificar la fuente de un ataque cibernético es sumamente difícil. Por ejemplo, encontrar a la nación agresora responsable de un ataque con misil es relativamente fácil porque "huellas" claves tales como el tamaño, velocidad, alcance y tipo de ojiva apuntan hacia una lista relativamente pequeña de países que cuentan con la tecnología, voluntad y experiencia para llevar a cabo ese tipo de ataque. Sin embargo, un ataque cibernético puede originar desde cualquier parte y por cualquiera, inclusive por "piratas informáticos" auspiciados por un estado, actores no estatales o "trabajadores por cuenta propia preparando un laptop golpe motivado políticamente".[22]

Las diferencias principales entre la ciberguerra y su prima, la guerra cinética, plantean preguntas pertinentes. Primero, ¿es realista esperar que inclusive operadores cibernéticos apoyados por el estado cumplan con los principios legales y la doctrina militar con base en nociones tradicionales de la guerra cinética en este nuevo ámbito? Segundo, ¿necesitamos una publicación conjunta nueva específicamente dedicada al ataque ciberespacial para justificar esas diferencias?

A pesar de las discrepancias en los ámbitos operacionales, los guerreros cibernéticos son básicamente lo mismo que sus homólogos en tierra, en el mar y en el aire. Ambos dependen de su conocimiento del ámbito, el entorno operacional y de las capacidades del sistema de armamento. La complejidad de librar una guerra resiste cualquier intento de reducirla a una lista de verificación estructurada para los comandantes. Los líderes astutos podrán discernir y aplicar las verdades duraderas de la guerra, inclusive el marco para su uso legal, dentro del contexto de un entorno operacional o estratégico en particular. Con unas pocas modificaciones, los operadores cibernéticos pueden aplicar principios legales y doctrina militar basada en la guerra cinética tradicional a las operaciones cibernéticas y aún producir los efectos previstos. De manera similar,

con solamente ligeros ajustes para las sutilezas cibernéticas, la JP 3-60 continúa sirviendo como la publicación fundamental de la milicia estadounidense para la localización cinética y no cinética de blancos.

La doctrina militar en el ciberespacio

En el pasado reciente, solamente una publicación conjunta se ocupaba exclusivamente de la conducción de las operaciones militares en el ámbito cibernético.[23] En la JP 3-13, *Information Operations* (Operaciones de Información), se identificaron las operaciones de información (IO, por sus siglas en inglés) como "el empleo integrado de la guerra electrónica (EW), operaciones en la red de computadoras (CNO), operaciones sicológicas (PSYOP), engaño militar (MILDEC) y operaciones de seguridad (OPSEC) en combinación con capacidades de apoyo y relacionadas especificadas para influenciar, interrumpir, corromper o usurpar la toma de decisiones humana y automatizada adversas a la vez que protegemos las nuestras".[24] Doctrinalmente, las CNO, inclusive los ataques a la red de computadoras (CNA) y la defensa de la red de computadoras (CND), representaban tan solo un subconjunto de una categoría mayor de actividades que podría decirse no son similares. En la doctrina se reafirma la centralidad de esas capacidades a la IO en su totalidad, destacando que ayudarían al comandante de la fuerza a influenciar un adversario. Pero agruparlas sugirió que la IO en sí es una especialidad bélica capaz de integrarse rápidamente a una fuerza de tarea conjunta. Lamentablemente, esta no es la manera como los servicios capacitan a su personal. Más bien, actualmente capacitan a un individuo en una o más aptitudes, tales como EW o PSYOP. Dentro de la CNO, rara vez una persona cuenta con pericia en CNA y CND. Por lo tanto, una célula IO a nivel de fuerza de tarea conjunta puede que conste de "cilindros de excelencia" (por ejemplo, individuos muy versados en su campo de entrenamiento limitado pero que poseen pocos conocimientos de las demás aptitudes). Esto es particularmente cierto con respecto al concepto de selección de blancos: la JP 3-13 no ofrece consejos sobre el tema.

Dado por hecho la naturaleza "básica" de esas capacidades, ¿por qué la JP 3-13 no incluye instrucción sobre la selección de blancos? Hay tres razones que acuden a la mente. Primero, la selección de blancos es tan esencial para la contienda que prácticamente todo miembro de la milicia tiene un entendimiento general del concepto. Sin embargo, la selección de blancos que logra exitosamente los objetivos tanto militares como políticos es un proceso sumamente complejo que relativamente pocos individuos han dominado. Sencillamente, la mayoría de los profesionales militares saben qué significa la selección de blancos, pero pocos saben cómo hacerlo. Segundo, en la JP 3-13 no se tratan los detalles de las aptitudes básicas. Más bien, refiere al planificador de IO a consultar otras publicaciones para recibir una guía, sugiriendo que esas aptitudes no están tan relacionadas como se afirma en la JP 3-13. En cambio, en las mentes de los planificadores militares convencionales, son tan solo son varias actividades militares singulares y poco convencionales difíciles de integrar en un plan de operaciones. Por último, muchos planificadores opinan que "la selección de blancos es selección de blancos", indistintamente de la plataforma o ámbito.

La mayoría de los planificadores operacionales cibernéticos declararía que comprenden el concepto general de la selección de blancos según se considera en la definición oficial de la doctrina y según se esboza en la JP 3-60. No obstante, su aplicación del concepto y la definición a su capacidad IO básica podría significar algo muy diferente. Por ejemplo, una actividad PSYOP propuesta podría "seleccionar" una audiencia extranjera cuyo comportamiento y acciones los seleccionadores de objetivos desearían influenciar, pero una operación EW podría seleccionar señales de una torre de radio. En la JP 3-13 se sugiere que los cinco tipos de funciones IO mencionados anteriormente están relacionados entre sí pero no ofrecen pautas sobre cómo atacar al adversario empleando esas funciones específicamente.[25] El planificador u operador de la IO entonces debe acudir a otra publicación específica en el tema para obtener una guía.[26] El hecho de

que la JP 3-13 representa la única orientación conjunta sobre las operaciones en la red complica la cuestión para el planificador de CNO.[27] Por lo tanto, los planificadores de las CNO al nivel conjunto a menudo tienen que referirse a la doctrina del servicio para ese tipo de orientación.

Recientemente la Fuerza Aérea hizo público el AFDD 3-12, *Cyberspace Operations* (Operaciones Ciberespaciales), que distingue entre las operaciones cibernéticas y las de información.[28] Este documento representa el mejor intento del servicio para comprender, organizar, capacitar y orientan a los hombres del aire en las operaciones ciberespaciales. Lo suficientemente básico para el novato en cibernética, pero suficientemente exhaustivo para el experto, el AFDD 3-12 les ofrece a los hombres del aire orientación técnicamente sensata y operacionalmente relevante a falta de una orientación al nivel conjunto—una hazaña particularmente sorprendente. Más impresionante aún, el documento relaciona los principios de las operaciones conjuntas con las operaciones ciberespaciales, ofreciendo información a lo largo de la gamas de las operaciones militares y esbozando los principios fundamentales para el ciber guerrero de la Fuerza Aérea.[29] Podría decirse que el AFDD 3-12 es el documento más exhaustivo sobre las operaciones cibernéticas en el DOD: de hecho, la fuerza conjunta se favorecería con una publicación conjunta que tuviese su alcance y profundidad. Hay que reconocer que aunque en el AFDD 3-12 se discuten muchos temas útiles para la selección cibernética de objetivos, tales como las relaciones técnicas en la infraestructura ciberespacial, seguridad en la información, ciclos de decisión comprimidos y el reto del anonimato y la atribución, no se trata específicamente la selección cibernética de blancos.[30] De hecho, el documento refiere a los lectores a la JP 3-60, sugiriendo que los principios, orientaciones y teoría de la publicación conjunta aplican correctamente a las operaciones ciberespaciales de la Fuerza Aérea.

Por un lado, el tema de la selección de blancos rara vez aparece en la doctrina actual, conjunta o del DOD sobre el ciberespacio, quizás porque la milicia recientemente ha comenzado a organizar oficialmente sus ciber fuerzas o porque los servicios no cuentan con una experiencia extensa y colectiva a la cual recurrir sobre la selección cibernética de objetivos.[31] Por otra parte, los líderes en el DOD puede que sencillamente opinen que los principios de selección de blancos de la JP 3-60 son tan sensatos que pueden traducirse fácilmente a las operaciones militares en el ámbito cibernético. Indistintamente de las razones, la JP 3-60 continúa siendo la publicación conjunta fundamental sobre la selección de blancos en el ciberespacio a pesar del hecho de que no hace ninguna referencia al ámbito en sí.

Repaso de la Publicación Conjunta JP 3-60

Organizada en tres secciones principales—fundamentos de la selección de blancos, el proceso conjunto de la selección de blancos y deberes y responsabilidades—la JP 3-60 pasa a explicar con lógica desde la definición del término *blanco*; a través de la selección de blancos, ataque al blanco y evaluación de daños, hasta responsabilidades de mando y supervisión. Un principiante en selección de objetivos captaría rápidamente los conceptos básicos de este documento conciso y bien redactado. Por ejemplo, una gráfica sencilla (figura II-I, Ciclo de selección conjunta de objetivos) transmite la esencia de la selección de blancos en combate.[32] Comprender el ciclo es comprender la selección de blancos.

EL ciclo de la selección conjunta de blancos esboza rápidamente el quién, qué, dónde, cuándo, por qué y cómo del ataque del adversario.[33] Luego de que el comandante de la fuerza conjunta anuncie un *estado final* y un *objetivo*, los planificadores *elaboran* y *colocan en orden de prioridad* los blancos con tal fin. La selección de blancos impulsa la *correlación arma/capacidad* que garantiza el ataque exitoso a la vez que minimiza los daños colaterales. El arma en particular seleccionada define la *asignación de la fuerza*, que informa la *planificación de la misión* e impulsa la *ejecución*, después de lo cual una *evaluación* le informa al comandante si la misión ha cumplido los objetivos o si es necesario localizar más blancos, según se determine a través de la evaluación

de medidas de eficacia predeterminadas y medidas de rendimiento. Saltar pasos en el ciclo pone en peligro la eficacia de la misión; agregar pasos fuera del ciclo es superfluo. Desde un punto de vista legal, acatar el proceso del ciclo de selección conjunta de blancos y otros principios fundamentales en la publicación, junto con juicio de mando firme, prácticamente garantiza el cumplimiento con el derecho de guerra.

Por lo tanto, el JP 3-60 parece ser la "guía" tipo para seleccionar blancos en cualquier ámbito. Lamentablemente, un análisis que de por sentado que el ámbito cibernético comparte esencialmente las mismas características con el aire, tierra, mar y espacio no explica su singularidad.

Al igual que los demás ámbitos, el ciberespacio ocupa un área, está sujeto a la explotación por parte de gobiernos y empresarios y sirve como un medio para el intercambio de comercio entre las corporaciones, naciones e individuos. Sin embargo, este medio singular "tiene que ser apreciado por sus propios méritos; es un concepto hecho por el hombre".[34] Las computadoras permiten acciones en casi tiempo real y puede que para el usuario provean una casi anonimidad. El hecho de que criminales, terroristas y actores estatales utilicen la misma infraestructura cibernética empleada por empresas comerciales e individuos para llevar a cabo sus operaciones le agrega un "contexto social" a las operaciones militares en este ámbito.[35] En los ámbitos del aire, espacio y mar relativamente pocos adversarios son lo suficientemente competentes como para amenazar o retar eficazmente a Estados Unidos y su milicia. Por el contrario, el ámbito cibernético está repleto de actores capaces de presionar, confrontar o intimidar a Estados Unidos, sus aliados y entre sí. Este espacio de batalla congestionado complica poder utilizar la JP 3-60 como una guía para la selección de blancos cibernética en cinco áreas clave: (1) identificación positiva de blancos, (2) ubicación de blancos, (3) atribución del ataque, (4) aparear la capacidad/blanco y (5) evaluación de posibles daños colaterales.

Primero, la complejidad de la infraestructura ciberespacial global de doble uso complica la identificación positiva de un posible blanco cibernético. Las dos secciones en la JP 3-60 que tratan la identificación de blancos—capítulo 2, "*The Joint Targeting Process*" (El proceso de selección conjunta de objetivos) y el Apéndice E, "*Legal Considerations in Targeting*" (Factores legales en la selección de blancos)—aclaran que un blanco militar válido y legal exige un grado de identificación y caracterización específica llevado a cabo durante un ciclo de selección de blancos o bien normal o dentro de un periodo de tiempo específico. Ninguna sección trata ni la naturaleza fugaz, ni la singularidad de los blancos cibernéticos ni destaca que éstos existen casi exclusivamente en un medio de uso doble.

A modo de ilustración, supongamos que los planificadores designan tres blancos a una junta conjunta de coordinación de blancos, un grupo que "facilita y coordina las actividades de selección de blancos de la fuerza conjunta. . . para garantizar que se cumplen con las prioridades del comandante de la fuerza conjunta". [36] El primer blanco designado es un tanque, el segundo un sitio en *Internet* y el tercero un "personaje" en línea. Inicialmente, la junta podría validar el tanque como un blanco militar pero mantener que ni el sitio en *Internet* ni el personaje califican como blancos militares válidos según se contempla en la JP 3-60 o las leyes de guerra porque no son un objeto físico sino una formula compuesta de unos y ceros—una evaluación incorrecta. De hecho, la JP 3-60 no limita un blanco al mundo físico, en cambio lo define como "una entidad u objeto considerado para posible ataque o acción" (énfasis añadido). [37] Esta definición amplia abarca el sitio *Internet* y el personaje.

La legitimidad de atacar el tanque de un adversario está clara por la finalidad exclusiva de esa arma de destruir y neutralizar dentro de los confines del conflicto armado, pero un análisis del derecho de guerra del sitio en *Internet* y el personaje debe ir un paso más allá. Tanto el sitio en *Internet* como el personaje tendrían que pasar la prueba del "uso" en lugar de "propósito"—o sea, al momento del ataque propuesto, ¿está el adversario usándolos para promover sus capacidades de combate o de sostener la guerra? De ser así, entonces puede que sean los objetos legales de un ataque militar. El momento exacto de cuándo estos objetos de doble uso, entidades o com-

portamientos en y a través del ciberespacio en realidad contribuyen a la causa del adversario dificulta el enfrentamiento. A diferencia de la validación de blancos durante la guerra cinética, el proceso con los blancos cibernéticos exige tanto una actualización consistente de la inteligencia de validación y una identificación positiva en casi tiempo real.

Segundo, la ubicación de un blanco cibernético presenta retos singulares. En la JP 3-60 y en las leyes de guerra se trata la ubicación de blancos en el contexto de la invasión física de una nación soberana. Ni en la doctrina ni en la ley se contempla que un blanco exista en varios lugares diferentes alrededor del mundo a la misma vez o que cause efectos en teatros múltiples de conflicto, como puede suceder en el ciberespacio. Por ejemplo, un adversario puede llevar a cabo mando y control a través de sitios de *Internet* alojados simultáneamente en servidores en diferentes países y puede frustrar el ataque moviendo frecuentemente esos sitios de *Internet*. Problemáticamente, las ROE particulares que aplican al planificador militar puede que excluyan acciones en ciertos lugares fuera de la zona de operaciones conjuntas aunque el adversario utilice una red global siempre cambiante para lograr que los efectos ocurran. Este dilema conduce a un debate significativo e importante. ¿Cuál es el blanco? ¿Acaso es el adversario ubicado físicamente en la zona de operaciones conjuntas, o es su red de mando y control distribuida globalmente? Si la ubicación excluye el enfrentamiento, entonces el planificador militar naturalmente reevalúa el blanco exacto. ¿Acaso son las fuerzas en campaña o sus redes?

Tercero, la atribución de las capacidades cibernéticas, equipo y uso para una entidad en particular declarada hostil es difícil en el ciberespacio. Aunque la atribución puede caer bajo la identificación positiva, en este artículo se trata como un problema aparte para aclarar las diferencias entre la selección ofensiva y defensiva de blancos cibernéticos.[38] La anonimidad que el ciberespacio ofrece le permite al enemigo enmascarar sus acciones y atribuirlas falsamente a un no combatiente o a cualquier otra entidad. Un adversario podría secuestrar las computadoras civiles inocentes, grupos o gobiernos y utilizarlas como una "red *botnet*" para lanzar un ciberataque. Una vez que la víctima del ataque lleva a cabo una investigación forense rudimentaria, la atribución del ataque señalaría a los no combatientes inocentes en lugar de al verdadero autor. Estrictamente hablando (dependiendo de la cantidad del daño), la ley de guerra consideraría un ataque de ese tipo como el crimen de guerra de perfidia. Hablando prácticamente, si el ataque fuese continuo (por ejemplo, una negación de servicio distribuida), ¿debe la víctima obtener la identificación positiva de cada blanco, atribuyéndolo en esencia a una entidad hostil declarada, antes de lanzar las medidas de defensiva a las computadoras que "atacan"? Afortunadamente, como se menciona arriba, la ley de guerra reconoce el derecho intrínseco de auto defensa (enfocándose en la ubicación de la amenaza) y no requiere una identificación positiva del agresor. Pero en el ciberespacio, inclusive una respuesta simple y llanamente defensiva a una computadora que ataca podría tener severas consecuencias en cascada y no intencionadas para la ciber infraestructura global—sin mencionar la pesadilla política de contraatacar la parte equivocada.

Cuarto, el apareamiento de la capacidad y el blanco en el ciberespacio involucra temas singulares. La acción ofensiva puede que requiera aptitudes de precisión para evitar daños colaterales significativos. Una postura defensiva (o respuesta en caso de crisis) puede que exija el uso de capacidades poderosas de contraataque y disuasión contra una amplia gama de agresores—creando más un *firewall* amplio en lugar de un ataque preciso.

Quinto, el arduo proceso de evaluar los posibles daños colaterales en el ciberespacio exige inteligencia significativa y la interconectividad de redes y redundancias en los sistemas que requieren una planificación meticulosa. Al momento no contamos con una metodología oficial para calcular daños colaterales para la selección de blancos cibernética.[39] Aplicar fórmulas cinéticas sería problemático porque el ciberespacio existe tanto al nivel físico como lógico.

A pesar de estos retos singulares a la localización de blancos en el ciberespacio, la JP 3-60 ofrece un marco doctrinal suficiente para el planificador militar de operaciones cibernéticas.[40] Sin embargo, hay camino por recorrer y aclaración con respecto a las operaciones cibernéticas,

particularmente en los campos de cálculos de daños colaterales y evaluación de daños ocasionados por la batalla.[41]

Recomendaciones

Las mejoras a la doctrina existente de selección de blancos deben comenzar con una declaración en la próxima edición de la JP 3-60 que los conceptos básicos descritos en la publicación aplican a la selección de blancos en el recién reconocido ámbito cibernético. Dicha aseveración tendría el doble propósito de reconocer la importancia y singularidad de las operaciones militares en el ciberespacio y afirmar la universalidad de los principios de selección de blancos en combate de la publicación.

Tal como se mencionó anteriormente, la JP 3-60 debe ofrecer una reseña de cómo llevar a cabo un cálculo de los daños colaterales y la evaluación de daños ocasionados por el combate en el ciberespacio, quizás incluir tácticas, técnicas y procedimientos para identificar otros sitios de *Internet* hostiles y civiles ubicados en un servidor o rastrear posibles efectos de segundo y tercer orden y su probable ubicación geográfica. En realidad, en vista de que la mayoría de las operaciones cibernéticas ofensivas no ocasionarían daños colaterales, la JP 3-60 debe describir la metodología para definir *efectos* colaterales en el ciberespacio distinguiendo entre efectos y daños en el ciberespacio. Esa distinción debe usa el "daño cinético" (destrucción física o degradación ocasionada por una operación cibernética) como el criterio determinante. Cualquier operación cibernética que no ocasione destrucción física solamente produciría "efectos". Los planificadores recopilarían las evaluaciones de daños ocasionados por el combate solamente para acciones que ocasionen daño físico a los blancos seleccionados y a los sistemas no seleccionados como blancos y medirían los efectos colaterales al igual que lo hacen para otras operaciones cibernéticas.

Una JP 3-60 actualizada debe incluir una sección breve sobre la complejidad del ámbito cibernético, utilizando las secciones del AFDD 3-12, "Comprendiendo el Ciberespacio" y "Entorno Operacional", como una plantilla excelente.[42] Una discusión de ese tipo le permitiría al planificador conjunto a reconocer las consideraciones singulares adicionales y la selección de blancos en periodos de tiempo específicos en y a través del ciberespacio.

Además, la siguiente versión del JP 3-60 debe prestar suma atención a las diferencias entre selección de blancos cibernética ofensiva y defensiva—específicamente el nivel de atribución necesario para la identificación positiva de un blanco cibernético. Para las operaciones cibernéticas de ofensiva (por ejemplo, CAN), la atribución de una red de computadora, sitio en *Internet,* individuo o infraestructura debe aproximarse a una certeza completa (una verdadera representación de la identificación positiva) de manera que cumpla con el principio de discriminación de las leyes de guerra. La aplicación del principio de auto defensa al ciberespacio le permite mayor flexibilidad al planificador conjunto, contando con la meta de repeler un ataque o ataque inminente contra sistemas de computadoras de aliados. El curso de acción recomendado para la defensa cibernética incluiría implementar una escala de atribución del adversario mediante la cual el nivel de confianza es acorde con el nivel de daño anticipado o efectos producidos por la respuesta. En un extremo de la escala, una respuesta cuyo alcance, duración e intensidad probablemente causará daño cinético significativo exigiría una certeza de atribución casi completa. En el otro extremo de la escala, una acción administrativa de auto defensa puramente técnica—quizás automatizada—que en realidad no llegue al uso de la fuerza no exigiría atribución. Esas "contramedidas" cibernéticas incluyen detectar, poner en cuarentena y eliminar un virus o sencillamente bloquear el tráfico malicioso e interrumpir las conexiones entre las computadoras que atacan y las que están siendo atacadas.

Por último, una JP 3-60 actualizada debe introducir conceptos sobre el *centro de gravedad cibernético de un adversario* y un *área ciberespacial de operaciones conjuntas.* La presencia cibernética de un adversario consta de computadoras, sistemas de informática, *hardware,* personas en línea, y de-

más, que puede que estén separadas geográficamente de su centro de gravedad físico. Una vez que los planificadores identifican el centro de gravedad cibernético (un punto crítico—una fuente de poder para las operaciones cibernéticas del adversario), lo pueden atacar. El comandante de la fuerza de tarea conjunta establecería las fronteras físicas y lógicas de un área de operaciones cibernéticas conjuntas y especificar las ROE de ataque para esa área. Dividir el ciberespacio de esta manera minimiza el potencial de daños colaterales y efectos en cascada.

En resumen, la JP 3-60 le ofrece al guerrero de guerra cibernética conjunta suficientes pautas para la selección de blancos en el ámbito cibernético. Sin embargo, con una ligera modificación y la incorporación de pautas específicas al ámbito, la publicación se tornaría aún más útil para los ciber guerreros. ❑

Notas

1. Wesley R. Andrues, "What U.S. Cyber Command Must Do" (Lo que el Comando Cibernético de EE.UU. debe hacer), *Joint Force Quarterly* 59 (4th Quarter 2010): 117, http://www.ndu.edu/press/lib/images/jfq-59/JFQ59_115-120_Andrues.pdf.

2. Tom Gjelten, "Extending the Law of War to Cyberspace" (Extendiendo el derecho de guerra al ciberespacio), National Public Radio Online, 22 de septiembre de 2010, consultado el 4 de octubre de 2010, http://www.npr.org/templates/story/story.php?storyId=130023318. Para fines de este artículo, *cinético* significa acciones físicas relacionadas tradicionalmente con el combate militar.

3. *DOD Directive* (DODD) (Directriz del DOD) 2311.01E, *DOD Law of War Program (Programa del DOD sobre el Derecho de Guerra)*, 9 de mayo de 2006 (incorporación del cambio 1, 15 de noviembre de 2010), 2, http://www.dtic.mil/whs/directives/corres/pdf/231101e.pdf.

4. En este artículo se emplea el término *principios* (1) dentro del contexto de selección de blancos para describir las creencias principales, mejores prácticas aceptadas y la filosofía militar para producir efectos operacionales y (2) dentro del contexto legal para describir los principios básicos de la ley. Sintetizados en publicaciones conjuntas, estos significados se dividen para destacar ciertas diferencias entre la acción militar cinética tradicional y posibles operaciones cibernéticas.

5. Joint Publication (Publicación Conjunta) (JP) 3-60, *Joint Targeting* (Selección de Blancos Conjunta), 13 de abril de 2007, https://jdeis.js.mil/jdeis/new_pubs/jp3_60.pdf.

6. JP 1, *Doctrine for the Armed Forces of the United States* (Doctrina para las Fuerzas Armadas de Estados Unidos), 2 de mayo de 2007 (incorporación del cambio 1, 20 de marzo de 2009), I-1, I-21, http://www.dtic.mil/doctrine/new_pubs/jp1.pdf.

7. El derecho de la guerra es "una rama del derecho internacional público, y consta de un conjunto de reglas y principios observados por las naciones civilizadas para la regulación de asuntos inherentes a, o secundarios a, la conducción de una guerra pública". *Black's Law Dictionary* (Diccionario de Derecho de Law), 6th ed. (St. Paul, MN: West Publishing, 1990), 1583.

8. Conferencias Internacionales (La Haya), *Hague Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land* (Convención IV de la Haya relativa a las leyes y costumbres de la guerra terrestre y su anexo: Regulaciones con respecto a las leyes y costumbres de la guerra terrestre), 18 de octubre de 1907, http://www.icrc.org/ihl.nsf/full/195. De aquí en adelante La Haya IV. Consultar también *Hague Convention (III) Relative to the Opening of Hostilities* (Convención III de la Haya relativa a la apertura de hostilidades), 18 de octubre de 1907, http://www.icrc.org/ihl.nsf/FULL/190?OpenDocument; *Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land* (Convención V de la Haya relativa a los derechos y deberes de las potencias neutrales y personas en caso de una guerra terrestre), 18 de octubre de 1907, http://www.icrc.org/ihl.nsf/FULL/200; y Geneva Conventions I–IV (Convenciones I-IV de Ginebra), 12 de agosto de 1949, International Committee of the Red Cross (Comité Internacional de la Cruz Roja), http://www.icrc.org/eng/war-and-law/treaties-customary-law/geneva-conventions/index.jsp.

9. Charter of the United Nations, Article 2(4) (Carta de las Naciones Unidas, Artículo 2(4)), 26 de junio de 1945, http://www.un.org/en/documents/charter/chapter1.shtml.

10. La Haya IV, Artículo 23(g).

11. La Haya IV, Artículo 23(e).

12. United Nations General Assembly Resolution 2444 (XXIII) (Resolución 2444 (XXIII(de la Asamblea General de las Naciones Unidas), 19 de diciembre de 1968, según se menciona en International Committee of the Red Cross (Comité Internacional de la Cruz Roja), *Weapons That May Cause Unnecessary Suffering or Have Indiscriminate Effects: Report on the Work of Experts* (Armas que pueden causar sufrimiento innecesario o que tengan efectos indiscriminados: Informe sobre la labor

de expertos) (Ginebra, Suiza: Comité Internacional de la Cruz Roja, 1973), 13, http://www.loc.gov/rr/frd/Military_Law/pdf/RC-Weapons.pdf.

13. Consultar Ginebra IV, Artículos 4 y 27.

14. Judge Advocate General's School (Escuela de Auditores Generales), *Air Force Operations and the Law: A Guide for Air, Space, and Cyber Forces* (Las operaciones de la Fuerza Aérea y la Ley: Una guía para las Fuerzas Aéreas, Espaciales y Ciberespaciales), 2nd ed. (Maxwell AFB, AL: Judge Advocate General's School, 2009), 21, http://www.afjag.af.mil/shared/media/document/AFD-100510-059.pdf. Consultar la introducción a La Haya IV: "Los habitantes y los beligerantes permanecen bajo la protección y la regla de los principios de derecho de las naciones, como resultado de los usos establecidos entre los pueblos civilizados, del derecho de la humanidad y los mandatos de la conciencia pública".

15. JP 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Diccionario de Términos Militares y Afines del Depto. de Defensa), 8 de noviembre de 2010 (según enmendado hasta el 15 de mayo de 2011), 362, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

16. Consultar al Mayor Keith E. Puls, ed., *Law of War Handbook* (Manual sobre el derecho de guerra) (Charlottesville, VA: International and Operational Law Department, Judge Advocate General's Legal Center and School, US Army, 2005), 139–42, http://www.loc.gov/rr/frd/Military_Law/pdf/law-war-handbook-2005.pdf.

17. Air Force Doctrine Document (AFDD) 2-1.9, *Targeting*, 8 de junio de 2006, http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-60.pdf.

18. El ciberespacio es un ámbito global. Consultar la JP 1, *Doctrine for the Armed Forces of the United States*, GL-7; and Cheryl Pellerin, "Cyberspace Is the New Domain of Warfare" (El ciberespacio es el nuevo ámbito de la guerra), *U.S. Air Force AIM Points*, 18 de octubre de 2010, consultado el 20 de octubre de 2010, http://aimpoints.hq.af.mil/display.cfm?id=41748&printer=no.

19. Mayor Steve Smart, "Warfare in the Cyberspace Domain" (La guerra en el ámbito ciberespacial) (tésis, Escuela Superior de Comando y Estado Mayor, Base Aérea Maxwell, AL, 2010), 3. Esta es la nueva definición de "ámbito ciberespacial" propuesta por el autor. La caracterización del ciberespacio como un ámbito operacional es sensible y controversial. Consultar el documento "White House Guidance Regarding the Use of 'Domain' in Unclassified Documents and Public Statements" (Guía de la Casa Blanca relativa al uso de "ámbito" en documentos no clasificados y declaraciones públicas), 14 de marzo de 2011. (FOUO)

20. Christina Mackenzie, "Do No Harm" (No hacer daño), *Aviation Week: Defense Technology International—Cyber War Issue*, Septiembre 2010, 37.

21. Ibid.

22. Michael Dumiak, "Casus Belli," *Aviation Week: Defense Technology International—Cyber War Issue*, Septiembre 2010, 31.

23. El subsecretario de la defensa para políticas y el presidente del Estado Mayor Conjunto revisarán la política y documentos de doctrina de las IO para reflejar la integración dirigida de las IO en las operaciones militares y alejadas de un enfoque en sus capacidades básicas. Este cambio marca un paso significativo hacia el alineamiento de las operaciones cibernéticas. Consultar memorándum de Robert Gates, secretario de la defensa, asunto: La comunicación estratégica y las operaciones de información en el DOD, 25 de enero de 2011, http://www.carlisle.army.mil/dime/documents/Strategic%20Communication%20&%20IO%20Memo%2025%20Jan2011.pdf.

24. JP 3-13, *Information Operations* (Operaciones de información), 13 de febrero de 2006, I-1, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf. La nueva definición de las IO es "el empleo integrado, durante las operaciones militares, de capacidades relacionadas con la información conjuntamente con otras líneas de operación para influenciar, interrumpir, corromper o usurpar la toma de decisiones de los adversarios y posibles adversarios a la vez que protegemos las nuestras". Ver Gates, memorándum 2.

25. JP 3-13, *Information Operations*, II-1.

26. Consultar JP 3-13.1, *Electronic Warfare* (Guerra electrónica), 25 de enero de 2007, https://jdeis.js.mil/jdeis/new_pubs/jp3_13_1.pdf; y JP 3-13.2, *Psychological Operations* (Operaciones psicológicas), 7 de enero de 2010, https://jdeis.js.mil/jdeis/new_pubs/jp3_13_2.pdf.

27. Esto no es para sugerir que el DOD no ofrece guías cibernéticas sino para destacar que hay muy pocas pautas para el guerrero. Consultar DODD 3600.01, *Information Operations (IO)* (Operaciones de información) 14 de agosto de 2006, http://www.dtic.mil/whs/directives/corres/pdf/360001p.pdf; and DODD O-8530.1, *Computer Network Defense (CND)*, 8 de eneero de 2001.

28. AFDD 3-12, *Cyberspace Operations* (Operaciones ciberespaciales), 15 de Julio de 2010, 2, http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-12.pdf.

29. Ibid., 16–20, 22–28.

30. Consultar AFDD 3-12, *Cyberspace Operations*.

31. El Comando Ciberespacial de EE.UU. está desempeñando varios roles y misiones en el ámbito cibernético y está creando una "visión unificada". Mark V. Schanz, "Cyber Command Working Out Roles and Relationships" (Comando Ciberespacial resolviendo roles y relaciones), Daily Report, *airforce-magazine.com*, 21 de octubre de 2010, http://www.airforce-magazine.com/DRArchive/Pages/default.aspx. La 460ª Ala Espacial en la Base Aérea Buckley, Colorado, completó su primer ejercicio enfocándose exclusivamente en asuntos cibernéticos. Sgto. 1º J. LaVoie, "A First-of-Its-Kind Cyber Exercise" (El primer ejercicio cibernético en su clase), Daily Report, *airforce-magazine.com*, 29 de octubre de 2010, http://www.airforce-magazine.com/DRArchive/Pages/default.aspx.

32. JP 3-60, *Joint Targeting*, II-3.

33. Ibid.

34. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Ciberdisuasión y ciberguerra) (Santa Monica, CA: RAND Corporation, 2009), 11, http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf.

35. Consultar Timothy L. Thomas, *Cyber Silhouettes* (Siluetas cibernéticas) (Fort Leavenworth, KS: Foreign Military Studies Office, 2005), 19.

36. JP 3-60, *Joint Targeting*, III-2.

37. Ibid., I-2.

38. Hay un debate de política en curso entre los profesionales cibernéticos y los líderes gubernamentales acerca de la necesidad de la identificación positiva para todas las operaciones cibernéticas y su factibilidad durante respuestas en casos de crisis

39. Consultar Comando de Fuerzas Conjuntas de Estados Unidos, *Joint Fires and Targeting Handbook* (Manual de fuego y selección conjunta de blancos) (Suffolk, VA: Joint Warfighting Center, Joint Doctrine; Norfolk, VA: Joint Capability Development, Joint Integrated Fires, 19 October 2007), http://www.dtic.mil/doctrine/doctrine/jwfc/jntfiretar_hdbk.pdf.

40. Mayor Kevin Beeker (acting J2T, US Cyber Command) y Sgto 1º Dustin Dargis (US Cyber Command), entrevistas con el autor, 2–4 de noviembre de 2010.

41. Ibid.

42. AFDD 3-12, *Cyberspace Operations*, 2–5.

El Mayor Steven J. Smart, USAF, (AA, Wentworth Military Academy Junior College; BS, John Brown University; MA, Air University; JD, Gonzaga University School of Law) es jefe de comunicaciones estratégicas, Oficina del Auditor General, Cuartel General de la Fuerza Aérea de Estados Unidos, Pentágono. Anteriormente se desempeñó en calidad de jefe de selección de blancos y derecho operacional en el Comando Cibernético de EE.UU. y sus organizaciones antecesoras, Comando Componente Funcional Conjunto-Guerra en la Red/Fuerza de Tarea Conjunta en la Red de Operaciones Global donde asesoró al comandante y a la Fuerza de Tarea Interinstitucional Conjunta sobre el derecho de guerra, reglas de enfrentamiento y derecho internacional durante la planificación de las operaciones militares en el ciberespacio. Fue el primer asesor jurídico para los equipos de selección de blancos y ataque cibernético, células de planificación de contingencia y en casos de crisis y para los planificadores de respuestas cibernéticas. Durante su carrera el Mayor Smart se ha desempeñado en calidad de fiscal militar y abogado de defensa al igual que abogado en derecho de suministros y ambiental. Además, desempeñó una función de liderazgo como vice auditor general. El Mayor Smart egresó en el 2011 de la Escuela Superior de Comando y Estado Mayor donde obtuvo el premio de investigación *Lt Gen Michael Hayden* por su contribución en el avance de las operaciones de información, inclusive influencia, guerra electrónica y operaciones de guerra en la red.