Consideraciones para las ciberespaciales ofensivas

Capitán de Corbeta Kallie D. Fink, Armada de EUA;
Mayor John D. Jordan, Cuerpo de la Infantería de Marina de EUA; y
Mayor James E. Wells, Fuerza Aérea de EUA

La capitán de corbeta Kallie D. Fink, Armada de EUA, es una oficial de guerra de información asignada al Comando de operaciones de información de la Armada, Maryland. Cuenta a su haber con una Licenciatura en alemán de la Universidad de Minnesota y una Maestría en Inteligencia estratégica de la Universidad Nacional de Inteligencia. La capitana de corbeta Fink anteriormente se desempeñó como Subdirectora Ejecutiva Asistente del Subjefe de operaciones navales para el dominio de Información (N2/N6).

El mayor John D. Jordan, Cuerpo de Infantería de Marina de EUA, está asignado al Estado Mayor Conjunto J-7, Desarrollo de fuerza conjunta, como analista de investigación de operaciones en proyectos ciberespaciales. Cuenta a su haber con una Licenciatura en Ingeniería aeroespacial de la Universidad de Virginia y una Maestría en Investigación de operaciones de la Escuela Post grado Naval. El mayor Jordan es un piloto de helicópteros CH-46E y sus asignaciones anteriores incluyen volar misiones de evacuación de víctimas en Irak, misiones de asistencia humanitaria a través del Comando del Pacífico de Estados Unidos y el servicio como controlador aéreo avanzado en Afganistán.

El mayor James E. Wells, Fuerza Aérea de EUA, está asignado a la Agencia de Inteligencia Geoespacial Nacional en calidad de jefe de programas de requisitos conjuntos. Cuenta a su haber con una Licenciatura en Comunicación visual y una Maestría en Relaciones humanas de la Universidad de Oklahoma. El mayor Wells, anteriormente se desempeñó como jefe de 3ª Ala de ejercicios y planes en la Base Conjunta Elmendorf-Richardson, Alaska.

Las operaciones ciberespaciales ofensivas (OCO, por sus siglas en inglés) se han vuelto omnipresentes en la última década y su inclusión en la planificación deliberada está en aumento. Sin embargo, gran parte de esta inclusión es una formalidad, mientras que las OCO son, en muchos sentidos, inescrutables para aquellos que no están familiarizados con las mismas. Además, el ciclo de adquisición y localización de blanco conjunto no toma en cuenta las distintas características de las OCO. Las mejoras en la percepción institucional de las OCO y la integración de las mismas en el ciclo de adquisición y localización de blanco conjunto permitirían que los comandantes de la Fuerza de Tarea Conjunta (JTF, por sus siglas en inglés) aprovecharan al máximo esta potente capacidad durante la planificación deliberada.

Sin embargo, dos problemas principales obstaculizan la incorporación efectiva de las OCO en la planificación operacional. El primer problema es que el personal de planificación tiene conceptos erróneos acerca de las capacidades y limitaciones de las OCO en un ambiente operacional. Además, el estado mayor se siente incómodo con los aspectos sumamente clasificados y técnicamente complejos del dominio ciberespacial porque no los comprenden. El segundo problema es que las OCO no encajan perfectamente en el ciclo de adquisición y localización de blanco conjunto y requieren mucho trabajo y tiempo adicional para incorporarlas en la planificación deliberada.

Los conceptos erróneos y desafíos en el uso operacional de las OCO

Entre las muchas ideas erróneas sobre las OCO, dos son particularmente importantes. La primera es que las OCO son habilitadores no letales que juegan un rol marginal en las operaciones. La segunda es que en vista de que los detalles de las OCO, son inescrutables debido a su complejidad técnica o inaccesible por su clasificación, no vale la pena intentar usarlas en un nivel operacional.

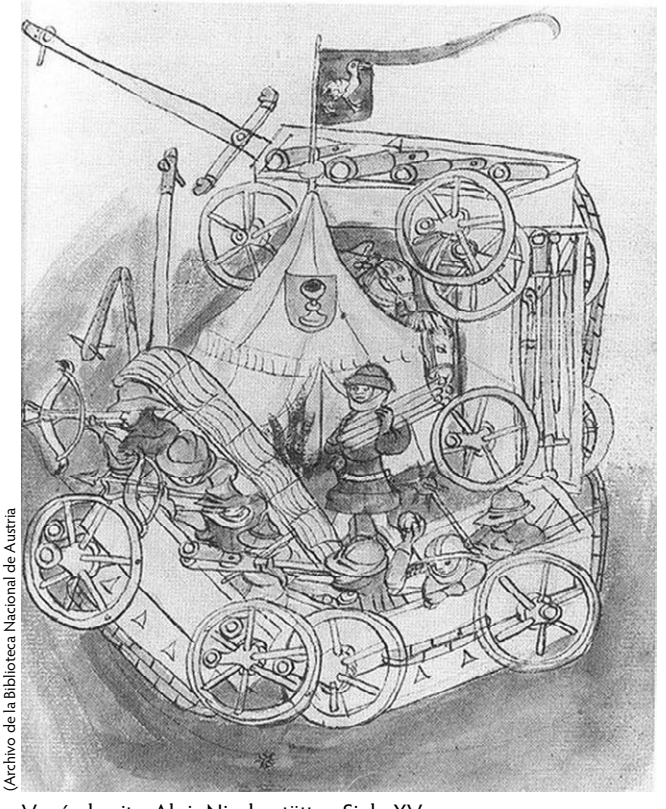
El concepto de "solo son computadoras". Una percepción común entre los planificadores es que las OCO son medios no letales de atacar a las redes de un oponente, con poco efecto físico. Sin embargo, en la última década, las OCO se han convertido más que un habilitador no letal como la guerra electrónica. La naturaleza y potencial de las OCO no han cambiado significativamente, pero sí nuestra comprensión de las mismas.

Un sistema de arma revolucionaria típicamente comienza como un arma asimétrica que puede, bajo condiciones favorables, usarse en contra de formas tradicionales del poder militar. Un ejemplo histórico es el uso de armas de pólvora en manos de los husitas, un grupo de disidentes religiosos del siglo XV quienes utilizaron armas primitivas para derrotar a los caballeros blindados.[1] En el siglo XXI, las capacidades ofensivas del ciberespacio puede proporcionarles a los actores estatales y no estatales una nueva arma asimétrica para usar contra los poderes tradicionales.

Un suceso en Estonia en 2007 es considerado por algunos, representativo del primero ataque ciberespacial ofensivo contra una nación. Comenzó luego de que el Gobierno de Estonia removiera un monumento soviético de la Segunda Guerra Mundial en conmemoración a una victoria rusa sobre los Nazis.[2] El Gobierno estonio sospechaba que Rusia coordinaba ciberataques en represalia contra la estructura digital de Estonia, el Mando y Control del gobierno (C2), las instituciones financieras y las redes de comunicación.[3] Los ataques masivos paralizaron el correo electrónico de las agencias del gobierno, publicaron documentos falsos y limitaron, en gran medida, el acceso a Internet. El bombardeo digital duró dos semanas y obligó a uno de los principales bancos, Hansabank, cerrar el servicio en línea por más de una hora; al final las pérdidas fueron calculadas

cerca de US$ 1 millón de dólares.[4] La negación e interrupción del Gobierno, los medios de comunicación y las redes financieras causó confusión y caos sin provocar daño físico o destrucción. El ataque ocasionó gran daño económico a Estonia. La coordinación de una respuesta defensiva fue muy difícil porque el ataque fue sumamente disperso —ninguna autoridad estoniana fue responsable de la defensa de los muchos y distintos recursos ciberespaciales.[5]

Cómo las nuevas armas asimétricas se convierten en parte integral de un arsenal militar estándar. Luego de que las fuerzas armadas usaron exitosamente una nueva arma asimétrica, a veces, la adoptan como un complemento del arsenal militar tradicional. Por ejemplo, en el siglo XVI, los ejércitos combinaron mosquetes con picas y caballeros armados. Durante la guerra entre Rusia y Georgia de 2008, algunos especularon que las fuerzas rusas integraron las OCO a las operaciones tradicionales para mejorar su eficacia operacional en general. Evidentemente, los rusos llevaron a cabo numerosos ataques ciberespaciales que hicieron inoperables al Gobierno de Georgia y las redes de los medios de comunicación.[6] Estos ataques perturbaron severamente al C2 militar georgiano. Fueron sincronizadas



(Archivo de la Biblioteca Nacional de Austria

Vagón husita, Alois Niederstätter, Siglo XV.

con las tropas rusas que cruzaban la frontera georgiana.[7] El experto en el ciberespacio, Eli Jellenc declaró que este evento representó "el verdadero nacimiento de la guerra cibernética operacional," mientras pareció ser el primer uso coordinado de ataques ciberespaciales y convencionales en un estado-nación.[8]

Eventualmente, un arma complementaria puede convertirse en un arma primaria. Por ejemplo, el mosquete equipado con una bayoneta de enchufe reemplazó la punta de lanza de principios del siglo XVIII como el arma de infantería universal. En 2010, un gusano informático conocido como *Stuxnet* obviamente se utilizó como un arma ofensiva principal para crear efectos operacionales tangibles. El *Stuxnet*, si bien de origen desconocido, era un programa de "disparar y olvidar", considerado como el primer "misil ciberespacial" del mundo.[9] Al parecer, el programa fue desplegado para sabotear las centrifugadoras de refinación de combustible nuclear de Irán las cuales podrían utilizarse para desarrollar el uranio de calidad militar, al alterar la corriente eléctrica.[10] Según el investigador alemán, Ralph Langner, el ataque pudo haberse concebido para destruir el rotor de la centrifugadora por vibración —que podría causar que la centrifugadora explotara— o sencillamente, degradar, con el tiempo, la salida eléctrica (al frenar y acelerar el motor).[11] El *Stuxnet* —si bien se pone en práctica a través de lo que se percibe como un dominio físico y no letal— logra, con eficacia, efectos físicos al averiar las instalaciones nucleares iraníes.

Los ejemplos presentados de Irán y Georgia muestran cómo las OCO han producido efectos que van desde operaciones no físicas de hostigamiento e información hasta daños físicos a la infraestructura clave. Sin fuerzas o armas con contacto físico directo, las OCO pueden crear efectos operacionales físicos y no físicos. Pueden cerrar los sistemas de defensa antiaérea y los nodos C2, abrir o cerrar las compuertas de una represa y destruir o averiar las máquinas industriales tales como las capacidades centrífugas nucleares.[12] Las capacidades ciberespaciales ofensivas, como las armas estándares letales y tangibles, pueden ser flechas en la aljaba del comandante de una Fuerza de Tarea Conjunta. Pueden habilitar a un comandante para, eficientemente, atacar una gran variedad de blancos, individualmente, o junto con otras armas.

El concepto erróneo de "No lo comprendo" o "No puedo hacerlo". Las capacidades ciberespaciales,

(AP Photo/Vahid Salemi)

Un técnico iraní trabaja en la Instalación de conversión de uranio justo fuera de la ciudad de Isfahan, 225 millas al sur de Teherán, Irán, 3 de febrero de 2007.

especialmente las OCO, suelen ser desarrolladas en secreto. Las OCO son sumamente clasificadas porque la naturaleza de estas operaciones podría divulgar las intenciones estratégicas y operativas en caso de ser reveladas. Si una potencia hostil se entera de un objetivo OCO en desarrollo, esa potencia podría aprender mucho acerca de las capacidades ciberespaciales y operaciones del comando combatiente de Estados Unidos. Si ciertos enemigos se enteran de un plan de operación que los involucra a ellos como blanco en un ataque ciberespacial en un nodo de infraestructura, podrían usar la doctrina militar estadounidense para desarrollar cierta comprensión del plan. Además, en caso de que los datos técnicos estén comprometidos, un oponente puede usar los datos para diseñar y construir un arma cibernética para atacar los intereses de Estados Unidos o de sus aliados.

Además de los desafíos que presenta la confidencialidad, los aspectos técnicos de las operaciones ciberespaciales son difíciles de comprender para las personas sin entrenamiento técnico. Esto es especialmente así en comparación con los sistemas de armas tradicionales. El ciberespacio no es como los dominios físicos tradicionales donde podemos tocar y ver todas las partes. Por el contrario, el ciberespacio, principalmente, es un reino virtual que puede ser manipulado para lograr efectos del mundo real en los dominios aéreos, terrestres, marítimos y espaciales. Poner una bomba en el blanco es más fácil de visualizar que lanzar un sinnúmero de ciberataques para penetrar una red y, eventualmente, debilitar o destruir un sistema crítico.[13]

La marginación por inaccesibilidad. Ya sea que el asunto sea difícil de comprender, obtener acceso, o usar capacidades ciberespaciales técnicamente complejas —la inaccesibilidad puede marginar más que cualquier defensa de los oponentes. Por desgracia, la inaccesibilidad puede hacer que los planificadores operacionales se rehúsen al uso de las OCO. Pueden considerar las operaciones ciberespaciales un término de moda que el jefe quiere divulgar en lugar de un conjunto de armas y

tácticas que ofrecen beneficios tangibles. En el mejor de los casos, las OCO pueden ser marginadas —usadas en las periferias de las operaciones porque no son comprendidas, inaccesibles, difíciles de usar y desconfiables.

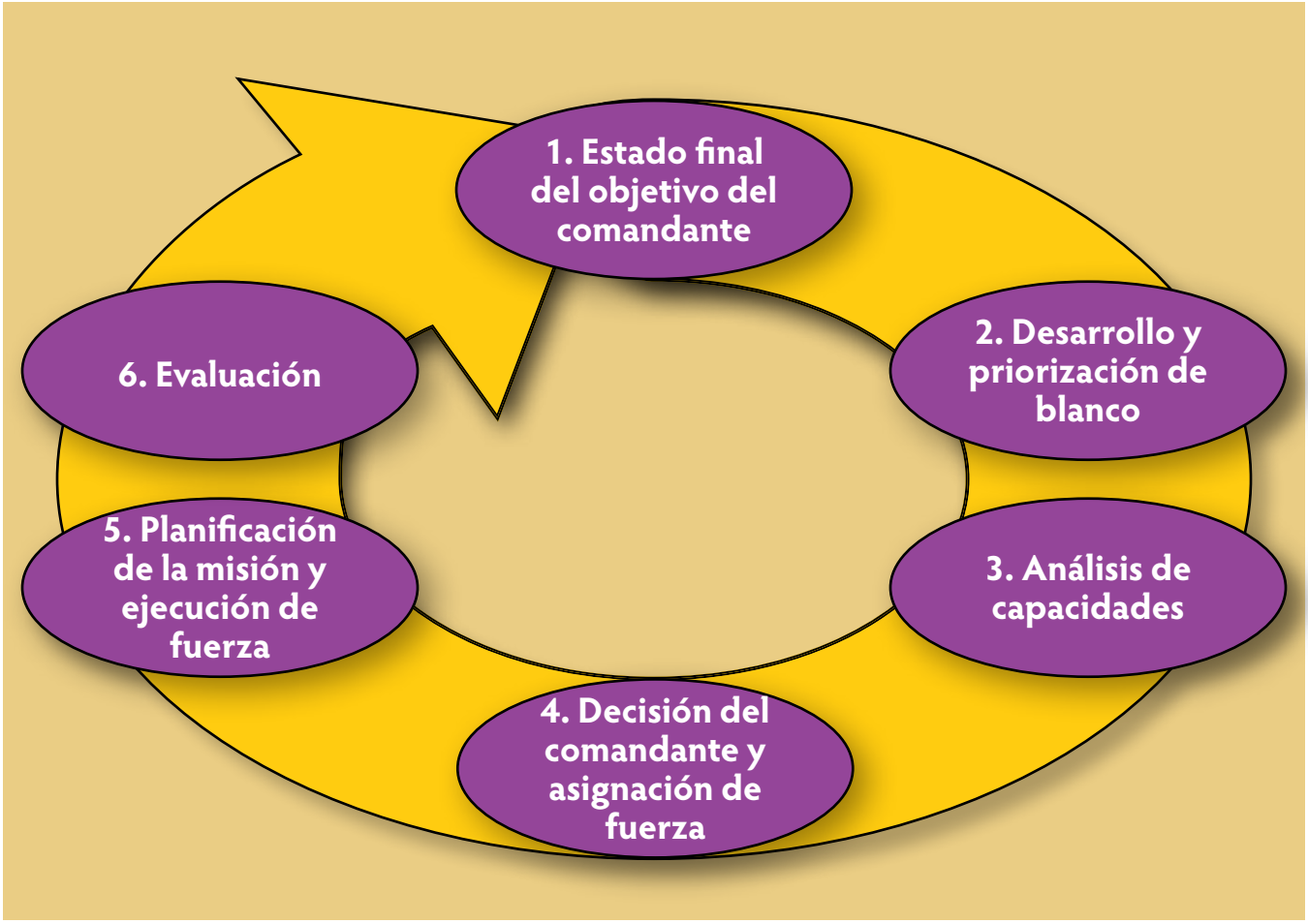
El ciclo de adquisición y localización de blanco conjunto. Además de los conceptos erróneos comunes y problemas de inaccesibilidad en torno a las OCO, ciertos desafíos son inherentes al encajar las OCO al ciclo de adquisición y localización conjunto (ver Figura).[14] Dos fases del ciclo de adquisición y localización conjunto —desarrollo y priorización de blanco y análisis de capacidades— tienen el efecto más significativo en la planificación del uso operacional de las OCO en los escalones superiores.

El Comando Ciberespacial de Estados Unidos (USCYBERCOM, por sus siglas en inglés) coordina los efectos ciberespaciales deseados contra un blanco, basado en las prioridades del comandante combatiente o del comandante de la Fuerza de Tarea Conjunta. Durante la planificación de contingencia, la fase de análisis de capacidades busca aparear los recursos y municiones con objetivo y efecto deseado. Una vez que se seleccione un blanco para ser atacado por medios tradicionales, el mismo se revisa periódicamente durante el ciclo de revisión del plan. No se invierten más recursos para mantener la accesibilidad del blanco hasta tanto se lleve a cabo el plan. Por el contrario, la designación de un ataque contra un blanco con las OCO empieza la inmediata asignación e inversión de recursos adicionales. El mantener y desarrollar un blanco requiere una cantidad significativa de tiempo. Durante la Operación *Odyssey Dawn* en el 2011, funcionarios estadounidenses debatieron el uso de las OCO contra Libia, pero se opusieron al uso de las mismas por varias razones —principalmente por la cantidad de tiempo que requería. Los analistas en el *New York Times* informaron que "en realidad se necesita un husmeo digital significativo para identificar los posibles puntos de entrada y nodos susceptibles en una red de sistemas de comunicaciones, radares y misiles operados por el Gobierno de Libia y, luego, escribir e insertar los códigos venenosos adecuados."[15]

¿Cómo tiene que ver el ciclo de adquisición y localización de blanco conjunto con las OCO? El primer paso para atacar un objetivo con las OCO es ganar acceso al mismo. Sin acceso físico o electrónico al blanco, resulta imposible proceder con las OCO. Por lo regular, un sistema vinculado a Internet es más accesible, aunque entrar a las partes específicas puede ser difícil debido a su propio ambiente de seguridad de red. Un sistema cerrado, como el programa nuclear iraní, requeriría acceso privilegiado para obtener conocimiento de primera mano del ambiente informático en la instalación blanco.[16] Una vez que las fuerzas ganen acceso a un sistema blanco, necesitan mantenerlo siempre y cuando deseen atacarlo. Las actualizaciones llevadas a cabo de la red o cambios de sistema en el mantenimiento regular del blanco, podrían dificultar mantener o recuperar el acceso. El riesgo de tener acceso a un sistema es que un adversario podría detectar la piratería informática mucho antes del ataque. El adversario descubriría qué sistemas fueron atacados. Por otra parte, el descubrimiento, sin duda alguna, podría ocasionar que se perdiera el acceso —y la posibilidad de que el adversario analice el ataque para comprender las operaciones ciberespaciales estadounidenses y desarrollar mejores defensas o, hasta contraataques.

Una vez que se obtenga acceso, el siguiente paso a seguir es aprender los atributos internos singulares del sistema blanco. Los atacantes ciberespaciales tendrán que adquirir el *software* amenazado para poder determinar su naturaleza y vulnerabilidades. En los sistemas disponibles en el mercado, esto es relativamente fácil de hacer —se puede comprar una copia. En los sistemas raros o los que cuyo desarrollo y uso se limitan a un determinado país o región, las fuerzas podrían necesitar obtener información privilegiada sobre el ambiente de la red (como pudo haber ocurrido con *Stuxnet*).[17]Según el sistema que ha de ser atacado, el código podría ser comentado en un idioma que no es el inglés. Si por cualquier motivo, el USCYBERCOM no puede obtener conocimiento técnico del *software* específico, entonces las OCO no pueden proceder; la coordinación del efecto adecuado es imposible. El comandante de la Fuerza de Tarea Conjunta debe tomar en cuenta estos atributos de las OCO cuando establece las prioridades del blanco durante la planificación deliberada.

Si el USCYBERCOM coordina un medio para el acceso continuo y conoce, a cabalidad, el sistema blanco, entonces debe coordinar la adquisición o desarrollo del arma con la cual atacarlo. Algunas armas diseñadas para atacar sistemas operativos comunes tales como *Windows* se encuentran disponibles en el mercado. Sin embargo, los sistemas producidos y usados solamente en ciertos países, típicamente requieren fuerzas para



Selección y adquisición conjunta de blancos

desarrollar, desde cero, las armas. Esto se convierte en un proyecto de adquisición de *software*, en el sentido tanto técnico como jurídico. Para efectos de adquisición de defensa, los proyectos de desarrollo de *software* son más complejos que los proyectos de ingeniería físicos.[18] El desarrollar un arma cibernética es un desafío complejo por esta razón y muchas más. Una vez que se haya desarrollado un arma, los atacantes constantemente deben mantener el acceso y vigilar el blanco. Deben garantizar que el mantenimiento rutinario del sistema no anule su trabajo hasta que se use el arma, o hasta que el blanco sea eliminado de la Lista de blancos priorizada integrada conjunta (JIPTL, por sus siglas en inglés).

Los desafíos que presenta la asignación de fuerza de las OCO. Todas estas acciones requieren una cantidad significativa de tiempo, tal vez meses, antes de que otra cosa que no sea un ataque rudimentario pueda ser lanzado con una presunción de éxito. Además, según el blanco y su accesibilidad, un arma puede necesitar navegar a través de varias redes hasta su blanco intencionado. Según los analistas forenses cibernéticos, el *Stuxnet* puede haber infectado el ambiente de su blanco a través de un dispositivo extraíble insertado por un tercero dispuesto o accidental, o espía.[19] El *Stuxnet* tuvo que haber necesitado numerosos desarrolladores de sistemas que trabajaron durante seis meses para infectar las computadoras blanco de la red cerrada del programa nuclear iraní.

En la actualidad, el USCYBERCOM coordina todas las OCO, con el consentimiento del comandante combatiente apropiado. Esto complica aún más el desafío de aparear los blancos con las armas. No solo un comandante combatiente debe solicitar al USCYBERCON que ataque un blanco, sino que cada blanco en la JIPTL de un comando también compite por recursos contra los blancos en las JIPTL de otros comandos. El

USCYBERCOM analiza todas estas listas, asigna una prioridad mundial a los blancos individuales y les asigna recursos escasos. Si bien el USCYBERCOM considera un blanco de alta prioridad, el comando puede que no cuente con los recursos necesarios para atacarlo. El USCYBERCOM debe informar a los comandantes combatientes y al JTF de su capacidad para atacar sus blancos en las JIPTL.

Los comentarios jurídicos onerosos. Stewart A. Baker, ex secretario adjunto del Departamento de seguridad nacional para la política y tecnología, sugiere que la interpretación jurídica de Estados Unidos de los convenios de la Haya reduce el uso operacional de las OCO.[20] Baker escribe lo siguiente: "los abogados gubernamentales han formulado tantas preguntas legales difíciles sobre la ciberguerra que dejaron a nuestros militares incapaces de luchar, o incluso, planear una guerra en el ciberespacio".[21]

Parte de esta complejidad jurídica surge de la naturaleza de las OCO. Según lo señalado anteriormente, cualquiera de los ataques ciberespaciales más rudimentarios contra un enemigo requiere la adquisición, desarrollo o modificación del *software* para generar los efectos que desea un comandante de Fuerza de tarea conjunta. Esto lleva a la Directriz del Departamento de Defensa (DODD) 5000.01, *The Defense Acquisition System*, al proceso. En la Directriz 5000.01 se requiere que "la adquisición o contratación de armas y sistemas de armas del DoD deberá ser coherente con las leyes internas, tratados y acuerdos internacionales pertinentes".[22] En cuanto a las operaciones de la Fuerza Aérea, en la Instrucción 51-402 de la Fuerza Aérea se establece que la oficina del Procurador General de la Fuerza Aérea llevará a cabo revisiones legales de toda nueva capacidad ciberespacial (incluyendo las armas) o cualquier modificación contemplada de una capacidad ciberespacial para asegurar la legalidad bajo la Ley del conflicto armado (LOAC, por sus siglas en inglés), la ley nacional e internacional.[23] El ataque tradicional en un blanco con misiles y bombas sólo tiene que pasar a través de un escrutinio legal durante el desarrollo y priorización del blanco, puesto que las armas empleadas desde hace mucho tiempo han pasado su evaluación (por la DODD 5000.01) durante el ciclo de adquisición y localización. Por el contrario, puesto que las armas ciberespaciales son singulares para cada blanco, las OCO de la Fuerza Aérea requiere dos revisiones legales: la primera durante la validación del blanco y la segunda durante el proceso de adquisición y localización. Esto pone la puesta en práctica de las OCO a merced de la lectura más restrictiva de la LOAC por dos equipos legales independientes.

Esta restricción y la ambigüedad general de cómo la LOAC tiene que ver con las operaciones ciberespaciales, ha creado lo que Stewart Baker interpreta como "una estrategia de guerra cibernética que simplemente omite cualquier plan para llevar a cabo operaciones ofensivas. Al parecer, todavía están esperando que todos estos abogados se pongan de acuerdo en cuanto al tipo de operaciones ofensivas militares que está permitido montar".[24]

Soluciones

Cómo aclarar la percepción de las OCO. La educación es la clave para cambiar cómo pensamos, planificamos y usamos las OCO. El ciberespacio, incluyendo la concienciación de las OCO, debería ser parte del acceso básico del currículo de cada oficial. El nivel de educación militar profesional conjunto (JPME, por sus siglas en inglés) debería incluir operaciones ciberespaciales fundacionales y doctrinales para todos los oficiales. Los oficiales en el nivel intermedio y de mayor antigüedad deberían estudiar e integrar las operaciones ciberespaciales operacionales y estratégicas en la planificación conjunta a través de la JPME II. Además, los cursos básicos deben incluir la instrucción en las capacidades y limitaciones de las OCO. La meta de esta educación no debería convertir a los oficiales en especialistas cibernéticos, sino, más bien, proporcionarles la misma concienciación básica de este dominio que tienen los oficiales quienes están en el campo de las armas de apoyo o de combate en cuanto a cómo desempeñan su profesión los que están en otros campos.

A diferencia de las complejidades de los sistemas sofisticados de armas convencionales, los detalles de las OCO deberían permanecer clasificados. Esto es un atributo de las operaciones ciberespaciales que debe tenerse en cuenta en la adquisición y localización de blancos: los conocimientos de los procesos específicos en el que se logran los efectos cibernéticos deberían limitarse a los que tienen una necesidad de saber. La inaccesibilidad de las capacidades ofensivas del ciberespacio —para cualquier persona que no trabaje directamente en el desarrollo y la ejecución de las mismas— aporta

un nivel de seguridad operacional que, con el tiempo, apoyará la capacidad. Además, mantener un nivel de inaccesibilidad en torno a las capacidades ciberespaciales proporciona la opción de enmascarar la intención operacional. La mayoría de los planificadores conjuntos no poseen el conocimiento o autorización de seguridad para saber cómo construir un misil crucero Tomahawk desde el principio; ni los planificadores conjuntos tienen acceso para analizar minuciosamente una capacidad ciberespacial ofensiva.

Un ejemplo de esta paradoja es el virus de espionaje *Flame*, descubierto en 2012 y que había circulado en Internet aproximadamente cuatro años antes de que fuera detectado.[25] Según Debra Van Opstal, *Flame* "se aprovecha del sistema operativo *Windows* para capturar audio, imágenes, actividad del teclado e información de tráfico de red de las computadoras infectadas."[26] El que decidió usar *Flame* probablemente no comprendió las complejidades de su funcionamiento interno, pero sí el efecto deseado. El virus *Flame* solo es un ejemplo de una herramienta ciberespacial ofensiva difícil de detectar, pero su compleja naturaleza ofrece una perspectiva singular en el nivel de detalle requerido para producir un efecto penetrante cibernético. El desafío para el comandante combatiente y el estado mayor de la JTF es aceptar y operar en este ambiente sin fronteras, que puede implicar pulsar el botón "Yo creo" cuando se analizan los efectos deseados y priorizados a través del USCYBERCOM.

Las mejoras en ciclo de adquisición y localización de blanco conjunto. A fin de utilizar mejor las capacidades de las OCO, el panel de coordinación de adquisición y localización de blanco conjunto (JTCB, por sus siglas en inglés) debe cambiar la manera en cómo elaboran sus JIPTL; deben coordinar la nominación del blanco cibernético con el USCYBERCOM. Esto permitirá a los JTCB mejorar el uso de las OCO, mientras integran plenamente las capacidades ciberespaciales con el poder tradicional terrestre, aéreo y marítimo.

El análisis de capacidades iterativas. Cada JTCB debe contar con un representante del ciberespacio asignado al mismo. El representante debe tener el mismo nivel de los representantes del comando del componente aéreo, terrestre y marítimo de fuerza conjunta. El representante del ciberespacio debe proporcionar una lista de nominación de blanco ciberespacial al JTCB. Cuando el JTCB comienza a sintetizar las listas de nominación de objetivo en el proyecto de las JIPTL, el representante del ciberespacio puede coordinar el proyecto de las JIPTL con el USCYBERCOM. Con esta información el USCYBERCOM puede informar al JTCB sobre qué objetivos se consideran susceptibles para las OCO, lo que permite al panel moldear mejor las JIPTL. Además, esta práctica permitirá al USCYBERCOM buscar las posibles sinergias, cuyo trabajo ya está asignado a otros planes. Este intercambio de información moldeará el diseño de las JIPTL y habilitará al JTCB para integrar su diseño a las OCO.

A fin de obtener los mejores resultados de las OCO, el JTCB también debe asegurarse de que los blancos para las OCO sean duraderos. El JTCB debe centrarse en los efectos necesarios en lugar de cómo se generan los mismos. Los blancos duraderos son necesarios porque permiten que el USCYBERCOM coordine los recursos lo más eficientemente posible y evite perseguir blancos fugaces. Un blanco duradero debe ser uno que perdure a través de varios ciclos de revisión del plan. Esto le proporciona al USCYBERCOM el tiempo suficiente para desarrollar las armas necesarias a fin de atacarlo exitosamente. Por otra parte, un enfoque en los efectos le permitirá al USCYBERCOM proponer cursos de acción alternos para el JTCB. Esto permitirá que el JTCB se concentre más en el panorama que en los detalles de las OCO. El representante del ciberespacio para el JTCB debe ser más que capaz de eliminar los conflictos y coordinar las OCO con el resto de las JIPTL.

La coordinación de la asignación global de la OCO. Cada JTCB debe permanecer flexible en cuanto a su JIPTL, como requisito del USCYBERCOM para proporcionar apoyo global lo cual significa que los recursos pueden cambiar. Ya sea que las prioridades cambien, o por otras razones, no todo blanco en cada JIPTL será atacado. El USCYBERCOM deberá informar a cada JTCB de la situación de sus blancos, especialmente, si cambian las prioridades, ya que esto podría tener un efecto significativo en la JIPTL de un comando. Cada JTCB debe prepararse para esta posibilidad al elaborar las JIPTL alternativas que reflejan la falta de acceso a un blanco ciberespacial. Esto, nuevamente, requiere que continuamente se revisen y actualicen las JIPTL en lugar de dejarla en el estante hasta la siguiente revisión del plan de operación. El enlace directo ofrecido por el representante del ciberespacio hace esto

menos oneroso, pero requerirá que el JTCB lleve a cabo otras investigaciones y planificaciones para satisfacer el estado final deseado del comandante. Obviamente, la tentación de ignorar o marginar las capacidades del ciberespacio persiste porque usarlas causaría frustración y más trabajo. El JTCB debe sopesar el beneficio potencial de las OCO con la carga de trabajo adicional que esto podría infligir durante la planificación deliberada. Sin embargo, la integración exitosa de las OCO puede permitir que una Fuerza de tarea conjunta extienda su alcance más allá de lo que permitirían los recursos de fuego tradicionales y reservar esos recursos para blancos más convenientes.

La revisión legal consolidada. Los desafíos legales de un JTCB parecen desalentadores, pero el panel puede abordarlos de una manera que satisfaga los requisitos del comandante combatiente. Si bien los detalles de las reglas de enfrentamiento y legitimidad del blanco residen en el reino de la ley, es, sobre todo, con las nuevas tecnologías, un campo subjetivo. El uso de dos procesos legales distintos —en el desarrollo del blanco y proceso de priorización descritos en la Publicación conjunta 3-60 y el proceso de adquisición y localización descrito en la DODD 5000.01— para aprobar el desarrollo y uso de un arma cibernética —es redundante y usa en exceso los escasos recursos legales.

En cambio, el USCYBERCOM debe llevar a cabo ambas revisiones legales. La revisión legal durante el proceso de priorización y desarrollo de blanco debería omitirse para los blancos ciberespaciales. El USCYBERCOM debe llevar a cabo una revisión inicial y final de la LOAC mientras coordina con el JTCB durante el desarrollo del arma cibernética. Además, en vista de que las armas cibernéticas son desarrolladas con especificaciones especiales para atacar un blanco, el equipo legal puede llevar a cabo las revisiones legales ordenadas por la DODD 5000.01, así como la validación del blanco. El USCYBERCOM, en coordinación con el representante del ciberespacio, debe contar con los conocimientos técnicos para revisar y ayudar en el desarrollo del arma. Esto mejorará la eficacia del desarrollo y uso de las OCO. Además, puesto que el equipo de revisión legal no forma parte del comando combatiente, hay menos oportunidades de que los "grupos especializados " y la influencia del comando alteren el proceso.

Conclusión

Las OCO ofrecen potentes herramientas para un comando combatiente o comandante de Fuerza de tarea conjunta. Sin embargo, nuestra propia fricción interna —manifestada como malentendido, inaccesibilidad y procesos de lenta evolución— no nos ha permitido aprovechar al máximo estas capacidades. Ninguna de las soluciones descritas anteriormente son particularmente costosas, ni implican comprar equipos o añadir a la estructura de fuerza. Por el contrario, se centran en el desarrollo de nuestra gente y procesos de manera que estén más dispuestos a atacar un adversario en todos los ámbitos. Si bien la implementación de estas soluciones sería una iniciativa a largo plazo, el retraso de la misma solo haría que el problema se agudizara y eficazmente negara el uso de las OCO a los comandantes de la fuerza conjunta. ■

Referencias Bibliográficas

1. David, Saul, The Illustrated Encyclopedia of Warfare: From Ancient Egypt to Iraq (London: DK Publishing, 2012), p. 95.

2. Bachmann, Sascha-Dominik "Hybrid Threats, Cyber Warfare and NATO's Comprehensive Approach for Countering 21st Century Threats—Mapping the New Frontier of Global Risk and Security Management," Amicus Curiae 88 (enero de 2012).

3. Landler, Mark y Markoff, John "After Computer Siege in Estonia, War Fears Turn to Cyberspace," New York Times (29 de mayo de 2007).

4. Ibíd.

5. Davis, Joshua, "Hackers Take Down the Most Wired Country in Europe," Wired.com (21 de agosto de 2007), http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

6. Farwell, P., James y Rohozinski, Rafal, "Stuxnet and the Future of Cyber War," Survival: Global Politics and Strategy 53, no. 1 (January 2011): págs. 23-40.

7. Korns, W., Stephen y Kastenburg, E., Joshua E., "Georgia's Cyber Left Hook," Parameters 38, no. 4 (Invierno de 2008-2009).

8. Jellenc, Eli, citado en Iain Thomson, "Georgia Gets Allies in Russian Cyberwar," Vnunet.com (12 de agosto de 2008), http://www.v3.co.uk/v3-uk/news/1997915/georgiaallies-russian-cyber-war; también ver Markoff, John, "Before the Gunfire, Cyberattacks,"

New York Times (12 de agosto de 2008), http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0.

9. Clayton, Mark "How Stuxnet Cyber Weapon Targeted Iran Nuclear Plant," The Christian Science Monitor (16 de noviembre de 2010): p. 4.

10. Farwell y Rohozinski, págs. 23-40.

11. Langner, Ralph, según lo reportado en Clayton, p. 4.

12. Handler, Gosnell, Stephenie, "The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare," Stanford Journal of International Law 48, no. 1 (Invierno de 2012): p. 209.

13. Singal, Anoop y Ou, Ximming, Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs (Gaithersburg, MD: NIST Interagency Report 7788, National Institute for Standards and Technology, U.S. Department of Commerce, agosto de 2011).

14. Joint Publication 3-60, Joint Targeting (Washington, DC: U.S. Government Printing Office [GPO], 31 de enero de 2013), Figura II-2.

15. Schmitt, Eric y Shanker, Thom "U.S. Debated Cyberwarfare in Attack Plan on Libya," New York Times (17 de octubre de 2011). http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=0.

16. Falliere, Nicolas, Murchu, Liam y Chien, Eric W32.Stuxnet Dossier (Cupertino: Symantec Corporation, 2011), http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

17. Ibíd.

18. Rendon, G., Rene y Snider, F., Keith, Management of Defense Acquisition Projects (Reston, Virginia: American Institute of Aeronautics and Astronautics, 2008), p. 66.

19. Falliere, Murchu, y Chien, p. 3.

20. Baker, A., Stewart y Dunlap, Charles Jr., "What Is the Role of Lawyers in Cyberwarfare?" ABA Journal (1 de mayo de 2012). http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare.

21. Ibíd.

22. Department of Defense Directive 5000.01, The Defense Acquisition System (Washington, DC: GPO, 12 de mayo de 2003), p. 7.

23. U.S. Air Force, Air Force Instruction 51-402: Legal Reviews of Weapons and Cyber Capabilities (Washington, DC: GPO, 27 de julio de 2011), p. 2.

24. Baker y Dunlap Jr.

25. Van Opstal, Debra "'Aha' Findings from the Workshop on Securing the Smart Grid: Best Practices in Supply Chain Security, Integrity, and Resilience," Center for Critical Infrastructure Protection and Homeland Security 11, no. 2 (agosto de 2012).

26. Ibíd.