AIR & SPACE POWER JOURNAL en ESPAÑOL

Tercer Trimestre 2012

CYBER WARFARE

AMENAZA MUNDIAL

OFICIALES DE LAS FUERZAS AERÉAS IBEROAMERICANAS EGRESADOS DE LA ESCUELA SUPERIOR DE GUERRA AÉREA (AWC), MAXWELL AFB, ALABAMA, PROMOCIÓN 2011–2012

De izquierda a derecha: Coronel Salvador Hernández (El Salvador), Coronel Homero Lobo (Brasil), Coronel Eusebio Lozano (España), Coronel José Luis Ramírez (México), Coronel William Tamayo (Colombia).

OFICIALES DE LAS FUERZAS AÉREAS IBEROAMERICANAS EGRESADOS DE LA ESCUELA SUPERIOR DE COMANDO Y ESTADO MAYOR (ACSC), MAXWELL AFB, ALABAMA, PROMOCIÓN 2011–2012

De izquierda a derecha: Mayor Walter Paz López (Honduras), Mayor Xavier Coral (Ecuador), Teniente Coronel Manuel Cristales (El Salvador), Mayor Josué Arguello (Nicaragua), Coronel Martín Fuentes Soto (República Dominicana), Teniente Coronel Mauricio Reyes Díaz (Colombia), Mayor Patricio Bogado (Paraguay), Mayor Pascual Soria (España), Mayor Enrique Sarabia Guerrero (México).

Portada diseñada por la Señora Susan Fair. Recuadro diseñado por el Señor Alastair Worden

http://www.af.mil

http://www.aetc.randolph.af.mil

http://www.au.af.mil

General Mark A. Welsh III
Jefe del Estado Mayor, Fuerza Aérea, EE.UU.

General Edward A. Rice Jr.
Comandante, Comando de Educación y Entrenamiento Aéreo

Teniente General David S. Fadok
Comandante, Universidad del Aire

General John A. Shaud, USAF-Retirado
Director, Air Force Research Institute

Editor, Edición en Español
Tte. Cnel. Luis F. Fuentes, USAF-Retirado

Asistente Editorial
Sra. Drina L. Marmolejo

Producción
Sra. L. Susan Fair, *Ilustradora*
Sr. Daniel Armstrong, *Ilustrador*
Sra. Vivian D. O'Neal, *Diagramación*

El *Air & Space Power Journal* (ISSN 1555-3833), se publica trimestralmente en Árabe, Chino, Español, Francés, Inglés, y Portugués. Es la revista profesional de la Fuerza Aérea de los Estados Unidos de Norteamérica y ofrece un foro abierto para la presentación y estímulo de ideas del pensamiento innovador militar sobre doctrina, estrategia, táctica, organización, alistamiento, historia y otros aspectos de defensa nacional. Las ideas expresadas en los artículos que aparecen en las páginas de la revista reflejan la opinión de los autores sin tener carácter oficial y por ningún motivo representan la política de la Secretaría de Defensa de los E.U.A. la Fuerza Aérea o la Universidad del Aire. Se autoriza la reproducción total o parcial de los artículos sin permiso; pero, si lo hace mencione la fuente, *Air & Space Power Journal–Español*, y al autor.

Para comunicarse con nosotros puede hacerlo por teléfono, fax, internet o dirija su correspondencia a: Editor, *Air and Space Power Journal–Español*, 155 N. Twining Sreet, Maxwell AFB, Alabama 36112-6026.

DSN: 493-6382
Fax: (334) 953-1626
E-mail: aspjspanish@maxwell.af.mil
aspjspanish@gmail.com (Alternativa)

AIR & SPACE POWER JOURNAL en ESPAÑOL

Volumen XXIII, Nº 3 TERCER TRIMESTRE 2012

ASPJ

EDICIÓN EN ESPAÑOL
DE LA REVISTA PROFESIONAL
DE LA FUERZA AÉREA DE
LOS ESTADOS UNIDOS

Editorial 3

Encaminándonos hacia el Éxito en la Misión Cibernética de la Fuerza Aérea: Aprovechándonos de nuestro legado para forjar nuestro futuro
Teniente General David S. Fadok, USAF
Dr. Richard A. Raines 5

La Intersección de la Ley y la Ética en la Ciberguerra: Reflexiones
Mayor General Charles J. Dunlap, Jr., USAF–Ret. 11

El Mundo se ha Vuelto "Ciberloco": Cómo el "Debilitamiento Mutuamente Asegurado" es la mayor Esperanza para la Disuasión Cibernética
Dr. Matthew D. Crosston 24

Los Años Interinos del Ciberespacio
Teniente 1º Robert M. Lee, USAF 36

Stuxnet: Revolución de Ciberguerra en los Asuntos Militares
Mayor Paulo Shakarian, USA 50

Preparación de la Inteligencia del Entorno de Información y Comunicaciones
Jeffrey Carr 60

Virtualmente Masivo: Comprendiendo la Concentración y el Poder de Combate en la Ciberguerra
Capitán John "Strider" Cobb, Fuerza Aérea de los Estados Unidos 66

Principios Bélicos del Ciberespacio
Coronel Steven E. Cahanin, USAF 73

La Guerra en el Ámbito Cibernético
Welton Chang
Sarah Granger 83

Pautas para Diseñar Estructuras Adaptativas de Mando y Control (C2) para las Operaciones Ciberespaciales
Teniente Coronel Jeffrey B. Hukill, USAF-Ret 91

Editorial

La evolución de la tecnología de la informática ha producido significativos adelantos y beneficios para la humanidad, al mismo tiempo que ha creado serios problemas relacionados con el alarmante auge de la delincuencia cibernética, el ciberespionaje, los ataques cibernéticos, y la inminente amenaza de una guerra cibernética. Y no se trata de algo que pueda suceder –es algo que ya se está librando. La difusión de la tecnología digital y las consecuencias de un inesperado ataque cibernético de mayores consecuencias ponen en peligro el orden y la seguridad mundial. Algunos advierten que los efectos de una guerra cibernética pueden ser tan destructivos como los de una guerra nuclear. De acuerdo con el presidente de la Comisión de Comercio del Senado, Jay Rockefeller, *"Los criminales cibernéticos de hoy en día tienen la capacidad de interrumpir los servicios de mantenimiento de la vida, causar catastróficos daños económicos, o degradar severamente las redes de las cuales depende nuestra defensa nacional y nuestras agencias de inteligencia."* Coherente con esta misma línea del pensamiento, encontramos el pronunciamiento bien fundamentado del Secretario de Defensa de los Estados Unidos y ex director de la CIA, León Panetta: *"Lo cierto es que existe la capacidad cibernética para tumbar nuestras redes eléctricas y/o paralizar el sistema financiero de nuestro país. Por lo tanto, considero que tenemos que estar preparados no solo para defendernos contra esta clase de ataques sino también, en caso necesario, para ser agresivos"*. Los Estados Unidos y muchos otros países se muestran actualmente vulnerables frente a la posibilidad de un ataque catastrófico inesperado, equivalente al de Pearl Harbor, del cual podrían ser víctimas inequívocas. Por lo tanto, no se pueden descuidar ni dejar de reforzar sus defensas cibernéticas como parte de su estrategia militar. Conscientes de esta realidad y de la seriedad que conlleva esta amenaza, dedicamos esta edición al tema de la guerra cibernética.

Teniendo en cuenta lo anterior, podemos afirmar que el entrenamiento y la preparación de nuestros líderes militares constituyen la forma mas acertada para enfrentar la amenaza de una guerra cibernética. Siendo consecuente con esta necesidad, el Teniente General Fadok y el Dr. Raines nos ofrecen su visión sobre la guerra cibernética en el artículo titulado "Encaminándonos hacia el éxito en la misión cibernética de la Fuerza Aérea" y presentan además los programas existentes y los planes futuros de la Universidad del Aire, respecto a la preparación académica de nuestros líderes para luchar exitosamente en futuros conflictos que abarquen todos los ámbitos posibles, tales como: agua, tierra, cielo, espacio, y ahora el ciberespacio.

Por otro lado, no podemos omitir las consideraciones más difíciles que enfrentan nuestros líderes, tanto civiles como militares, y que se originan en las diferencias ideológicas entre la ética y la ley relacionadas con la cibernética aplicada a las operaciones, ya que éstas pueden causar destrucción masiva por estar regidas por leyes internacionales de la guerra –aunque aún no muy claras en relación con la guerra cibernética. En su ensayo titulado "La intersección de la ley y la ética en la ciberguerra" el General Dunlap puntualiza algunos temas que ilustran cómo los conceptos legales y éticos se cruzan en el ámbito del ciberespacio, y concluye que los actuales principios básicos de la ley de los conflictos armados son suficientes para hacer frente a los temas más importantes de la guerra cibernética.

La propagación del gusano cibernético conocido como *Stuxnet* marca el primer episodio de una nueva era en los anales de la guerra moderna, similar al primer uso de armas nucleares. Su difusión debe hacernos tomar conciencia sobre la necesidad de una adecuada preparación que impida que las naciones se enfrenten a una guerra en el ciberespacio sin antes despejar muchos interrogantes relacionados con la ciberseguridad y las leyes cibernéticas. Stuxnet, el arma cibernética más sofisticada del mundo hasta el momento, fue un programa de sabotaje masivo de secreto a alto nivel dirigido a las instalaciones de enriquecimiento de uranio de la planta Natanz, Irán, en donde se destruyeron alrededor de 1000 de las 5000 centrífugas iraníes y con el que frenaron el programa nuclear de Irán. El gusano Stuxnex fue increíblemente complicado y sofisticado como lo detalla mucho mejor el Mayor Shakarian en su artículo "Stuxnet: Revolución de ciberguerra en los asuntos militares."

Los ataques contra los sistemas de información e infraestructura tanto del gobierno como de las organizaciones privadas y gobiernos extranjeros, podrían derivarse en un futuro no muy lejano, en un conflicto militar a gran escala. El peligro más grande de un ataque cibernético proviene de la ca-

rencia de un mecanismo internacional de regulación de las armas cibernéticas, incrementado por la dificultad de determinar con seguridad y exactitud el origen o intento de un ataque y la posibilidad de que un país erróneamente pueda actuar en contra de otro país que no hubiera tenido participación directa o indirecta en el ataque. El Dr. Crosston sostiene en su escrito "El mundo se ha vuelto "ciberloco", que una política de disuasión equilibrada y clara sería mucho más efectiva y deseable que una política solo de disuasión defensiva. Crosston concluye, que frente a una doctrina de destrucción cibernética mutuamente asegurada, basada en un temor mutuamente compartido de una amenaza ofensiva, los adversarios perderían el incentivo de iniciar un ataque.

Para un mayor entendimiento acerca de los aspectos concernientes a la evolución, retos, y lecciones aprendidas del Poderío Aéreo y los que actualmente presenta el nuevo ámbito ciberespacial, es necesario que repasemos la historia del viejo y nuevo ámbito. Al respecto, el Teniente Lee en su artículo titulado "Los años interinos del ciberespacio" analiza las ventajas, similitudes y diferencias del poder de la cibernética y se pronuncia sobre los ataques cibernéticos más recientes, concluyendo que para poder tener éxito en el ámbito ciberespacial, el DoD y los socios civiles deben hacer mayor énfasis en la educación y el entrenamiento de la próxima generación de líderes cibernéticos.

Para ilustración de todos en esta materia, es conveniente tener en cuenta que este año se ha realizado un número sin precedentes de eventos catalogados bajo el tema de la guerra cibernética. Nuestra base industrial ha sido el objetivo de muchos de estos "ciberataques" mostrándose vulnerable a los ataques de espionaje o de robo de propiedad intelectual por parte de gobiernos y delincuentes cibernéticos. Pese al esfuerzo continuado de la política de ciberseguridad de Estados Unidos para responder a estos desafíos, encontramos aún intervalos críticos y vitales para la seguridad industrial y nacional. En su escrito titulado "Preparación de la inteligencia del entorno de información y comunicaciones" el Sr. Carr propone una función que ha llamado Preparación de Inteligencia del Entorno de Información y Comunicaciones (IPICE), cuya implementación mejoraría la táctica defensiva, por parte de entidades tanto comerciales como gubernamentales.

Continuado la reflexión en esa misma dirección Chang y Granger, autores de "La Guerra en el Ámbito Cibernético", aciertan cuando afirman que para diseñar exitosamente una estrategia en el nuevo campo de batalla, es necesario comprender y asimilar el nuevo concepto cibernético, sin descuidar nuestras vulnerabilidades cibernéticas, facilitando para ello el intercambio de información y los mecanismos de coordinación de la seguridad e involucrando en la educación a todos los actores militares y civiles.

Finalmente, agotamos la cobertura del ciberespacio y la guerra cibernética con la presentación de dos interesantes artículos escritos uno por el Teniente Coronel (Ret) Jeffey Hukill y el otro por el Capitán John Cobb. De acuerdo a su presentación, Coob en su artículo "Virtualmente masivo: comprendiendo la concentración y el poder de combate en la ciberguerra", hace un paralelismo entre el concepto del efecto de un ataque masivo cibernético sumamente preciso y concentrado, lanzado por medio de un gran número de paquetes de bitios o de un gran número de viruses liberados simultáneamente y el efecto de varios ataques devastadores lanzados desde cualquier parte del mundo, por un puñado de agresores. A su vez Hukill, en su escrito titulado "Pautas para diseñar estructuras adaptativas de mando y control (C2) para las Operaciones Ciberespaciales", basado en un estudio sobre el C2 ordenado por el General Mark Welch, Jefe del Estado Mayor de la Fuerza Aérea, y en que él fue un participante, sostiene que el enfoque en operaciones ciberespaciales exige un C2 adaptable apoyado en la descentralización de decisiones, intercambio de información e interacción entre comandantes y planas mayores al nivel de organización más bajo capaz de integrar recursos.

Teniente Coronel Luis F. Fuentes, USAF-Retirado
Editor, *Air & Space Power Journal—Español*

Encaminándonos hacia el Éxito en la Misión Cibernética de la Fuerza Aérea

Aprovechándonos de nuestro legado para forjar nuestro futuro

Teniente General David S. Fadok, USAF
Dr. Richard A. Raines

HACE TAN SOLO unas décadas, considerábamos que el poderío aéreo era principalmente tripulaciones calificadas piloteando aeronaves de combate y lanzando bombas sobre blancos. Hoy significa mucho más. Por ejemplo, 16 de los 18 hombres del aire cuyos logros heroicos se destacan en la última edición de *Portraits in Courage* del Jefe de Estado Mayor de la Fuerza Aérea no son aviadores y 15 son personal alistado.[1] Sin embargo, todos ellos suministraron poderío aéreo en las líneas del frente de combate, ya sea conduciendo convoyes, deshaciéndose de pertrechos explosivos, ofreciendo seguridad fuera de los cuarteles, desempeñándose como instructores de las fuerzas afganas e iraquíes u ordenando ataques de precisión desde aeronaves en vuelo. De hecho, en la versión más reciente de nuestro documento de doctrina culminante, AFDD 1, *Air Force Basic Doctrine, Organization, and Command* (Doctrina básica, organización y mando de la Fuerza Aérea), se reconoce esta naturaleza cambiante del poderío aéreo al definirlo como "la capacidad de proyectar poder militar o influencia a través del control y utilización del aire, espacio y ciberespacio para lograr objetivos estratégicos, operacionales y tácticos".[2]

El General de Fuerza Aérea, Henry "Hap" Arnold, ofreció asesoramiento sabio cuando expresó que "debemos pensar en términos del mañana".[3] Gran parte del poderío aéreo del mañana tendrá lugar en el ámbito operacional emergente del ciberespacio. El adelanto rápido en las tecnologías de computadoras y comunicaciones, al igual que el vínculo estrecho del "ámbito digital" con las operaciones físicas, hacen que el ciberespacio sea cada vez más importante para el éxito militar. Los retos planteados por el ciberespacio reflejan su naturaleza global, las soberanías políticas que trasciende y el hecho de que las operaciones ocurren a la velocidad de la luz. Estados Unidos, por mucha imaginación que pongamos, no puede disfrutar en el ciberespacio la ventaja clara y asimétrica que disfrutamos en los ámbitos de la tierra, mar, aire y espacio.

Por medio de correos electrónicos, sitios web sociales y otras formas de comunicación electrónica compartimos información instantáneamente a lo largo de la red informática mundial. A pesar de que esta capacidad ha disminuido sustancialmente, el tiempo necesario para tomar decisiones ha aumentado nuestra dependencia en los sistemas de comunicación. La información a través del ciberespacio a velocidades extremadamente rápidas y, a diferencia de los ataques cinéticos tradicionales, los ataques ciberespaciales pueden comenzar, detenerse y cambiar completamente en cuestión de segundos…sin avisar. Por consiguiente, nuestros hombres del aire deben estar preparados para reaccionar de inmediato—y aquí radica el reto.

Las proverbiales "computadora portátil y conexión a la *Internet*" proveen una entrada a un costo extremadamente bajo al juego de la explotación del ciberespacio. Como resultado, el adversario ciberespacial moderno es, y continuará siendo, sumamente ágil e innovador. Nos esforzamos por crear pautas y políticas para operaciones ciberespaciales rápidas y precisas, pero los adversarios han resultado ser expertos en crear métodos nuevos y creativos para explotar y atacar el ciberespacio, muchas veces utilizando contra nosotros las restricciones de nuestro propio sistema jurídico. El entorno cibernético cambia tan rápidamente que alguien puede alegar que puede que nuestras directrices sean obsoletas cuando finalmente se aprueben. Además, enfrentamos el verdadero peligro de que no podemos elaborar doctrina y tácticas lo suficientemente rápido como para seguir el ritmo de las amenazas operacionales cambiantes en el ciberespacio.

Por años, el ciberespionaje y la explotación han existido a una escala global. No limitadas a las naciones estados, estas acciones también han involucrado actores de la industria, el crimen organizado, grupos activistas y terroristas. Obviamente, los motivos varían según el grupo, pero en la mayoría de los casos, el ciberespionaje y la explotación son impulsados por ganancias en finanzas y la propiedad intelectual. En la Fuerza Aérea estamos preocupados por proteger nuestros recursos críticos y la propiedad intelectual al igual que perseguir blancos mediante medios cibernéticos según lo permiten el Código de Estados Unidos y las autoridades competentes. Para ello, debemos crear los líderes de pensamiento, la fuerza laboral cibernética, conceptos operacionales y las capacidades tecnológicas para poder ejecutar con éxito durante tiempos de conflictos cibernéticos o ciberguerra.

En los debates en curso se trata lo que constituye la ciberguerra y si estamos o no en guerra en el ciberespacio. En este artículo no se tratan esos temas; en cambio, se sugiere cómo la Fuerza Aérea y la Universidad del Aire deben seguir adelante para estar al frente y apoyar las necesidades de seguridad cibernética de nuestra nación. Por lo tanto, se enfoca en lecciones análogas aprendidas de la historia, nuestra postura en la actualidad y lo que necesita ser, y los planes para llegar ahí con respecto a nuestras capacidades ciberespaciales.

Nuestro legado: La escuela táctica del cuerpo aéreo

Durante los años entre la Primera y la Segunda Guerra Mundial, grandes pensadores se reunieron en la Escuela Táctica del Cuerpo Aéreo (ACTS, por sus siglas en inglés), la progenitora de la Universidad del Aire. ACTS reunió algunas de las personas más inteligentes disponibles

para definir, crear y demostrar la mejor manera para controlar y explotar el ámbito nuevo del espacio aéreo. Estos aviadores pioneros emplearon sus talentos colectivos para impulsar el desarrollo de tecnologías necesarias para implementar las capacidades de poderío aéreo. Desde los pizarrones en los salones de clase hasta la práctica en los cielos, ACTS ofrecía un entorno de aprendizaje para el desarrollo inicial del poderío aéreo y un campo de prueba para el perfeccionamiento de los conceptos y tecnologías propuestas. Los estudiantes se convirtieron en instructores y viceversa, compartiendo ideas y conceptos por casi 20 años. Al promover el pensamiento de poderío aéreo, ellos ejercieron una gran influencia sobre cómo condujimos las operaciones aéreas durante la Segunda Guerra Mundial.

Uno de esos grandes pensadores, el General Muir Fairchild, se convertiría en el primer comandante de la Universidad del Aire. Cuando sus puertas abrieron en 1946, él decidió que esta nueva institución adoptaría el lema "ACTS: *Proficimus More Irretenti* (Progresamos sin ser obstaculizados por las costumbres). Desde los inicios de ACTS, la Fuerza Aérea ha continuado como líder del adelanto de los conceptos y capacidades del poderío aéreo mediante métodos nuevos e innovadores para mejorar nuestra eficacia en el ámbito aéreo. Estos éxitos podemos atribuirlos en gran parte a los talentosos e ingeniosos aviadores, hombres y mujeres, que encontraron soluciones a los problemas.

Solucionando los retos cibernéticos de hoy para la fuerza aérea del mañana

Mucho ha cambiado desde que ACTS estableció las bases del poderío aéreo. Ahora nos encontramos en un entorno global, de acceso instantáneo a la información donde el conflicto puede comenzar en un abrir y cerrar de ojos sin pruebas aparentes. El ciberespacio ha creado un ámbito en el que el conflicto puede pasar desapercibido y sin atribuciones. Como se mencionó anteriormente, el ámbito ciberespacial admite jugadores a un precio bajo de entrada, muchos de ellos sumamente capacitados y hábiles. En vista de la rapidez de los eventos ciberespaciales, la protección y el control de la información para garantizar el éxito de nuestra misión son de suma importancia. La exfiltración de información de nuestros recursos cibernéticos, al igual que ataques a nuestros recursos críticos, exige que desarrollemos rápidamente los medios para contrarrestar esas acciones adversarias y que a la vez elaboremos y maduremos nuestras capacidades en las operaciones cibernéticas de ofensiva. La Fuerza Aérea y el Departamento de Defensa (DoD, por sus siglas en inglés) deben contar con el liderazgo y una fuerza laboral capaz de comprender cómo el ciberespacio se puede y se usará contra nosotros, y cómo lo podemos utilizar para entregar opciones soberanas a nuestros líderes políticos nacionales. Debemos avanzar, crear, comprobar y desplazar esas opciones a nuestros guerreros. La educación, adiestramiento, investigación, pruebas, evaluación y desarrollo deben recalcar la seguridad de la misión, indistintamente del ámbito en el que se opera.

Actualmente, el ciberespacio de la Fuerza Aérea debe tomar en cuenta dos tareas: crear y sostener una fuerza laboral para cumplir con los problemas del mañana, y crear conceptos y capacidades para contrarrestar al igual que mitigar los esfuerzos de nuestros adversarios expertos. La primera tarea resultara difícil, impulsada principalmente por presupuestos de defensa reducidos y compromisos con nuestras áreas de misión básicas.

Las operaciones ciberespaciales continuarán retándonos con incógnitas y amenazas que surgen rápidamente de complejidades cada vez mayores. La excelencia cibernética debe basarse en la *educación e investigación* cibernética superior. Las operaciones a la velocidad de la luz exigen un desarrollo rápido y eficaz y el empleo de conceptos operacionales y capacidades tecnológicas para ayudar a disminuir las demandas en el guerrero/operador cibernético. Los conceptos y las

capacidades deben cumplir con las necesidades de la misión del comandante y garantizar operaciones eficaces con un nivel de certeza sumamente elevado.

El camino a seguir: La escuela táctica del cuerpo aéreo ciberespacial

Últimamente, hemos escuchado varias referencias a la noción de que, en términos ciberespaciales, nos encontramos nuevamente en los años entre las guerras. Si esto es cierto, quizás es hora de establecer una ACTS "Cibernética" (C-ACTS, por sus siglas en inglés), donde podamos reunir pensadores estratégicos importantes de todos los participantes principales en el gobierno (tanto dentro como fuera de la Universidad del Aire) y del sector privado con el propósito de identificar ideas en nuestro ámbito más nuevo del ciberespacio. Una C-ACTS exitosa lograría lo siguiente:

- Enlazaría y se aprovecharía de talentos y recursos de la educación, ciencia y tecnología, al igual que de las comunidades operacionales.
- Albergar e interactuar de cerca con innovadores de las comunidades mencionadas anteriormente quienes poseen credenciales excelentes en el mundo académico, investigación y desarrollo y experiencia.
- Ofrecer un foro para la creatividad, innovación e intercambio, no solo para cultivar ideas sino también para crear y probar rápidamente los prototipos y poner en funcionamiento los sistemas.
- Unir fuertemente las innovaciones y el desarrollo tecnológico con la evolución de las tácticas y doctrina.
- Mezclar la educación moderna con el aprendizaje interactivo (o sea, "echar a volar" las ideas cibernéticas).
- Integrar estrechamente los desarrollos cibernéticos en los requerimientos generales de la seguridad de la misión para ofrecer cursos de acción no cinéticos eficaces al encargado de tomar decisiones.

En vista de que vivimos y operamos en un entorno descentralizado, no debemos alojar una C-ACTS exclusivamente dentro de la estructura de una sola organización. Contamos con muchas organizaciones duchas en cibernética que podemos y debemos aprovechar. A nivel nacional, la Agencia Central de Inteligencia, DOD, Departamento de Energía, Departamento de Seguridad Interna y la Agencia Federal de Investigación poseen operaciones cibernéticas intrínsecas y capacidades de desarrollo con responsabilidades cibernéticas singulares pero que a veces coinciden. Dentro del DOD, el Comando Cibernético de EE.UU., la Agencia de Seguridad Nacional y cada uno de los servicios armados cuentan con operaciones cibernéticas decretadas para llevar a cabo operaciones bajo la autoridad de los Títulos 10, 18, 32 y 50. Las academias de los servicios del DOD pueden ofrecer educación cibernética básica, mientras que en instituciones tales como el Instituto de Tecnología de la Fuerza Aérea y la Escuela de Posgrado de la Armada ofrecen educación cibernética continua, avanzada y a nivel de posgrado. La Fuerza Aérea y la Armada ostentan poseer extensas capacidades a través de sus Comandos de Educación y Adiestramiento de la Fuerza Aérea y las Fuerzas Cibernéticas, respectivamente. El Ejército y el Cuerpo de Infantería de Marina se aprovechan de las capacidades existentes de educación y adiestramiento de los servicios hermanos a la vez que crean capacidades específicas a la misión mediante sus propios Comandos Cibernéticos. Además, las capacidades de investigación y desarrollo radican en

los laboratorios de investigación de cada uno de los servicios armados. También la industria y el ámbito académico desempeñan papeles importantes en el desarrollo del capital cibernético tanto humano como tecnológico.

La Universidad del Aire está avanzando con el concepto C-ACTS para crear un entorno mejor para compartir información y fomentar ideas. Basándonos en asociaciones existentes y creando nuevas según sea apropiado, buscamos colaborar de cerca con nuestros socios operacionales en la Vigésima Cuarta Fuerza Aérea y nuestros socios de investigación y desarrollo en el Laboratorio de Investigaciones de la Fuerza Aérea para garantizar el rendimiento de la inversión en actividades cibernéticas. A lo largo de la Universidad del Aire, contamos con recursos que apoyan la C-ACTS. El Centro para Investigaciones Cibernéticas, designado como el Centro de Excelencia Técnico Ciberespacial de la Fuerza Aérea y ubicado en el Instituto de Tecnología de la Fuerza Aérea, está encargado de coordinar los esfuerzos C-ACTS. Esta tarea complementa aquellas emitidas en el 2008 por el Secretario de la Fuerza Aérea para que el Centro de Investigaciones Ciberespaciales "estableciera los vínculos" con respecto a quién hace qué en la educación, investigación y desarrollo ciberespacial.

Reflexiones finales

La Fuerza Aérea está llevando a cabo operaciones durante un tiempo de cambio dinámico. Las operaciones en y a través del ciberespacio exigirán tácticas, técnicas y procedimientos nuevos al igual que mentalidades de liderazgo nuevo para contrarrestar las acciones del enemigo. Debemos crear rápidamente y mantener la siguiente generación de líderes y guerreros cibernéticos que enfrentarán una era de información compleja y el ámbito ciberespacial de las operaciones. Nosotros en la Universidad del Aire enfrentaremos el reto de crear y dotar a nuestros líderes y guerreros cibernéticos con el conocimiento y la experiencia que necesitan para garantizar la misión y el éxito operacional. Tal como el General Arnold aconsejó, continuaremos pensando en términos del mañana, buscando un progreso sin ser obstaculizados por las costumbres en el ámbito operacional más nuevo del ciberespacio. ❑

Notas

1. Department of the Air Force, *Portraits in Courage: Airmen in the Fight*, vol. 6 (Washington, DC: Department of the Air Force, 2011), http://www.af.mil/shared/media/document/AFD-110921-035.pdf.

2. Air Force Doctrine Document 1, *Air Force Basic Doctrine, Organization, and Command*, 14 de octubre de 2011, 11, http://www.e-publishing.af.mil/shared/media/epubs/afdd1.pdf.

3. H. H. Arnold, *Global Mission* (Misión global) (New York: Harper, 1949), 615.

El Teniente General David S. Fadok, USAF (USAFA; MA, Oxford University; MAAS, School of Advanced Airpower Studies, Air University) es comandante y presidente de la Universidad del Aire, Base Aérea Maxwell, Alabama. Él ofrece el espectro completo de educación, investigación y divulgación en cada nivel mediante la educación militar profesional, la educación continua profesional y el otorgamiento de títulos académicos. El General está al frente del centro intelectual y de liderazgo de la Fuerza Aérea de EE.UU., de donde anualmente egresan más de 50.000 oficiales residentes y 120.000 oficiales no residentes, al igual que personal alistado y civil. Además, el General es responsable del nombramiento de oficiales mediante la Escuela de Capacitación para Oficiales y el Cuerpo de Adiestramiento de Oficiales de la Reserva. Anteriormente, se desempeñó en calidad de comandante del Centro Curtis E. LeMay para el Desarrollo de la Doctrina y la Educación y en calidad de Vicecomandante de la Universidad del Aire. El General Fadok culminó sus estudios de posgrado como becado de Rhodes antes de obtener sus alas de piloto en 1985. Un piloto comandante con más de 4.000 horas de vuelo, anteriormente se desempeñó en calidad de comandante a los niveles de escuadrón, grupo y ala. Voló en misiones de combate y de apoyo de combate en las operaciones Causa Justa, Escudo en el Desierto, Tormenta en el Desierto y *Southern Watch*. En calidad de egresado distinguido de la Escuela para Oficiales de Escuadrón y de la Escuela Superior de Comando y Estado Mayor de la Fuerza Aérea, al igual que Becado de la Defensa Nacional, en 1988 el General Fadok recibió el Premio de Liderazgo del Secretario de la Fuerza Aérea.

El Dr. Richard A. Raines (BSEE, Florida State University; MS, Air Force Institute of Technology; PhD, Virginia Tech) es el director del Centro de Investigaciones Ciberespaciales de la Fuerza Aérea, presidente de Transformación de la Fuerza del Departamento de Defensa y profesor de ingeniería eléctrica en el Instituto de Tecnología de la Fuerza Aérea, Base Aérea Wright-Patterson, Ohio. El Dr. Raines se desempeña en calidad de asesor técnico para numerosas organizaciones del gobierno de Estados Unidos y grupos de trabajo federales de seguridad cibernética. Ha escrito más de 150 publicaciones técnicas y estratégicas sobre comunicaciones y ciberseguridad. En el 2007 fue iniciado en la Asociación *Old Crows' Hall of Fame* por sus aportes a las operaciones de información y en el 2008 recibió el premio del año al Educador de Ciencia y Energía de la Fuerza Aérea. El Dr. Raines es miembro principal del Instituto de Ingenieros Electricistas y Electrónicos.

La Intersección de la Ley y la Ética en la Ciberguerra

Reflexiones

MAYOR GENERAL CHARLES J. DUNLAP, JR., USAF–RET.

POCOS TEMAS de seguridad han acaparado la atención del público como lo ha hecho el espectro de la ciberguerra. En un editorial reciente, el Presidente Obama advierte que la "ciberamenaza a nuestra nación es uno de los desafíos económicos y de seguridad nacional más graves que enfrentamos".[1] Esto, a su vez, ha planteado numerosas interrogantes sobre los parámetros legales de las ciberoperaciones, incluyendo las reglas aplicables a la ciberguerra actual.[2]

Paralelamente al creciente interés en los aspectos legales de la ciberguerra hay un número creciente de interrogantes que se centran en la dimensión ética. Éste es un aspecto importante para cualquier esfuerzo militar que apenas está surgiendo con respecto a las ciberoperaciones.[3] La creciente preocupación acerca de los aspectos éticos de las actividades en el ciberespacio dio lugar a una conferencia dedicada al tema auspiciada por la Academia Naval de los Estados Unidos en la primavera de 2012.[4] Y más recientemente, apareció un artículo en la revista *The Atlantic* titulado *Is it Possible to Wage a Just Cyberwar? (¿Es posible luchar una ciberguerra justa?)* que discute varios temas intrigantes.[5]

El objetivo de este corto ensayo es reflexionar sobre algunos temas que ilustran cómo los temas legales y éticos se cruzan en el ámbito del ciberespacio. Tal intersección no debe ser muy

sorprendente, insiste el historiador Geoffrey Best, "Nunca se debe olvidar que la ley de la guerra, dondequiera que haya comenzado, comenzó principalmente como un asunto de religión y ética . . . "Comenzó en ética" dice Best "y desde entonces ha mantenido un pie en la ética."[6] Es vital entender esa relación para entender el alcance global de las responsabilidades de un cibergue-rrero en el siglo 21.

Ley y ética

¿Qué relación hay entre ley y ética? Ciertamente el cumplimiento de la ley es una responsabilidad ética de línea de referencia, pero es solo eso: una línea de referencia. En la edición de marzo de 2012 del *Armed Forces Journal*[7] el Teniente de la Marina de los Estados Unidos Gabriel Bradley señala que "La ley del conflicto armado establece estándares mínimos" y prosigue afirmando persuasivamente que es esencial inculcar valores morales y éticos individuales e institucionales–un sentido de honor si se quiere–para asegurar el cumplimiento *real* de la ley.[8] Y ciertamente tiene razón cuando cita la observación de Christopher Coker que "las leyes pueden reafirmar el espíritu del guerrero; pero no la pueden reemplazar". [9]

Por supuesto, incluso determinar la línea de referencia–es decir, la ley–no siempre es fácil en las operaciones del siglo 21, pero en especial en relación a las ciber-actividades. Entre las varias razones para esto está el hecho que gran parte de la ley del conflicto armado fue diseñada para abordar conflictos librados principalmente con armas cinéticas. No obstante, en la opinión de este escritor, la ley existente puede aplicarse fácilmente a las ciberoperaciones. Esto quizás nos lleva al primer tema relacionado a la intersección de ley, ética y ciberoperaciones, es decir, la noción escuchada algunas veces de que el ciberespacio es un dominio tan nuevo que ninguna ley existente podría–o incluso *debería*–aplicarse a operaciones militares en él.

Simplemente esto no es cierto. La mayor parte de la ley del conflicto armado no es específica de un dominio. En este sentido considérese un proyecto reciente del Programa de Harvard sobre Política Humanitaria e Investigación de Conflictos para escribir un manual específico sobre la ley internacional aplicable a la guerra aérea y con misiles.[10] Produjo un volumen útil, pero relativamente débil ya que se encontró que había una parte de ley comparativamente modesta que podría considerarse única para los dominios del aire o del espacio. Lo mismo puede decirse sobre el dominio del ciberespacio, para incluir consideraciones éticas.[11]

Además, lo que algunas veces se disfraza como un problema legal en ciberoperaciones a menudo es más un tema técnico o una cuestión de política–*no* un problema legal auténtico. El muy publicitado asunto de lo que constituye el proverbial "acto de guerra" en el dominio del ciberespacio es un buen ejemplo. Aunque la frase "acto de guerra" es un término político, no un axioma legal, *hay* frases como "uso de fuerza" y "ataque armado" que *sí tienen* significado legal, y se podrían relacionar con un *incidente bélico* en términos de una respuesta contundente.[12]

La interpretación de tales expresiones en el ámbito del ciberespacio, de hecho, se puede resolver con arreglo a la ley, sí–y, sólo "sí" - la tecnología puede proporcionar datos adecuados en relación, por ejemplo, al daño actual causado por el supuesto "ataque", y también suficiente información sobre quién lo hizo. Por supuesto, la ausencia de datos de asignación de atribución (autoría)–técnicamente muy difícil de obtener en el ámbito del ciberespacio–puede ser una barrera legal y ética definitiva para una respuesta contundente. Esto puede ser frustrante cuando la gente quiere "hacer algo" en respuesta a un ciber-incidente, aunque no es excesivo que la ley–*y la ética*–demanden información confiable sobre quién podría ser responsable antes de lanzar un contrataque de alguna clase.

El hecho que, desde el punto de vista tecnológico, determinar la autoría sea una tarea difícil *no* es un problema para los abogados o los éticos, sino algo que deben resolver los tecnólogos. Es interesante por eso que los autores del artículo de *The Atlantic* antes referidos afirmen, en rela-

ción al uso supuesto de un arma cibernética (Stuxnet) contra las instalaciones de desarrollo nuclear de Irán, que "la falta de atribución de Stuxnet plantea inquietudes éticas porque negó a Irán la capacidad de contraatacar, fomentando un comportamiento más extremo".[13]

Aparte de la cuestión de si habría necesariamente una base legal o moral para que Irán contraataque como resultado de la supuesta operación Stuxnet,[14] es interesante que los autores del documento de *The Atlantic* digan que "para que la atribución funcione, necesitemos convenios internacionales".[15] Estos incluirían, alegan, acuerdos que "los ciberataques deberían llevar una firma digital de la organización atacante" y que se podrían usar ciertos protocolos de red para "facilitar la atribución".[16]

Aunque posiblemente la mayoría de expertos dirían que la ley actual no requiere que se facilite la atribución del acto cibernético,[17] los autores del artículo de *The Atlantic* no obstante abogan por "mejoras en el monitoreo internacional para rastrear el origen de los ataques" y parecen creer que "los incentivos económicos, como la amenaza de sanciones comerciales, pueden hacer que tales acuerdos sean deseables".[18] Hay en estas propuestas mucho para discrepar, pero se debe elogiar a los autores por al menos iniciar el diálogo de cómo se puede abordar una de las cuestiones legales y morales más desconcertantes de la ciberguerra.

Como en el caso de la atribución, los problemas tecnológicos–no la ley, *por sí misma*–son también el aspecto más difícil de fijar como objetivo las armas cibernéticas. Los principios fundamentales legales y éticos de distinción y proporcionalidad[19] requieren datos técnicos que proporcionen información a los elementos decisorios sobre quién estaría afectado por una técnica particular, y en qué medida. El que esto sea técnicamente difícil de hacer no es un problema legal o ético, es un problema científico. De hecho, se puede decir que una de las capacidades más necesarias en el mundo de las ciberoperaciones es la capacidad de modelar efectos con precisión confiable para proporcionar a los elementos decisorios -para no mencionar abogados o éticos- la clase de información realmente esencial para lograr juicios razonados acerca del empleo de una ciber-metodología.

¿Ponen los valores legales y éticos dificultades indebidas a los ciberguerreros?

Por encima de las dudas sobre la aplicación de regímenes legales y costumbres éticas para un ciber-escenario particular, está la cuestión más amplia de si se debería aplicar restricciones. Más específicamente, algunos creen que los esfuerzos para aplicar la ley dificultarán tanto los ciberesfuerzos estadounidenses que se pondrá en peligro la seguridad nacional. Este asunto más bien sorprendente está al centro de un debate serio en el que Stewart Baker y su redactor se empeñaron bajo los auspicios de la Asociación Americana de Abogados.[20]

Solo como contexto, el Sr. Baker es un reconocido abogado del cabinete legal Steptoe & Johnson de Washington, y ha servido previamente en el gobierno como consejero general de la Agencia de Seguridad Nacional, y también como Secretario Asistente de Política en el Departamento de Seguridad Nacional de los Estados Unidos. Comienza su polémica de esta manera:

> Los abogados no ganan guerras. ¿Pero pueden perder una guerra? Probablemente lo sepamos pronto. Abogados de diferentes ramas del gobierno han planteado tantas cuestiones legales sensacionales acerca de la ciberguerra que han dejado a nuestros militares incapaces de luchar, o incluso planear para una guerra en el ciberespacio.[21]

El Sr. Baker afirma además que los intentos de "imponer límites en la ciberguerra" están, en su opinión, "condenados al fracaso".[22] Entre los aspectos más preocupantes de su argumento se encuentra uno ético de primer orden que señala la devastación causada por la guerra aérea de la Segunda Guerra Mundial y referencia la declaración del ex Primer Ministro Británico Stanley

Baldwin en 1930 que en la guerra aérea "la única defensa es la ofensa, lo que significa que hay que matar más mujeres y niños más rápido que el enemigo si se quiere salvar uno mismo".[23]

El Sr. Baker prosigue su aparente *apoyo* del concepto de "matar más mujeres y niños más rápido" del Sr. Baldwin afirmando que si "deseamos defendernos contra los horrores de la ciberguerra, primero debemos encararlos, *con el candor de un Stanley Baldwin.*"[24] Solo después de desarrollar una estrategia de ciberguerra tan encasillada consideraría el Sr. Baker apropiado "pedir que los abogados" den sus "ideas".[25]

Queda fuera del alcance de este ensayo repetir totalmente mi respuesta (aunque el título -¿Ciberguerra ilegal? No si desea ganar"–puede ser indicativo de su contenido), pero bastará decir que es muy importante en la ciberguerra (como en cualquier operación militar) anclar los "límites" cuando sea posible no solo en la ley o la ética, *per se*, sino también en la lógica práctica de la lucha de guerra. En el caso del ciberespacio, esto no es particularmente difícil de hacer, especialmente si los guerreros actuales no perciben una asimetría entre lo que la ley y la ética pueden requerir, y lo que creen que necesitan para cumplir su misión.

No obstante la afirmación del Sr. Baker de que las maquinaciones legales han dejado a las fuerzas armadas "incapaces de luchar, o incluso planear para una guerra en el ciberespacio", el General de la Fuerza Aérea Robert Kehler, comandante del Comando Estratégico de los Estados Unidos cuya organización subordinada el Cibercomando Estadounidense es el principal proponente de planeamiento y operaciones ciberespaciales militares, parece discrepar. En noviembre de 2011 declaró que "no creía que necesitemos nuevas autoridades explícitas para realizar operaciones ofensivas de cualquier clase". [26] Además, dijo que "no pensaba que hubiera ningún problema sobre autoridad para realizar [ciber] operaciones".[27] En otras palabras, los *combatientes de guerra* aparentemente no ven incompatibilidad entre las restricciones legales y éticas y su capacidad de "planear efectivamente para una guerra en el ciberespacio".

El respeto del estado de derecho es especialmente importante en el ámbito ciberespacial porque casi todos los expertos concuerdan en que la confrontación de la amenaza requiere de la cooperación de otros países a fin de rastrear y neutralizar las ciberamenazas -en tiempo de paz o de guerra.[28] Las naciones vitales para este esfuerzo, incluyendo especialmente las grandes democracias del mundo, indudablemente no estarían dispuestas a cooperar con ningún país que rechace límites en las operaciones militares, ciberespaciales o de cualquier otra forma. Los profesores Michael Riesman y Chris T. Antoniou señalan en su libro de 1994, *The Laws of War (Las leyes de la guerra)*:

> En las democracias populares modernas, incluso un conflicto armado limitado requiere una base importante de apoyo público. Ese apoyo puede reducirse e incluso revertirse rápidamente, sin importar lo digno que sea el objetivo político, *si la gente cree que la guerra se está llevando a cabo de una manera injusta, inhumana o indigna.*[29]

Sin embargo, un rechazo del concepto del Sr. Baker para la ciberguerra no sugiere que las preocupaciones éticas y legales acerca de la ciberguerra se pueden desestimar. Por ejemplo, uno de los temas más serios tiene que ver con el papel de los civiles en las ciberoperaciones.

Ciberguerreros civiles

Casi se deja de mencionar que hay enorme especialización ciberespacial en la comunidad civil, y que es esencial que las fuerzas armadas tengan acceso a ella. Dicho esto, la extensión de tal acceso, y precisamente lo que significa—o *debe significar*— el acceso, es propiamente el tema de escrutinio legal y ético.

Los fundamentos no son difíciles. Para disfrutar del privilegio del combatiente, es decir una "licencia"–por así decirlo- para emprender actos destructivos legales contra la persona o propiedad del enemigo sin temor de enjuiciamiento, hay que ser miembro de las fuerzas armadas

propiamente constituidas de un beligerante en un conflicto armado.[30] A menudo esto se ha confundido con la creencia de que un civil no puede participar directamente en las hostilidades. En realidad, los civiles pueden hacerlo sin necesariamente cometer un crimen de guerra, pero hay consecuencias.

Entre las principales se encuentra el hecho de que si caen en manos del enemigo, podrían quedar sujetos a la ley criminal doméstica del enemigo por actos que, si los realizara un miembro de los militares oponentes, quedarían exentos de acusación. Lo que es más, según la ley de guerra, los civiles pueden ser objetivos adecuados -cinética o ciberespacialmente- cuando participan directamente en las hostilidades. En el contexto del ciberespacio, se debe entender que incluso el Comité Internacional de la Cruz Roja explícitamente utiliza como ejemplos de participación directa actos que son la clase de cosas que se esperaría del ciberguerrero, es decir, "Interferir electrónicamente con redes de computadoras militares (ataques de redes de computadoras) y transmitir inteligencia de selección táctica de objetivos para un ataque específico".[31]

¿Qué significa todo esto desde una perspectiva ética? Por un lado es esencial que los civiles entiendan las consecuencias potenciales, especialmente cuando el civil está lejos del sitio de trabajo, como en casa con su familia. Aunque hay debate en la comunidad internacional sobre lo que es necesario para que un civil sea considerado objetivo en la misma base que un miembro de las fuerzas armadas, el Comité Internacional de la Cruz Roja concuerda en que los civiles que asuman una "función de combate continua" (en oposición a simplemente "participar en hostilidades de forma espontánea, esporádica o desorganizada") pueden ser seleccionados como objetivos en una base similar a los miembros de las fuerzas armadas.[32]

Miembros de las fuerzas armadas–junto con los civiles que regularmente participan en una "función de combate continua" como ataques a redes de computadoras–pueden ser atacados con cualquier arma legal en cualquier lugar y en cualquier momento, independientemente de si en ese momento en particular el individuo presenta una amenaza inminente o esté realizando una función militar. Esto quiere decir, por ejemplo, que un ciberguerrero civil que participa regularmente en operaciones de ataque a redes de computadoras podría ser legítimamente atacado por un beligerante (no terroristas) en su hogar en un suburbio de Washington. Y no solo con ciber-armas; se puede usar cualquier arma legal si cumple con la ley de la guerra.

Por consiguiente, si el civil es suficientemente importante para las ciberoperaciones militares, se le podría asaltar con gran violencia donde se encuentre, siempre y cuando la muerte y lesiones incidentales de civiles inocentes–como la propia familia del ciberguerrero–que pudieran ocurrir en el ataque no "fueran excesivas en relación a la ventaja militar concreta y directa anticipada" (siendo esa "ventaja militar", por supuesto, la eliminación o neutralización del ciberexperto).[33]

Por tanto, el tema ético para los ciberguerreros puede ser la medida en que sea apropiado pedir a los civiles exponerse a esta clase de riesgos. Una cosa es que los miembros de las fuerzas armadas asuman voluntariamente el proverbial "contrato de responsabilidad ilimitada" del servicio militar para ponerse en peligro; otra cosa es, sin embargo, pedir que los civiles hagan eso, y aún más esperar que sus familiares acepten que pueden convertirse en daño colateral en un conflicto que tiene expresiones violentas junto con ciber-efectos no cinéticos. En la ciberguerra, los "frentes de batalla" pueden estar lejos de lo que cualquiera podría reconocer como el campo de batalla tradicional.

Es imposible saber lo real que puede ser esta clase de amenaza. Sin embargo, en una era de "celdas durmientes" y la proliferación de fuerzas de operaciones especiales clandestinas de otros entre muchos países, esta clase de contrarresto a las capacidades ciberespaciales de Estados Unidos podría no ser tan extravagante como algunos podrían pensar. En cualquier caso, esta discusión del riesgo personal que podrían ocasionar las ciberoperaciones hace irónico que los ciberguerreros tengan que fortificarse para resistir el cruel asalto de algunos críticos sobre su ética y profesionalismo.

¿Desafíos a la ética marcial de los ciberguerreros?

Tal vez una de las críticas más desconcertantes que ha acompañado al uso creciente de tecnologías avanzadas en la guerra es la tendencia de algunos comentaristas contemporáneos a suponer que su empleo es "impropio de un hombre" o "poco digno". Considérese la experiencia de los operadores de vehículos teledirigidos que, como los cibercombatientes, luchan la guerra desde consolas de computadora. Un artículo muy reciente de un experto titulado "Con sus mortales vehículos teledirigidos, Estados Unidos está luchando una guerra de cobardes" es un ejemplo de la clase de retórica desagradable que se usa.[34] Aunque tales calumnias aún no se han formulado contra los ciberguerreros, parecería que es solo cuestión de tiempo antes de que se les someta a la misma clase de insulto a su ética profesional.

¿Cómo comenzó todo esto? Puede remontarse a los comentarios de hace algunos años del Dr. David Kilcullen, un Teniente Coronel retirado del Ejército Australiano que se ha convertido en uno de los más destacados proponentes de la forma de contrainsurgencia centrada en tierra con utilización intensiva de personal que encontró lugar en el Manual de Contrainsurgencia del Ejército y la Infantería de Marina, (FM 3-24) publicado en 2006.[35] Es importante entender que el Manual es más bien hostil a las operaciones aéreas en general, y les dedica sólo cinco páginas en un documento de 300 páginas, por lo que la crítica del Dr. Kilcullen a los vehículos teledirigidos no parece incoherente con su visión más amplia del poderío aéreo.

En cualquier caso, el Dr. Kilcullen afirmó ante el Congreso en 2009 que los ataques con vehículos teledirigidos contra terroristas eran "contraproducentes".[36] "En la cultura tribal Pashtun de honor y revancha", dijo, "el combate frente a frente es visto como valiente; disparar a la gente con misiles desde 6.500 metros no lo es".[37] Según Kilcullen, "usar robots desde el aire ... parece cobarde y débil."[38] Es obvio que su tesis podría fácilmente aplicarse a las ciberoperaciones y a quienes la realizan.

Lo que hace espectaculares estas declaraciones en su ironía es que el adversario al que se refiere Kilcullen no solo usa dispositivos explosivos improvisados detonados a control remoto para asesinar fuerzas estadounidenses al resguardo de la distancia, sino que también emplean niños para implantarlos. ¿No los convertiría eso, según sus propios estándares de "cultura de honor", en "cobardes y débiles"? No obstante, toda esta discusión, desmoralizadora o inexacta, es –en términos de la lucha de guerra actual– más bien inmaterial. El "objeto de la guerra", como el General Patton lo puso gráficamente, "no es morir por su país sino hacer que el otro individuo muera por el suyo".

El coraje físico, por muy admirable que sea, no es la única cualidad que se necesita para la victoria en el siglo 21, y quizás siempre. Por ejemplo, los nativos estadounidenses, lucharon una guerra con extraordinaria valentía. En la edición de Abril de 2012 del *Journal of Military History* el historiador Anthony R. McGinnis señala que la forma individualizada y estilizada de guerra de los nativos estadounidenses no era rival para "una nación moderna tecnológicamente avanzada" que tiene la "victoria final como meta".[39] Por supuesto, no hay nada malo en ser "una nación moderna tecnológicamente avanzada" que tiene la "victoria final como meta" siempre y cuando esos avances tecnológicos se utilicen en una forma legal y éticamente apropiada.

La verdad es que no solo no hay nada poco ético en luchar una guerra desde lejos, en realidad no hay nada especialmente inusual en ello. Desde tiempos inmemoriales, los guerreros han buscado combatir a sus adversarios en formas que negaban a sus oponentes la oportunidad de poder usar sus armas. Por ejemplo, como este escritor dijo en alguna otra parte:

> David mató a Goliat con un proyectil antes de que el gigante pudiera usar sus armas; las lanzas de 16 pies de las falanges de Alejandro el Grande alcanzaron sus objetivos mucho antes que las lanzas de 12 pies que llevaban sus oponentes; los arqueros ingleses destruyeron lo mejor de los caballeros franceses de Agincourt desde lejos cuando hicieron llover flechas sobre los jinetes; y, más recientemente, los tanques estadounidenses y británicos destruyeron el núcleo de las fuerzas blindadas de Saddam durante la "Ba-

> talla de 73 Easting" en 1991 principalmente porque sus cañones tenían más alcance que los tanques T-72 de Irak. No hay nada nuevo acerca de matar a distancia.[40]

Pero hay algo acerca de la guerra computarizada que atrae escarnio de algunos, no obstante equivocada e injustamente. Por ejemplo, Phillip Altson, un profesor de leyes de la Universidad de Nueva York fue nombrado por las Naciones Unidas como "Relator especial" para redactar un informe sobre homicidios selectivos. El documento que produjo también incluyó sus opiniones sobre los operadores de vehículos teledirigidos.[41] En él, sostiene que debido a que las operaciones con vehículos teledirigidos se pueden realizar "enteramente desde pantallas de computadora y enlaces de audio remotos, hay un riesgo, "dice él, "de desarrollar una mentalidad 'PlayStation' para matar".[42]

¿Mentalidad 'PlayStation' para matar? La simple sugerencia de que tal falta insultante de profesionalismo aparezca en un informe oficial de las Naciones Unidas, de por sí, es inquietante. La evidencia principal del hallazgo del profesor Alston parece ser sus propias especulaciones acerca del esquema mental de quienes realizan una tarea que él nunca ha realizado. Sin embargo, la evidencia real apunta en una dirección diferente a la sugerida por Alston, y refuerza la idea de que estos oficiales difícilmente consideran sus obligaciones un juego. De hecho, el Dr. Peter Singer del Brookings Institution dijo en 2010 que en sus estudios encontró "niveles de tensión de combate más altos entre [algunas unidades de vehículos teledirigidos] que entre algunas unidades en Afganistán".[43] Concluyó que los operadores sufrían "fatiga, cansancio emocional y agotamiento crecientes".[44] Estos malestares son poco indicativos de "jugadores".

Más recientemente, el *Air Force Times* citó a un oficial de la Fuerza Aérea que respondió directamente a la acusación de "juego de video" señalando que las responsabilidades de los operadores de vehículos teledirigidos eran tremendamente estresantes, y que las operaciones eran un "evento profundamente emocional. No es un acto despreocupado. No es un juego de video".[45] Aunque el debate aún causa agitación,[46] demuestra la rapidez con la que algunos críticos ridiculizan el profesionalismo de gente de principios que hacen lo que su misión les pide hacer. Ciertamente, la comparación con las ciberoperaciones no es similar, pero–en cualquier caso–los ciberoperadores están en el asunto muy serio de defender su patria y, al hacerlo, se les puede pedir que hagan estragos mediante ciber-metodologías en cualquier adversario. Aunque los medios de hacerlo pueden ser diferentes, el profesionalismo que demandan las operaciones es muy alto, y las cargas psicológicas sobre aquellos que las realizan son igualmente muy grandes.

Ha surgido otro aspecto de las campañas con vehículos teledirigidos que podría encontrar analogía en la ética y el profesionalismo que deben demostrar los ciberoperadores. Se expresa en el artículo del 29 de abril de 2012 en *Rolling Stone* del controversial escritor Michael Hastings). En él, Hastings declara:

> La naturaleza de control remoto de las misiones no tripuladas habilita...al Pentágono y la CIA a lanzar ahora ataques militares u ordenar asesinatos sin poner una sola bota en el terreno–y sin preocuparse de una reacción pública contraproducente respecto a soldados estadounidenses que vuelven a casa en bolsas mortuorias. La inmediatez y lo confidencial de los vehículos teledirigidos hacen más fácil que nunca que los líderes desaten el poder militar estadounidense–y más difícil que nunca evaluar las consecuencias de tales ataques clandestinos.[47]

Por todas sus bravatas, Hastings tiene algo de razón cuando dice que "la inmediatez y lo confidencial de los vehículos teledirigidos hacen más fácil que nunca que los líderes desaten el poder militar estadounidense". La experiencia de este escritor es que los elementos decisorios principales están muy conscientes de que cualquier operación militar puede tener consecuencias no intencionadas–no importa el 'poco costo' que pareciera tener durante la planificación. Sin embargo, lo que dice respecto a los vehículos teledirigidos podría encontrar un paralelo con las ciberoperaciones, y podría exigir que los ciberguerreros exhiban virtudes éticas, incluyendo especialmente candor y coraje.

La necesidad de consejo franco, holístico

La novedad de las ciberoperaciones, la incertidumbre de su efecto preciso, y la pura dificultad de su ejecución no siempre pueden entenderlas todos los participantes en la cadena de decisión, y estas condiciones pueden dar lugar a otra responsabilidad ética, que es prestar consejo franco, holístico. No es imposible que en una situación dada los involucrados en el proceso tengan que salirse de su carril, por así decirlo, para hacer las preguntas difíciles, o señalar hechos inconvenientes. Si debe "desencadenarse" el ciberpoderío estadounidense como diría Hastings, es imperativo que se haga con el mismo cuidado que se haría en cualquier operación militar tradicional. Esto podría exigir que alguien haga más de lo que requiere la norma, solo para cerciorarse que se toman en cuenta todas las consideraciones correctas–incluyendo éticas y legales–de manera que se tomen las mejores decisiones.

Afortunadamente, para los abogados, el Código Modelo de Conducta Profesional de la Asociación Americana de Abogados -la "biblia" de los abogados- específicamente permite tal consejo holístico. La Regla 2.1 del Código exige que los abogados "ejerzan juicio profesional independiente y produzcan consejo cándido".[48] Además, los abogados no están limitados a proporcionar asesoramiento legal como continúa diciendo la Regla que al "brindar asesoramiento un abogado se puede referir no solo a la ley sino a otras consideraciones tales como factores morales, económicos, sociales y políticos, que puedan ser pertinentes a la situación del cliente".[49] En realidad, ésta es la guía apropiada no solo para los abogados, sino para *todos* los profesionales civiles y militares que participan en ciberoperaciones porque su éxito depende de una amplia gama de factores, y corresponde a todos los involucrados trabajar juntos para asegurar que se identifiquen y consideren.

La regla menciona candor. Esto no es algo simplemente para los abogados, es una virtud ética fundamental para todos los profesionales de defensa.[50] Entre otras cosas, es un rasgo importante que se debe tener en cuenta al evaluar la amenaza potencial que representa el ciberespacio. Falsear, o peor aún, tergiversar deliberadamente la amenaza, puede dar lugar a deficientes asignaciones de recursos y otros errores de juicio. Las opciones acerca del ámbito y la naturaleza de la amenaza difieren ampliamente; en una entrevista en PBS Newshour en la primavera de 2012, Terry Benzel del Instituto de Investigación de la Información insiste que "todos en la cibercomunidad, hablamos sobre ciber-Pearl Harbor. Y no se trata de si va a suceder. Es cuándo va a suceder".[51] Similarmente, un "importante experto en ciberseguridad europea dice que se necesita acción internacional para evitar una ciberguerra y ciberterrorismo catastróficos".[52]

Sin embargo, no todos están de acuerdo. En abril de 2012 el Contralmirante Samuel Cox, director de inteligencia del Cibercomando Estadounidense, supuestamente "restó importancia al prospecto de que un enemigo de los Estados Unidos pudiera inhabilitar la red de energía eléctrica de la nación o interrumpir la Internet, diciendo que esos sistemas están diseñados para resistir ciberataques serios".[53] Más punzante es un artículo de febrero de 2012 de *Wired,* en que los investigadores Jerry Brito y Tate Watkins refutan gran parte del discurso histriónico acerca de la amenaza de la ciberguerra.[54] Según Brito y Watkins, "la evidencia para sustentar graves advertencias [sobre la ciberguerra] brilla por su ausencia".[55]

Congruente con las conclusiones de Brito y Watkins es un informe de 2011 de la Organización para Cooperación y Desarrollo Económico.[56] Al tiempo que afirma que los gobiernos "necesitan hacer preparaciones detalladas para resistir y recuperarse de una amplia gama de cibereventos indeseados, tanto accidentales como deliberados",[57] los autores de ese estudio concluyen "que muy pocos eventos relacionados con el ciberespacio tienen la capacidad de causar una conmoción global".[58] Escribiendo en *Foreign Policy* el analista Thomas Rid sostiene que la ciberguerra es "aún más ruido que peligro".[59]

Todo esto plantea inquietudes porque Brito y Watkins dicen que "en muchos aspectos, la retórica sobre la ciber-catástrofe se asemeja a la exageración de la amenaza que vimos en el pe-

ríodo previo a la Guerra de Irak".[60] También señalan que la "ciberseguridad es una industria grande y floreciente" y que "en Washington abunda gente que tiene intereses particulares en combinar y exagerar las amenazas a nuestra seguridad digital".[61] Aunque no llegan a acusar realmente a nadie de empujar temores de ciberguerra por beneficio personal, piden un "alto" en la "retórica apocalíptica" e insisten que los "escenarios alarmistas que dominan el discurso político pueden ser buenos para el complejo de ciberseguridad industrial, pero no hacen ningún favor a la seguridad real".[62]

El ámbito y la inmediatez de la amenaza se debate con razón, pero todos podrían estar de acuerdo en que, en cualquier caso, la exageración deliberada (o subestimación) de la amenaza, *aunque sea por razones de apoyo activo bien intencionadas*, puede plantear cuestiones de ética y profesionalismo. Como Brito y Watkins sugieren, al considerar el período previo a la guerra con Irak en 2003 es claro lo que puede pasar cuando se malinterpreta una amenaza, lo que puede explicar el título de su polémica "Cyberwar Is the New Yellowcake (La ciberguerra es el nuevo óxido de uranio concentrado)." En resumen, candor–y retórica moderada *si procede*–son cualidades críticas de los ciberguerreros. El lenguaje mesurado del Presidente Obama que urge a la gente a tomar "seriamente" la ciberamenaza y planear para ello como una "prioridad", representa un enfoque responsable que resalta los peligros sin caer víctima de la exageración contraproducente y engañosa.[63]

La virtud de competencia

Finalmente, una de las responsabilidades éticas de los ciberguerreros es la competencia. Las Reglas Modelo de Conducta Profesional de la Asociación Americana de Abogados proporcionan pautas que todos los profesionales del ciberespacio deberían considerar en analogía a sus responsabilidades. La Regla 1.1 de ese Código dice que "la representación competente requiere el conocimiento legal, habilidades, escrupulosidad y preparación razonablemente necesarios para la representación".[64] Para quienes se preocupan de los aspectos legales y éticos de la ciberguerra, el mandato ético de competencia va más allá del conocimiento y entendimiento de la ley y/o la ética, *per se*.

Sin duda hay muchos aspectos de las ciberoperaciones que son extraordinariamente complejos. Por tanto, les incumbe a los asesores legales y de otro tipo familiarizarse lo más que sea posible con el "negocio" del ciberciente para incluir sus aspectos técnicos. Un conocimiento práctico de la tecnología no solo ayudará a los asesores a entender los hechos de manera suficiente para aplicarles principios legales y éticos; también les dará gran *credibilidad* con aquellos que buscan su asesoramiento. Los elementos decisorios en el ámbito ciberespacial–y los que buscan asesoramiento en otras actividades–naturalmente gravitarán hacia los que muestren un entendimiento genuino de las muchas complejidades de su disciplina.

Esto no es una tarea fácil. Mantenerse actualizado con la tecnología en este campo tan complicado es un trabajo que tarda mucho y nunca termina. Pero se debe realizar con bastante anticipación de la necesidad, ya que no hacerlo puede dar lugar a una vida de lamentos. Winston Churchill observó una vez:

> Para todo hombre llega una vez en su vida ese momento especial en que figurativamente se le da una palmada en el hombro y se le ofrece una oportunidad para hacer algo muy especial, exclusivo para él y adaptado a sus talentos. Qué tragedia si ese momento lo encuentra desprevenido o sin la calificación para el trabajo que podría ser su mejor momento.[65]

Observaciones finales

Este ensayo busca ilustrar solo algunos ejemplos de cómo se podrían cruzar la ley y la ética. Este esfuerzo puede suscitar la pregunta: ¿cuáles de estos imperativos funcionará mejor para imponer los límites en la ciberguerra que gente honorable, y aún práctica, demanda? Kenneth Anderson, un profesor de leyes en la American University, tuvo recientemente la ocasión de considerar uno de sus primeros escritos sobre la eficacia de la ley y el honor como "motores" para el comportamiento correcto en el conflicto. El profesor Anderson sostiene que:

> La fe en la legalidad como el motor que impulsa tal adhesión a las leyes de la guerra me parece, no obstante, totalmente equivocada; es una fantasía hecha a la medida para los abogados, y especialmente para los abogados estadounidenses. Los abogados creen que el problema es uno de imposición, mientras que en realidad es uno de lealtad. Las codificaciones de la ley internacional son una plantilla útil para organizar las categorías de los deberes de un soldado. Pero, al final, la cultura pertinente al respeto de la ley humanitaria internacional no es la cultura de la legalidad y al culto de los abogados, sino más bien es la cultura del honor profesional de soldados, y lo que están dispuestos a hacer o no hacer en el campo de batalla.[66]

El que el "honor" colinde con la ética, o un subconjunto de la misma, puede ser apropiado para un debate activo en la universidad. Sin embargo lo que es más importante observar, como lo hace Anderson, es que John Keegan, quizás el historiador militar más eminente de la era moderna, no tuvo reservas para decir que "no hay sustituto para el honor como medio de imponer decencia en el campo de batalla, nunca lo ha habido, y nunca lo habrá".

Los "campos de batalla" del ciberespacio no se parecen mucho a los que se refiere Keegan, pero su punto de vista ciertamente tiene igual aplicabilidad. Al final, el honor y la mentalidad ética que implica, es indispensable. Pero la discusión no puede terminar allí, porque el simple hecho de haber desarrollado el carácter para llegar a la respuesta correcta no es suficiente, ya que se puede requerir coraje para insistir en ella.

El coraje que necesitan los ciberguerreros no es necesariamente el coraje *físico* que deben demostrar los combatientes del campo de batalla. Más bien, es mucho más probable que los cibercombatientes tengan que demostrar coraje *moral*. Esto es particularmente cierto a medida que se desarrollan las normas para las ciberoperaciones. Puede ser un gran reto hacer lo correcto, particularmente en circunstancias de extrema urgencia donde no hay orientación explícita salvo referencias a los principios clásicos de la ley y la ética.

Los cibercombatientes quizás deseen considerar que Max Hastings, otro historiador británico, en su estudio clásico del heroísmo militar concluye que "la bravura física se encuentra [en los militares] con más frecuencia que la variedad espiritual".[67] "El coraje moral", insiste "es raro."[68] Sin embargo es exactamente esta clase rara la que más necesitan demostrar los ciberguerreros. La ley puede proporcionar una arquitectura, pero es solo cuando se cruzan el honor y el coraje moral que podemos estar realmente seguros que los principios éticos dignos de defender son los que se conservan. ❑

Notas

1. Barack Obama, *Taking the Cyberattack Threat Seriously (Tomar en serio la amenaza del ciberataque),* WALL STREET JOURNAL, 19 de julio de 2012, http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html. Barack Obama, *Taking the Cyberattack Threat Seriously (Tomar en serio la amenaza del ciberataque),* WALL STREET JOURNAL, 19 de julio de 2012, http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html.

2. Por ejemplo, la División de Ley Internacional del U.S. Naval War College organizó una conferencia dedicada a los aspectos legales de la ciberguerra en junio de 2012, http://www.usnwc.edu/ILDJune2012.

3. *Véase por ejemplo,* Randall R. Dipert, *The Ethics of Cyberwar (La ética de la ciberguerra),* J. OF MIL. ETHICS, Vol. 9, No. 4 (2010), en 384, 385 (no hay discusiones informadas, abiertas, públicas o políticas de lo que sería una política ética y acertada para el uso de tales ciber-armas.").

4. Stockdale Center for Ethical Leadership de la Academia Naval de los Estados Unidos, *Warfare in a New Domain: The Ethics of Military Cyber Operations (La guerra en un nuevo dominio: La ética de las ciberoperaciones militares),* 26-27 de abril de 2012 http://www.usna.edu/ethics/publications/mccain2012.php. Gran parte de este ensayo viene de una presentación que hizo el autor en esa conferencia.

5. Patrick Lin, Fritz Allhoff, y Neil Rowe, *Is it Possible to Wage a Just Cyberwar? (¿Es posible luchar una ciberguerra justa?),* THE ATLANTIC, 5 de junio de 2012, http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/.

6. Geoffrey Best, *Law and War Since 1945 (La ley y la guerra desde 1945),* 1994, p. 289

7. Teniente Gabriel Bradley, Honor, Not Law, (Honor, no ley) ARMED FORCES JOURNAL, marzo de 2012, *disponible en* http://www.armedforcesjournal.com/2012/03/9563756 (consultada por última vez el 23 de abril de 2012).

8. *Id.*

9. *Id.*

10. Program on Humanitarian Policy and Conflict Research, Manual on International Law Applicable to Air and Missile Warfare (2009) (Programa sobre política humanitaria e investigación de conflicto, Manual sobre ley internacional aplicable a la guerra aérea y con misiles) http://ihlresearch.org/amw/HPCR%20Manual.pdf [de aquí en adelante el Manual AMW].

11. *Véase por ejemplo,* Roger Crisp, *Cyberwar: No New Ethics Needed (La ciberguerra: No se necesita nueva ética),* PRACTICAL ETHICS (blog), 19 de junio de 2012, http://blog.practicalethics.ox.ac.uk/2012/06/cyberwarfare-no-new-ethics-needed/.

12. Estos términos se usan, por ejemplo, en el Artículo 2 y el Artículo 52, respectivamente de la Carta de las Naciones Unidas, http://treaties.un.org/doc/Publication/CTC/uncharter.pdf.

13. *Véase la nota 5, supra.*

14. Si, por ejemplo, se puede hacer un caso objetivo para la aplicación correcta de la doctrina de autodefensa preventiva por una nación-estado, no habría base legal o moral para que Irán responda. Para una discusión de la autodefensa preventiva, *consulte en general,* Kinga Tibori Szabó, ANTICIPATORY ACTION IN SELF-DEFENCE: ESSENCE AND LIMITS UNDER INTERNATIONAL LAW (ACCIÓN PREVENTIVA EN DEFENSA PROPIA: ESENCIA Y LÍMITES SEGÚN LA LEY INTERNACIONAL) (2011).

15. *Id.*

16. *Id.*

17. *Véase por ejemplo,* Crisp, *supra* nota 11.

18. *Véase supra* nota 5.

19. Harold Koh, el asesor legal del Departamento de Estado de los Estados Unidos, explica los términos:

> Primero, el principio de distinción, que requiere que los ataques se limiten a objetivos militares y que los civiles o los objetos civiles no deben ser objeto del ataque; y Segundo, el principio de proporcionalidad, que prohíbe los ataques que podrían causar pérdidas incidentales de vidas civiles, lesiones a civiles, daño a objetos civiles, o una combinación de ellos, que serían excesivos en relación a la ventaja militar concreta y directa anticipada.

Harold Koh, *The Obama Administration and International Law (La administración Obama y la ley internacional),* discurso, American Society of International Law, 25 de marzo de 2010, http://www.state.gov/s/l/releases/remarks /139119.htm.

20. Stewart A. Baker y Charles J. Dunlap Jr., *What Is the Role of Lawyers in Cyberwarfare? (¿Cuál es la función de los abogados en la ciberguerra?),* ABA JOURNAL,1 de mayo de 2012, http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare/.

21. *Id.*

22. *Id.*

23. *Id.*

24. *Id.* (se añaden las cursivas).

25. *Id.*

26. Jim Wolf, "U.S. Military better prepared for cyber warfare: general (Militares estadounidenses mejor preparados para la ciberguerra: general)", *Reuters* (16 de noviembre de 2011) http://www.reuters.com/article/2011/11/17/us-usa-cyber-military-idUSTRE7AG03U20111117?feedType=RSS&feedName=everything&virtualBrandChannel=11563

27. *Id.*

28. *Véase por ejemplo, Department of Defense Strategy for Operating in Cyberspace (Estrategia del Departamento de Defensa para operar en el ciberespacio)* del Departamento de Defensa de los Estados Unidos, 2011, en 9, http://www.defense.gov/news /d20110714cyber.pdf ("El ciberespacio es una red de redes que incluye miles de proveedores de servicio Internet (ISP) en el mundo; ningún estado u organización puede mantener ciberdefensas efectivas por su cuenta".).

29. W. Michael Riesman y Chris T. Antoniou, THE LAWS OF WAR (LAS LEYES DE LA GUERRA) (1994), en xxiv.

30. *Véase en general,* Gary D. Solis, THE LAW OF WAR (La ley de la guerra) (201), en 41-42.

31. *Direct Participation in Hostilities: Questions and Answers (Participación directa en hostilidades: Preguntas y respuestas),* Comité Internacional de la Cruz Roja, 6 de febrero de 2009, http://www.icrc.org/eng/resources/documents/faq /direct-participation-ihl-faq-020609.htm.

32. *Id.*

33. *Véase* Koh, supra, nota 19.

34. George Monbiot, *With its deadly drones, the US is fighting a coward's war (Con sus mortales vehículos teledirigidos, Estados Unidos está luchando una guerra de cobardes),* The Guardian (U.K.), 30 de enero de 2012, http://www.guardian.co.uk/commentisfree/2012/jan/30/deadly-drones-us-cowards-war.

35. Departamento del Ejército de los Estados Unidos, Manual de Campo 3-24, 2006, http://www.fas.org/irp/doddir/army/fm3-24.pdf.

36. Doyle McManus, *U.S. drone attacks in Pakistan 'backfiring,' Congress told (Los ataques con vehículos teledirigidos en Paquistán son 'contraproducentes', se le advierte al Congreso),* LOS ANGELES TIMES, 3 de mayo de 2009, http://articles.latimes.com/2009/may/03/opinion/oe-mcmanus3

37. *Id.*

38. *Id.*

39. Anthony R. McGinnis, *When Courage Was Not Enough: Plains Indians at War with the United States Army (Cuando el coraje no era suficiente: Los Indios de las Llanuras en guerra con el Ejército de los Estados Unidos),* J. OF MIL. HISTORY, abril de 2012, en 473.

40. Charles J. Dunlap, Jr., *Does Lawfare Need an Apologia, Does Lawfare Need an Apologia? (¿Necesita la ley de la guerra una apología?* 43 CASE WES. RES. J. INT'L L. (2010), en 121.

41. Relator especial sobre ejecuciones extrajudiciales, sumarias o arbitrarias, *Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Execution: Study on Targeted Killings, entregado al Consejo de Derechos Humanos,* U.N. Doc. A/HRC/14/24/Add.6 (28 de mayo de 2010), *disponible en* http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.24.Add6.pdf (consultado últimamente el 2 de septiembre de 2010).

42. *Id.*, en 25.

43. Marc Pitzke, *Interview with Defense Expert P.W. Singer (Entrevista con el experto en defensa P.W. Singer),* SPIEGEL ONLINE INTERNATIONAL, 12 de marzo de 2010, thttp://www.spiegel.de/international/world/0,1518,682852,00.html.

44. *Id.*.

45. Jeff Schogol y Markeshia Ricks, *Demand grows for UAV pilots, sensor operators (Aumenta la demanda de pilotos de UAV, operadores de sensores),* Air Force Times, 21 de abril de 2012,

46. *Véase por ejemplo, Kenneth Anderson, Laurie Blank on Mark Mazzetti's 'The Drone Zone'–Último en una serie de Lewis, Dunlap, Rona, Corn, y Anderson,* LAWFARE, 21 de julio de 2012, http://www.lawfareblog.com/2012/07/laurie-blank-on-the-mazzetti-the-drone-zone-last-in-series-from-lewis-dunlap-rona-corn-and-anderson/.

47. Michael Hastings, *The Rise of the Killer Drones: How America Goes to War in Secret (El auge de los vehículos teledirigidos asesinos: Cómo va Estados Unidos a la guerra en secreto),* ROLLING STONE, 16 de abril de 2012, http://www.rollingstone.com/politics/news/the-rise-of-the-killer-drones-how-america-goes-to-war-in-secret-20120416#ixzz22VDkfR00.

48. Regla modelo de conducta profesional de la ABA 2.1, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_2_1_advisor.html.

49. *Id.*

50. Compare lo siguiente de la lista de "Valores éticos primarios" encontrados en el Reglamento Conjunto de Ética del Departamento de Defensa (se añaden las cursivas):

> a. Honestidad. Ser veraz, simple y *cándido* son aspectos de la honestidad.
>
> (1) La veracidad es obligatoria. Los engaños se descubren con facilidad y usualmente lo son. Las mentiras erosionan y socavan la confianza del público. Las falsedades dichas por razones aparentemente altruistas (para no herir sentimientos, fomentar la buena voluntad, etc.) las resienten los recipientes.
>
> (2) La simpleza añade franqueza a la veracidad y usualmente es necesaria para fomentar confianza pública y asegurar la conducción efectiva y eficiente de las operaciones del Gobierno Federal. Las verdades que se presenten de tal manera que lleven a los recipientes a la confusión, interpretación errónea o conclusión inexacta no son productivas. Tales engaños indirectos pueden fomentar mala voluntad y erosionar la apertura, especialmente cuando hay una expectativa de franqueza.
>
> (3) Candor es el ofrecimiento directo de información no solicitada. Es necesario de acuerdo con la gravedad de la situación y la naturaleza de las relaciones. Se requiere candor cuando una persona razonable se sentiría traicionada si se retiene información. En algunas circunstancias, el silencio es deshonesto, y en otras circunstancias, revelar información sería incorrecto y quizás ilegal.

Reglamento 5500.07-R del Departamento de Defensa de los Estados Unidos, *Joint Ethics Regulation (Reglamento Conjunto de Ética),* 17 de noviembre de 2011, para 12-401a, http://www.dtic.mil/whs/directives/corres/pdf/550007r.pdf.

51. *Preventing a 'Cyber-Pearl Harbor' (Evitar un 'Ciber-Pearl Harbor'),* PBS NEWSHOUR, 16 de abril de 2012, http://www.pbs.org/newshour/bb/science/jan-june12/deterlab_04-16.html.

52. *Expert warns on cyberwar threat (Experto advierte sobre la amenaza de la ciberguerra),* UPI.COM, 16 de marzo de 2012, http://www.upi.com/Science_News/2012/03/16/Expert-warns-on-cyberwar-threat/UPI-33781331937216/#ixzz1sRYZauJc (cita a Eugene Kaspersky, director ejecutivo y cofundador de Kaspersky Lab, que dice ser la empresa antivirus más grande de Europa).

53. Richard Lardner, *US Needs Top-level Approval to Launch Cyberattacks (EE.UU. necesita aprobación del más alto nivel para lanzar ciberataques),* SALON.COM, 24 de abril de 2012, http://www.salon.com/2012/04/24/us_needs_top_level_approval_to_launch_cyberattacks/.

54. Jerry Brito y Tate Watkins, *Cyberwar is the New Yellowcake (La ciberguerra es el nuevo óxido de uranio concentrado),* WIRED, 14 de febrero de 2012, *disponible en* http://www.wired.com/threatlevel/2012/02/yellowcake-and-cyberwar/.

55. *Id.*

56. Peter Sommer y Ian Brown, *Reducing Systemic Cybersecurity Risk (Reducción del riesgo sistémico de ciberseguridad),* Organización para Cooperación y Desarrollo Económico, 14 de enero de 2011, en 5, http://www.oecd.org/dataoecd/57/44/46889922.pdf.

57. *Id.*

58. *Id.*

59. Thomas Rid, *Think Again: Cyberwar (Repensar la ciberguerra),* FOREIGN POLICY, Marzo/Abril de 2012, en 80, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=full.

60. Brito and Watkins, *supra* note 54.

61. *Id.*

62. *Id.*

63. Véase nota 1, *supra.*

64. ABA Model Rule of Professional Conduct 1.1 (Regla modelo de conducta profesional de la ABA 2.1), http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence.html.

65. Según cita del Mayor General Stephen R. Lorenz, *Lorenz on Leadership (Liderazgo según Lorenz),* AIR & SPACE POWER JOURNAL, Verano de 2005, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj05/sum05/lorenz.html

66. Kenneth Anderson, *Sir John Keegan, Ave Atque Vale,* LAWFARE, 3 de agosto de 2012, http://www.lawfareblog.com/2012/08/sir-john-keegan-ave-atque-vale/.

67. Max Hastings, WARRIORS: PORTRAITS FROM THE BATTLEFIELD (GUERREROS: RETRATOS DEL CAMPO DE BATALLA), (2005), en XVII.

68. *Id.*

El Mayor General Charles J. Dunlap, Jr., USAF (Ret.) es el Director Ejecutivo del Centro de Ley, Ética y Seguridad Nacional en la Escuela de Leyes de Duke University. Su carrera de 34 años como abogado militar incluyó asignaciones en el Reino Unido y Corea, y participó en operaciones militares en África y Oriente Medio. Un graduado distinguido del National War College, las publicaciones recientes del General Dunlap relacionadas con el ciberespacio incluyen *Perspectives for Cyber Strategists on Law for Cyberwar (Perspectivas para ciber-estrategas sobre la ley de la ciberguerra),* en *Strategic Studies Quarterly* (2011) y *Towards a Cyberspace Legal Regime in the 21st Century: Considerations for American Cyberwarriors (Hacia un régimen legal en el ciberespacio en el siglo 21: Consideraciones para los ciberguerreros estadounidenses),* en la publicación *Law Review* de la University of Nebraska (2009). El General Dunlap y Stuart Baker debaten temas legales del ciberespacio en *Patriot Debates,* publicado en 2012 por la Asociación Americana de Abogados.

El Mundo se ha Vuelto "Ciberloco"

Cómo el "Debilitamiento Mutuamente Asegurado" es la mayor Esperanza para la Disuasión Cibernética

Dr. Matthew D. Crosston

En las extensiones invisibles del ciberespacio, nuestros enemigos están llevando a un nuevo nivel, sin hacer mucho ruido, la forma posmoderna de la guerra de la que fuimos testigos el 11 de septiembre: ya no son simplemente transnacionales—son no nacionales, que ocultan y atacan en un mundo donde no hay fronteras. Ya no son del tipo sin estado—son sin ubicación. Tampoco son virtualmente invisibles—son, bien, virtuales.

—Alan W. Dowd, *Fraser Forum* (2008)

MUCHOS EXPERTOS cibernéticos dicen que Estados Unidos está muy mal preparado para un ciberataque refinado y que cada día que pasa lo acerca un paso más a un Apocalipsis potencial virtual. Mientras que los problemas que obstaculizan el desarrollo de una política de disuasión cibernética efectiva y completa son claros (medición de la amenaza, atribución, reparto de información, desarrollo de códigos legales y mala infraestructura, entre otros), este artículo se concentra en un aspecto del debate que de ahora en adelante se ha omitido relativamente: que la futilidad de la innovación gubernamental en términos de eficacia defensiva es una debilidad relativamente constante y compartida por todas las grandes potencias modernas, ya sea Estados Unidos, China, Rusia u otras. En otras palabras, todos los estados preocupados con el reino cibernético desde una perspectiva de seguridad global son igualmente deficientes y vulnerables al ataque ofensivo; por lo tanto, es probable que los cibersistemas defensivos sean relativamente impotentes en general.

Estados Unidos tiende a ver este problema como si tuviera una carga exclusiva que llevar. Aunque los estados más pequeños que no consideren prever una función global para ellos temen un ciberataque masivo mucho menos que Estados Unidos, esto no es necesariamente cierto para los estados mencionados anteriormente y otros que desean ser protagonista globales importantes. Como consecuencia, el objetivo para las potencias importantes no debe ser la esperanza inútil de desarrollar un sistema defensivo perfecto de disuasión cibernética, sino la capacidad de inculcar la disuasión basada en un temor mutuamente compartido de una amenaza ofensiva. Estados Unidos está mejor ubicado pasando a una política abierta transparente que trata de disuadir de la eficacia de sus capacidades cibernéticas ofensivas. Esta estrategia tiene mayor proba-

bilidad de estar por delante de los sistemas de disuasión rivales y establecer la percepción entre rivales que Estados Unidos tendría ciertamente las capacidades eficaces de realizar un segundo ataque si es atacado. Es verdad que el objetivo de cualquier potencia importante sería lograr el dominio sobre dichas capacidades (es la forma de las grandes potencias), pero esto también resultaría en el problema de la ciberseguridad transformándose en un juego de suma cero donde el dominio de un estado aumenta la inseguridad de los demás. Por esta razón es lógicamente más estable y potencialmente pacífico tener un sistema de disuasión estructurado mutuamente entre potencias importantes, sin dar a ningún estado la capacidad de alterar el equilibrio cibernético.

Si se adopta, este cambio de política podría tener el mismo potencial que la destrucción nuclear mutuamente asegurada tan eficaz durante tanto tiempo sin ser retado físicamente durante la guerra global. La disuasión nuclear, se basó al principio en la capacidad esperada de un segundo ataque después de sobrevivir un ataque inicial durante un tiempo suficientemente largo para lanzar un contraataque igualmente devastador. Pero con el tiempo—a medida que las grandes potencias nucleares siguieron acumulando arsenales enormes—la eficacia de hecho de la disuasión nuclear no estaba basada tanto en la probabilidad de la capacidad de un segundo ataque como en la aceptación por parte de todos los protagonistas que participan en el juego nuclear que inevitablemente devastarían todo. Una lógica de disuasión emergió de admitir que no tenían defensas.

Quizá podría ser así con esta nueva destrucción cibernética mutuamente asegurada—en un sistema ofensivo abierto y transparente de amenazas cibernéticas, cada protagonista importante en el sistema global llegaría a temer el debilitamiento por igual y por lo tanto no se arriesgaría a iniciar el primer ataque. Aprovechándose de esta vulnerabilidad compartida para atacar y hacer propaganda sobre la acumulación abierta de capacidades ofensivas, habrá discutiblemente un mayor sistema de disuasión cibernética manteniendo seguro el espacio común virtual. Aunque parezca un oxímoron, la defensa más eficaz en este nuevo mundo de peligro virtual es una capacidad ofensiva ciberletal de enormes proporciones; no tanto para usarla realmente, sino para infundir el temor de que pueda usarse. Aunque el caos anárquico y la libertad de Internet será siempre un refugio para actores no estatales que traten de dañar sistemas estatales, una política de destrucción cibernética mutuamente asegurada abierta y transparente daría sistemáticamente a las potencias principales la capacidad de llevar a cabo un segundo ataque para influir potencialmente y disuadir también a estos actores no estatales. En la actualidad, los sistemas de disuasión cibernética defensiva básicamente dan total libertad a estos actores.

Resulta interesante que algunos estados están respetando ya claramente esta estrategia, al menos en el sentido informal aunque no tengan una posición política explícita—el apoyo ferviente de China a los "honkers" [piratas patrióticos] y la dependencia frecuente de la Federación Rusa de los "piratas patrióticos" se nos vienen a la mente inmediatamente. Estados Unidos ciertamente tiene la capacidad tecnológica de igualar a China y Rusia en letalidad virtual. Se podría decir que la carencia formal de una política abierta indica las dudas de parte de Estados Unidos para desarrollar un "espacio común virtual armado". En vez de una indicación de inviabilidad, esta renuencia parece ser una aprobación a consideraciones de inteligencia, lo que significa que Estados Unidos está discutiblemente más satisfecho desarrollando sus capacidades ofensivas en secreto como parte de operaciones más encubiertas que como parte de una política manifiesta. Este artículo indica que el énfasis en una capacidad ofensiva encubierta en vez de manifiesta es un error que pone en peligro la eficacia de la seguridad cibernética de Estados Unidos.

La necesidad de una nueva doctrina, nuevas preguntas y nuevas respuestas

La inercia institucional y la rigidez doctrinal son a menudo obstáculos importantes que bloquean la reforma de la política y pueden incluso obstaculizar la aparición de nuevas ideas de política. No obstante, en el reino cibernético, estos bloqueos no están casi tan arraigados como otros problemas/principios de seguridad. Durante los últimos 10 años la ciberseguridad se ha

convertido en un área cada vez más importante de interés nacional, no obstante el contexto de la ciberseguridad es una era completamente nueva de pensar y de peligros. No fue hasta finales del segundo período del Presidente George W. Bush que se hicieron esfuerzos más definitivos entre agencias para desarrollar explícitamente algo similar a la ciberdoctrina nacional (lo más claro de esta novedad gubernamental fue la creación en 2009 del Cibercomando de EE.UU.). Como analista Mark Young dijo recientemente,

> Es necesaria una ciberdoctrina nacional. Es el enlace entre estrategia y la ejecución de las misiones del sector de seguridad nacional. La doctrina puede ser tradicionalmente una noción militar, pero las agencias reconocen la sabiduría de establecer principios de guía. Una ciberdoctrina nacional puede ser un vehículo usado para definir las funciones de los departamentos y las agencias para todo el gobierno de EE.UU. Al contrario que una orden ejecutiva presidencial o una directiva del Consejo de Seguridad Nacional, una doctrina se desarrolla de una forma abiertamente en colaboración.[1]

Esta evidencia afirma la ausencia de una política abierta, manifiesta y bien definida que guía los intereses de Estados Unidos a largo plazo en lo que se refiere a la seguridad cibernética. Young tiene razón en reconocer que una política cibernética explícita y bien definida es esencial para desarrollar un sistema de ciberseguridad completo y eficaz, en su mayor parte debido a la intensa complejidad inherente a los ciberataques y a la disuasión cibernética. Sigue,

> La naturaleza de los ataques de la red resalta en particular la importancia de una ciberdoctrina bien revisada, ya que los líderes de la seguridad nacional tendrán poco tiempo para consultar con el Consejo de Seguridad Nacional o con el Comandante en Jefe cuando se vean ante un ataque que podría devastar la economía nacional, corromper el flujo del comercio o alterar las cadenas de suministro militares. Debido a los retos técnicos, los contraataques siguen siendo una proposición que lleva mucho tiempo. La alteración de un ciberataque se logra con más facilidad pero tal vez no se logre con tiempo para proteger datos críticos o sistemas de seguridad nacionales.[2]

El problema principal tratado por este artículo es que el debate para crear una ciberdoctrina unificada, explícita y verdaderamente nacional no reconoce abiertamente el axioma más básico del dominio cibernético: la ofensa siempre prevalecerá frente a la defensa lo que, por lo tanto, no incluirá todas las opciones y estrategias potenciales.

Es decir, el lenguaje que utilizan los analistas y especialistas cibernéticos es inherentemente defensivo—es siempre sobre la naturaleza problemática de los contraataques, los retos técnicos para alterar un ataque en curso, y lamentar la ventaja ofensiva que tienen los adversarios sobre los especialistas defensivos. Estos lamentos son reales, pero inexplicablemente no conducen a Estados Unidos a reconocer lo obvio: la doctrina cibernética nacional de Estados Unidos no debe basarse en medidas defensivas que van a estar siempre por detrás de las medidas ofensivas, sino en capacidades ofensivas que den la percepción explícita a los adversarios potenciales que cualquier maniobra agresiva provocará ataques de represalia debilitadores más severos que cualquier agresión inicial—una verdadera política de destrucción cibernética mutuamente asegurada, consagrando inicialmente la capacidad de un segundo ataque y, es de esperar, institucionalizando la admisión disuasoria de la futilidad de un primer ataque.

Ya se está haciendo algún trabajo excelente en los tipos de preguntas que se necesitan al considerar las opciones de seguridad cibernética. Aunque la mayoría de estas preguntas tratan en la actualidad de la disuasión cibernética desde una postura puramente defensiva, las más importantes siguen siendo aún pertinentes para una política de destrucción cibernética mutuamente asegurada:

- ¿Debe el objetivo revelar el ataque cibernético?
- ¿Cuándo debe anunciarse la atribución?
- ¿Deben ser evidentes las represalias cibernéticas?

- ¿Más valen las represalias tarde que nunca?
- ¿Puede haber una confrontación sin represalias?[3]

Todas estas preguntas son increíblemente importantes pero indiscutiblemente tienen respuestas diferentes, dependiendo del tipo de sistema de ciberseguridad que se esté construyendo. Un sistema puramente defensivo basado en el carácter secreto de la inteligencia produce respuestas ineficaces que dejan lagunas en la infraestructura de la seguridad nacional. Las respuestas proporcionadas por una política de destrucción cibernética mutuamente asegurada abierta, transparente y ofensiva sería agresiva y suficientemente explícita para rellenar estas lagunas aprovechándose de la lógica y la eficacia de la disuasión nuclear. El carácter abierto y la transparencia terminan con el "dilema" de revelar objetivos y problemas de atribución, mientras que una concentración en la capacidad ofensiva no solo justifica más las represalias sino que también crea la posibilidad de una confrontación efectiva sin represalias y, por último, evitar una confrontación directa. Este fue posiblemente el verdadero legado de paz dejado por la disuasión nuclear. ¿No podría una política de destrucción cibernética mutuamente asegurada producir la misma esperanza?

Un argumento en contra respondería no a esa pregunta: sigue siendo poco práctico y poco realista pensar que un sistema cibernético de destrucción mutuamente asegurada pueda desarrollarse de forma efectiva. Simplemente hay demasiados problemas para desarrollar y garantizar que se pueda lograr ese "debilitamiento mutuamente asegurado" e, incluso si se logra, garantizarlo podría causar la disuasión de amenaza necesaria para prevenir o limitar los ciberataques. En este caso, los expertos de doctrina deben evitar convertirse en puramente académicos y en simples cascarrabias de política—afirmando que el dominio cibernético es un campo ofensivo sin esperanza donde la disuasión basada en técnicas defensivas no puede ser efectiva, mientras que también indica que un sistema de disuasión cibernética basado en tecnologías ofensivas es igualmente poco práctico e ineficaz. En otras palabras, existe una tendencia a declarar que la defensa no funciona y que la ofensa no da resultado simultáneamente. Esto crea un callejón sin salida erudito y de política, atacando sin esperanza molinos de viento intelectuales y yendo a ninguna parte.

Rumores rusos

El casi apagón virtual de Estonia en 2007 coincidió con la decisión del gobierno de Estonia de trasladar un monumento de la guerra de la era soviética. En esencia, toda la estructura virtual dentro de Estonia se vio inundada y abrumada con "basura" durante un período de tres semanas. Eso puso en peligro fundamentalmente si es que no paralizó temporalmente la red de comunicaciones estonia, ya que periódicos, teléfonos móviles, sistemas de respuesta de emergencia y el banco más grande del estado fueron objetivos de los ataques. Además, un esfuerzo de ataque concentrado se apuntó a las oficinas del presidente, del primer ministro, del parlamento y del ministerio de asuntos exteriores.[4]

No obstante, la importancia de este ataque resalta algunos de los problemas para desarrollar un sistema de disuasión cibernética eficaz: aun cuando Estonia dio a entender que pudo identificar algunos ataques a oficinas del gobierno ruso, no estableció de hecho ningún enlace gubernamental directo. Rusia mantuvo siempre que los ataques vinieron de cibernacionalistas renegados, que actuaban de acuerdo a su propio sentido de patriotismo deformado pero no por órdenes de ninguna oficina o agencia gubernamental oficial. Es más un testimonio de estado de percepción pública global que nadie hoy en día cree la versión rusa de los ataques y da por sentada la versión estonia—nunca hubo una prueba irrefutable que demostrara que la política gubernamental formal rusa fuera la culpable principal de los ataques estonios.

Se trata de un ejemplo perfecto del mundo real del problema de atribución a menudo explicado por la teoría de especialistas cibernéticos: con frecuencia es demasiado difícil identificar

con precisión el origen de un ciberataque. Y lo que es aún peor, en casos en que el punto de origen pueda al menos ser discutido de forma apremiante, aún no existe una forma definitiva de demostrar simplemente quién apretó el "gatillo" y lanzó el ataque. La resolución de ambos problemas sería esencial para el desarrollo de un sistema de disuasión cibernética verdaderamente eficaz. La incapacidad de demostrar la culpabilidad obstaculiza considerablemente cualquier esfuerzo para tomar medidas defensivas. Realmente es tan sencillo como "¿cómo se sabe contra quién tomar represalias si no se está seguro de quién dio el puñetazo virtual?" No se puede, y como consecuencia cualquier esfuerzo para construir un sistema de disuasión cibernética efectivo aparece ya muy quebrantado.

Realidad china

Tal vez el único otro estado asociado en la actualidad con los ataques cibernéticos y el ciberespionaje tanto como la Federación Rusa es China. Ya a finales de la década de los 90, Estados Unidos acusó a China de atacar a varias agencias gubernamentales y trató de infiltrar las instalaciones nucleares de Estados Unidos. En el momento en que Estonia estaba siendo atacada y acusando a Rusia, Alemania sufrió varias infiltraciones en sus agencias gubernamentales y culpó a China. Al igual que con el caso estonio, tanto Estados Unidos como Alemania, a pesar de su convicción inflexible de saber a quién culpar, no tenían de hecho ninguna evidencia real que relacionara al gobierno chino con las incursiones detectadas.[5]

Esto no es un problema pequeño y no es un asunto de semántica de culpabilidad. La respuesta de la comunidad internacional a la evidencia de una implicación directa del gobierno en un ataque cibernético contra otro estado podría considerarse muy fácilmente como una acción bélica, incluso si por el momento es una guerra de menor grado. Por lo tanto, la atribución directa es de la máxima importancia, ya que podría conducir al compromiso de las fuerzas militares y a exponer a un estado a las más serias consecuencias—baja en un campo de batalla. Por lo tanto, cualquier sistema de disuasión cibernética debe poder superar el problema de atribución para que sea pertinente en el asunto más importante de todos—la seguridad del estado. Está claro que el mundo, no simplemente Estados Unidos, es incapaz actualmente de idear un sistema que pueda superar este problema.

A diferencia de Rusia, que siempre ha sido muy reservada sobre sus actividades cibernéticas y férrea en su negativa de participar en cualquier ataque cibernético patrocinado por cualquier estado, China ha sido sorprendentemente abierta sobre su creencia en la necesidad e idoneidad de establecer un ejército de ciberguerreros. China recluta activamente y facilita el apoyo de algunos de los piratas más brillantes desarrollados localmente, llamados "honkers." Los "honkers", en su descarado patriotismo virtual, creen en la filosofía de que la "mejor defensa es una ofensa capaz". No se consideran ellos mismos empleados necesarios del gobierno ni miembros de la comunidad de inteligencia china; simplemente creen que China necesita protegerse de sus adversarios. Si se hace llegar a su atención que otro estado o corporación está iniciando maniobras dañinas contra su país, entonces su obligación es responder del mismo modo. Observe que responder del mismo modo no es sencillamente detener un ciberataque sino formular un ataque cibernético de represalia que de hecho es más intenso y más completo que el ataque inicial.

De algunas formas esta realidad da argumento a la posibilidad de una guerra cibernética que existe más allá de la guerra convencional; no porque la guerra convencional se vaya a volver obsoleta alguna vez o porque sea la forma de seguridad más suprema, sino porque la ciberguerra puede ser considerada por muchos estados como menos conflictiva y una maniobra más orientada a resultados. La piratería informática efectiva y los ataques ciberestratégicos en el momento siguen dando muchas más oportunidades para ocultar la participación mientras se obtienen con éxito secretos económicos, políticos, diplomáticos y militares. Haciendo un cálculo sencillo de costos-beneficios, la ciberguerra es mucho más económica que la guerra convencional, por lo que es discutible que su popularidad crezca exponencialmente con el tiempo. Al considerar la

impotencia de los sistemas defensivos cuya tarea es detener tales esfuerzos, la ciberguerra es un concepto fundamentalmente complejo, complicado y difuso por diseño. Estas características serían retadas al menos por un sistema de destrucción cibernética mutuamente asegurada abierto y transparente en formas en que los métodos de disuasión cibernética actuales no lo son.

Por el momento es justo suponer que los "honkers" chinos no están tratando explícitamente de crear una versión cibernética de la teoría de destrucción nuclear mutuamente asegurada, pero esto no significa que no hayan creado dicha política en sus acciones de hecho. Lo que parece indiscutible es que China ha decidido que no hay consideraciones éticas en el dominio cibernético. De hecho, es fácil ver cómo un estado podría hacer uso del argumento contrario—si la ciberguerra no quiere decir necesariamente derramamiento de sangre inmediato y directo debido a ciberataques, entonces se podrían retirar libremente las esposas éticas de las consideraciones estatales. Y lo que es más importante, China ha dado al resto del mundo un esquema teórico justificando esa política—la filosofía ofensiva de los "honkers" no se basa en ningún sentido vengativo de derramamiento de sangre, sino en un cálculo cuidadoso de lo que es realmente eficaz en el reino cibernético: las capacidades defensivas están comprometidas de forma irremediable; por lo tanto, solamente las amenazas ofensivas tienen el potencial de disuadir iniciativas enemigas.

En algunas maneras este proceso de pensamiento ya ha sido apoyado nada menos que por el vicepresidente del Estado Mayor Conjunto actual, el General James Cartwright, que dijo en 2007 ante el Subcomité de las Fuerzas Estratégicas del Comité de las Fuerzas Armadas del Senado que era "hora de aplicar los principios bélicos al dominio cibernético . . . y la defensa de la nación se hace mejor usando capacidades que *nos permitan luchar contra nuestros adversarios* cuando sea necesario disuadir acciones negativas para nuestros intereses".[6] La disuasión cibernética tal como se cree actualmente no tiene esta capacidad y no permite a Estados Unidos luchar contra sus adversarios. No se trata de insistir continuamente en algo que ya se ha tratado, sino en hacer el énfasis necesario sobre cómo Estados Unidos se aferra a la defensa. El país está determinado en ser diferente, incluso si va en contra de su propia seguridad. Aunque pueda ser políticamente incómodo modelar algo importante para la seguridad nacional de EE.UU. imitando a los piratas chinos, está claro que por el momento los "honkers" están aplicando de forma más abierta y con mayor éxito los principios bélicos al dominio cibernético. Entretanto, Estados Unidos, se niega a considerar y desarrollar de forma transparente sus propias posibilidades y capacidades y por lo tanto sigue siendo el objetivo cibernético más vulnerable.

Contraciberespacio

Un desarrollo fascinante, inspirado tal vez por la amonestación del General Cartwright, viene con el concepto de contraciberespacio, definido como "una función que consiste en operaciones para lograr y mantener un grado deseado de superioridad ciberespacial debido a la destrucción, degradación o alteración de las capacidades de un enemigo de usar el ciberespacio".[7] Este trabajo procede de una nueva conceptuación de la doctrina básica de la Fuerza Aérea y es una admisión de la necesidad de producir nuevas ideas (aunque discutiblemente mediante la aplicación de ideas bélicas viejas ya demostradas) en el dominio del ciberespacio y su defensa. El asunto a mano es por supuesto tratar de establecer una "superioridad ciberespacial", cuyo documento de doctrina AF 2-11, "Operaciones ciberespaciales", borrador de versión definida como "el grado de ventaja poseído por una fuerza sobre otra que permite llevar a cabo operaciones en el ciberespacio en un momento y en un lugar dados sin interferencias prohibitivas de la fuerza contraria".[8] Al tomar en consideración estos conceptos y definiciones, se pone claramente de manifiesto lo ineficaz que será siempre la disuasión cibernética mientras sea un sistema construido a partir de prioridades defensivas. En el dominio cibernético, un sistema defensivo, por definición, pone a un estado en desventaja y no dispone del potencial de llevar a cabo operacio-

nes sin una interferencia prohibitiva. La doctrina cibernética de Estados Unidos debe lograr esta capacidad.

En mayo de 2007, el Presidente Bush ordenó a la Agencia de Seguridad Nacional (NSA) llevar a cabo un ciberataque contra redes de teléfonos móviles y computadoras que los insurgentes iraquíes habían usado o tratado de usar en la colocación de bombas en carreteras. La NSA cumplió, y su éxito subsiguiente esencialmente destruyó lo que hasta ese momento era para ellos una red de comunicaciones insurgente eficaz. Muchos analistas militares indican que ese esfuerzo fue primordial para cambiar el curso de la guerra.[9] Es cierto que una destrucción cibernética mutuamente asegurada no puede ser exactamente igual a una nuclear. No se trata de semántica cuando destrucción se reemplaza por debilitamiento. Así pues, mientras que la analogía tal vez no se adapte perfectamente, funciona de forma eficaz, basada en el hecho de que se puede decir que la guerra en el siglo XXI se ha alejado de ser global y apocalíptica y ha pasado a ser algo más regional y temporalmente dañino. Como tal, las armas en una política de destrucción cibernética mutuamente asegurada no destruye estados convirtiéndolos en arena y vidrio sino simplemente los paraliza e incapacita en dominios tan cruciales para su funcionamiento y gobierno eficaces. Dichos daños no son insignificantes.

Claramente, Estados Unidos tiene la capacidad técnica y la agresividad estratégica de llevar a cabo dichas operaciones. Ahora debe conceptuar una mente ofensiva para empezar a defender el ciberespacio. El problema hasta este momento ha sido su esfera de utilización relativamente limitada—el ejemplo de Irak fue un caso de guerra abierta y explícita dirigido a un objetivo que estaba atacando de forma activa y agresiva el personal militar estadounidense. Por supuesto, esto tal vez no sea tan políticamente limpio, pero puede ser dramáticamente más efectivo para limitar a los adversarios que están motivados para atacar a Estados Unidos u otros países en el espacio virtual común. Tenga en mente que en el siglo XXI, el ciberespacio no es menos espacio que proteger. Es cierto que los medios de comunicación no podrán mostrar los cuerpos o campos de batalla sangrientos cuando un país es víctima de un ciberataque masivo, pero la devastación y la destrucción de dicho ataque es de muchas maneras más completo y de mayor alcance.

Carencia de infraestructura

Los argumentos lógicos para una política de destrucción cibernética mutuamente asegurada se hacen aún más apremiantes cuando se examinan por completo los obstáculos técnicos que hacen frente a una verdadera disuasión cibernética defensiva. Durante los últimos 10 años, Estados Unidos ha invertido mucho en tecnologías de ciberseguridad. A pesar de este compromiso e inversión, quedan problemas importantes en las áreas más fundamentales. Aún sigue sin producirse un despliegue a gran escala de tecnología de seguridad capaz de proteger completamente la infraestructura estadounidense vital.[10] La necesidad de nuevas tecnologías de seguridad es esencial, pero hasta la fecha los mejores desarrollos solamente han sido en las instalaciones de investigación privadas de escala pequeña a intermedia. Lo que se requeriría para hacer avances rápidos a gran escala en nuevos mecanismos de seguridad de redes es de enormes proporciones:

- desarrollo de plataformas de pruebas de seguridad a gran escala, combinado con nuevas estructuras y normas para pruebas y referencias;
- superar deficiencias e impedimentos actuales para evaluar mecanismos de seguridad de redes, que hasta la fecha sufren de una carencia de rigor;
- datos de redes pertinentes y representativos;
- modelos de mecanismos de defensa adecuados; y
- modelos adecuados de la red y para datos de tráfico básicos y de ataque.

La mayoría de estos asuntos son problemáticos debido a la gran complejidad de las interacciones entre el tráfico, la topología y los protocolos.[11] En pocas palabras, es simplemente más sencillo atacar que defender en el dominio cibernético, y las complejidades innatas de preparación de la infraestructura hacen que probablemente no se trate simplemente de una estimación de asuntos actuales sino de un axioma que perdurará durante eras. Los piratas prevalecerán siempre ante los defensores. Estados Unidos no debe desperdiciar el tiempo atacando molinos de viento virtuales cuando ya tiene la tecnología, el talento y la capacidad de crear una ruta de políticas diferentes.

Un argumento contrario a estos rechazos es que el dominio cibernético seguirá dominado inherentemente por capacidades ofensivas. Las medidas defensivas alabadas más a menudo que presuntamente están alcanzando a las amenazas ofensivas (IPV-6 y tecnologías de portal) son desgraciadamente un poco exageradas, ya que el dominio cibernético no es nunca estático—sean cuales sean las contramedidas defensivas que se desarrollen, uno puede estar seguro de que habrá respuestas a esas medidas. Y las respuestas ofensivas hasta ahora han ido por delante de las "mejoras" defensivas. No hay nada en el futuro previsible que parezca retar ciertamente esta realidad básica. Estados Unidos debe continuar de veras desarrollando, mejorando y refinando sus tecnologías defensivas. Pero no debe ser uno tan ingenuo como para pensar que ser capaz de desarrollar una disuasión defensiva se podrá superar continuamente y de forma rutinaria en trabajo y maniobra las amenazas ofensivas. Simplemente no parece que la estructura del dominio cibernético permita emerger esta realidad.

La naturaleza asimétrica de la ciberguerra

El fracaso de Estados Unidos de participar ofensivamente en la ciberguerra, como reflexión de una política abierta y transparente (o incluso crear la percepción de voluntad para enfrentarse ofensivamente), solamente ha exacerbado la naturaleza asimétrica de los ciberataques. La comercialización, la normalización y el bajo costo de la alta tecnología alrededor del globo hacen que librar campañas cibernéticas sea dramáticamente más sencillo que defenderse de ellas. Literalmente una docena de programadores determinados es capaz de amenazar la red logística de EE.UU., robando planes de operaciones, cegando capacidades de inteligencia u obstaculizando la capacidad de suministrar armas conforme a los objetivos.[12] Eso nunca fue más evidente que en 2008, cuando el Departamento de Defensa sufrió una intrusión significativa en sus redes militares supuestamente seguras. Se introdujo una unidad flash infectada en una computadora portátil militar en Oriente Próximo. Puesta allí por una agencia de inteligencia extranjera, la unidad tuvo éxito en enviar código informático malicioso que pudo propagarse a gran distancia y en gran medida en información clasificada y sin clasificar de modo que se consideró similar a establecer una "cabeza de playa digital".[13]

Estos ejemplos explican perfectamente el carácter malicioso y la futilidad potenciales de luchar contra la asimetría. Es un problema estructural innato que no puede superarse, debido a la naturaleza de la tecnología y al mercado libre. Internet se diseñó para ser abierta y accesible, no solamente para facilitar el uso entre los consumidores más básicos sino también para animar y estimular bajas barreras para la innovación. Como consecuencia, la ofensa tendrá siempre la ventaja.[14] Pero en vez de dejar que la lógica de esta realidad condujera a Estados Unidos a una nueva conceptuación de "defensa ofensiva", el pensamiento de Estados Unidos está aferrado a una mentalidad defensiva que solamente puede resultar en un sistema de disuasión arriesgado.

Aunque la asimetría hace que estar adelantado a los adversarios atacantes sea muy dudoso, Lynn dice que esto solamente enfatiza a necesidad de que Estados Unidos sea más adaptable para ajustarse constantemente y mejorar su defensas. Incluso dice que las tradiciones antiguas de disuasión de la Guerra Fría (modelos de represalias aseguradas) *no* darán resultado en el ciberespacio debido al problema de atribuciones mencionado arriba, imposibilitando casi saber justo contra quien tomar represalias. Por lo tanto, se supone que la disuasión tenga tanto éxito

en negar las ventajas a un atacante, en vez de tratar de imponer costos a través de represalias agresivas.[15]

Aunque este artículo evidencia el problema de la atribución, esto no conduce a un argumento para alejarse de los antiguos modelos de disuasión de represalias sino que en realidad es lo contrario: un modelo cibernético de represalias no sería sobre a quién lanzar misiles, sino en forzar la percepción de un debilitamiento tecnológico/infraestructural masivo incluso si se determina y atribuye la sospecha de un ataque. La destrucción nuclear mutuamente asegurada tuvo éxito no porque diversos estados lanzaran realmente armas nucleares; tuvo éxito gracias a la convicción entre todas las partes de que un ataque de esta naturaleza sería tan universalmente destructor que el costo superaba con mucho las posibles ventajas potenciales. Un modelo de destrucción cibernética mutuamente asegurada tiene que operar con este mismo principio, solamente con armas virtuales en vez de armas cinéticas. Si se hace bien, armando esencialmente la doctrina cibernética de Estados Unidos, entonces es prohibitivamente caro para un adversario que se arriesgue a atacar.

No se trata de hecho de discutir sobre la creación de cierta variante cibernética de una máquina del fin del mundo del Dr. Strangelove, cuyas repercusiones resuelvan el problema de atribución. Extrapolando al máximo, una política de destrucción cibernética mutuamente asegurada disuade una destrucción nuclear mutuamente asegurada—la percepción de devastación virtual realista mediante ataques de represalia provoca temor de acción, haciendo así que el sistema global sea seguro mediante un equilibrio peligroso, pero estable. Lo mismo que con las armas nucleares, la capacidad de destruir universalmente el espacio común virtual no puede ser la última esperanza de paz en el sistema. Este no es un argumento para dar al presidente una opción entre rendirse o piratear el mundo moderno hasta hacerlo volver a la Edad Media. En vez de eso, una política de destrucción cibernética mutuamente asegurada—al ser abierta, transparente, mutua y ofensiva—tendría suficientes nuevos controles disuasorios integrados en ella estructuralmente para no solamente proporcionar más opciones sino también para hacer vacilar a los malhechores de un comportamiento que podría poner a prueba sus límites.

Recuerde que la mutualidad no solo aumenta el temor sino que ese mismo temor permite la posibilidad de aumentar la confianza mediante un enfrentamiento repetido. Hasta ahora la naturaleza dinámica del dominio cibernético favorecía demasiado a los que lo dañarían. La destrucción cibernética mutuamente asegurada pondría finalmente parte de ese dinamismo en manos de potencias importantes con un interés mutuo en reglas, regulaciones y estabilidad.

Ciberguerra, disuasión cibernética y complejidad política

Tratar de estudiar las consecuencias del impacto del dominio cibernético sobre la guerra y el conflicto es un avispero de complicaciones políticas. Incluso al tratar de desarrollar un sistema de protección puramente defensivo no atacante, existe una preponderancia de consideraciones complejas. ¿Cómo puede estar uno seguro del atacante? ¿Pueden arriesgarse los haberes cuando se sospeche de un ciberataque? ¿Envían las represalias el mensaje correcto al lado defensivo? ¿Debe haber un umbral de respuesta? ¿Cómo se evita la escalada?[16] Todas estas preguntas plantean problemas no solo porque son complicadas sino porque la naturaleza de un sistema cibernético defensivo exacerba los defectos dentro de esa política en vez de eliminarlos, y sin embargo otras preguntas discutiblemente aparecen solamente debido a estos defectos inherentes en una mentalidad defensiva.

La complejidad se reduce al considerar el desarrollo de una política de destrucción cibernética mutuamente asegurada, pero admitimos que puede poner a Estados Unidos en una posición política incómoda al principio. Considere simplemente la teoría de la guerra. En el primer ejemplo, derecho a la guerra, cuando los estados pueden legalmente considerar pasar de la paz a la guerra, hay al menos tres criterios inmediatos que la mayoría de los estados preferirían tener a su favor: finalidad adecuada, autoridad debidamente constituida y último recurso.[17] Una política

de destrucción cibernética mutuamente asegurada sería especialmente dura en cada criterio: la política no opera solamente yendo a la guerra en defensa propia, ya que la naturaleza de la seguridad cibernética excluye cualquier noción real de poder defenderse eficazmente contra un ciberataque masivo; también existe el riesgo de que la destrucción cibernética mutuamente asegurada eluda la notificación gubernamental apropiada debido a que el debilitamiento total dependería en gran parte del elemento de sorpresa, que funciona contra la transparencia y el carácter abierto premeditados; y por último, la destrucción cibernética mutuamente asegurada por naturaleza propia es la antítesis del último recurso—la eficacia de la posición procede de no ser puramente de represalia sino potencialmente prioritaria, indicando la voluntad de usar armas virtuales en circunstancias no solamente desesperadas.

Muchos argumentarían que desde una perspectiva puramente política/diplomática, estas posiciones parecen algo insostenibles. Esto sería cierto si la destrucción cibernética mutuamente asegurada se configurara estructuralmente, de modo que Estados Unidos domine esas capacidades ofensivas solo y de hecho, convirtiéndose en un tirano virtual cara a cara con otras grandes potencias. Pero según se trató antes, la estructura inherente del dominio cibernético hace que dicho objetivo, incluso si es lógico para una gran potencia, es muy poco probable y casi imposible. Por lo tanto, todos los estados que se afanen en una destrucción cibernética mutuamente asegurada harían esfuerzos relativamente iguales en armarse. Esto permite la posibilidad con el tiempo de una percepción de igual debilitamiento para surtir efecto y discutiblemente crear estímulos de disuasión similares a la destrucción nuclear mutuamente asegurada.

La incomodidad política y diplomática inicial relacionada con la destrucción cibernética mutuamente asegurada no mejora cuando se considera el derecho a la guerra, o el deseo de que los estados mantengan los principios de justicia en guerra. Nuevamente, se pueden resaltar tres criterios principales: inmunidad para los no combatientes, proporcionalidad y más bien que mal.[18] Una política de destrucción cibernética mutuamente asegurada seguiría teniendo la ventaja principal de cualquier sistema de defensa cibernético: que es relativamente incruento. No obstante, la ventaja empieza a ser más ambigua según la destrucción cibernética mutuamente asegurada; un ataque masivo contra la infraestructura de un estado, el debilitamiento de los mecanismos y funciones sociales importantes, resultaría casi ciertamente en sufrimiento para los no combatientes y por lo tanto no garantizaría inmunidad en el sentido más formal. La proporcionalidad claramente no puede cumplirse simplemente porque el punto de una política de destrucción cibernética mutuamente asegurada sería asegurar la defensa mediante un segundo ataque de represalia *no proporcional*. Sería la garantía de la respuesta/ataque no proporcional la que causaría el impulso disuasorio. Por último, el criterio de más bien que mal según la destrucción cibernética mutuamente asegurada sería realmente, al final, una interpretación completamente arbitraria basada en qué lado y qué objetivos de seguridad se están considerando.

Se ha hecho poco trabajo hasta la fecha en una conceptuación explícita de una ciberestrategia ofensiva y transparente para aumentar la seguridad nacional. Lo que se ha hecho es lograr un consenso general de que hay tres formas evidentes en que un estado podría crear la capacidad de infringir daños a otro adversario tipo estado o no estado mediante un ciberataque. La primera opción es simplemente crear la capacidad de nuestras propias fuerzas y tecnologías. La segunda opción es cultivar una fuerza de voluntarios que pueda guiarse para atacar objetivos designados con poca o ninguna atribución del gobierno que los apoya. La tercera opción es subcontratar al menos partes del problema a otros gobiernos, entidades comerciales u organizaciones clandestinas criminales siguiendo un modelo prácticamente mercenario.[19] Cada opción tiene claramente sus propios errores.

Tanto China como Rusia formal e informalmente juegan con la idea de utilizar las opciones una y dos. Estados como Irán, Corea del Norte y Nigeria han estado al menos curiosamente relacionados con la opción tres. Tal vez esta es la mayor dificultad que impacta la formulación de políticas de Estados Unidos—parece plausible que Estados Unidos simplemente no quiera con-

siderar un cambio de política que se asocie tan claramente con este grupo de países, fueran cuales fueran las ventajas. De las tres opciones, la primera opción tiene la mayor posibilidad de ser considerada por parte de Estados Unidos, ya que esta política de creación propia sería al menos discutiblemente controlable y podría ser definida explícitamente por instituciones democráticas estadounidenses con sus controles inherentes informados por principios de transparencia y responsabilidad.

Estados Unidos tiene ciertamente la capacidad de desarrollar cuadros orgánicos asignados a la tarea de desarrollar un dominio cibernético armado. Pero donde se ha hecho esto hasta ahora ha sido en pequeña escala y en áreas muy secretas. Estas características hacen que sea una capacidad de *ataque* evidente estructurada más eficazmente para usar en el contexto de una agresión abierta y guerra en vez de según se necesita en última instancia—como una capacidad *disuasoria* diseñada para prevenir que dicha agresión se produzca en épocas de paz. Nuevamente, la máxima ventaja de la destrucción cibernética mutuamente asegurada no radica en lograr verdaderamente una capacidad de segundo ataque *útil* sino en crear con el tiempo la credibilidad en dichas represalias de modo que no sea necesario nunca el segundo ataque.

Las otras dos opciones no permiten dicha oportunidad de una política realmente gobernable y responsable y no es probable que sea considerada por Estados Unidos. Este artículo no reta la premisa que inicialmente una política de destrucción cibernética mutuamente asegurada pondría a Estados Unidos en algunas posiciones políticas bastante extrañas. En vez de eso, adopta la posición más fundamentalmente maquiavélica de que la seguridad nacional se administra mejor mediante eficacia y control, incluso a expensas de la imagen diplomática y las percepciones públicas de rectitud.

Conclusión

La mayoría de los analistas, especialistas militares y oficiales del gobierno admiten que la vida en el siglo XXI incluirá ciberataques. No existe una visión de un mundo libre sin tales ataques. Esta simple admisión socava la eficacia de un sistema de disuasión cibernética cuya razón de ser es la prevención de dichos ataques. Este artículo no lleva tanto la contraria como para discutir anárquicamente el abandono del esfuerzo a fin de lograr una seguridad cibernética real. En vez de eso, pide que finalmente se dé a ciertas realidades estructurales un espacio intelectual en la mesa de debates y que se permita ese espacio para considerar nuevas opciones y posibilidades. Hay dos realidades estructurales en particular en las que se debe hacer hincapié. Primero, en el dominio cibernético la ofensa domina siempre y siempre lo hará. Es estructural y axiomático. Segundo, las capacidades, la tecnología y el talento existen para instituir este sistema en Estados Unidos. Lo que se necesita es un cambio de mentalidad y estimular nuevas ideas y políticas—de modo transparente. No es fácil en absoluto, pero se puede lograr.

La imposición de una política de destrucción cibernética mutuamente asegurada podría demostrar ser más efectiva, aun cuando pueda incomodar más a Estados Unidos política y diplomáticamente. El debate continúa y el argumento sigue: se puede conseguir una mayor seguridad cibernética mediante un debilitamiento mutuamente asegurado para todos. ❑

Notas

1. Mark Young, "National Cyber Doctrine: The Missing Link in the Application of American Cyber Power" (Doctrina cibernética nacional: el eslabón perdido en la aplicación del poder cibernético de EE.UU.), *Journal of National Security Law and Policy* 4, no. 1 (2010): 173–96.

2. Ibid.

3. Martin C. Libicki, *Cyberdeterrence and Cyberwar (La disuasión y la guerra cibernéticas),* (Santa Monica, CA: RAND, 2009).

4. Arthur Bright, "Estonia Accuses Russia of Cyberattack" (Estonia acusa a Rusia de un ataque cibernético), *Christian Science Monitor*, 17 mayo de 2007, http://www.csmonitor.com/2007/0517/p99s01-duts.html.

5. Alan W. Dowd, "Are We Ready for WWI?" (¿Estamos listos para la Primera Guerra Mundial?), *Fraser Forum,* septiembre de 2009, 12–14.
6. James Cartwright, "Afirmación ante el Subcomité de Fuerzas Estratégicas del Comité de Servicios Armados del Senado", 28 de marzo de 2007.
7. Eric D. Trias y Bryan M Bell, "Cyber This, Cyber That . . . So What?" (Ciberesto, cibereso ... ¿y qué?) *Air and Space Power Journal* 24, no. 1 (Verano de 2010): 90–100.
8. Ibid.
9. Ibid.
10. Ruzena Bajcsy y otros, "Cyber Defense Technology Networking and Evaluation" (Redes y evaluación de la tecnología de defensa cibernética), *Communications of the Association of Computing Machinery* 47, no. 3 (marzo de 2004): 58–61.
11. Ibid.
12. William J. Lynn, "Defending a New Domain" (Defensa de un nuevo dominio), *Foreign Affairs* 89, no. 5 (septiembre/octubre de 2010).
13. Ibid.
14. Ibid.
15. Ibid.
16. Libicki, *Cyberdeterrence and Cyberwar (Disuasión y guerra cibernéticas).*
17. Andrew Liaropoulos, "War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory" (La guerra y la ética en el ciberespacio: conflicto cibernético y teoría de la guerra justa), *Minutas del 9º Congreso Europeo sobre guerra y seguridad de información* (Reading, Reino Unido: Academic Publishing, Ltd., 2010), 177–82.
18. Ibid.
19. Rain Ottis, "Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability" (El modelo teórico para crear una capacidad cibernética ofensiva a nivel de nación-estado), *Minutas del 8º Congreso Europeo sobre guerra y seguridad de información,* (Reading, Reino Unido: Academic Publishing, Ltd., 2009), 177–82.

El Dr. Matthew Crosston es presidente de Seguridad Industrial e Internacional de la Fundación Miller y Director del Programa de Estudios Internacionales de Seguridad e Inteligencia (ISIS, por sus siglas en inglés) en la Universidad Bellevue, Nebraska. Es autor de dos libros bien reconocidos y diez artículos revisados por homólogos sobre temas que abarcan contraterrorismo, corrupción, democratización, Islam radical y disuasión cibernética. Su agenda de investigación continúa en esos campos a la vez que se enfoca en conceptos nuevos de conflictos futuros. Crosston ha hecho presentaciones y ha hablado por todo el mundo para fomentar la interacción transnacional entre las agencias de inteligencia que comparten intereses comunes pero que carecen de canales de conectividad. El Dr. Crosston ostenta una licenciatura en arte de la Universidad Colgate, New York; una maestría de la Universidad de Londres, y un doctorado de la Universidad Brown, Rhode Island (2003). Después de terminar sus estudios de posdoctorado en la Universidad de Toronto, Crosston pasó a formar parte del cuerpo docente en Relaciones Internacionales y Política Comparativa en la Universidad Clemson, South Carolina, antes de trasladarse al Instituto Militar de Virginia para enfocarse en la Seguridad Nacional y Estudios Internacionales. En el 2010 llegó a la Universidad Bellevue para desarrollar el programa ISIS, una iniciativa que fue comenzada bajo los auspicios del programa ISIS, una iniciativa que fue comenzada bajo los auspicios del USSTRATCOM. Dos características destacadas del programa ISIS son la relación proactiva con miembros militares actuales y antiguos que buscan continuar su educación y el uso emprendedor de la tecnología de punta con métodos de entrega en línea a la vez que no se sacrifican ni el rigor intelectual ni el aprendizaje activo.

Fuente: Publicado anteriormente en nuestra revista Strategic Studies Quarterly, Spring 2011

Los Años Interinos del Ciberespacio

Teniente 1° Robert M. Lee, USAF

No hay nada más difícil de emprender, ni más peligroso de llevar a cabo, ni más incierto de hacer triunfar que tomar la iniciativa en la introducción de un nuevo orden de cosas.

—Maquiavelo

EN LOS PRIMEROS años del ámbito ciberespacial el papel que el ciberpoder desempeñaba era principalmente considerado como un medio para lograr el mando y control a lo largo de los ámbitos bélicos. La comunicación era el enfoque principal del ámbito y garantizar que las líneas de comunicación se mantuviesen era imprescindible para el éxito operacional. A medida que el ámbito creció, funciones adicionales fueron definidas para ofrecer una fuerza de apoyo a las operaciones militares tradicionales mientras se exploraban otras funciones con los niveles más altos de confidencialidad. Muchos de los primeros líderes ciberespaciales se percataron que los recursos cibernéticos ofrecían varias opciones de ataque, defensa y explotación que nunca se les había permitido a los comandantes militares. En un mundo sumamente conectado con grandes adelantos en la tecnología en común, las capacidades y el armamento ciberespacial se tornaron cada vez más impresionantes.

La etapa actual del desarrollo ciberespacial es similar a los años interinos entre la Primera y Segunda Guerra Mundial cuando el poderío aéreo fue retado y surgió como una herramienta militar principal y poderosa. Ninguna otra situación le hace mejor justicia a la situación actual en el ciberespacio que el poderío aéreo durante esos años iniciales. Fue durante los años iniciales del poderío aéreo que teóricos y oficiales militares, entre ellos el Mariscal del Aire italiano, Giulio Douhet; el Mariscal de la Real Fuerza Aérea, Hugh Trenchard; y el General de Brigada William "Billy" Mitchell, ayudaron a guiar la dirección del poderío aéreo. Mediante un enfoque en compartir inteligencia cibernética procesable, exhibiendo capacidades cibernéticas selectas, adoptando el desarrollo de la cibercultura y dedicando un mayor enfoque en la educación, la dirección del ciberpoder se puede guiar por igual. A medida que el ciberespacio alcanza su potencial completo como un dominio bélico igual a los ámbitos tradicionales, es imprescindible que se oriente correctamente.

Los años interinos del poderío aéreo

Antes de la Primera Guerra Mundial el empleo de aeronaves estaba sumamente limitado y muchos no lo consideraban como una opción militar viable. Por ejemplo, William H. Pickering, en su libro titulado *Aeronautics* publicado en 1908, expresó que "otra falacia popular es suponer que las máquinas voladoras se podrían volar para lanzar dinamita sobre un enemigo durante una guerra". Sin embargo, tan solo seis años más tarde, el 14 de agosto de 1914, una aeronave francesa *Voisin* fue utilizada para bombardear los hangares de zepelines alemanes en Metz-Frascaty.[1] La idea de que una guerra aérea se pudiese emplear en combate rápidamente cobró importancia. Durante los próximos años, se fabricaron aeronaves de bombardeo estratégico y se utilizaron en redadas aéreas, inclusive durante las redadas alemanas en Gotha en Inglaterra.[2] Sin embargo, el concepto de utilizar aeronaves y globos en la guerra no era una idea nueva. Uno de los usos en la antigüedad fue en el Siglo III en China cuando el General Zhuge Liang utilizó linternas Kongming para enviar señales a las fuerzas militares y ahuyentar a los enemigos.[3] Sin embargo,

tomó adelantos en la tecnología y demostraciones de fuerza poderosas durante la Primera Guerra Mundial para agilizar la importancia y el uso del ámbito.

Con el éxito del poderío aéreo durante la Primera Guerra Mundial, inclusive la destrucción por parte del Tte. Frank Luke, Jr., de catorce globos alemanes muy vigilados[4], para muchos líderes militares les fue obvio que las aeronaves podrían ofrecer una misión de apoyo a los ámbitos tradicionales de la guerra terrestre y naval. En aquel entonces el debate no era si se podría o no emplear el poder aéreo, sino cómo se desarrollaría y cuál rama del servicio tomaría la delantera. En los años durante la Primera y la Segunda Guerra Mundial el enfoque de la aviación era ofrecer defensa de los adversarios.[5] El enfoque en la defensa era uno importante pero algunas de las capacidades de defensa aérea también ofrecieron posibilidades de ofensiva. La flexibilidad del poder aéreo creó debates intensos entre el Ejército y la Armada porque las aeronaves del Cuerpo Aéreo del Ejército podían cumplir funciones que tradicionalmente le pertenecían a la Armada.

En 1921, el General William "Billy" Mitchell llevó a cabo una prueba en la que intentó hundir buques navales con sus bombarderos MB-2 desde Langley Field, Virginia. Su misión fue un éxito y los bombarderos hundieron tres buques que se utilizaron para la prueba, inclusive un buque de guerra capturado de los alemanes con el nombre de *Ostfriesland*.[6] La prueba del General Mitchell mostró que las aeronaves podían actuar independientemente para atacar blancos costa afuera. Además demostró que si el Ejército continuaba otorgándole poderes a su Cuerpo Aéreo, la Armada podría perder su responsabilidad principal de proveer defensa en la costa.

En 1925, en parte refutando la prueba del General Mitchell contra el *Ostfriesland*, la Armada reveló un plan para aumentar la cifra de aeronaves basadas costa afuera de 334 a 583.[7] El General de División Mason Patrick, Jefe del Servicio Aéreo, opinaba que esta era una movida por parte del Departamento de la Armada para lograr el control de la misión de defensa de toda la costa.[8] La disputa entre el Ejército y la Armada continuó intensificándose y los líderes de ambos servicios se preocuparon porque si no llegaban a una solución el Congreso podría crear un cuerpo aéreo independiente.[9] A pesar de los intentos de intervención por parte del Departamento de Guerra y el Congreso para satisfacer ambos servicios, el conflicto continuó.[10] En medio de los desacuerdos de los servicios, el General Mitchell recomendó fuertemente que se necesitaba una rama del servicio aparte. Se dirigió al público para hacer declaraciones y obtener su apoyo en un intento de presionar al Congreso para que actuara.[11] Después del consejo de guerra del General Mitchell, en 1926 renunció del Servicio Aéreo del Ejército de EE.UU., y continuó haciendo campaña públicamente por una Fuerza Aérea independiente.[12]

En 1934, al General Henry "Hap" Arnold, se le encomendó la misión de volar desde Dayton, Ohio, hasta Alaska con diez bombarderos B-10 *Martin*. Durante su regreso a Ohio se desvió de su ruta volando un tramo del viaje sobre el océano en lugar de atravesar Canadá. Esto demostró el alcance de los bombarderos sobre la costa y al hacerlo enojó al Jefe de Estado Mayor del Ejército, General Douglas MacArthur.[13] Comenzó a tornarse obvio para los miembros del Congreso y del Departamento de Guerra que quizás se necesitaba otra rama del servicio. El General Mitchell y otros defensores del poderío aéreo continuaron abogando por esta rama aparte.[14] Las acciones de miembros clave tales como el General Arnold y el General Mitchell ayudaron a crear una Fuerza Aérea independiente, pero esas acciones no se necesitan en el ámbito ciberespacial. Sin embargo, las lecciones aprendidas de la creación del ámbito aéreo ofrecen opiniones importantes en cuanto a estrategias eficaces para la creación del ámbito ciberespacial.

Lecciones aprendidas del Poderío Aéreo

El ámbito ciberespacial no usurpa las misiones tradicionales ni del Ejército, ni de la Fuerza Aérea, ni de la Armada. La cibermisión tiene la capacidad de trabajar tanto independientemente de, y sinérgicamente con, los ámbitos bélicos tradicionales a lo largo de cada sector del servicio.

El ciberpoder también puede proveer apoyo a la defensa nacional, capacidades de recopilación de inteligencia y acciones de ofensiva iguales o mayores que otras acciones militares. Sin embargo, la idea de que las capacidades cibernéticas por sí solas pueden ganar una guerra es un razonamiento limitado. El ciberpoder, muy parecido al poderío aéreo, puede ser un poder destructivo si se ejerce por sí solo y en su totalidad. Los primeros hombres del aire sentían orgullo al creer que los ataques aéreos solamente podrían conducir a la victoria en la guerra; aunque no comprendían cuán destructivos podían ser si no se les controlaba y la importancia de limitar el conflicto. [15] Asimismo, los ciberentusiastas deben adoptar el ciberpoder, pero en su verdadera capacidad como un componente de la fuerza militar combinada.

Durante la Guerra de Vietnam, el Presidente Lyndon Johnson y el Secretario de Defensa, Robert McNamara, se reunían semanalmente para discutir los blancos que los pilotos bombardearían. Lo que antes se consideraba una fiscalización política, el verdadero motivo de escoger blancos era para controlar las implicaciones políticas que los ataques aéreos presentaban.[16] El poder nuevo, y en muchos casos aterrador, ocasionado por los ataques aéreos fue una afirmación fuerte no solamente para los norvietnamitas sino también para otras naciones que seguían la situación muy de cerca. El ciberpoder también tiene la capacidad de hacer afirmaciones influyentes y no se puede controlar a la ligera. Un ciberataque que destruye una aeronave, inutiliza un buque de guerra o colapsa la bolsa de valores tendrá consecuencias enormes en un sentido político. Estos tipos de ataques no solamente son poderosos sino que se pueden lanzar desde cualquier parte del mundo.

El Mariscal del Aire italiano Douhet pensaba que el alcance de las aeronaves lograría que civiles y combatientes por igual serían atacados en guerras futuras. Según su razonamiento, el poder aéreo no conocía los límites de los campos de batalla tradicionales y podría actuar sin inhibiciones. Los civiles no se sentirían seguros en ninguna zona sin fronteras en el campo de batalla.[17] De esta misma manera, la capacidad del ciberpoder de atacar rápida y específicamente las redes y sistemas de informática en el mundo torna borrosa las líneas de los campos de batalla. Es esta característica, en combinación con su fuerza destructiva, lo que causa un nivel de temor en torno a las capacidades cibernéticas. La opinión entre la población de que pueden ser impactados instantáneamente por los ciberataques puede ser tan poderosa como el temor en torno a los ataques terroristas. No se puede pasar por alto el poder de esa opinión para influenciar la opinión popular y la política al igual que su capacidad de guiar la dirección del desarrollo de la capacidad cibernética. El ciberpoder siempre tiene que ser una de las muchas herramientas políticas a disposición de los comandantes militares y los líderes civiles. Nunca deber ser el único propósito de la guerra.

La idea de que la tecnología eliminará la naturaleza desagradable de la guerra es una que ha influenciado a los planificadores militares a lo largo de la historia de la guerra.[18] El Mariscal del Aire Douhet opinaba que la naturaleza intrínsecamente ofensiva de la guerra, luego reafirmada famosamente por la declaración de Sir Stanley Baldwin que "el bombardero siempre sobrevivirá"[19], limitaría el derramamiento de sangre durante la guerra. Él creía que bombardear ciudades y atacar civiles resultaría en menos bajas que el choque de ejércitos y las bajas resultantes de la guerra.[20] La opinión del Mariscal del Aire Douhet que el estado de ánimo de los civiles sería destrozado con la introducción del bombardeo estratégico era errónea. Según él, este estilo de ataque haría que los civiles les exigieran a sus líderes que le dieran fin a la guerra lo antes posible. En cambio, los bombardeos por lo regular reafirmaban el estado de ánimo de los civiles contra el enemigo.[21] La cuestión en el ciberespacio es que sin la atribución correcta puede que nunca se conozca al enemigo. Esto podría surtir efectos desconocidos en la población civil, inclusive un estado de ánimo destrozado similar a lo que el Mariscal del Aire Douhet había pronosticado originalmente. Indistintamente de los efectos de un ciberagresor desconocido, el Mariscal del Aire Douhet continuaría equivocado acerca de la capacidad de la tecnología de darle fin al derramamiento de sangre. La tecnología se debe investigar y debe haber nuevos adelantos

tanto en el ciberespacio como en los ámbitos bélicos tradicionales, pero la naturaleza de la guerra siempre prevalecerá; la guerra es algo desagradable.[22]

La idea del General Mitchell sobre el poder aéreo era notablemente diferente a las filosofías del Mariscal del Aire Douhet en que el General Mitchell no creía en atacar civiles. Sin embargo, opinaba que era eficaz atacar la infraestructura y los sectores de la industria para limitar las capacidades del adversario. Tampoco creía que los bombarderos eran el prototipo del poderío aéreo. El General Mitchell pensaba que se necesitaban múltiples tipos de aeronaves, inclusive aquellas con misiones enfocadas, en la ofensiva y el reconocimiento.[23] El concepto que el General Mitchell tenía del poder aéreo es más similar a la naturaleza diversa actual del ciberpoder y varios recursos. Además, poder contar con múltiples aeronaves daba lugar al desarrollo de plataformas aéreas de inteligencia, vigilancia y reconocimiento (ISR, por sus siglas en inglés) y capacidades aéreas de ofensiva que ayudan a garantizar el dominio aéreo y el apoyo a otros ámbitos bélicos.[24] Agregar otros tipos diferentes de capacidades ciberespaciales provee un incremento directo a las operaciones ISR y de ofensiva ya establecidas a la vez que permite el desarrollo de operaciones nuevas.

Los comandantes y la ciberinteligencia procesable

El ciberpoder ofrece ventajas imprescindibles para la planificación de la campaña. Para poderles ofrecer opciones más oportunas a los comandantes es beneficioso que las ciberoperaciones existan en la preparación de la fase del entorno operacional. Esta fase incluye comprometer las redes enemigas y preparar las armas cibernéticas para usarlas en caso de un conflicto. Mientras se preparan para las ciberoperaciones defensivas, la información se puede aprovechar de sistemas comprometidos y puede ayudar en la Preparación de Inteligencia Conjunta del Entorno Operacional (JIPOE, por sus siglas en inglés).[25] Mediante esta información recopilada, los comandantes cuentan con más concienciación de la situación del campo de batalla.

Los comandantes emplean la planificación de la campaña para "sincronizar esfuerzos" y plantear pautas complementarias.[26] Las dos fases más importantes del proceso de planificación, planificación de contingencia y planificación de acción en caso de crisis, se benefician de la información oportuna y de las opciones de ataque que el ciberpoder presenta. Mientras más las suposiciones y los planes elaborados en la fase de contingencia se aproximen a la fase de acción en caso de crisis, más se agiliza el Proceso Conjunto de la Planificación Operacional (JOPP, por sus siglas en inglés).[27] Este proceso de selección rápido le confiere a los comandantes la capacidad de atacar primero, seleccionar el blanco con precisión y estar más aprestos para defenderse de contraataques. La información recopilada de la fase de preparación del entorno operacional también disminuye la eficacia de los intentos de engaño por parte del enemigo.

Con acceso a la doctrina militar, las fuerzas enemigas podrían optar por evitar cursos de acción (CoA, por sus siglas en inglés) eficaces o inclusive falsos, y de lo contrario interesantes. La combinación de capacidades cibernéticas e ISR pueden detectar esos engaños. Las múltiples plataformas ISR, tales como aeronaves piloteadas, aeronaves piloteadas por control remoto (RPA, por sus siglas en ingles), satélites e inteligencia recopilada por humanos, contribuyen a la creación de la preparación de inteligencia del campo de batalla (IPB).[28] Individualmente, la cibernética e ISR debilitan gravemente la capacidad del enemigo de esconder tropas, información confidencial, planes operacionales y centros de gravedad (CoG, por sus siglas en inglés). La combinación de los dos mediante la inteligencia de imágenes (IMINT), la inteligencia de señales (SIGINT), la inteligencia humana (HUMINT) y las operaciones en la red de computadoras (CON) les ofrecen a los comandantes un nivel sin precedentes de la concienciación de la situación en el campo de batalla. Esta concienciación de la situación también permite las operaciones ciberespaciales que proveen capacidades, inclusive plataformas de sistemas de armamento que

degradan, interrumpen y destruyen las comunicaciones, el control y los recursos físicos del adversario.

La concienciación de la situación que la cibernéticas e ISR les proveen a los comandantes ayuda a establecer enunciados de intención realistas y holísticos tal come se discute en el modelo JOPP. Mediante la creación de mejores enunciados de intención, la guía de planificación del comandante será más precisa y ayudará en la selección de mejores cursos de acción.[29]

Nunca antes se habían presentado esas capacidades al proceso de planificación militar. Esas opciones son presentadas en la totalidad de las operaciones militares y minimizan la incertidumbre de la guerra a la que Carl von Clausewitz le llamaba la niebla de la guerra.[30] Mediante una planificación más precisa y operaciones cibernéticas ofensivas y defensivas oportunas las probabilidades de lograr el éxito operacional son más altas que nunca a la vez que también limitan los costes humanos y financieros de la guerra.

Sin embargo, estas capacidades cibernéticas no han pasado desapercibidas y la organización del Comando Cibernético de Estados Unidos indicó que el ámbito ciberespacial se está moviendo en la dirección correcta.[31] No obstante, se necesitaba, y aún se necesita, más acción para proporcionarles a los comandantes inteligencia procesable y capacidades a través de las operaciones cibernéticas. El General de División Brett T. Williams esbozó su opinión para la dirección del ciberespacio en su escrito titulado "*10 Propositions Regarding Cyberspace Operations*" (Diez propuestas con respecto a las operaciones ciberespaciales). En su escrito, el General de División Williams mencionó que los Comandantes de la Fuerza Conjunta y los Comandantes Combatientes (COCOM, por sus siglas en inglés) necesitaban que se les confirieran capacidades cibernéticas y comando y control (C2) de las operaciones cibernéticas. Sin la visibilidad de los componentes cibernéticos, los cuales son esenciales para el éxito de una misión, los comandantes están en desventaja. El General de División Williams sugirió la creación del Comando de Operaciones Cibernéticas en el Teatro, similar al Comando de Operaciones Especiales en el Teatro, para ofrecerles a los comandantes combatientes capacidades cibernéticas bajo el control de los COCOM.[32] La aptitud para los comandantes de solicitar facultades cibernéticas pertinentes a su misión y contar con la concienciación de la situación cibernética para hacerlo correctamente es uno de los componentes más esenciales de sacarle provecho al ciberpoder.

Este aspecto de sacarle provecho eficazmente al ciberpoder en los COCOM ha adquirido atención desde el escrito del General de División Williams. Durante el verano de 2011, el General Keith Alexander, jefe del Comando Cibernético de EE.UU., discutió los progresos en apoyo a las operaciones en Irak y Afganistán mediante el despliegue de equipos expedicionarios. Luego pasó a revelar que el progreso se ha llevado a cabo en apoyar la planificación operacional por parte de los comandantes combatientes a través de una mayor facultad para ellos de solicitar apoyo cibernético.[33]

Hay mucho por hacer en el ámbito ciberespacial para proveerles a los comandantes ciberinteligencia y capacidades. Uno de los temas relacionados con esto es la clasificación de la información. Para proteger las aptitudes cibernéticas resulta importante no revelar ciertos detalles y tecnologías, hacerlo le permitiría a los adversarios contrarrestarlas o protegerse contra ellas. Sin embargo, en la actualidad la inteligencia y la información recopilada de las aptitudes cibernéticas se clasifica demasiado. Muchos comandantes sencillamente no conocen todo lo que hay disponible y por lo tanto no pueden solicitar esas capacidades. En lugar de solamente proveer procesos para solicitar requisitos cibernéticos, debe haber un verdadero esfuerzo para desclasificar la ciberinteligencia e información que no debilitan las aptitudes cibernéticas. Esto no solo apoyará a los comandantes sino que también les permitirá a los líderes a nivel táctico hacer solicitudes razonables a sus líderes en apoyo a las operaciones diarias. Además, la desclasificación de alguna ciberinteligencia e información permitiría compartir más entre las agencias gubernamentales y los líderes civiles que operan en las agencias policiales. Posiblemente aún más importante, compartir ciberinteligencia procesable que pueda ayudar a las redes de defensa les permitiría a los líderes

civiles proteger mejor sectores tales como la infraestructura imprescindible. Poder compartir información resultaría en una correlación directa en mayor seguridad nacional.

Armas cibernéticas y el frente interno

En junio de 2010 el gusano *Stuxnet* fue descubierto y rápidamente se granjeó la mala fama de ser uno de los pedazos de *malware* más avanzados jamás descubiertos. El gusano, un pedazo de *malware* que se autogenera y se esparce entre los sistemas de informática, se aprovechó de cuatro vulnerabilidades sin precedentes de sistemas no actualizados, conocidas como vulnerabilidades de día cero, a la vez que empleaba el primer *rootkit* de controlador lógico programable (PLC, por sus siglas en inglés), o un pedazo de código que permite el acceso persistente, a la vez que se aprovechaba del uso de dos servidores de mando y control y certificados firmados legítimamente.[34] El sistema de armamento parte de esta arma cibernética fue impresionante pero palideció en comparación con la naturaleza avanzada de la porción de carga útil.

Stuxnet fue concebido específicamente para atacar los sistemas *SCADA* (Control de Supervisión y Adquisición de Datos) y los sistemas de control industriales (ICS, por sus siglas en ingles); con más exactitud, la carga útil atacaba específicamente los PLC que controlaban las centrífugas en la instalación nuclear iraní en Natanz. La carga útil del gusano pudo dañar físicamente las centrífugas haciéndolas girar rápidamente y luego aminorando la velocidad al punto de llevarlas a las velocidades correctas para lograr una degradación máxima.[35] Aunque se desconocen los resultados completos del gusano, se sabe, a través de imágenes de satélite, que más de mil centrífugas fueron destruidas en la planta de Natanz. [36] Esta hazaña requirió algunos de los mejores programadores e ingenieros ICS/PLC del mundo a la vez que le sacaron provecho a un mejor entendimiento de la distribución de la instalación secreta de Natanz que la mayoría de los ingenieros que en algún momento trabajaron en la instalación.[37]

Considerado en gran medida como una arma cibernética creada y empleada por al menos una nación estado, *Stuxnet* lanzó discusiones intensas y múltiples escritos académicos sobre el uso del ciberespacio como un ámbito de la guerra. El embajador ruso ante la OTAN llegó a expresar que el gusano *Stuxnet* pudo haber ocasionado "un Chernobyl nuevo" si el programa hubiese dejado escapar gas de uranio en las centrífugas en lugar de causar una degradación. [38] Aunque las operaciones cibernéticas anteriormente habían tenido lugar en el ciberespacio, la descripción de los medios de comunicación del poder del arma cibernética *Stuxnet* hizo que la discusión de la ciberguerra fuese una muy pública. *Stuxnet* hizo para el ciberespacio lo que los bombardeos iniciales durante la Primera Guerra Mundial hicieron para el poder aéreo; hizo que la discusión fuese pública e indudablemente obligó a muchas corporaciones y naciones estados a investigar más a fondo en cuanto las capacidades cibernéticas. De cierta manera este evento, junto con las operaciones cibernéticas del pasado durante las últimas décadas inclusive los ciberataques en el 2007 contra el gobierno y sectores financieros en Estonia[39] y los ciberataques en el 2008 que coincidieron con la invasión rusa del Georgia[40], representan el inicio de los años interinos del ciberespacio.

Aunque el *Stuxnet* pudo infectar y extenderse a miles de sistemas de computadoras sus únicos blancos reconocidos fueron las centrífugas en Natanz. El evento no surtió gran impacto en los sistemas en Estados Unidos ni llegó al nivel de un ciberataque que empujó a una nación a la guerra. No obstante, el Secretario de Defensa, Leon Panetta, expresó que "El potencial para el próximo Peral Harbor podría muy bien ser un ciberataque".[41] Junto con las declaraciones del General Alexander en las que ha expresado que hay segmentos de la infraestructura crítica de la nación que en la actualidad no están preparados para lidiar con ciberataques, y que esto es lo que más le preocupa[42], resulta obvio que proteger estos recursos contra ciberataques es de suma

importancia. Además, *Stuxnet* ha mostrado que estas capacidades cibernéticas existen y al menos una nación estado las ha utilizado.

Pero el relato del *Stuxnet* no ha terminado. Un pedazo del *malware* identificado como *Duqu* se encontró el 14 de octubre de 2011, y rápidamente se reconoció que estaba relacionado con el *malware Stuxnet*. *Duqu* es diferente al *Stuxnet* en que es un Troyano de Acceso Remoto (RAT, por sus siglas en inglés) que roba información en lugar de un gusano que daña centrífugas.[43] El RAT infectó varios sitios diferentes, inclusive universidades, fábricas y autoridades de certificación en un estilo de ataques que su utilizarían para crear otra arma cibernética al estilo *Stuxnet*.[44] Aunque diferente en estilo y blancos, *Duqu* empleo gran parte del mismo código fuente de *Stuxnet* y los dos han sido vinculados como que han sido creados por el mismo equipo de codificación empleando una plataforma de codificación común conocida como *Tilded*.[45]

La plataforma *Tilded* ha sido descrita como ser similar a un "conjunto de legos" donde se unen diferentes piezas, o módulos, de código para crear un *malware* completamente diferente.[46] Este método basado en una plataforma le permite al equipo crear un arma cibernética que puede adaptarse rápidamente a usar diferentes módulos y cargas útiles para emplearlas contra diferentes blancos a la vez que produce resultados diferentes. Además, el *malware* creado de la plataforma se puede actualizar con diferentes medidas furtivas inclusive cambiar los algoritmos de codificación empleados para esconder su código como se hizo con una versión actualizada del *Duqu* descubierto en febrero de 2012.[47]

Un método basado en plataforma hacia el armamento es una dirección que la guerra aérea ha estado tomando por años. En lugar de diseñar aeronaves con una sola función, el DoD ha comprado aeronaves tales como el F-16, F-22 y MQ-1 que pueden cumplir con conjuntos de misiones completamente diferentes con base en el tipo de carga útil con las que están equipadas. Este método basado en plataforma está cobrando popularidad en el ámbito ciberespacial y plantea una serie de riesgos a diferentes aspectos de la seguridad nacional. Un sola plataforma de arma cibernética puede ser responsable de robar información de universidades y fabricantes para crear múltiples armas cibernéticas que luego atacarían aeronaves, nódulos de *Internet* esenciales para el mando y control, sistemas de defensa aérea e infraestructura crítica.

El General Norton Schwartz ha declarado que la Fuerza Aérea está buscando "métodos cibernéticos para derrotar aeronaves" mientras que otras fuentes han indicado que la tecnología ya está disponible.[48] El Tte. Gen. Herbert Carlisle expresó, "Los rusos y los chinos han diseñado plataformas específicas de guerra electrónica para atacar nuestros recursos de gran valor. El ataque electrónico puede ser el método de penetrar un sistema para implantar viruses".[49] A medida que los sistemas de armamento tradicionales basados en plataforma se tornan más diversos y emplean más capacidades, tales como sistemas de radar avanzados, se tornan más vulnerables a los ciberataques. Estas vulnerabilidades cibernéticas hacen que los beneficios de las plataformas de armas cibernéticas sean más atrayentes para los adversarios. Las vulnerabilidades combinadas con las capacidades demostradas por la plataforma *Tilded* muestran que la amenaza de un sistema de armamento cibernético basado en plataforma atacando múltiples sectores del DoD y civiles no es solo posible sino probable.

Es durante estos años interinos del ciberespacio que el gobierno debe acudir a los líderes civiles en sectores tales como la infraestructura crítica para garantizar la seguridad nacional. Los operadores, ingenieros y diseñadores de infraestructura crítica ofrecen perspicacia aguda en cuanto a los sistemas que se deben proteger activamente; sin embargo, ellos solo pueden ofrecer detalles completos acerca de sus sistemas y el entendimiento que tienen de esos sistemas cuando reciben inteligencia procesable del gobierno. Si se les presenta con ciberinteligencia procesable, desclasificada al nivel correcto, las contrapartes civiles pueden ofrecer un mejor asesoramiento sobre cómo defender los sistemas que ellos han estado operando por años. Si bien tiene sentido clasificar algunas capacidades de ofensiva cibernética, también es igual de prudente dejar algu-

nas capacidades de defensa cibernética clasificadas. Algunas defensas cibernéticas deben ser transparentes en gran parte de manera que las debilidades se puedan identificar y remediar.[50]

Inclusive incidentes no cibernéticos relacionados con ICS y el sistema SCADA surten impactos significativos que muestran la capacidad de poder afectar drásticamente las poblaciones civiles. El 17 de agosto de 2009, la represa Shushenskaya, la más grande en Rusia con una altitud de 245m, experimentó un ataque no cibernético que estremeció el centro sur de Siberia. Una turbina de novecientas cuarenta toneladas fue rasgada cuando un aumento repentino en la presión del agua que fue el resultado de un incendio en una planta de energía a más de quinientas millas. El incidente resultó en la muerte de 75 personas y costos de reconstrucción de $1,3 mil millones de dólares.[51] Este incidente no estuvo relacionado con un ciberataque ni Shushenskaya fue el blanco de ninguna nación estado, pero el evento representa un incidente que se podría llevar a cabo mediante un ciberataque deliberado. Si un incidente similar fuese el resultado de un ataque sumamente deliberado, el evento podría tener impactos más severos con mayor muertes de civiles y costos financieros.

La instalación de enriquecimiento nuclear Natanz y la represa Shushenskaya son tan solo dos ejemplos de los usos de los sistemas ICS y SCADA. Estos sistemas afectan cada aspecto de la vida cotidiana inclusive desempeñando funciones en la bolsa de valores, la industria del petróleo, la red de suministro eléctrico, filtración de agua y las redes de comunicación en la *Internet* y por satélite. Por lo tanto los sistemas ICS y SCADA son unos de los blancos más solicitados y viables de armamento cibernético basado en las naciones estados y deben tratarse como corresponde. La protección de estos sistemas es importante en la evolución del ámbito ciberespacial, pero el enfoque más importante se debe colocar en ganar el ámbito a la larga. No hay mejor manera de garantizar el éxito de la seguridad nacional a largo plazo que en la educación de la próxima generación.

Ganando la próxima generación

Para poder tener éxito en el ámbito ciberespacial, el DoD y los socios civiles deben colocar énfasis en la educación de la próxima generación. Hay una escasez crítica en la disponibilidad de profesionales expertos en ciberseguridad para trabajos, inclusive investigación forense y programación. La escasez hace que llenar trabajos, tales como los de la División Cibernética del FBI, sea difícil.[52] El DoD también se encuentra en una posición difícil cuando se trata de la educación de la próxima generación. El Dr. Michael Wertheimer, Director de Investigación y Desarrollo de la NSA, les informó a los miembros del Subcomité de Servicios Armados del Senado, que la agencia estaba teniendo problemas en reclutar y retener profesionales en el campo de la ciencia de la computación. Continuó expresando que el 75% de del personal de tecnología de informática en la NSA renuncia antes de jubilarse.[53] Si bien el tema de hacer que los salarios sean competitivos con los de la empresa privada puede que sea uno que hay que tratar, la estrategia a largo plazo tiene que ser una de aprender de las lecciones obtenidas del ámbito aéreo.

Durante los inicios del poderío aéreo había emoción y un sentido de magia en torno a las aeronaves y sus pilotos. Los primeros pilotos desafiaron situaciones peligrosas en un ámbito previamente desconocido para batir el récord y cautivar a las multitudes. La *Reims Air Meet*, que tuvo lugar el 22 de agosto de 1909 en Francia, fue la primera demostración de acrobacia aérea más importante del mundo y abrió las puertas para que muchos shows aéreos se celebraran en el mundo.[54] Estos primeros hombres y mujeres mantuvieron a las multitudes cautivadas en las demostraciones de acrobacia y competencias aéreas que no tan solo inspiraron a pilotos futuros sino que educaron al público sobre las capacidades del poderío aéreo. [55] Las demostraciones de acrobacia aérea cobraron más atención durante el periodo entre la Primera y la Segunda Guerra

Mundial con las Competencias Aéreas Nacionales; en 1929, una sola demostración de acrobacia aérea atrajo más de medio millón de personas.[56]

Durante la década de los años veinte hubo una era dorada y un misticismo en torno al vuelo. Había competencia para volar más alto, más rápido y más lejos que nadie. Tres veces entre 1919 y 1921 pilotos del Ejército batieron records mundiales de altitud.[57] Los ciberoperadores no tienen que desafiar velocidades peligrosas ni acrobacias como lo hicieron los primeros pilotos, pero hay una capacidad real para que las capacidades cibernéticas cautiven muchedumbres e inspiren a la próxima generación de ciberoperadores.

La piratería informática y las conferencias de seguridad muestran los últimos adelantos en la seguridad, las vulnerabilidades y las explotaciones. Las conferencias también ofrecen una manera para aquellos que asisten de entrar en contacto con personas con una variedad de experiencias quienes poseen en común una cierta pasión por el ciberespacio. Lamentablemente, esas conferencias no son tan baratas como las primeras demostraciones de acrobacia aérea ni son tan adoptadas por el público. Si bien algunas conferencias bastante conocidas, tales como DEF CON, cuestan $150 dólares para asistir[58] otras cuestan miles de dólares para asistir con adiestramiento opcional que es inclusive más costoso.[59] Aunque los precios se pueden entender en gran medida con base en el tipo de audiencia a la que el evento trata de llegar al igual que los costos operacionales, hay problemas con lograr que la mayoría del público asista a conferencias relacionadas con el ciberespacio.

Hay otras conferencias y adelantos en la educación relacionados con la cibernética que se organizan y benefician al ámbito. El *Defense Cyber Crime Center (DC3)* (Centro de Crímenes Cibernéticos del Depto. de Defensa) auspicia anualmente competencias y convenciones de cibernética forense que son una gran oportunidad para hacer contactos, aprender acerca de los últimos adelantos en la tecnología e inscribirse para asistir a cursos de entrenamiento. Las competencias forenses son gratis pero el costo para asistir a las conferencias es $500 dólares.[60] El gobierno y el DoD deben hacer más esfuerzos para crear conferencias a un bajo costo semejantes a las demostraciones de acrobacia aérea. En estas conferencias se pueden mostrar las capacidades y se le puede permitir al ciberespacio la oportunidad de crear su propio sentido de magia y atractivo.

El vice presidente retirado del Estado Mayor Conjunto, General (USMC) James Cartwright, expresó que algunas de las capacidades de ofensiva cibernética se deben tratar abiertamente y debe haber entrenamiento en ellas en un esfuerzo de aumentar la disuasión cibernética.[61] Las conferencias cibernéticas serían un lugar de reunión perfecto para que los miembros del DoD exhibieran algunas de las capacidades cibernéticas de la nación. Esto tendría el beneficio de atraer espectadores y exhortar a la generación siguiente a la vez de disuadir a los adversarios que retasen la nación. Además, los ciberoperadores podrían dictar clases a bajo costo, o quizás gratis, sobre los conceptos básicos de la ciberseguridad y la piratería de informática las cuales ofrecerían maneras divertidas e interactivas de permitir que la generación siguiente se interesase en el ámbito que van a heredar.

Educar a los jóvenes y lograr que se interesen en la cibernética es increíblemente importante y es un campo en el cual la nación en la actualidad carece conocimientos. No obstante, el DoD está tomando medidas en la dirección correcta en sus esfuerzos para educar y entrenar a líderes jóvenes, oficiales y suboficiales por igual, que se han inscrito para tomar parte en el ámbito ciberespacial. Un ejemplo excelente es la escuela técnica de Entrenamiento Básico en Cibernética (UCT, por sus siglas en inglés) de la Fuerza Aérea, ubicada en la Base Aérea Keesler, Mississippi. La UCT abrió sus puertas el 21 de junio de 2010, y les ofrece a los oficiales especializados en cibernéticas un curso de seis meses de duración que concluye con los estudiantes obteniendo sus Alas Ciberespaciales.[62] La escuela reprueba a los estudiantes que no pasan los bloques de instrucción ofrecidos y a los estudiantes o bien se les vuelve a entrenar en nuevos Códigos de Especialidad de la Fuerza Aérea (AFSC, por sus siglas en inglés) o se les separa de la Fuerza Aérea.

La educación ofrecida en la UCT es de gran calidad debido en parte al cuerpo docente que consta de oficiales y suboficiales de la Fuerza Aérea que cuentan con conocimiento y experiencia personal en las operaciones ciberespaciales. Estos instructores trabajan para inspirar y capacitar a la siguiente generación de oficiales ciberespaciales a la vez que cumplen con la visión del General Norton Schwartz que una carrera exitosa deben incluir desempeñarse como instructor.[63] Desempeñarse en calidad de instructor no solo le permite al cuerpo docente a superarse en sus destrezas y objetivos académicos sino también relacionarse y capacitarse con aquellos que serán los líderes jóvenes en sus futuros escuadrones. Estas relaciones crean un nivel de participación tanto en instructores como estudiantes y contribuye a la cultura cibernética en general.

A medida que los instructores hablan de sus experiencias y los estudiantes se emocionan por crear sus propios relatos hay un nivel de pasión que se le agrega al ámbito. Los pilotos instructores y los veteranos de guerra tienen la capacidad de inspirar a la siguiente generación al igual que individuos que participan en varias misiones cibernéticas.

La cultura inicial en torno al poder aéreo inclusive actuó en desafío hacia sus superiores y personal que no eran pilotos para granjearse aceptación y reverencia entre sus coetáneos. Integrantes del Cuerpo Aéreo del Ejército obtendrían estatus en sus grupos al provocar problemas y reprimendas de líderes del Ejército. Ellos adoptaron por ser los marginados y esto les confirió más poder. Ellos crearon un grupo diverso de individuos y cultura en torno al vuelo.[64] Los profesionales militares del ciberespacio no necesitan tomar medidas tan drásticas ni retar a las autoridades. El entorno militar actual es favorable para el crecimiento del ámbito ciberespacial y, como se ha mencionado anteriormente, no hay necesidad de contar con un servicio cibernético independiente como lo hubo para el poder aéreo durante el periodo del Cuerpo Aéreo del Ejército. Sin embargo, la cultura ciberespacial militar puede sentirse como un grupo marginado a causa del hecho de que el ámbito es relativamente nuevo con capacidades no exploradas e incomprendidas.

La cibercultura ya existe en su infancia y debe ser adoptada en lugar de rechazarla. Con un enfoque en la educación y la acogida de una opción competitiva y provechosa de poder desempeñarse como instructor para los miembros militares, la cibercultura crecerá y se desarrollará por derecho propio. Los mejores operadores ciberespaciales deben competir para desempeñarse en calidad de instructores y se les debe premiar con oportunidades de crecimiento personal y profesional como resultado. De esta manera, la educación ofrecida será actualizada continuamente a la vez que vigoriza a los operadores ciberespaciales que participan en ella. Asimismo, una cibercultura fuerte y singular se desarrollará e intrínsecamente atraerá y mantendrá apasionados a los individuos dedicados al establecimiento del dominio cibernético.

Conclusión

Las semejanzas entre los ámbitos bélicos tradicionales, especialmente el ámbito aéreo, ofrecen muchas lecciones que los líderes pueden utilizar para guiar la dirección del ciberespacio. No obstante, el ámbito cibernético es intrínsecamente diferente de los demás ámbitos de la guerra ya que es un ámbito creado por el hombre y como tal puede cambiarse drásticamente.[65] La infraestructura que compone el ciberespacio se puede modificar y dividir en varias redes como es obvio en el uso de NIPR, SIPR, JWIC y NSANet por parte de los militares. Al separar redes de otras redes y sitios web, añadir protocolos de seguridad y métodos de autenticación tales como un CAC, y vigilar las redes en busca de actividad de redes maliciosas, la seguridad de una red puede aumentar exponencialmente. Esta habilidad de cambiar el ámbito ciberespacial no solo se extiende a la porción militar del ámbito sino al ámbito ciberespacial a nivel nacional. La infraestructura civil también se puede separar donde las redes que requieren seguridad en la red, un ejemplo de ello son los sectores financieros, podrían operar independientemente de la *World*

Wide Web (red de redes mundial o www). Los portales entre la *World Wide Web* y las redes más seguras existirían para ofrecer acceso a cualquiera, sin embargo, en esos portales puede haber capas adicionales de seguridad para disminuir la capacidad de llevar a cabo actividad maliciosa en la red.[66] Las opciones diferentes para el ámbito ciberespacial en términos de infraestructura física se deben analizar y colocarse bajo un examen muy riguroso. No obstante, este no es el enfoque de lo que el ámbito debe fijarse en la actualidad.

El enfoque actual para el ámbito ciberespacial debe ser cibernética procesable, compartir ciberinteligencia y educación. Los comandantes deben contar con el conocimiento de lo que pueden solicitar en términos de apoyo de los ciberoperadores quienes se beneficiarán directamente de sus misiones. La reducción de información demasiado clasificada en lo que se refiere a la ciberinteligencia y capacidades cibernéticas, le otorgará el poder a los líderes a los niveles táctico, operacional y estratégico. Además, la información desclasificada se puede compartir con los sectores civiles para aumentar la concienciación cibernética y la creación de estrategias de defensa significativas. Esto reafirmaría la seguridad nacional al permitirles a los líderes civiles ayudar a defender sus sectores en lugar de depender únicamente del DoD y el DHS. Por último, algunas de las capacidades cibernéticas y ciberinteligencia podrían exhibirse en eventos de aprendizaje y conferencias. Esto no solo aumentaría la disuasión cibernética a los adversarios sino que inspiraría a la generación siguiente a participar en el ámbito ciberespacial. La generación siguiente debe continuar siendo la estrategia a largo plazo para proteger el ámbito y establecer el dominio cibernético.

Tal como expresó el General Alexander, "Si las personas que buscan hacernos daño en el ciberespacio aprenden que hacerlo es costoso y difícil, creemos que veremos cambios en sus patrones de comportamiento".[67] No es solamente la tecnología la que está preparada. Las partes interesadas a lo largo del ciberespacio inclusive el DoD, sectores civiles y la siguiente generación también están preparados para los retos venideros. El ciberpoder es una herramienta política y militar poderosa y deben ser guiada y su lugar en la historia fortalecido. Los años interinos del ciberespacio están ocurriendo ahora y los líderes a todos los niveles deben actuar como corresponde para garantizar el éxito de la era siguiente. ❑

Notas

1. Alan Axelrod, *Little-known Wars of Great and Lasting Impact: The Turning Points in Our History We Should Know More About* (Guerras poco conocidas de gran impacto y duración: Momentos decisivos en nuestra historia que debemos saber) (Beverly, MA: Fair Winds Press, 2009), 222.

2. D. Stevenson, *With Our Backs to the Wall: Victory and Defeat in 1918* (Con nuestras espaldas contra la pared: Victoria y derrota en 1918) (London: Penguin, 2012), 186.

3. Andreas Wittmer y Thomas Bieger, *Aviation Systems Management of the Integrated Aviation Value Chain* (Gestión de sistemas de aviación de la cadena de valor de la aviación integrada) (Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg, 2011), 7.

4. Portal oficial de la Fuerza Aérea de EE.UU., "2nd Lt. Frank Luke Jr.," 2 de noviembre de 2010, http://www.af.mil/news/story.asp?storyID=123006460.

5. Tte Col Dr. James P. Tate (ret.), *The Army and its Air Corps: Army Policy Toward Aviation, 1919-1941* (El Ejército y su Cuerpo Aéreo: Política del Ejército hacia la aviación, 1919-1941) (Maxwell Air Force Base, AL: Air University Press, 1998), 33.

6. Capt B. Chance Saltzman y Thomas R. Searle, *Introduction to the United States Air Force* (Introducción a la Fuerza Aérea de Estados Unidos) (Maxwell AFB, AL: Airpower Research Institute, College of Aerospace Doctrine, Research and Education and Air University Press, 2001), 6.

7. Tte Col Dr. James P. Tate (ret.), *The Army and its Air Corps: Army Policy Toward Aviation,* 62.

8. Pamela Feltus, "Mason Patrick and the Creation of the U.S. Air Corps," (Mason Patrick y la creación del Cuerpo Aéreo de EE.UU.) *U.S. Centennial of Flight Commission,* http://www.centennialofflight.gov/essay/Air_Power/Patrick/AP15.htm.

9. Tte. Col Dr. James P. Tate (ret.), *The Army and its Air Corps: Army Policy Toward Aviation,* 67.

10. Ibid., 68.
11. Ibid., 190.
12. National Museum of the U.S. Air Force (Museo Nacional de la USAF), "Brig. Gen. William 'Billy' Mitchell," 11 de febrero de 2010, http://www.nationalmuseum.af.mil/factsheets/factsheet.asp?id=739.
13. Capt B. Chance Saltzman y Thomas R. Searle, *Introduction to the United States Air Force*, 12.
14. Ibid.
15. Col David A. Moore, *The Art of Aerial Warfare* (El arte de la guerra aérea) (Maxwell Air Force Base, AL: Air University Press, 2005), 17.
16. Ibid., 19.
17. Giulio Douhet, *The Command of the Air* (El comando del aire) (Washington, D.C.: Office of Air Force History, 1983), 9.
18. Col David A. Moore, *The Art of Aerial Warfare*, 68.
19. Sir Stanley Baldsin, "A Fear for the Future" (Temor del futuro), discurso pronunciado ante el Parlamento británico el 9 de noviembre de 2011.
20. Giulio Douhet, *The Command of the Air,* 22-23.
21. Col David A. Moore, *The Art of Aerial Warfare*, 33.
22. John Stuart Mill, "The Contest in America" (La competencia en Estados Unidos) *Dissertations and Discussions* 1 (1868): 26.
23. David R. Mets, *The Air Campaign: John Warden and the Classical Airpower Theorists* (La campaña aérea: John Warden y los teóricos clásicos del poderío aéreo) (Maxwell Air Force Base, AL: Air University Press, 1999), 39.
24. Benjamin S. Lambeth, "Airpower, Spacepower, and Cyberpower" (Poder aéreo, poder espacial y ciberpoder) en *Toward a theory of Spacepower: Selected Essays* (Hacia una teoría del poder espacial: Ensayos seleccionados) editado por Charles D. Lutes, Peter L. Hays, Vincent A. Manzo, Lisa M. Yambrick y M. Elaine Bunn (Washington, DC: National Defense University Press, 2011).
25. Joint Publication 5-0 (Publicación Conjunta 5-0), *Doctrine for Joint Operations* (Doctrina de las operaciones conjuntas) 11 de agosto de 2011.
26. U.S. Army War College, *Campaign Planning Primer* (Manual para la planificación de la campaña), Department of Military Strategy, Planning, and Operations (Departamento de Estrategia Militar, Planificación y Operaciones), AY 08.
27. Joint Publication 5-0, *Doctrine for Joint Operations*, 11 de agosto de 2011.
28. Maj Eric D. Trias y Capt Bryan M. Bell, "Cyber This Cyber That, So What?" (Ciber esto, ciber aquello, ¿y qué?), *Air and Space Power Journal* (Primavera 2010): 90-100.
29. Joint Publication 5-0, *Doctrine for Joint Operations*, 11 de agosto de 2011.
30. Carl von Clausewitz, Michael Howard y Peter Paret, *On War* (Sobre la guerra) (Princeton, NJ: Princeton University Press, 1976), 101.
31. U.S. Department of Defense (Depto. de Defensa de EE.UU.), "News Release: Cyber Command Achieves Full Operational Capability" (Comunicado de prensa: Comando Cibernético logra capacidad operacional total), *News Release*, 3 de noviembre de 2010, http://www.defense.gov/releases/release.aspx?releaseid=14030.
32. Gral de División Brett T. Williams, "Ten Propositions Regarding Cyberspace Operations" (Diez propuestas con respecto a las operaciones ciberespaciales), *Joint Force Quarterly*, no. 61 (2nd Quarter 2011): 10-17.
33. Gen Keith B. Alexander, "Building a New Command in Cyberspace" (Creando un comando nuevo en el ciberespacio), *Strategic Studies Quarterly* 5, no. 2 (Primavera 2011): 3–12.
34. Nicolas Falliere, Liam O Murchu y Eric Chien, *W.32 Stuxnet Dossier* (Expediente *Stuxnet* W.32), Symantec White Paper (Informe de *Symantec*) (Symantec: Security Response, February 2011), 1-2. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.
35. Ralph Langner, "*Stuxnet: A Deep Dive*"(*Stuxnet*: Un salto profundo). Vídeo 18 de enero de 2012, http://www.digitalbond.com/2012/01/31/langners-stuxnet-deep-dive-s4-video/.
36. Yaakov Katz, "Stuxnet May Have Destroyed 1,000 Centrifuges at Natanz" (*Stuxnet* puede haber destruido 1.000 centrífugas en Natanz), *The Jerusalem Post*, 24 de diciembre de 2010, http://www.jpost.com/Defense/Article.aspx?id=200843.
37. Ralph Langner, "*Stuxnet: A Deep Dive,"* 18 Jan 2012 video.
38. Ellen Messmer, "Stuxnet Could Have Caused 'New Chernobyl,' Russian Ambassador Says" (Embajador ruso alega que *Stuxnet* pudo haber provocado un "Chernobyl nuevo"), *Network World*, 27 de enero de 2011, http://www.networkworld.com/news/2011/012711-stuxnet-chernobyl.html.
39. Biony Kampmark, "Cyber Warfare Between Estonia and Russia" (Ciberguerra entre Estonia y Rusia), *Contemporary Review* (Autumn, 2003): 288-293.

40. John Markoff, "Before the Gunfire, Cyberattacks" (Antes de los disparos, ciberataques), *The New York Times*, 12 de agosto de 2008. http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1.

41. Jason Ryan, "CIA Director Leon Panetta Warns of Possible Cyber-Pearl Harbor" (Secretario de la CIA, Leon Panetta, advierte de un posible ciber-Pearl Harbor) *ABC News,* 11 de febrero de 2011, http://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905#.T5M2ABHoK5I.

42. Charlie Rose, "Charlie Rose Talks to General Keith Alexander" (Charlie Rose conversa con el General Keith Alexander), *Businessweek,* 21 de julio de 2011, http://www.businessweek.com/magazine/charlie-rose-talks-to-general-keith-alexander-07212011.html.

43. Boldizsar Bencsath, Gabor Pek, Levente Buttyan y Mark Felegyhazi, *Duqu: A Stuxnet-like Malware Found in the Wild* (*Duqu:* Se descubre un *malware* parecido a *Stuxnet*) , Laboratory of Cryptography and System Security Technical Report (Budapest University of Technology and Economics: Department of Telecommunications, October 2011), 6-7.

44. Symantec, "W32.Duqu: The Precursor to the Next Stuxnet" (W32.*Duqu*: El precursor al siguiente *Stuxnet*), Symantec *Security Response*, 24 de octubre de 2011, http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet.

45. Kaspersky Lab, "Duqu and Stuxnet Not the Only Malicious Created by the Responsible Team" (Duqu y Stuxnet no son los únicos maliciosos creados por el equipo responsable), *Virus News*, 29 de diciembre de 2011, http://www.kaspersky.com/about/news/virus/2011/Kaspersky_Lab_Experts_Duqu_and_Stuxnet_Not_the_Only_Malicious_Programs_Created_by_the_Responsible_Team.

46. Rob Waugh, "Lethal Stuxnet Cyber Weapon is 'Just one of Five' Engineered in Same Lab" (Arma cibernética letal *Stuxnet* es "una de cinco" diseñadas en el mismo laboratorio), *Daily Mail*, 29 de diciembre de 2011, http://www.dailymail.co.uk/sciencetech/article-2079725/Lethal-Stuxnet-cyber-weapon-just-engineered-lab.html.

47. Greg Masters, "Duqu Variant Uncovered" (Se descubre variante del *Duqu*), SC *Magazine*, 23 de marzo de 2012, http://www.scmagazine.com/duqu-variant-uncovered/article/233385/.

48. TSgt Richard A Williams Jr., "CSAF Stresses Importance of Ready Future Force" (Jefe de Estado Mayor de la USAF recalca la importancia de una fuerza preparada para el futuro), *Official Site of the U.S. Air Force*, 24 February 2012, http://www.af.mil/news/story.asp?id=123291264.

49. Eloise Lee, "Electronic Warfare Weapons" (Armas de guerra electrónica), *Business Insider*, 15 de marzo de 2012, http://www.businessinsider.com/electronic-warfare-weapons-2012-3.

50. Thomas Rid, "Cyber War Will Not Take Place" (Ciberguerra no ocurrirá), *Journal of Strategic Studies* 35, no. 1 (Febrero de 2012): 5-32.

51. Thomas Rid y Peter McBurney, "Cyber-Weapons" (Armas cibernéticas), *The RUSI Journal* 157, no.1 (Febrero/Marzo de 2012), 6-13.

52. Kevin Coleman, "United States at Risk from Shortage of Trained Cybersecurity Professionals" (Estados Unidos en riesgo de escasez de profesionales capacitados en ciberseguridad), *Defense Systems*, 22 de junio de 2011, http://defensesystems.com/articles/2011/06/08/digital-conflict-cyber-worker-shortage.aspx.

53. Brian Donohue, "Experts Tell Senate: Government Networks Owned, Resistance Is Futile", *Threatpost*, 21 de marzo de 2012, http://threatpost.com/en_us/blogs/experts-tell-senate-government-networks-owned-resistance-futile-032112.

54. David H. Onkst, "Explorers, Daredevils, and Record Setters: An Overview" (Exploradores, temerarios y establecedores de record), *U.S. Centennial of Flight Commission,* http://www.centennialofflight.gov/essay/Explorers_Record_Setters_and_Daredevils/EX_OV.htm.

55. David H. Onkst, "The First U.S. Airshows - the American Air Meets of 1910" (Las primeras demostraciones de acrobacia aérea en EE.UU. – Las competencias aéreas de 1910), *U.S. Centennial of Flight Commission,* http://www.centennialofflight.gov/essay/Explorers_Record_Setters_and_Daredevils/Early_US_shows/EX4.htm.

56. David H. Onkst, "Air Shows - An International Phenomenon" (Demostraciones de acrobacia aérea – Un fenómeno internacional), *U.S. Centennial of Flight Commission,* http://www.centennialofflight.gov/essay/Social/airshows/SH20.htm.

57. Tte Cnel Dr. James P. Tate (ret.), *The Army and its Air Corps: Army Policy Toward Aviation,* 27.

58. DEF CON, "Official DEF CON FAQ," https://www.defcon.org/html/links/dc-faq/dc-faq.html.

59. Hacker Halted, "Registration" (Matrícula), http://www.hackerhalted.com/2011/Registration.aspx.

60. DoD Cyber Crime Conference (Conferencia del DoD sobre Crimen Cibernético), "Registration" http://www.dodcybercrime.com/12CC/register.asp.

61. Andrea Shalal-Esa, "Ex-U.S. General Urges Frank Talk on Cyber Weapons" (Ex-general de EE.UU. exhorta discusiones sinceras sobre armas cibernéticas), *Reuters,* 6 de noviembre de 2011, http://uk.reuters.com/article/2011/11/06/us-cyber-cartwright-idUKTRE7A514C20111106?mid=520.

62. Bruce Rolfsen, "3,000 Officers Switch to Cyberspace Specialty" (Tres mil oficiales cambian a especialidad en ciberseguridad), *Air Force Times,* 17 de mayo de 2010, http://www.airforcetimes.com/news/2010/05/airforce_cyber_careers_051710/.

63. Gen Norton A. Schwartz, Jefe de Estado Mayor. A todo el personal de Fuerza Aérea, Memorándum, 8 de marzo de 2012.

64. Tte Cnel Dr. James P. Tate (ret.), *The Army and its Air Corps: Army Policy Toward Aviation,* 192.

65. Gen de División Brett T. Williams, "Ten Propositions Regarding Cyberspace Operations."

66. Richard A. Clarke y Robert K. Knake, *Cyber War* (Ciberguerra), (NY: HarperCollins, 2010), 161.

67. Gen Keith B. Alexander, "Building a New Command in Cyberspace."

En la actualidad el Teniente 1° Robert M. Lee, USAF, está destacado en Alemania trabajando para la Agencia de Inteligencia, Vigilancia y Reconocimiento de la Fuerza Aérea. Es egresado de la Academia de la Fuerza Aérea y de la escuela técnica de Adiestramiento Básico en Cibernética. El Teniente Lee ha publicado y hecho presentaciones a nivel internacional en temas que incluyen sistemas de control de ciberseguridad, ciberguerra, amenazas cibernéticas avanzadas y armas cibernética de naciones estados en el futuro.

Stuxnet: Revolución de Ciberguerra en los Asuntos Militares

Mayor Paulo Shakarian, USA

EL 17 DE JUNIO DE 2010, investigadores de seguridad en una pequeña empresa belarusa conocida como *VirusBlockAda* identificó un *software* malicioso (*malware*) que infectó memorias USB.[1] En los meses siguientes, hubo una oleada de actividades en la comunidad de seguridad informática—revelando que este descubrimiento identificaba solamente un componente de un nuevo gusano informático [2] conocido como *Stuxnet*. Este *software* fue diseñado específicamente para afectar equipo industrial. Una vez que se reveló que la mayoría de las infecciones fueron descubiertas en Irán,[3] junto con un inexplicable retiro del servicio de centrífugas en la planta de enriquecimiento de combustible (FEP, por su siglas en inglés) iraní en Natanz,[4] muchos en los medios de comunicación especularon que la meta final de *Sutxnet* era atacar las instalaciones nucleares iraníes. En noviembre de 2010, algunas de esas sospechas fueron confirmadas cuando el presidente iraní, Mahmoud Ahmadinejad, aceptó públicamente que un gusano informático había creado problemas para una "cifra limitada de nuestras centrífugas nucleares". [5] Expertos acreditados en la comunidad de seguridad informática ya han catalogado al *Stuxnet* como "sin precedentes"[6], un "salto evolutivo "[7], y el "tipo de amenaza que esperamos nunca más ver nuevamente".[8] En este artículo, yo sostengo que este *software* malicioso representa una revolución de asuntos militares (RMA, por sus siglas en inglés)[9] en el ámbito virtual—o sea, que *Stuxnet* básicamente cambia la naturaleza de la ciberguerra. Hay cuatro razones para sustentar lo anterior: (1) *Stuxnet* representa el primer caso en el que equipo industrial es atacado con un arma cibernética, (2) hay pruebas que el gusano tuvo éxito en su ataque de dicho equipo, (3) esto representa un adelanto significativo en el desarrollo de *software* maliciosos y (4) *Stuxnet* ha mostrado que varias suposiciones comunes acerca de la seguridad cibernética no siempre son válidas. En este artículo analizo estos cuatro puntos al igual que exploro las implicaciones futuras del *Stuxnet* RMA.

STUXNET ATACA EQUIPOS INDUSTRIALES

Varias empresas importantes de seguridad informática han analizado el *Stuxnet*[10] a cabalidad y todas concuerdan que la meta principal de este *software* fue causar fallas imperceptibles al equipo industrial. Aunque la posibilidad de atacar ese equipo por medios cibernéticos hace mucho tiempo fue planteada como una hipótesis, este nuevo gusano cibernético en realidad intentó la hazaña. Además, este tipo de ataque fue probablemente la única meta del *software*. Por ejemplo, otros *malware* incluyen códigos estándares para una variedad de actividades delictivas—inclusive robo de identidad y de contraseñas, lanzamiento de ataques de denegación de servicio y envío de correos electrónicos *spam*.[11] A pesar de su alto grado de complejidad técnica, *Stuxnet* no fue concebido para llevar a cabo ninguna de esas actividades.[12] Más bien, el *software* intenta auto propagarse con la meta de infectar una computadora basada en *Microsoft Windows* que se comunica con el equipo industrial. Esto es en marcado contraste con el gran número de *software* en la *Internet* que se emplea para una variedad de fines delictivos. *Stuxnet* fue concebido para el sabotaje, no para la delincuencia.

El tipo de equipo industrial que *Stuxnet* infecta se conoce como los sistemas *SCADA* (Control de Supervisión y Adquisición de Datos). Estos sistemas están diseñados para la recopilación, control y vigilancia de datos en tiempo real de infraestructuras críticas, inclusive plantas de ener-

gía, oleo/gasoductos, refinerías, sistemas de agua u otras aplicaciones que requieren equipo controlado por computadoras.[13] Los sistemas *SCADA* a menudo utilizan PLCs (controladores lógicos programables) —*hardware* para controlar un componente físico. Para programar el PLC, el administrador lo conecta a una computadora *Windows* estándar. Entonces por lo regular el PLC se desconecta de la computadora cuando está listo para usarse. Por ejemplo, si el administrador desea que las centrífugas funcionen a una velocidad más rápida, conecta el PLC a la computadora *Windows,* instala un *software* que se comunica con el PLC y sube las nuevas instrucciones. Supongamos que *Stuxnet* ha infectado la computadora conectada al PLC. El *malware* básicamente lleva a cabo un "ataque mediante intermediario" en contra del sistema. El administrador intenta enviar los comandos al PLC. *Stuxnet* los intercepta y envía sus propias instrucciones. Sin embargo, el *software* somete un informe falso a la computadora *Windows* que las instrucciones originales fueron cargadas. Al someter un informe falso, *Stuxnet* se esconde, convirtiéndolo más difícil de detectar.

Stuxnet fue diseñado para atacar los PLC controlados por el *software Step 7* de *Siemens.*[14] Además, solamente infecta dos modelos de PLC—el *Siemens S7-315* y el *S7-417.* El S7-315 es un controlador de uso general que funciona una sola gama de dispositivos. Esa gama, o grupo, de dispositivos controlados por el *S7-315* puede, por ejemplo, operar diferentes fases de un proceso de fabricación. El *S7-417* es el mejor modelo en la línea, operando múltiples gamas de dispositivos—por ende, capaz de controlar más equipo que el *S7-315.*[15] Expertos en seguridad han concluido que *Stuxnet* solamente lanza ataques si el PLC está conectado a dispositivos configurados de una manera muy específica. Por ejemplo, cuando el gusano detecta el *S7-315*, solamente ataca si el PLC está conectado a 33 o más convertidores de frecuencia—dispositivos empleados para controlar la velocidad de cierto equipo (por ejemplo, las revoluciones por minuto de un motor).[16] Asimismo, al atacar el PLC *S7-417*, espera encontrar 6 cascadas de 164 convertidores de frecuencia.[17] El *malware* también garantizaba que los convertidores de frecuencia fuesen fabricados por la compañía iraní *Fararo Paya* o la compañía finlandesa *Vacon.*[18]

Una vez que *Stuxnet* ha determinado que ha infectado la configuración objetivo de los convertidores de frecuencia, lanza el ataque. Con base en el análisis del *software*, expertos han descubierto que esperan que los convertidores de frecuencia estén funcionando entre los 807 y 1.210 Hz. Luego, periódicamente altera estos valores entre 2 y 1.410 Hz.[19] De esta manera, el dispositivo que está controlado por el convertidor de frecuencia funciona de una manera inesperada. A medida que *Stuxnet* reporta que el PLC fue programado correctamente, el operador daría por sentado que los dispositivos están funcionando en la gama normal. El hecho de que *Stuxnet* ajusta estas configuraciones ilustra un punto importante—que el propósito del gusano cibernético era en realidad dañar el equipo industrial. Si *Stuxnet* fuese tan solo una prueba del concepto, o un truco, el ajuste de las frecuencias probablemente sería innecesario.[20]

STUXNET PROBABLEMENTE TUVO EXITO

Stuxnet fue concebido no solamente para atacar equipo industrial sino que hay pruebas que tuvo éxito en ello. Los indicadores del éxito surgen del siguiente razonamiento. Primero, parece que las infecciones iniciales del gusano ocurrieron en Irán. Segundo, las estructuras de los datos en el código *Stuxnet* se asemejan a la configuración de las centrífugas en el FEP iraní en Natanz. Tercero, funcionarios del gobierno iraní admitieron que las operaciones de sus centrífugas fueron afectadas por el gusano.

Tal parece que Irán fue el epicentro de los ataques. Esto es corroborado por el volumen de infecciones al igual que los análisis de las muestras de *malware.* La empresa de seguridad *Symantec* rastreó 100.000 máquinas infectadas a partir del 29 de septiembre de 2010—aproximadamente 60.000 de las cuales se encontraban en Irán. Luego le siguió Indonesia con 15.000 infecciones.[21] *Symantec*, en combinación con otras empresas de seguridad, recopiló 3.280 ejemplos singulares

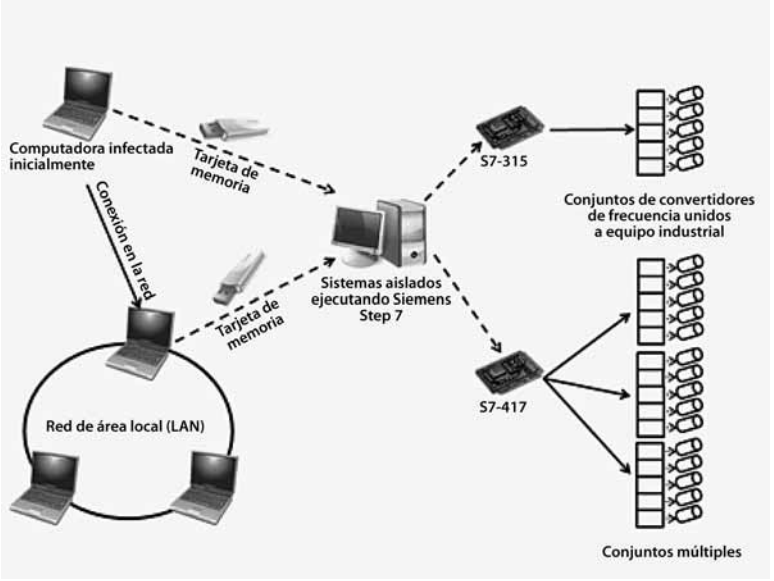

Figura: La propagación del gusano cibernético Stuxnet

del *software Stuxnet* y sus variantes.[22] Esas muestras representaron un total de 12.000 infecciones. *Stuxnet* mantiene una lista de sistemas infectados anteriormente. Por ende, para una muestra en particular, los investigadores pudieron determinar la trayectoria que el gusano cibernético propagó para poder llegar a esa computadora. Al revisar esas muestras, Symantec pudo rastrear el historial de la infección a una de cinco organizaciones diferentes—las cuales todas tienen una presencia en Irán.[23]

De lo que se sabe de la FEP en Natanz, parece haber una semejanza asombrosa entre la configuración de su centrífuga y el código *Stuxnet*. Según la Agencia Internacional de Energía Atómica (IAEA, por sus siglas en inglés), las centrífugas IR-1 en el FEP en Natanz funcionan en cascadas de 164.[24] Esto se alinea justamente con la configuración que *Stuxnet* busca cuando ataca el controlador S7-417. Otro indicador potencial es la velocidad máxima de una centrífuga IR1: 1.400-1.432 Hz.[25] Este alcance de frecuencia es muy cerca a la velocidad máxima que el *malware* establece durante el ataque—1.410 Hz.[26] Una centrífuga IR-1 configurada a una frecuencia tan elevada probablemente causaría daños.

El proceso de enriquecimiento de uranio se puede optimizar si se divide en una serie de fases con centrífugas múltiples funcionando en cada fase.[27] En una entrevista en el 2006 se dio a conocer que los iraníes estaban llevando a cabo su enriquecimiento de uranio con ese método utilizando quince fases.[28] En cada fase, cierto número de centrífugas se distribuyen para lograr una producción óptima. Alexander Glaser, un profesor en el laboratorio de Futuros Nucleares de Princeton, analizó el arreglo óptimo de las centrífugas en una cascada de centrífugas de 164. Ralph Langer, fundador de *Langer Communications GmbH*, que se especializa en los sistemas SCADA, comparó este análisis a las estructuras de datos en *Stuxnet*. Él descubrió que el *malware* posiblemente funciona de una manera que interfiere significativamente con la distribución óptima de las centrífugas en cada fase. La distribución resultante parece ser lo contrario de óptimo según lo establecido por Glaser.[29] Si *Stuxnet* atacó las centrífugas en Natanz, hubiese resultado en

la producción menos que optima de uranio enriquecido—por ende la cantidad producida probablemente sería muy por debajo de la capacidad.

Además del análisis técnico mencionado anteriormente, también hay pruebas de la posible eficacia del *software* en las declaraciones de los líderes iraníes. En noviembre de 2010, el Presidente Ahmadinejad confirmó que la presencia de *software* malicioso había afectado sus centrífugas—aunque no describió explícitamente la presencia de *Stuxnet*.[30] En una entrevista con *SPIEGEL ONLINE* al secretario general del Consejo Supremo de Seguridad Nacional de Irán, Saeed Jalili, se le preguntó específicamente acerca del uso de *Stuxnet* para atacar a Natanz. Aunque Jalili no entró en detalles sobre los daños ocasionados por el gusano (nuevamente minimizando los efectos que tuvo), reconoció que había ocurrido un incidente al declarar que "nuestros expertos ya habían prevenido sobre este ataque hace mucho tiempo".[31]

Además, es interesante destacar que hay una posibilidad que *Stuxnet* fue instalado en Natanz por un saboteador utilizando una tarjeta de memoria.[32] En ese caso, los diseñadores del gusano aumentarían en gran medida sus probabilidades de éxito en lugar de esperar pasivamente que el *software* se propague a la instalación. En octubre de 2010, el ministro de inteligencia de Irán, Heydar Moslehi, anunció que una cifra no especificada de "espías nucleares" fueron arrestados en conexión con el *Stuxnet*.[33] Aunque se desconocen los detalles y la naturaleza de los arrestos, esto (como mínimo) ilustra que Irán reconoce que los diferentes métodos mediante los cuales el gusano pudo haberse propagado—al igual que la gravedad de su impacto en sus operaciones.

Cabe destacar que a finales del 2009, inicios del 2010, Irán retiró del servicio y reemplazó alrededor de mil centrífugas IR-1 en el FEP en Natanz (seis cascadas de 164 centrífugas cada una).[34] El momento escogido para retirar del servicio, junto con la cantidad de centrífugas que se sacaron del servicio, concuerda con el momento y las estructuras de datos del *Stuxnet*. La explicación obvia de la falla es un defecto de fábrica pero no está claro por qué un defecto de esa índole tomaría tanto tiempo en manifestarse.[35] Del análisis mencionado anteriormente, parece que *Stuxnet* no intenta destruir inmediatamente las centrífugas. Más bien, ajusta las frecuencias de una manera más sutil con el tiempo—lo que dificulta determinar si un problema fue ocasionado por el gusano o alguna otra parte del proceso de enriquecimiento. Este comportamiento del *malware* es una explicación más consistente con la retirada del servicio de las centrífugas. Además de retirar las IR-1, el FEP en Natanz también experimentó niveles menos que óptimos de la producción de uranio del 2009-2010. Informes de la IAEA muestran que la cantidad de uranio enriquecido producido en Natanz permaneció relativamente estable en ese momento a pesar del incremento considerable en la cifra de centrífugas.[36] Esto indica que el sistema estaba produciendo uranio por debajo del nivel óptimo.

A pesar de las alegaciones de los iraníes a fines del 2010 que el gusano *Stuxnet* tuvo un impacto mínimo en sus operaciones nucleares, el experto en seguridad, Ralph Langer, asegura que el *malware* atrasó dos años el programa nuclear de Irán.[37] Hay dos motivos por ello. Primero, como se mencionó anteriormente, el daño ocasionado por *Stuxnet* es más sutil—aunque probablemente muy eficaz. Por lo tanto, es difícil atribuir que la falla del equipo fue ocasionada por el *software*. Segundo, a causa de la naturaleza prolífera de *Stuxnet*, es muy difícil limpiar el *malware* de todos los dispositivos de computadora que participaron en el proceso de enriquecimiento. Puede que estas inquietudes expliquen por qué Irán detuvo temporalmente todas las operaciones de enriquecimiento en Natanz en noviembre de 2010 (por motivos desconocidos).[38]

Una pregunta natural de plantear es "¿Qué otros países fueron afectados por el *Stuxnet*?" Aunque hubo informes del gusano en equipo SCADA en Alemania[39], Finlandia[40] y China[41], ninguna de esas infecciones resultó en daños a los sistemas industriales. Esto puede que se deba a la configuración específica del PLC, ya que *Stuxnet* solamente lanza ataques en ciertos sistemas. *Siemens* alega que usuarios de solamente quince sistemas que usan su *software* reportaron infecciones. De esos quince sistemas, ninguno experimentó daños.[42] Es muy probable que Irán no informara las infecciones a *Siemens*. Aunque en el periodo de 2002-2003 adquirieron tarjetas controladoras S7-

315 y S7-417, la IAEA estableció que Irán desvió ese *hardware* a su programa nuclear—lo que resultó en *Siemens* poniéndole fin a las ventas.[43] Sin embargo, se sabe que la S7-417 fue instalada en Bushehr, que puede haber sido un blanco *Stuxnet*.[44] En Bushehr, la S7-417 no se obtuvo directamente de *Siemens*, sino de una empresa rusa conocida como *Power Machines Corp.*, que bajo su contrato iraní la instaló como parte de su sistema *Teleperm*.

STUXNET ES UN ADELANTO SIGNIFICATIVO EN MALWARE

Al igual que con otros *malware* maliciosos, *Stuxnet* se aprovecha de fallas de seguridad no identificadas anteriormente en el *software* del sistema conocidas como vulnerabilidades tipo "día cero". Ya que este tipo de hazaña no se ha detectado anteriormente, un *software* anti-virus no las puede identificar. Como punto de referencia, el *malware* "*Arora*", responsable de los ataques a Google a fines del 2009 (que fueron generalmente atribuidos a China)[45] depende de una vulnerabilidad tipo día cero. El uso de dos vulnerabilidades tipo día cero sería inaudito.[46] *Stuxnet* contiene cuatro vulnerabilidades tipo día cero para el sistema operativo *Microsoft Windows* y una adicional para el *software* de *Siemens*. Dos de las vulnerabilidades de *Windows* que se emplean en *Stuxnet* tienen que ver con la escalada de privilegios. Estos le permiten al gusano acceso ilegítimo básico o a nivel de administrador al sistema infectado. Los otros dos tienen que ver con la propagación del gusano ya sea a través de una tarjeta de memoria o una red local. Al momento que este artículo fue redactado, la auto-propagación es menos común en *malware* ya que a menudo es difícil de controlar. Por ejemplo, veamos un *"botnet"*–una gran cantidad de computadoras infectadas con *malware* y controladas por un servidor de "mando y control" que no está afiliado legítimamente con las máquinas infectadas.[47] Esta es una plataforma muy común para llevar a cabo delitos cibernéticos. Con un *botnet*, la propagación ocurre principalmente mediante correos electrónicos basura y sitios web maliciosos—los métodos de auto-propagación son muy limitados.[48]

STUXNET INVALIDA VARIAS SUPOSICIONES DE SEGURIDAD

Nuestro aspecto final del *Stuxnet* RMA es que invalida varias suposiciones de seguridad. La primera de esas suposiciones es que los sistemas aislados son más seguros. En vista de que los sistemas SCADA, por definición, controlan maquinaria crítica para la misión, muchos administradores no conectan esas computadoras a la red—tratando de lograr la seguridad mediante el aislamiento. Como resultado, la transferencia de archivos a esas máquinas se hace por medios removibles. Los diseñadores de *Stuxnet* se aprovecharon de esta suposición permitiéndole al gusano propagarse a través de tarjetas de memoria. Una vez que la tarjeta está infectada, el *software Stuxnet* se auto instala en las computadoras que posteriormente utilizan la tarjeta infectada. La infección comienza cuando el usuario sencillamente hace clic en el ícono asociado en *Windows*. Esta es una aplicación directa de una de las vulnerabilidades tipo día cero de las cuales *Stuxnet* se aprovecha.

Otra suposición de seguridad clave que *Stuxnet* invalida es la relación de confianza establecida por certificados firmados digitalmente. Para poder ofrecer más estabilidad, los sistemas operativos modernos, inclusive *Microsoft Windows,* limitan el acceso de un programa de computadora a los componentes del sistema. Un programa normal solicita desarrollos del sistema al *hardware* mediante el controlador *software*. Como este es el caso, el controlador de *software* tiene más acceso a los componentes del sistema de nivel más bajo que otros programas. Para evitar la creación fácil de controladores de *software* maliciosos, *Stuxnet* utiliza certificados legítimos firmados digitalmente. Este es otro aspecto del *malware* que no se ha observado anteriormente. Versiones anteriores de *Stuxnet* empleaban certificados por sistemas semiconductores *Realtek*—versiones posteriores utilizaban certificados de *JMicron Technology Corp.* El uso de estos certificados la da al

gusano la apariencia de *software* legítimo de *Windows*. Expertos de seguridad en ESET destacan que ambas compañías estaban en Taiwán y que los certificados eran robados. Además, ellos creen que probablemente fue robo físico (quizás un trabajo interno) ya que los certificados digitales para los controladores de *software* por lo regular no se encuentran en los mercados negros en la *Internet*.[49]

CONSECUENCIAS PARA EL FUTURO

Stuxnet es sumamente significativo—es un pedazo de *malware* de la nueva generación que introdujo fallas a suposiciones de seguridad existentes y pudo ocasionar daño en los sistemas industriales que estaban fuera de la *Internet*. Veamos otros dos ataques como una comparación. Primero, los ciber ataques rusos contra Georgia en el 2008 dependieron principalmente de *botnets* y *hackers* activistas para llevar a cabo ataques de negación de servicios contra la infraestructura *Internet* de Georgia.[50] Estos ataques resultaron en que Georgia perdió temporalmente su acceso a la *Internet,* principalmente durante operaciones convencionales rusas. Si bien los métodos del ataque eran bien conocidos en la comunidad de seguridad en aquel momento, aún eran significativos por su escala y que ocurrieron a la par de las operaciones convencionales. No obstante, los ataques contra Georgia estaban dirigidos a la infraestructura de las computadoras—no SCADA. De muchas maneras, esos ataques fueron un ejemplo clásico de CBA (ataque a la red de computadoras) —la meta de la actividad cibernética fue degradar una red de computadoras.

En una operación cibernética más reciente conocida como *Aora,* hackers chinos se las arreglaron para penetrar las redes corporativas de Google en diciembre de 2009 para robar información, inclusive cuentas de correos electrónicos y posiblemente códigos fuentes de computadoras. *Arora* utilizó una vulnerabilidad tipo día cero en *Microsoft Internet Explorer*—aprovechándose de una aplicación común que las personas utilizan a diario.[51] Este ataque Cibernético en particular es un buen ejemplo de CNE—explotación de la red de computadoras—ya que los agresores buscaban robarle información al blanco.

Stuxnet es diferente de estos dos casos de varias maneras. Ambos ataques en Georgia y Google estaban dirigidos a redes de computadoras ligadas directa o indirectamente a la *Internet*. En cualquiera de esos dos casos, un sistema desconectado de la red no se hubiese dañado. Pero no con *Stuxnet*. Este gusano avanzado tenía la capacidad de cerrar la "brecha aérea". Los administradores de la red a cargo de la seguridad de esos sistemas aislados enfrentan un dilema interesante. Para poder garantizar que esos sistemas están protegidos del último *malware,* periódicamente deben llevar a cabo actualizaciones. No obstante, al hacerlo, corren el riesgo de propagar una infección (o sea, mediante una tarjeta de memoria o a través de una red en el área local—a través de las cuales *Stuxnet* se puede propagar).

Otra diferencia clave es que los blancos en los ataques *Arora* y de Georgia eran otras computadoras. Por otra parte, *Stuxnet* inflige daños mínimos a los sistemas de informática. En cambio, su meta es dañar un pedazo de equipo en el mundo físico. La admisión de los iraníes nos indica que *Stuxnet* afectó con éxito una identidad no virtual. Este es un adelanto significativo en armamento—una pieza de *software* que solamente existe cuando una computadora se enciende fue capaz de conducir un sabotaje con éxito en el mundo real. *Stuxnet* demuestra claramente que las armas cibernéticas pueden desempeñar un papel significativo en las operaciones—a diferencia de la idea anterior que ese *software* solamente equivale a "armas de irritación en masa".[52]

¿Cuáles son las consecuencias del *software* malicioso que pueden afectar equipo en el mundo real? Hay numerosas preguntas que ahora se deben tratar. Recientes audiencias del Senado a raíz del *Stuxnet* analizan cómo Estados Unidos puede mejorar la protección de sus infraestructuras críticas de esos ataques.[53] Sin embargo, esa es solamente una parte del rompecabezas. Hay muchas preguntas sobre directrices—algunas relacionadas con la ciberguerra en general—que se tornan más importantes.[54] ¿Cómo atribuimos ese tipo de ataque? ¿Cómo respondemos a ata-

ques cibernéticos en la infraestructura SCADA por parte de grupos fuera del gobierno? ¿Cómo el derecho de guerra terrestre aplica a las armas cibernéticas que pueden ocasionar daños en el mundo real?

Hay varias preguntas operacionales y técnicas que también se deben responder. En el ámbito de la ciberguerra, inquietudes técnicas y operacionales a menudo se unen. Por ejemplo, ¿cuál es la mejor manera de identificar vulnerabilidades tipo día cero (las cuales, por definición se desconocen)? ¿Cómo podemos localizar *software* malicioso, como el *Stuxnet,* que fue diseñado para no detectarse? ¿Cuáles suposiciones de seguridad estamos haciendo que se pueden invalidar? ¿Cómo hacemos una plantilla de una amenaza cibernética desconocida?

¿Se proliferarán las armas cibernéticas tales como el *Stuxnet*? Varios expertos de seguridad han pronosticado que variaciones tipo *Stuxnet* se tornarán más comunes en el 2011.[55] Ya ha habido informes de ataques cibernéticos que no son *Stuxnet* en equipo industrial en China.[56] Cabe destacar que los análisis gratis de *Symantec*, *Kaspersky Labs*, *ESET* y *Langer Communications GmbH*, si bien son útiles desde un punto de vista defensivo, pueden utilizarse a la inversa como una inspiración para gusanos tipo *Stuxnet*.

Por su naturaleza, la ciberguerra cambia rápidamente. Individuos y grupos motivados del gobierno, corporaciones, academia y comunidades de *hackers* de sombrero negro están escudriñando constantemente los sistemas en busca de las últimas vulnerabilidades. Sin embargo, *Stuxnet* representa un adelanto evidente en la tecnología de punta como un *software* y lo que logra. Ha revelado fallas en las suposiciones de seguridad que se deben retomar en niveles múltiples, pero quizás lo más importante es que mostró que el *software* también se puede emplear como un sistema de armamento decisivo. ❑

Fuente: Este artículo fue publicado anteriormente en Small Wars Journal, abril de 2011, small warsjournal.com

Notas

1. Kupreev Oleg and Ulasen Sergey, *Trojan-Spy.0485 and Malware-Cryptor.Win32.Inject.gen.2 Review,* VirusBlockAda, julio de 2010.

2. Un gusano se define como un pedazo de *software* malicioso que se auto propaga.

3. Nicolas Falliere, Liam O Murchu y Eric Chien, *W32.Stuxnet Dossier Version 1.4.* Symantec Corporation, febrero de 2011, 7.

4. David Albright, Paul Brannan y Christina Walrond, *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?* Institute for Science and International Security (ISIS), diciembre, 1.

5. Thomas Erdbrink, *"Ahmadinejad: Iran's nuclear program hit by sabotage"* (Ahmadinejad: Programa nuclear de Irán atacado por sabotaje), *Washington Post,* 29 de noviembre de 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/11/29/AR2010112903468.html (consultado el 16 de febrero de 2011).

6. Cita de Roel Schouwenberg, Investigador superior de antivirus en Kaspersky Labs en una entrevista en la conferencia *Virus Buletin,* octubre de 2010, http://www.youtube.com/watch?v=C9H3MrtLgUc (consultado el 156 de febrero de 2011).

7. Martin Brunner, Hans Hofinger, Christoph Krauss, Christopher Roblee, Peter Schoo y Sascha Todt, *Infiltrating Critical Infrastructures with Next-Generation Attacks W32.Stuxnet as a Showcase Threat* (Infiltrando infraestructuras críticas con ataques de la próxima generación W32.Stuxnet como vehículos para amenazar) , Fraunhofer SIT, diciembre 2010, 23.

8. Falliere, et. al., 55.

9. Williamson Murray, *Thinking about Revolutions in Military Affairs* (Pensando en las revoluciones en asuntos militares), *Joint Forces Quarterly,* Verano 1997.

10. Estos incluyen *Symantec, Kaspersky Labs, ESET y Langer Communications GmbH.*

11. Paul Barford y Vinod Yegneswaran, "An Inside Look at Botnets" (Un vistazo a los botnets) en *Malware Detection* (Detección de *malware*), ed. Mihai Christodorescu, Somesh Jha, Douglas Maughan, Dawn Song y and Cliff Wang, Springer, 2007.

12. Aleksandr Matrosov, Eugene Rodionov, David Harley y Juraj Malcho, *Stuxnet Under the Microscope* (*Stuxnet* bajo el microscopio), *Revision 1.2,* ESET, noviembre de 2010, 5.

13. John D. Fernández y Andrés E. Fernández , "SCADA systems: vulnerabilities and remediation" (Sistemas SCADA: Vulnerabilidades y remedies), *Journal of Computing Sciences in Colleges,* Vol. 20, No. 4, Abril 2005, 160-168.

14. Thomas Brandstetter, *"Stuxnet Malware" CIP Seminar,* Siemens, November, 2010.

15. Ralph Langer, *"How to Hijack a Controller - Why Stuxnet Isn't Just About Siemens PLCs"* (Cómo secuestrar a un controlador – por qué *Stuxnet* no solo se trata de los PLCs de Siemens), Control Magazine, 13 de enero de 2011, http://www.controlglobal.com/articles/2011/IndustrialControllers1101.html (consultado el 16 de febrero de 2011).

16. Falliere, et. al., 39.

17. Ralph Langer, "417 Data Structures = Cascade Structure = Reported Damage" (Estructuras de datos 417 = Estructura en Cascada = Daños reportados) *Langer Communications GmbH Blog,* 29 de diciembre de 2010, http://www.langner.com/en/2010/12/29/417-data-structures-cascade-structure-reported-damage/ (consultado el 16 de febrero de 2011).

18. Falliere, et. al., 39.

19. Ibid., 41.

20. Langer, *Control Magazine.*

21. Falliere, et. al., 5.

22. Los diseñadores del *Stuxnet* lanzaron ataques en tres fases, cada fase utilizando una versión actualizada del *software.* Los detalles técnicos aparecen en Falliere, et. al.

23. Ibid., 7.

24. Albright, et. al., 2.

25. Ibid., 4.

26. Falliere, et. al., 41.

27. Alexander Glaser, "Characteristics of the Gas Centrifuge for Uranium Enrichment and Their Relevance for Nuclear Weapon Proliferation (corrected)", (Características de la centrífuga de gas para el enriquecimiento de uranio y su relevancia para la proliferación de armas nucleares [corrección]), *Science and Global Security,* junio de 2008, 14.

28. Ibid.

29. Ralph Langer, "Applying Aqazadeh's revelations to Stuxnet forensic analysis" (Aplicando las revelaciones de Agazadeh al análisis forense de *Stuxnet), Langer Communications GmbH Blog, 30 January 2011,* http://www.langner.com/en/2011/01/30/applying-aqazadeh%E2%80%99s-revelations-to-stuxnet-forensic-analysis/ (consultado el 16 de febrero de 2011).

30. Erdbrink.

31. Dieter Bednarz y Erich Follath, "Iran's Chief Nuclear Negotiator: 'We Have to Be Constantly on Guard" (Negociador nuclear principal de Irán: Tenemos que estar constantemente alertas), *SPIEGEL ONLINE,* 18 de enero de 2011, http://www.spiegel.de/international/world/0,1518,739945-2,00.html (consultado 16 febrero de 2011).

32. Falliere, et. al., 3.

33. John Leyden, "Iran boasts of Stuxnet 'nuclear spies' arrests" (Irán se jacta de arrestos de "espías nucleares" *Stuxnet*), *The Register,* 4 de octubre de 2010, http://www.theregister.co.uk/2010/10/04/stuxnet_conspiracy_theories/ (consultado el 16 de febrero de 2011).

34. Albright, et. al., 2.

35. Ibid., 3.

36. Ibid., 9.

37. De una entrevista de Yaakov Katz con Ralph Langer en "Stuxnet Virus Set Back Iran's Nuclear Program by 2 Years" (Virus *Stuxnet* atrasa por 2 años programa nuclear de Irán), *Jerusalem Post,* 15 de diciembre de 2010, http://www.studentnewsdaily.com/daily-news-article/stuxnet-virus-set-back-irans-nuclear-program-by-2-years/ (consultado el 16 de febrero de 2011).

38. Albright, et. al., 6.

39. "Stuxnet also found at industrial plants in Germany" (Se descubre *Stuxnet* en fábricas industriales en Alemania), *The H Security,* 17 de septiembre de 2010, http://www.h-online.com/security/news/item/Stuxnet-also-found-at-industrial-plants-in-Germany-1081469.html (consultado el 16 de febrero de 2011).

40. "Stuxnet Spreads to Finland" (*Stuxnet* se propaga a Finlandia), *The New Internet,* Octubre 2010, http://www.thenewnewinternet.com/2010/10/14/stuxnet-spreads-to-scandinavia/ (consultado el 16 de febrero de 2011).

41. John Leyden "Stuxnet worm slithers into China" (Gusano *Stuxnet* se desliza a China), *The Register,* 1 de octubre de 2010, http://www.theregister.co.uk/2010/10/01/stuxnet_china_analysis/ (consultado el 16 de febrero de 2011).

42. Brandstetter.

43. Albright, et. al., 5.

44. Ralph Langer, "417 Installed in Bushehr NPP" (Se instala 417 en Bushehr NPP), *Langer Communications GmbH Blog, 14 de diciembre de 2010,* http://www.langner.com/en/2010/12/14/417-installed-in-bushehr-npp/ (consultado el 16 de febrero de 2011).

45. Timothy L. Thomas, "Google Confronts China's 'Three Warfares,'"(Google confronta las "tres guerras" de China), *Parameters,* Verano 2010, 101.

46. Entrevista con Roel Schouwenberg en *Virus Buletin* (ver nota 2).

47. Barford y Yegneswaran, 2.

48. Ibid., 3.

49. Matrosov, et. al., 13. Además consultar el *blog* técnico ESET en http://blog.eset.com/2010/07/22/why-steal -digital-certificates (consultado el 16 de febrero de 2011).

50. Para más detalles sobre los ataques cibernéticas rusos en Georgia en el 2008, consultar a Stephen Korns y Joshua Eastenberg, "Georgia's Cyber Left Hook" *Parameters, Winter 2008-09, 60-76* y Paulo Shakarian, "Analysis of the 2008 Russian Cyber-Campaign Against Georgia" (Análisis de la campaña cibernética rusa en el 2008 contra Georgia), *Military Review,* por publicarse.

51. Matrosov, et. al., 5.

52. Noah Shachtman, "Terrorists on the Net? Who cares?" (¿Terroristas en la red? ¿A quien le importa?), *Wired,* 20 de diciembre de 2002, http://www.wired.com/techbiz/it/news/2002/12/56935 (consultado el 16 de febrero de 2011).

53. Para más detalles sobre audiencias del Senado de EE.UU. en noviembre de 2010 a raíz del *Stuxnet* consultar http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_id=954c3149-042e-4028-ae23 -754868902c44 (consultado el 16 de febrero de 2011).

54. Ver Jeffrey Carr, *Inside Cyber Warfare* (Dentro de la ciberguerra) para un análisis detallado de estos problemas.

55. Ataques tipo *Stuxnet* han sido pronosticados por varias empresas profesionales de seguridad en las computadoras, inclusive *Symantec Corporation (ver MessageLabs Intelligence: 2010 Annual Security Report).* Varios expertos también han hecho esas predicciones en eWeek (http://www.eweek.com/c/a/Security/Stuxnet-Variants-Will-Wreak-Havoc-on-More-Information -Systems-in-2011-373179/) *ComputerWeekly* (http://www.computerweekly.com/Articles/2010/12/22/244626/StuxNet -prepare -for-worse-in-2011.htm).

56. Fahmida Rashid, "Stuxnet-Like Trojans Can Exploit Critical Flaw in Chinese Industrial Software" (Virus troyanos tipo *Stuxnet* pueden aprovecharse de fallas críticas en *software* industrial chino), eWeek, 12 de enero de 2011, http://www .eweek.com/c/a/Security/StuxnetLike-Trojans-Can-Exploit-Critical-Flaw-in-Chinese-Industrial-Software-296674/ (consultado el 16 de febrero de 2011).

REFERENCIAS:

1. Kupreev Oleg and Ulasen Sergey, *Trojan-Spy.0485 and Malware-Cryptor.Win32.Inject.gen.2 Review,* VirusBlockAda, julio de 2010.
2. Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32.Stuxnet Dossier Version 1.4.* Symantec Corporation, febrero de 2011, 7.
3. David Albright, Paul Brannan, and Christina Walrond, *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?* (¿Stuxnet puso fuera de servicio 1.000 centrífugas en la planta de enriquecimiento en Natanz?), Institute for Science and International Security (ISIS), diciembre, 1.
4. Martin Brunner, Hans Hofinger, Christoph Krauss, Christopher Roblee, Peter Schoo, and Sascha Todt, *Infiltrating Critical Infrastructures with Next-Generation Attacks* (Infiltrando infraestructuras críticas con ataques modernos), *W32.Stuxnet as a Showcase Threat,* Fraunhofer SIT, diciembre de 2010, 23.
5. Williamson Murray, *Thinking about Revolutions in Military Affairs* (Pensando acerca de revoluciones en asuntos militares), Joint Forces Quarterly, Verano 1997.
6. Paul Barford and Vinod Yegneswaran, "An Inside Look at Botnets" (Un vistazo a los *botnets*), en *Malware Detection,* ed. Mihai Christodorescu, Somesh Jha, Douglas Maughan, Dawn Song y Cliff Wang, Primavera, 2007.

7. Aleksandr Matrosov, Eugene Rodionov, David Harley, and Juraj Malcho, *Stuxnet Under the Microscope Revision* 1.2 (*Stuxnet* bajo el microscopio), ESET, Noviembre 2010, 5.
8. John D. Fernandez and Andres E. Fernandez , "SCADA systems: vulnerabilities and remediation" (Sistemas SCADA: Vulnerabilidades y remedies), *Journal of Computing Sciences in Colleges,* Vol. 20, No. 4, abril de 2005, 160-168.
9. Thomas Brandstetter, "Stuxnet Malware" *(Malware Stuxnet), CIP Seminar,* Siemens, noviembre de 2010.
10. Ralph Langer, "How to Hijack a Controller - Why Stuxnet Isn't Just About Siemens PLCs" (Cómo secuestrar un controlador – por qué *Stuxnet* no se trata solamente de los PLC de Siemens), Magazine, 13 de enero de 2011, http://www.controlglobal.com/articles/2011/IndustrialControllers1101.html (consultado el 16 de febrero de 2011).
11. Alexander Glaser, "Characteristics of the Gas Centrifuge for Uranium Enrichment and Their Relevance for Nuclear Weapon Proliferation (corrected)", (Características de la centrífuga de gas para el enriquecimiento de uranio y su relevancia para la proliferación de armas nucleares [corrección]), *Science and Global Security,* junio de 2008, 14.
12. Timothy L. Thomas, "Google Confronts China's 'Three Warfares,'"(Google confronta las "tres guerras" de China), *Parameters,* Verano 2010, 101.

El Mayor Paulo Shakarian, Ejército de los EE.UU., es un Profesor Auxiliar en el Departamento de Ingeniería Eléctrica e Informática de la Academia Militar West Point, Ejército de Estados Unidos. Obtuvo su Doctorado y Maestría en Informática de la Universidad de Maryland en College Park y su licenciatura en Informática, con especialización en Seguridad de Información, en West Point. El Mayor Shakarian ha publicado numerosos artículos en varias revistas académicas y profesionales en una variedad de temas, inclusive ciberguerra, informática e inteligencia artificial.

Las opiniones expresadas en este artículo son las del autor y no reflejan ni la política oficial ni la postura de la Academia Militar de Estados Unidos, del Comando Cibernético de Estados Unidos, del Departamento del Ejército, del Departamento de Defensa ni del gobierno de Estados Unidos.

Preparación de la Inteligencia del Entorno de Información y Comunicaciones

Jeffrey Carr

MIENTRAS QUE LA Preparación de Inteligencia Conjunta del Entorno de Operación (JIPOE) es para fines ofensivos, este artículo propone una función que el autor ha llamado Preparación de Inteligencia del Entorno de Información y Comunicaciones (IPICE) que, si se implementa, mejorará la táctica defensiva por medio de entidades comerciales así como gubernamentales. Los componentes de IPICE pueden invertirse y aplicarse de manera ofensiva contra un objetivo extranjero, sin embargo ese es un tema para un artículo diferente.

La tendencia actual entre compañías de seguridad de información es "seguridad impulsada por la inteligencia". Lockheed Martin puede haber iniciado el concepto gracias al trabajo de sus empleados como Eric M. Hutchins, Michael J. Cloppert y Rohan M. Amin que escribieron el artículo "Defensa de redes de computadoras impulsadas por inteligencia informada por análisis de campañas del adversario y cadenas de aniquilamiento de intrusión"[1]. Cloppert creó más adelante un modelo muy detallado para ataques de APT[2] que condujeron al artículo al que se hace referencia arriba y del que RSA tomó prestada amplia información de su artículo "Adelantarse a las amenazas avanzadas: logro de seguridad de información impulsada por la inteligencia".[3]

Hoy en día, el modelo de Lockheed Martin es utilizado ampliamente entre los miembros de la Base Industrial de Defensa (DIB) y el Centro de Delitos Cibernéticos de Defensa del Departamento de Defensa que envía inteligencia de amenazas a la DIB. De hecho, Lockheed recientemente ganó un contrato[4] de más de 400 millones para proporcionar investigaciones digitales y soporte de análisis a DC3. Aunque este sistema da buen resultado para la finalidad prevista, representa un punto de vista inadecuado del conjunto de amenazas en general. Esto se debe en gran parte a los vendedores de seguridad que apoyan a la DIB y a la mayor parte de las compañías Fortune 500 con sus soluciones de ciberseguridad; soluciones que tienen una eficacia limitada contra objetivos deseados y un alcance muy limitado del entorno operacional de una compañía.

Antes de que una corporación privada o el gobierno federal puedan evaluar la eficacia de cualquier proceso de ciberseguridad, especialmente algo llamado "impulsado por la inteligencia", es necesario ver por completo el conjunto de amenazas u entorno medioambiental de la organización. La cadena de aniquilamiento de intrusión de Lockheed Martin solamente se fija en ataques típicos estilo APT que se basan en "spear phishing" con anexos de correos electrónicos, que alienta al lector a hacer clic en un enlace malicioso, y cargas útiles maliciosas suministradas a través de medios removibles. Los defensores de este método dicen que representa la mayoría de los ataques que observan. El objetivo de este artículo es dar una imagen más completa del conjunto de amenazas usando la Preparación de Inteligencia Conjunta del Entorno Operacional (JIPOE) del Departamento de Defensa.[5] La JIPOE puede servir como modelo efectivo para crear un plan de seguridad completo de Tecnología de Información y Comunicación (ICT) basado no en el conjunto de amenazas limitadamente definidas en la actualidad (es decir, Lockheed Martin y la cadena de aniquilamientos de intrusión de RSA) sino en una imagen operacional más completa. A continuación indicamos un resumen de la JIPOE según se describe en la Publicación Conjunta 2-01.3:

Primer paso de la JIPOE: Definición de un entorno operacional

- Identificar el área operacional

- Determinar las características significativas del entorno operacional
- Determinar las lagunas de inteligencia e información

Segundo paso de la JIPOE: Describir el impacto del OE

- Desarrollar una perspectiva geoespacial del OE
- Desarrollar una perspectiva del sistema del OE

Tercer paso de la JIPOE: Evaluación del adversario

- Actualizar o crear modelos de adversario
- Determinar la situación del adversario actual
- Identificar las capacidades y vulnerabilidades del adversario

Cuarto paso de la JIPOE: Determinación de los cursos de acción de adversario

- Identificar los objetivos probables del adversario y el estado final deseado
- Identificar el conjunto completo de COA del adversario

He simplificado los pasos anteriores de cuatro a tres, a saber:

1. Definir la superficie de ataque (es decir, entorno operacional)
2. Evaluar al adversario
3. Determinar los cursos de acción del adversario

¿Qué es "Inteligencia"?

La palabra inteligencia en la frase "ciberinteligencia" es utilizada de forma confusa por la industria de seguridad de información y los medios de comunicación. A veces se usa de forma intercambiable con datos de "malware". Otras veces, se usa para describir investigaciones de código abierto de Anonymous y otros piratas. La palabra "ciber" tiene sus propios problemas de definición, por lo que para las intenciones de este artículo, el autor recomienda la de Nicolas Eftimiades, autor de la definición de "Operaciones de inteligencia china"[6] que en realidad es más una descripción informal del proceso de inteligencia tradicional:

> "Las agencias de inteligencia mundiales comparten el mismo objetivo general: proporcionar inteligencia precisa y oportuna a sus consumidores. Para ello reúnen información sin procesar de una variedad de fuentes humanas y técnicas. Después deben cotejar y analizar estos datos para separar la realidad de la ficción y opinar sobre una variedad de sucesos pasados, actuales y futuros. El producto analítico completo, inteligencia, se disemina después al consumidor, cuyo requisito de información empezó el proceso. Esa persona o ese grupo está entonces en una posición para pedir un análisis adicional o implementar una política basada en la inteligencia recibida. Todo el proceso se denomina ciclo de inteligencia".

La superficie de ataque

Una Corporación Multinacional (MNC) tiene una vasta superficie de ataque. Antes de poder construir una estructura de seguridad eficaz, se necesita establecer la superficie de ataque. El entorno de información de una corporación, un gobierno o una organización militar incluye amenazas internas y externas. La amenaza interna, lo que significa una acción hostil contra la compañía por parte de un empleado, es un problema activo y a menudo sin reportar para muchas compañías y una que normalmente cuesta más que los incumplimientos por parte de agentes externos.[7] Otra forma de amenaza interna es lo que ocurre cuando una compañía contrata a ingenieros extranjeros para dotar a sus oficinas de investigación y desarrollo en China, Rusia, Francia y otros países. Mientras estén empleados en la compañía, estos ingenieros adquieren

información propietaria que se llevan cuando dejan de trabajar para empezar a trabajar en una compañía dirigida por el estado con intereses similares en uno o dos años. A esto se le denomina "transferencia de tecnología".

Entre las amenazas externas se incluyen muchos más vectores de ataque que los usados por ataques de estilo APT. Se incluye lo siguiente entre otras cosas:

- A las oficinas de las compañías de fuera de Estados Unidos que están sujetas a leyes de ICT extranjeras sobre recopilación de información se les puede interceptar y monitorear legalmente todas sus comunicaciones. Esto incluye correo electrónico, VOiP, móvil, terrestres, satélite y VPN.
- Es posible que se requiera a las corporaciones multinacionales proporcionar su código a servicios de inteligencia extranjeros para la inspección a fin de asegurar que no plantee ninguna amenaza a su seguridad nacional. De no cumplir con esto, significaría ser detenido y no poder realizar actividades comerciales dentro de las fronteras de ese país.
- Empleados de la compañía, particularmente ejecutivos, que ponen en riesgo sus dispositivos al irse de viaje al extranjero.
- Los vendedores extranjeros a los que la compañía contrata pueden estar afiliados con su gobierno autóctono y pasar secretos comerciales a ese gobierno a petición gracias a su acceso autorizado a la red de compañías de EE.UU.
- Los subcontratistas, las subsidiarias y los socios estratégicos de los vendedores pueden tener afiliaciones con su gobierno autóctono y hacer lo mismo de arriba.

Evaluar el adversario

Hay 28 naciones estado[8] que tienen capacidades de guerra/espionaje cibernéticos. Muchas de ellas tienen conocidas relaciones con grupos de piratas y un número creciente dispone de milicias de voluntarios adiestrados para operar en el ciberespacio. Mientras que las capacidades rusas[9] y chinas[10] se han documentado ampliamente, el Consejo Nacional de Autoridad de India dispone de autoridades para ciberoperaciones ofensivas asignadas a la Agencia de Inteligencia de Defensa y a la Organización Nacional de Investigación Técnica[11]. La Unidad 8200 de Inteligencia Militar de Israel y su Directorado C4I han anunciado una operación de reclutamiento entre los piratas de élite de Israel[12]. Actualmente los siguientes países disponen de comandos equivalentes o basados en el Cibercomando de EE.UU.: Australia, Brasil, Bulgaria, Canadá, China, Chequia, Estonia, Finlandia, Francia, Georgia, Alemania, India, Irán, Israel, Italia, Myanmar, Países Bajos, Corea del Norte, Pakistán, Polonia, Rumania, Rusia, Singapur, Sudáfrica, Corea del Sur, Suecia, Taiwán, Ucrania y Zimbabue. De éstos, los estados más activos que participan en ataques de ciberespionaje por medio de actores estatales y no estatales son Brasil, Bulgaria, China, Francia, Georgia, India, Irán, Israel, Países Bajos, Corea del Norte, Rumania, Rusia, Corea del Sur, Taiwán y Ucrania. Las compañías multinacionales de EE.UU. que tienen oficinas en estos estados deben considerar que sus redes están ya intervenidas y tomar las medidas apropiadas para mitigar los efectos de ese estado.

Autoridades legales de servicios de inteligencia extranjeros

Tanto Rusia como China han promulgado leyes que dan a sus servicios de seguridad respectivos mucha libertad para recopilar información de corporaciones extranjeras que disponen de oficinas dentro de sus fronteras. A continuación se indica una encuesta de lo que significan esas leyes para las compañías extranjeras, sin embargo eso no se aplica solamente a Rusia y China. India ha estado utilizando agresivamente tácticas similares y otros países disponen de sus propias

políticas y procedimientos. El Centro de Operaciones de Seguridad y el Consejo Principal de cada MNC debe ser consciente del impacto que estas autoridades tienen en su compañía y sus datos sensibles.

Ley de Seguridad del Estado de la República Popular China

La Ley de Seguridad del Estado de la República Popular China (RPC) gobierna la forma en que pueden operar los servicios de seguridad de China y obliga a la participación de su población si se le pide. En otras palabras, si usted es un visitante que se hospeda en un hotel de Shanghai, el personal de ese hotel debe cooperar con cualquier solicitud del servicio de seguridad para darle acceso a su habitación sin su conocimiento o consentimiento si se presenta como un asunto de seguridad estatal. Aquí hay algunas partes relevantes de las leyes, que pueden encontrarse completas en china.org.cn:

> Artículo 8. Cualquier funcionario de un órgano de seguridad del Estado, al ejecutar una tarea de seguridad del Estado, puede entrar en cualquier sitio interesado después de presentar un certificado apropiado, y puede, según las estipulaciones pertinentes del Estado, con aprobación y después de producir un certificado apropiado, entrar en áreas, sitios o unidades restringidas interesadas; y puede tener acceso a archivos, materiales y artículos relacionados para su examen.
>
> Artículo 10. Donde el reconocimiento de una acción que pone en peligro la seguridad del Estado, un órgano de seguridad del Estado puede emplear, según las disposiciones pertinentes del Estado y después de pasar estrictos procedimientos de aprobación, medios de reconocimiento tecnológicos.
>
> Artículo 11. Donde la seguridad del Estado lo requiera, un órgano de seguridad del estado puede inspeccionar los instrumentos y aparatos de comunicación electrónicos y otros equipos e instalaciones similares que pertenezcan a cualquier organización o individuo.
>
> Artículo 16. Los ciudadanos y las organizaciones deben proporcionar comodidades u otra asistencia para el trabajo de seguridad del Estado.
>
> Artículo 18. Cuando el órgano de seguridad del Estado investiga y averigua cualquier circunstancia que pone en peligro la seguridad del Estado y reúne evidencia relacionada, los ciudadanos y las organizaciones interesados deben suministrar lealmente la información pertinente y no pueden rechazar hacerlo.

Ley Federal de la Federación Rusa No. 40

La versión rusa de la ley china anterior se denomina Ley Federal No. 40 "Sobre el Servicio de Seguridad Federal (FSB)". La ley original se promulgó en 1995 y la última enmienda se promulgó en 2008. Capítulo II Artículo 8 establece las actividades autorizadas principales del FSB. Son, a saber:

- actividades de contrainteligencia;
- combate del terrorismo;
- combate de la delincuencia;
- actividades de inteligencia;
- actividades en la frontera;
- garantizar la seguridad de información.

La seguridad de información se considera una actividad principal, no subsidiaria. Los diversos artículos siguientes dan más detalles sobre cada actividad específica, a menudo con implicaciones de seguridad de información. Por ejemplo, las actividades de contrainteligencia incluyen la autoridad para monitorear comunicaciones. De hecho, las medidas para asegurar la información mediante actividades de monitoreo y recopilación aparecen de forma clara en los artículos.

Observe que el FSB está autorizado a llevar a cabo actividades de inteligencia, específicamente actividades de inteligencia extranjera, aun cuando Rusia mantiene un Servicio de Inteligencia Extranjero (SVR) separado. La ley indica que las operaciones de inteligencia extranjeras se hacen según acuerdos conjuntos con el SVR.

El Artículo 11.2 establece los detalles de actividad de seguridad de información. Son, a saber:

- la formación e implementación de una política pública y científico-técnica en el campo de la seguridad de información, incluido el uso de medios de ingeniería y criptográficos;
- proporcionar métodos criptográficos y de ingeniería de seguridad para sistemas de información y telecomunicación, y sistemas codificados, secretos y los otros tipos de comunicaciones especiales en Rusia y agencias rusas ubicadas fuera de Rusia.

En resumidas cuentas, la autoridad de seguridad de información del FSB es muy amplia. Establecen una política administrativa y técnica. El FSB está a cargo efectivamente de la infraestructura criptográfica de Rusia con autoridad sobre software y hardware. De hecho, el Artículo 3 pone a la Academia de Criptología de Rusia, nominalmente una institución académica, bajo la autoridad ejecutiva federal para seguridad, el FSB. Las regulaciones de implementación del FSB indican específicamente que el FSB opera la Academia de Criptología. La implementación de regulaciones, firmada por el entonces Presidente Putin, proporciona los detalles adicionales dando al FSB la autoridad de regular el desarrollo, la importación, la venta y la exportación de tecnologías criptográficas. Las regulaciones de implementación también permiten al FSB ayudar a organizaciones para proteger secretos comerciales.

Según el Artículo 15, las autoridades públicas así como las empresas, las instituciones y las organizaciones están obligadas a ayudar al Servicio de Seguridad Federal para llevar a cabo sus obligaciones asignadas.

Los individuos y las entidades legales en Rusia que proporcionan servicios postales y telecomunicaciones de todas clases, incluidos sistemas, comunicación de datos y comunicaciones confidenciales vía satélite, están obligados a petición del Servicio de Seguridad Federal a incluir hardware, equipos y software adicionales, así como a crear otras condiciones necesarias para las medidas operacionales y técnicas del Servicio de Seguridad Federal.

Para cumplir con los retos de RF, las fuerzas de seguridad del Servicio de Seguridad Federal pueden asignarse a autoridades, empresas, instituciones y organizaciones públicas sin que importe quienes sean los propietarios, con el consentimiento de sus gerentes en la manera prescrita por el presidente de Rusia, dejando su servicio militar. En otras palabras, si el FSB le pide su ayuda, usted debe ayudar. Si le piden modificar hardware o software para que puedan ejecutar una operación o monitorear una red, usted lo debe hacer. Y si desean poner a alguien en su organización para apoyar objetivos del FSB, puede hacerlo con el permiso de su gerencia.

Las regulaciones de implementación incluyen disposiciones no mencionadas específicamente en la ley. Por ejemplo, se permite al FSB establecer bancos y efectuar cambios de divisas. El FSB lleva a cabo operaciones de investigación y desarrollo, y fabrica tecnología independientemente y con "otras empresas, instituciones y organizaciones", incluido el campo de seguridad de información. Significativamente, estas disposiciones valen para todas las actividades del FSB, no solo para la seguridad de información. Por ejemplo, el FSB podría indicar a una compañía, incluido un exportador de software, que modifica ese software para ayudar a la operación de recopilación técnica del FSB. El FSB podría formar una compañía encubierta y vender software adaptado directamente por internet aceptando pagos en divisas extranjeras. De hecho, el uso agresivo del FSB de las disposiciones indicadas en la ley y las regulaciones del FSB presentan una amenaza considerable solamente limitada por los objetivos y la imaginación del FSB.

Determinación de los cursos de acción del adversario

Gracias a innovaciones globales continuas en tecnología de información y comunicaciones, no hay forma de identificar todos los posibles vectores de ataque pero los cursos de acción conocidos incluyen entre otros ingeniería social, "spear phishing", "exploits" de software, puertas traseras de hardware, intercepciones de ICT y amenazas internas. Todas las organizaciones comerciales, gubernamentales y militares necesitan ser conscientes de cada uno de estos vectores de ataque y tener un plan organizado para contrarrestarlos. ❑

Notas

1. Hutchins, Eric M., Cloppert, Michael J., Amin, Rohan M., "Intelligence-Driven Computer Network Defense Informated by Analysis of Adversary Campaigns and Intrusion Kill Chains" (Defensa de redes de computadoras impulsadas por inteligencia informada por análisis de campañas del adversario y cadenas de aniquilamiento de intrusión), minutas del 6º Congreso Internacional sobre Guerra de Información, Veran de 2011.
2. "Security Intelligence: Defining APT Campaigns" (Inteligencia de seguridad: definición de las campañas de APT) http://computer-forensics.sans.org/blog/2010/06/21/security-intelligence-knowing-enemy/.
3. "Getting Ahead of Advanced Threats: Achieving Intelligence-Driven Information Security" (Adelantarse a las amenazas avanzadas: logro de seguridad de información impulsada por la inteligencia) por RSA, basados en conversaciones con el Consejo de Seguridad para la Innovación de Empresas.
4. Lockheed Martin To Assist Department Of Defense In Fight Against Growing Threat: Cyber Crime" (Lockheed Martín ayudará al Departamento de Defensa en la lucha contra una amenaza creciente; los ciberdelitos): PR Newswire, 3 de mayo 2012.
5. Publicación conjunta 2-01.3, Estado Mayor Conjunto, Departamento de Defensa de EE.UU. http://www.fas.org/irp/doddir/dod/jp2-01-3.pdf.
6. Eftimiades, Nicholas (2011-02-19). Chinese Intelligence Operations (Operaciones de inteligencia chinas) (Kindle Locations 169-173). Naval Institute Press. Kindle Edition.
7. US-CERT "Interesting Insider Threat Statistics" (Estadísticas interesantes de amenazas internas), 25 de octubre de 2010: http://www.cert.org/blogs/insider_threat/2010/10/interesting_insider_threat_statistics.html.
8. Se hace un estudio de 28 Estados en el Capítulo 16 de Inside Cyber Warfare (Ciberguerra interna), 2a edición (O'Reilly, 2011), no obstante hay Estados adicionales que han añadido esas capacidades en 2012. Con el tiempo cada nación con unas Fuerzas Armadas tendrá también algo similar al Cibercomando de EE.UU.
9. "Inside Cyber Warfare: Mapping the Cyber Underworld" (Ciberguerra interna: mapeo del submundo cibernético), 2a edición, capítulo 15 "The Russian Federation: Information Warfare Framework" (La Federación Rusa: estructura de la guerra de información), 12/2011.
10. USCC, ""Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage" (Ocupación del terreno elevado de la información: capacidades chinas para las operaciones de la red de computadoras y ciberespionaje), 2012: http://www.uscc.gov/.
11. http://www.theregister.co.uk/2012/06/11/india_state_sponsored_attacks/.
12. http://www.jpost.com/Defense/Article.aspx?id=253487.

Jeffrey Carr es el fundador y CEO de Taia Global, Inc. y es el autor de "Inside Cyber Warfare: Mapping the Cyber Underworld" (Ciberguerra interna: mapeado del submundo cibernético) (O'Reilly Media 2009 y 2011 (2a edición)). Su libro ha sido recomendado por el General Chilton, antiguo Comandante de USSTRATCOM y el prefacio de la Segunda edición fue escrito por el antiguo Secretario de Seguridad Nacional Michael Chertoff. Jeffrey ha tenido el privilegio de dirigirse al US Army War College, Instituto de Tecnología de la Fuerza del Aire, el Grupo de Estudios Estratégicos de Jefe de Operaciones Navales, la Agencia de Inteligencia de Defensa, el Centro de Códigos Abiertos de la CIA y en más de 60 congresos y seminarios.

Virtualmente Masivo: Comprendiendo la Concentración y el Poder de Combate en la Ciberguerra

Capitán John "Strider" Cobb, Fuerza Aérea de los Estados Unidos

La cantidad tiene una calidad totalmente suya.
—Atribuido apócrifamente a Josef Stalin, discutiendo la producción de armamento ruso durante la Segunda Guerra Mundial

LA FUERZA AÉREA DE EE.UU. define "masa" como "la concentración de los efectos del poder de combate en el lugar y el momento más ventajoso para lograr resultados decisivos"[1]; en el Air Force Doctrine Document (Documento de Doctrina de la Fuerza Aérea) (AFDD) 3-12 se hace eco de esta definición a la vez que se destaca que las fuerzas cibernéticas "deben integrarse y sincronizarse con otras fuerzas"[2]. Pero, ¿qué significa esto para la estrategia en el ámbito cibernético? Algunos han sugerido que el concepto de masa (concentración) ya no aplica en el ciberespacio y que un puñado de agresores podría lanzar ataques devastadores desde cualquier parte del mundo.[3] El Col Gregory Rattray (USAF, Retirado) en "*Strategic Warfare in Cyberspace*" (Guerra estratégica en el ciberespacio) discute las funciones de apoyo, tales como inteligencia de la red, localización de blancos y desarrollo de herramientas, que pueden hacer que los ataques cibernéticos sean más eficaces. Esto sugiere otra perspectiva en cuanto a la concentración—una que incluye no tan solo los operadores iniciales atacando blancos, sino el resto de operadores que se requieren para organizar un equipo capaz de lanzar consistentemente ataques exitosos ya que él sugiere que los analistas y los programadores quizás tengan que sobrepasar la cifra de personas que realmente llevan a cabo los ataques.[4] Esta es una diferencia significativa, y una pregunta importante que resolver, pero los temas de personal no son la única manera para comprender la concentración en la ciberguerra.

También podemos pensar sobre la concentración en términos de volumen del tráfico de ataque—al nivel más sencillo, en términos de cantidades de bitios o paquetes que pasan hacia el blanco. En otras ocasiones una definición más significativa de volumen podría ser el número de viruses que son liberados simultáneamente, típicamente desde la perspectiva de los *firewalls* (servidor de seguridad) y herramientas antivirus que tratarán de bloquear el *malware* (programas maliciosos). Lo que los agresores o investigadores consideran un virus podría utilizar un código que se modifica a sí mismo para que luzca como cientos de viruses diferentes que tratan de colarse a hurtadillas. Por otro lado, los números de nódulos bajo ataque podría ser una definición útil de volumen—al nivel más bajo, la cantidad de dispositivos que están siendo atacados; a un nivel más elevado, la cantidad de ámbitos en la red o sitios físicos (por ejemplo, bases) bajo ataque. Esto es una simplificación excesiva, pero se puede pensar que estos aspectos diferentes de "volumen" son una versión ciberespacial de potencia de fuego. Una tercera manera de entender la concentración en la ciberguerra es en términos de la solidez o supervivencia de las redes que se están defendiendo. Una red con muchos dispositivos de repuesto, ancho de banda y rutas redundantes tendrá más posibilidades de supervivencia o al menos se recuperará más rápido contra una variedad de ataques. Asimismo, la cantidad y las destrezas de los técnicos que mantienen y defienden las redes bajo ataque es a menudo una manera de pasar por alto el tomar en cuenta la concentración. Por último, la mayoría de los países estarán más limitados durante ac-

ciones cibernéticas en tiempo de paz que cuando lanzan ataques cibernéticos en tiempo de guerra, de manera que la concentración puede que no adopte tantos aspectos durante acciones encubiertas durante tiempo de paz como en una guerra cibernética abierta.

En vista de que muchos lectores no están familiarizados con cómo los *firewalls* y el *software* antivirus protegen las redes, he aquí una explicación rápida. Típicamente un *firewall* explora el tráfico que entra o sale de una red local, mientras que el *software* antivirus explora el disco duro de una computadora en particular. Hay excepciones, tales como los Sistemas de Detección de Intrusión basados en la red o los filtros de la lista de control de acceso de enrutadores, pero la mayoría de los dispositivos que protegen una red son *firewalls* o antiviruses tradicionales—y la mayoría de las herramientas alternativas utilizan reglas similares para sus exploraciones y filtros.[5] Hay dos maneras principales que ellos utilizan para explorar en busca de viruses, firmas y heurísticas. La manera más común para las defensas de una red de buscar *malware* es verificando firmas, por lo regular apareando parte de, o de todo un archivo (o paquete de red) contra una lista de *malware* conocido. Esto puede ser bastante eficaz contra ataques conocidos, pero obviamente no detecta la mayoría de ataques nuevos, y a menudo no detectan ataques conocidos que han recibido cambios inclusive menores.[6]

La otra manera como las defensas de la red encuentran *malware* es empleando "heurística"—en lugar de buscar un texto específico o archivos que se sabe son maliciosos, buscan patrones o comportamientos sospechosos. Esto es más eficaz, aunque no es perfecto, para encontrar ataques nuevos ("día cero") y mucho mejor para atrapar variaciones nuevas de ataques antiguos. Sin embargo, la mayoría de los algoritmos heurísticos tienen índices positivos falsos elevados. En vista de que con frecuencia muestran o bloquean aplicaciones y tráfico legítimo más a menudo que ataques reales, pueden demandar mucho más tiempo y ser frustrantes de operar. Estos filtros enfrentan problemas estadísticos similares a algunas detecciones de cáncer[7]—en vista de que la gran mayoría del tráfico en la red no es malicioso, mostrando 95% de viruses y 1% de tráfico legítimo resultarán en más positivos falsos que viruses reales.[8] Muchos productos comerciales emplean una combinación de ambos métodos, y los investigadores de seguridad están trabajando en varias maneras alternativas de detectar ataques, pero hoy todas, salvo la mayoría de las redes más importantes y seguras, tienden a depender en gran medida en la detección basada en la firma ya que la falta de recursos hace que otros métodos no sea factibles.[9] Como resultado, en muchas redes militares e industriales grandes los ataques nuevos no se detectarán hasta que sea demasiado tarde y ya hayan invadido la red.

A causa de estas limitaciones, en el estado actual del ciberespacio los efectos de un ataque no son siempre en proporción a su sofisticación. El tamaño, complejidad, defensas e interconexión del blanco determinan cuán sofisticado debe ser un ataque para tener éxito. Las limitaciones políticas de un agresor, tales como exigir furtividad y no atribución—o atribución falsa—a menudo aumenta el nivel de sofisticación requerido, al igual que la carga de trabajo para los agresores. Sin embargo, en vista de que esos factores varían entre blancos militares y de infraestructura importantes, algunos blancos críticos son prácticamente imposibles de asegurar sin paralizar su capacidad de funcionar, mientras que otros—principalmente blancos más pequeños—aún si son menos críticos, puede que requieran ataques sumamente sofisticados. Los ataques de DoS (negación de servicio) pueden a menudo darse el lujo de ser menos sofisticados que los intentos de espionaje; las redes grandes, distribuidas geográficamente y de nódulos múltiples ofrecen más oportunidades para introducir un ataque y hacer que la labor de vigilar las defensas sea más difícil. *Hardware* y *software* disponible en el mercado (COTS por sus siglas en inglés) se puede atacar con entrenamiento y herramientas estándar, mientras que los sistemas especializados que a menudo se encuentran en contextos de inteligencia, nuclear o infraestructura puede que requieran reconocimiento extenso y ataques hechos a la medida.[10]

Aunque en su obra hay suposiciones sumamente dudosas, Thomas Rid[11] está correcto al destacar que ataques furtivos, sumamente precisos y "estratégicos" como el *Stuxnet*[12] requieren re-

cursos significativos para prepararlos y no se pueden volver a usar fácilmente. Este tipo de ataque requiere docenas de analistas de inteligencia, programadores y operadores para diseñarlo, montarlo y lanzarlo. Mientras que grupos diferentes puede que combinen algunas o todas esas funciones en el adiestramiento que recibe un guerrero cibernético, este tipo de ataque contra un blanco sumamente defendido aún requerirá meses de trabajo de docenas de personal bien entrenado. En la medida en que una campaña cibernética trata de corromper o desactivar grandes cantidades de blancos protegidos y autónomos, claramente necesitará inversiones significativas y esas inversiones aumentan si se necesitan furtividad y no atribución—particularmente en vista de que los equipos que trabajan en el blanco autónomo no estarán disponibles para trabajo de ciberinteligencia de "rutina" que supuestamente aún será necesario.

Sin embargo, también hay muchos blancos ciberespaciales que son defendidos menos vigorosamente y algunos de ellos pueden ser blancos de gran valor. Si bien las instalaciones nucleares como las que fueron atacadas por *Stuxnet* probablemente permanecerán muy protegidas y defendidas cuidadosamente, muchos sistemas militares e industriales requieren un acceso más amplio para ser eficaces. Por ejemplo, las redes de energía no pueden funcionar eficazmente a menos que estaciones de energía se estén comunicando entre sí constantemente. Puede que no estén en "en línea" en el sentido de enviar tráfico no codificado directamente por la *Internet,* pero esta interconexión aún se puede emplear para controlar, degradar o destruir toda la red con un solo ataque—aunque se debe destacar que en países grandes como Estados Unidos o Rusia, "la red de energía" es en realidad un conjunto de redes regionales sin conexión directa: por ejemplo, EE.UU. cuenta con tres redes regionales[13] y Rusia, aunque más centralizada que la de EE.UU., cuenta con siete regiones con interconexiones limitadas.[14] Muchas redes militares enfrentan la misma situación—tienen que unir un gran número de unidades y bases para proveer los efectos de multiplicador de fuerza de la que todos los militares modernos dependen, lo que dificulta evitar que ataques sofisticados se esparzan una vez que comprometen un nódulo en la red.

En este entorno, la segunda definición es probablemente una mejor manera para entenderlo. Algunos blancos son vulnerables a los ataques que pueden ser creados por un solo equipo y luego lanzados contra toda una red y, si tienen éxito, pueden obstaculizar toda una región. Los servicios públicos enlazados son un ejemplo, particularmente las redes de energía, que tienden a ser redes más grandes y más interdependientes que otras redes de servicios públicos. Otras podrían ser las redes militares para C2, logística y concienciación de la situación operacional. Esas funciones son necesarias al nivel táctico u operacional, y por lo tanto requieren típicamente una red compartida a lo largo de una gran cantidad de nódulos críticos. Al extremo sumamente sencillo del espectro de posibles ataques cibernéticos, la concentración en un ataque de negación de servicio distribuido (DDoS, por sus siglas en inglés) es sencillamente la cantidad de ancho de banda empleado para intentar abrumar la red objetivo. A medida que progresamos en el espectro, si un ataque emplea un código que se auto modifica, el defensor puede que necesite bloquear no una sino cientos de firmas nuevas de viruses en docenas y hasta miles de perímetros de la red (cada *firewall* protegiendo el área o la red local tiene que ser actualizada con todas las firmas de viruses relevantes para poder bloquearlas). En algunos casos, la cantidad de aprovechamientos a la vulnerabilidad (*exploit*) que los viruses están utilizando puede que sea más relevante que cómo un virus se muta para colarse a hurtadillas a través de los filtros—una activación es el código malicioso que emplea un error en el *software* de un blanco para controlar el sistema; cuando se explotan más vulnerabilidades, es más probable que el virus tenga éxito.[15] La mayoría de las redes militares cuentan con técnicos que invierten grandes cantidades de tiempo intentando corregir las vulnerabilidades conocidas antes de que un ataque se aproveche de ellas, a sabiendas que las *firewalls* y los antivirus no impiden todos los ataques. Un ataque que solamente emplea un aprovechamiento fracasará si la vulnerabilidad correspondiente está completamente reparada. Si bien reparar rápida y completamente es un problema muy difícil[16], hay herramientas que permiten que las redes modernas grandes reparen la mayoría de los sistemas en cuestión

de días.[17] Si un ataque emplea más de un aprovechamiento de la vulnerabilidad (*exploit*), aumenta el reto al defensor; sin embargo, los aprovechamientos, particularmente aprovechamientos de día cero, pueden ser recursos de inteligencia valiosos, y muchas autoridades advierten contra revelarlos arbitrariamente.[18] Por otra parte, estos aprovechamientos son más numerosos de lo que las personas se imaginan; por ejemplo, entre enero y mayo de 2012, *Microsoft* anunció—y difundió parches—para 31 vulnerabilidades graves en el sistema operativo *Windows* 7 y sus aplicaciones comunes (por ejemplo, *Microsoft Office*).[19]

En cambio, hay ataques en los que la concentración se entiende mejor como el número de redes señaladas para ser atacadas por un ataque o series de ataques. En la obra anterior del autor se discuten ataques que pueden desconectar las redes locales del control centralizado o respuesta[20]; en esos tipos de ataques la cantidad de lugares geográficos o las redes locales puede que tengan más significado que el personal utilizado para crear los ataques o la variedad de ataques empleados. Esto aplica principalmente a los ataques de negación de servicio (DoS) y de negación de servicio distribuido (DDoS)[21], o defensas de la red sumamente centralizadas—si hay defensores de la red experimentados en cada lugar, ellos deben poder resolver ataques sencillos relativamente fácil, particularmente ataques DDoS, mientras que un método más centralizado en cuanto a la defensa de la red puede que conlleve en desconectar a los defensores de las redes debajo de ellos, o a que los defensores abarquen demasiado como para poder reaccionar en todos los lugares simultáneamente.

Por otra parte, en estos tipos de ataques el personal puede ser un elemento crítico de concentración para los defensores; a diferencia de ataques sumamente selectivos, estos tipos de ataques DoS pueden ser sumamente asimétricos. Aunque están sujetos a la carrera armamentista entre agresores y defensores, a medida que los filtros, exploraciones y herramientas de la red se apresuran para ponerse al día con las técnicas de piratería, estos ataques DoS los pueden lanzar equipos bastante pequeños, y pueden requerir un gran número de defensores para arreglar y limpiar cada red local bajo ataque.

La medida relevante del poder de combate en el ciberespacio varía dependiendo de los tipos de ataque en juego y las redes que necesitan defensa. Si bien los técnicos y los operadores duchos siempre son importantes[22], el balance adecuado entre calidad y cantidad depende de los ataques y herramientas que un militar anticipa usar y enfrentar. En vista de los límites presupuestarios que todos los militares enfrentan, y la amplia gama de posibles ataques cibernéticos, estos son compromisos que todos los militares deben hacer. Si la amenaza principal es de ataques furtivos similares al *Stuxnet,* cuya intención es dañar datos furtivamente o dañar invisiblemente instalaciones específicas, entonces los defensores de la red tienen que estar bien capacitados, especialmente en técnicas forenses. Sin embargo, puede que no necesiten ser más numerosos que sus agresores, y las defensas de la red a menudo pueden darse el lujo de atrapar ataques después que el ataque ha tenido éxito, al menos en parte, ya que los ataques a menudo se esparcirán lentamente y causarán el daño lentamente para evitar ser detectados. En cambio, si la amenaza principal son ataques concebidos para interrumpir o aislar rápidamente los sistemas críticos, los defensores de la red tendrán que ser más numerosos y sus destrezas deben enfocarse en contrarrestar ataques ocultos y reconstruir los sistemas que un agresor desmantela exitosamente. Para poder contar con suficientes conocimientos acerca de posibles adversarios para saber cuál caso aplica, por lo regular requiere una inversión significativa en personal de inteligencia enfocado en cibernética; más personal de ese tipo será necesario para poder llevar a cabo ataques exitosos en respuesta.[23] Es posible que ambos tipos de ataque se puedan lanzar simultáneamente, pero en la mayoría de los casos si estos ataques van dirigidos a las mismas redes y sistemas interferirán entre sí, a menudo resultando en un agresor perdiendo el control de los ataques más precisos; lo que es más probable es que los ataques encubiertos DoS o DDoS ataquen un área mientras que una red o sistema diferente es atacado más cuidadosa y furtivamente, lejos del ataque obvio. Por supuesto, en cualquier conflicto hoy en día coordinar y ar-

monizar ataques cibernéticos—entre sí y de ataques cinéticos en la proximidad—es un esfuerzo de planificación crítico.[24]

Un vistazo a la historia del poderío aéreo podría ayudar a aclarar estos métodos diferentes—de alguna manera, los agresores cibernéticos enfrentan un problema similar al que enfrentaron la USAAF y la RAF en sus campañas de bombardeo contra el sistema industrial de Alemania durante la Segunda Guerra Mundial. Los ataques sumamente específicos (al estilo *Stuxnet*)—eliminar un puñado de blancos aislados de gran valor con un solo ataque elaborado con precisión, a menudo lenta y furtivamente—pueden ser considerados similares al método de bombardeo estratégico empleado por EE.UU. durante la Segunda Guerra Mundial. En este método, el agresor encuentra un puñado de nódulos críticos e invierte grandes cantidades de personal, tiempo y poder de combate para derribar esos sistemas[25], confiado de que el enemigo no podrá funcionar sin esos nódulos críticos. En comparación, las diferentes formas de ataques DoS pueden considerarse similares al método británico de atacar—en lugar de atacar directamente sistemas críticos, y a menudo sumamente defendidos, el agresor intenta derribar algún aspecto de la red local o regional de la cual esos sistemas críticos dependen. El método para atacar de la RAF durante la Segunda Guerra Mundial se basaba inicialmente en atacar fábricas claves, pero después de fracasos iniciales y grandes pérdidas, la RAF cambió a sencillamente bombardear las ciudades industriales principales, atacando todo el ecosistema industrial en lugar de una serie de "nódulos claves" discretos. A pesar de un inicio desalentador similar, la USAAF atacaba lo que consideraba nódulos vitales—principalmente la fabricación de aeronaves, combustible, transporte y rodamiento de bolas—desde 1943-1945, intentando aplastar el sistema industrial alemán destruyendo o desactivando un puñado de nódulos claves (tales como la fábrica de rodamientos de bolas en *Schweinfurt* y la refinería en *Ploesti*).[26] Por supuesto, en ejecución, ni el método de la USAAF ni el de la RAF no siempre eran tan diferentes, los B-17 y B-24 de la USAAF a menudo no podían lanzar bombas en el blanco con la interferencia del clima y las defensas alemanas[27], pero los dos métodos de ataque tienen similitudes con los equivalentes cibernéticos discutidos anteriormente. Desde luego, las PC y los interruptores en una red militar son blancos menos controversiales que la población de ciudades industriales, pero muchos ataques DoS son menos precisos y más probables de extenderse tener consecuencias no intencionales en el ciberespacio civil. Resulta importante destacar que, dependiendo de la situación, ambos tipos de ataque pueden ser muy eficaces; los ataques DDoS en Estonia en el 2007 constituyen un ejemplo de un ataque DDoS que tuvo impactos significativos[28], mientras que los supuestos ataques DoS coordinados por Rusia dañaron la capacidad de Georgia de responder a ataques armados rusos en el 2008.[29]

Por consiguiente, si bien destruir un solo reactor es extremadamente difícil y típicamente requiere planificar cuidadosamente un ataque completamente nuevo, interrumpir el C2 o la logística militar es a menudo práctico empleando herramientas "comerciales" para la piratería con el fin de organizar un ataque relativamente no refinado. A diferencia de la mayoría de los demás ámbitos, en el ciberespacio un blanco más distribuido y más grande es mucho más fácil de atacar y paralizar. En discusiones recientes sobre la ciberguerra a menudo se ha confundido el espionaje con la guerra, y como resultado algunos comentaristas han dado por sentado que el aprovechamiento de las vulnerabilidades es más valioso de lo que sería en tiempo de guerra, que la furtividad es más necesaria de lo que sería en tiempo de guerra y que las redes grandes de la milicia o infraestructura poseen las mismas defensas de los que a menudo poseen sistemas pequeños de inteligencia o nucleares.[30] Estas malas interpretaciones distorsionan la naturaleza de la concentración en la ciberguerra, y pueden resultar en errores graves al organizar unidades de ciberguerra o crear defensas de la red. Si bien el espionaje cibernético—inclusive ataques cibernéticos encubiertos en tiempo de paz—tienden a incluir ataques furtivos y sumamente precisos, los ataques cibernéticos en una guerra abierta pueden abarcar todas las diferentes formas de concentración y poder de combate discutidos anteriormente. Las limitaciones diplomáticas y políticas puede que varíen de un conflicto "solamente cibernético" a una guerra tradicional (ci-

nética) que incluye ataques cibernéticos, pero ambos probablemente incluirán ataques abiertos que sacrifican la furtividad para atacar más fuerte y más rápido, permitiendo ataques generalizados con recursos limitados.

La concentración es importante en la ciberguerra, pero su significado varía dependiendo de la naturaleza del ataque y del blanco. Si bien el nivel táctico no siempre será impactado muy severamente, particularmente en las milicias o fuerzas terrestres que no son estadounidenses donde las redes no se emplean demasiado, al nivel operacional las milicias modernas dependen en gran medida de sus redes para la logística y la concienciación de la situación. Estas redes son "centros de gravedad", y si se pueden interrumpir pueden reducir significativamente la eficacia de las fuerzas que dependen de ellas. Aunque ataques sumamente precisos pueden ser devastadoramente eficaces, también hay alternativas DoS que pueden paralizar cuando se llevan a cabo correctamente. Las definiciones correctas de concentración y poder de combate en la ciberguerra son fluidas, al igual que el ciberespacio en sí, y las milicias que se limitan a una fase corren el riesgo de la derrota cuando un adversario ataca en maneras que no son iguales ni a su doctrina ni a su organización. ❑

Notas

1. *Air Force Doctrine Document* (Documento de Doctrina de la Fuerza Aérea) (AFDD) 1, pág. 32.
2. *AFDD 3-12, Cyberspace Operations* (Operaciones Ciberespaciales), pág. 16.
3. Martin Libicki, *Cyberdeterrence and Cyberwar* (Ciberdisuasión y Ciberguerra) (Santa Monica, CA:RAND Corp, 2009), pág. 59. Disponible en http://www.rand.org/pubs/monographs/MG877.html.
4. Gregory J. Rattray, *Strategic Warfare in Cyberspace* (La guerra estratégica en el ciberespacio) (Boston: MIT Press, 2001), págs. 100, 464.
5. Consultar Edward Skoudis, ed. Franklin D. Kramer, Stuart H. Starr y Larry K. Wentz, "*Information Security Issues in Cyberspace*" (Temas sobre seguridad en el ciberespacio), *Cyberpower and National Security* (Ciberpoder y la seguridad nacional) (Dulles, VA: Potomac Books, 2009).
6. "Antivirus Software" (*Software* antivirus), Wikipedia, http://en.wikipedia.org/wiki/Antivirus_software. Consultado el 30 de mayo de 2012.
7. Maia Szalavitz, "*Why People Stick with Cancer Screening, Even When it Causes Harm*" (Por qué las personas continúan con las pruebas de cancer inclusive cuando son dañinas), Healthland, Time.com, http://healthland.time.com/2012/05/25/why-people-cling-to-cancerscreening-and-other-questionable-medical-interventions-even-when-they-cause-harm/.
8. "Antivirus Software", Wikipedia.
9. Para más información, consultar, see Shon Harris, *CISSP All in One Exam Guide* (Guía para examen CISSP), *4th ed.* (New York:McGraw Hill, 2008), págs.. 250-257.
10. Sin embargo, esos sistemas especializados puede que sean más débiles y vulnerables que sus contrapartes estándar COTS una vez que los agresores los entienden—especialmente sistemas de infraestructura, que a menudo fueron concebidos sin pensar en lo absoluto en la seguridad.
11. Thomas Rid, "*Think Again: Cyberwar*" (Piense nuevamente: Ciberguerra), Foreign Policy (Política Exterior), 27 de febrero de 2012, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=0,2.
12. *Stuxnet* fue un virus troyano sumamente significativo que se propagó en unidades de memoria flash (thumb drives) que infiltraron y sabotearon instalaciones nucleares iraníes en el 2010 por varios meses antes de ser detectados. Consultar "*The Stuxnet Outbreak*" (La epidemia *Stuxnet*), *The Economist*, 30 de septiembre de 2010. http://www.economist.com/node/17147818.
13. Richard A. Clarke y Robert K. Knake, *Cyberwar: The Next Threat to National Security and What to Do about It* (La próxima amenaza a la seguridad nacional y qué hacer) (New York: HarperCollins, 2010), 167.
14. Rinat Abdurafikov, *"Russian Electricity Market: Current State and Perspectives"* (El mercado de la electricidad rusa: Estado actual y Perspectivas), VTT Technical Research Centre of Finland (Centro Técnico VTT de Finlandia), 2009. http://www.vtt.fi/inf/pdf/workingpapers/2009/W121.pdf.
15. "*Exploit*" (Aprovechamiento de la vulnerabilidad), Wikipedia, http://en.wikipedia.org/wiki/Exploit_(computer_security), consultado el 27 de mayo de 2012. Consultar también a Harris, pág. 62.
16. Ver Stephen Northcutt, et al, *Inside Network Perimeter Security, 2nd ed.* (Dentro de la seguridad del perímetro de la red, 2a Edición) (Indianapolis: Sams Publishing, 2005), págs. 257-258 para una discusión de los factores que hace que la reparación (*patching*) sea una dificultad grande en la red.
17. *Microsoft Security Update Guide, 2nd ed.* (Guía para actualización de seguridad *Microsoft*), Microsoft, 2011 http://www.microsoft.com/en-us/download/details.aspx?id=559 Para un breve resumen de un sistema de *patching,* consultar "*WSUS Overview*", *Microsoft Technet*, http://technet.microsoft.com/en-us/library/cc539281.aspx.

18. Libicki, p. 57.

19. "*Patch Tuesday (January-May 2012)*" *Microsoft Technet*, http://technet.microsoft.com/en-us/security/bulletin/ms12-jan, http://technet.microsoft.com/en-us/security/bulletin/ms12-feb, http://technet.microsoft.com/en-us/security /bulletin/ms12-mar, http://technet.microsoft.com/en-us/security/bulletin/ms12-apr , http://technet.microsoft.com/en-us/security/bulletin/ms12-may.

20. John Cobb, "*Centralized Execution, Decentralized Chaos: How the Air Force is Poised to Lose a Cyber War*" (Ejecución centralizada, caos descentralizado: Cómo la Fuerza Aérea está destinada a perder una ciberguerra), *Air and Space Power Journal*, Verano 2011, http://www.au.af.mil/au/cadre/aspj/airchronicles/apj/2011/2011-2/2011_2_16_cobb.pdf.

21. DoS se refiere a cualquier ataque enfocado en desmantelar un sistema o red sobrecargándola. EL DDoS es un tipo de DoS específico donde cantidades masivas de tráfico de la red proveniente de computadoras alrededor del mundo se envían para abrumar el servidor o la red objetivo, causando que se congele y deje de responder al tráfico legítimo. Ver Harris págs. 1010-1013.

22. Para una discusión más profunda sobre este tema, consultar Kamal Jabbour, "*Cyber Vision and Cyber Force Development*" (Visión cibernéticas y desarrollo de la fuerza cibernética), *Strategic Studies Quarterly*, Primavera 2010, www.au.af.mil/au/ssq/2010/spring/jabbour.pdf.

23. Rattray, pág. 142.

24. Consultar el AFDD 3-12, págs. 25-26 para una discusión adicional sobre cómo armonizar ataques cibernéticos.

25. Elinor Mills, "*Expert: Stuxnet was Built to Sabotage Nuclear Plant*" (Experto: *Stuxnet* fue creado para sabotear una planta nuclear). Insecurity Complex, CNET.com, http://news.cnet.com/8301-27080_3-20017201-245.html?tag=mncol;1n.

26. Geoffery Perret, *Winged Victory* (New York: Random House, 1993), págs. 240-244.

27. Rattray, pág. 280.

28. Los ataques DDoS que supuestamente fueron coordinados por Rusia ocasionaron interrupciones significativas a los bancos y gobierno de Estonia (Rusia negó cualquier participación oficial). Ver Clarke y Knake, págs. 11-16.

29. David Hollis, "*Cyberwar Case Study: Georgia 2008*" (Estudio sobre la ciberguerra: Georgia 2008). *Small Wars Journal*, 6 de enero de 20122, http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008 , p. 5.

30. Ejemplos de estas suposiciones erróneas incluye Rid (especialmente pág. 5) y Libicki (ver págs. 56-59, y compare a las guías de la industria sobre el *patching* mencionado anteriormente, particularmente *Northcutt, et al*—una red grande de reparación requiere un esfuerzo significativo durante el transcurso de días, a menudo semanas, y cuando se hace muy rápido el *patch* en sí puede dañar sistemas críticos).

EL Capitán John M. Cobb, USAF (BS, USAFA) es Jefe, Ingeniería de Informática para la Dirección de Educación en Logística y Comunicaciones en el Cuartel General de la Universidad del Aire, Base Aérea Maxwell, Alabama. En este puesto, él es responsable de crear el software educativo que se emplea en la Fuerza Aérea, asesorar a los líderes de la dirección sobre la tecnología educativa y asesorar a los suboficiales programadores. Antes de desempeñar su cargo actual, el Capitán Cobb se desempeñó en calidad de Oficial a Cargo, Operaciones de la Red en la Base Aérea Misawa, Japón, donde estuvo a cargo de mantener y asegurar una red base para más de cuatro mil miembros del servicio conjunto. El Capitán Cobb fue desplegado en apoyo a las operaciones Nuevo Amanecer y Paz Duradera, y es egresado de la Escuela Superior para Oficiales de Escuadrón.

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 cibespacio 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 el 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 cibespacio 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 ciberspaciales 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 las guerra aérea tenía nuevos aspectos propios. Hoy hemos encontrado que el ciberespacio también tiene aspectos propios, aspectos de 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 conceptuar 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 lazo .[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 sicológica y el uso de estrategias en vez de fuerza.[19] Por ejemplo, están desarrollando a lago 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 realidad[26] —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 nuestra 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 podían 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 aplicarían 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 luchen 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 cibesespacio 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 Air War 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 april 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) htttp://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 sicológicas 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.

La Guerra en el Ámbito Cibernético

Welton Chang
Sarah Granger

DAR SENTIDO A LA ciberguerra requiere un entendimiento del ámbito cibernético. Las características intrínsecas del ámbito cibernético hacen que sea un reto determinar las implicaciones de la ciberguerra en la política de seguridad nacional. Es imprescindible definir correctamente el ámbito cibernético. Comprender cómo funciona y se comporta el medio ambiente al igual que las implicaciones de los conceptos, como por ejemplo la convergencia (la integración de tecnologías múltiples en un número más pequeño de plataformas y la armonización cada vez mayor del mundo virtual y del físico) ayudan a enmarcar el panorama más amplio.

El entorno cibernético le da forma a la porción "guerra" de la ciberguerra. Lamentablemente, las discusiones sobre la ciberguerra han sido polarizadas por los comentaristas, quienes algunos de ellos opinan que un "Pearl Harbo cibernético" es inevitable y otros opinan justamente lo contrario. La realidad radica en algún lugar en el medio. Resulta importante recordar que la guerra es una extensión de la política y que este axioma aplica en el ámbito cibernético. La planificación operacional debe tomar en cuenta el espectro de las amenazas. Comprender las implicaciones de la complejidad y las intenciones de los actores en el sistema será clave para crear estrategias eficaces de guerra cibernética.

Presentando el ámbito cibernético: Complejidad y transparencia

¿En qué consiste un ámbito cibernético?[1] La *Internet,* por supuesto, pero también mucho más. El ámbito cibernético incluye la arquitectura organizadora de la *Internet,* los dispositivos conectados a la *Internet* y las redes convencionales e inalámbricas. Algunas de esas redes son administradas por entidades del gobierno y del sector privado, algunas están conectadas a la *Internet* más amplia y algunas no. La escala de la *Internet* dificulta su comprensión. Esto nos conduce a un exceso de confianza en analogías imprecisas. Si bien técnicamente la *Internet* simple y llanamente es el primer ámbito creado por el hombre, su estructura puede ser difícil de conceptualizar. En lugar de existir dentro de fronteras finitas, imita otros sistemas naturales tales como colonias bacterianas y galaxias en expansión, donde billones de nódulos se expanden en todas las direcciones.[2] Como resultado, el ámbito cibernético, principalmente redes de computadoras conectadas, operando en un protocolo omnipresente de transferencia de datos, es complejo interactiva y estructuralmente.[3]

La complejidad hace que el ámbito cibernético sea difícil de estudiar. La complejidad estructural es el resultado del crecimiento exponencial del poder de la computación y la cantidad de dispositivos conectados a la *Internet.* La complejidad interactiva se deriva de la participación del ser humano en el sistema. El cambio tecnológico exponencial ha tornado el medio ambiente más complejo que nunca. Las cifras que ilustran este cambio son asombrosas: más de 2,1 mil millones de personas conectadas vía la *Internet,* 1,8 *zettabytes* de datos electrónicos creados en el 2011 y un total de 555 billones de sitios web. Se proyecta que en el 2016 la cifra de dispositivos móviles conectados a la *Internet* supere la cantidad total de personas en el planeta.[4] La transacción de información entre cualquiera de esos dispositivos es posible, conduciendo a una multitud de interacciones y consecuencias que la humanidad aún tiene que comprender totalmente.[5]

La seguridad no formaba parte del diseño original del ciberespacio. El ámbito cibernético fue concebido para la transparencia. Los protocolos estandarizados para la transmisión de datos son el pegamento que mantiene junta a la *Internet* y los servicios para nombrar los ámbitos ayudan a dirigir los datos donde tienen que ir. Un diseño enfocado en la transparencia significa que la seguridad no es parte intrínseca en el sistema y debe ser injertada después. Cuando se crearon los protocolos no había mucho conocimiento del concepto de *malware* masivo a las computadoras. Las redes y el *software* creados encima de ellos viajan en una red central intrínsecamente abierta y, como resultado, hay que incorporar múltiples capas de seguridad para garantizar la integridad del sistema y los datos.[6] Las vulnerabilidades esparcidas son semejantes a las deficiencias en el sistema inmunológico humano. La falta de variedad genética entre los seres humanos significa que enfermedades contagiosas pueden afectar a muchas personas. El ciberespacio tiene un tipo de uniformidad genética similar: la ubicuidad de los sistemas operativos como *Microsoft Windows* ejecutando programas como *Internet Explorer* significa que las vulnerabilidades no tratadas se esparcirán.

Describiendo el ámbito cibernético: Convergencia, el elemento humano, velocidad y asimetría

Más allá de la complejidad y la transparencia, varias características importantes del entorno cibernético le dan forma a la ciberguerra, inclusive niveles crecientes de convergencia, la velocidad de las interacciones, el elemento humano inextricable y facultar al individuo dentro del ámbito cibernético.

La convergencia es un concepto del cual se escribe a menudo, algunas veces se comprende y es criticado por muchos. La convergencia se ha referido en gran parte a la marcha aparentemente inexorable de la integración de tecnologías digitales en cada vez menos plataformas de entrega. Por ejemplo, la diferencia entre el correo electrónico, la televisión y las comunicaciones por voz ha sido nublada por la adopción a gran escala de *smartphones* capaces de llevar a cabo las tres funciones operando en protocolos de *Internet*. La convergencia también es la unión de los mundos virtual y físico. A medida que más sistemas estén conectados a una *Internet* más amplia para fines de eficacia y conveniencia, muchos objetos físicos tendrán una presencia en el mundo virtual. En un extremo, la eliminación virtual se convierte en el equivalente de la destrucción física. Por ejemplo, la mayoría de las finanzas del mundo existen solamente como datos, y arreglar la corrupción de datos dependería de datos electrónicos a falta de expedientes físicos.[7] La unión de los mundos físico y virtual también se ha extendido a los humanos y la tecnología. La convergencia también significa que las vulnerabilidades identificadas actualmente en programas de computadora que controlan entidades físicas tales como los sistemas de control industrial (ICS, por sus siglas en inglés) se esparcirán aún más.[8] ICS es el término genérico para una clase de sistemas electrónicos que controlan una gama amplia de infraestructura tales como los sistemas de agua, gas y eléctricos. En un sistema intrínsecamente abierto, la convergencia significa más vulnerabilidades virtuales, algunas análogas a las físicas.

El elemento humano es una parte fundamental del ámbito cibernético que no se puede pasar por alto. En vista de que seres humanos construyeron la arquitectura cibernética, será intrínsecamente imperfecta. Además, hacer cumplir las medidas de seguridad tales como la instalación de *software* antivirus, la creación de contraseñas difíciles y el rechazo de tácticas de ingeniería social tales como "*phishing*", recae sobre el usuario. Y en la mayoría de los casos, el *software* en sí tiene fallas, ya sea si se encuentra en el sistema operativo o al nivel de aplicación.

La velocidad también es un elemento importante del ámbito cibernético que se debe tomar en cuenta cuando se opera en el ciberespacio. La acción en el ciberespacio puede ser más rápida y puede conducir a efectos geográficos de mayor alcance que en otros ámbitos. Sin embargo, los

operadores de los sistemas de computadoras son seres humanos que no trabajan a la velocidad de la luz. Los humanos actúan como restricciones funcionales en el medio ambiente hasta el punto que están en control del dispositivo y un programa en funcionamiento. Sin bien los electrones se mueven a la velocidad de la luz, embotellamientos en la arquitectura de la red y la velocidad del procesador común a lo largo de una ruta de datos también son restricciones. Por último, si bien los electrones son más rápidos que las fuerzas terrestres, cuando las operaciones en el ciberespacio apoyan operaciones militares de mayor escala en otros ámbitos, las fuerzas refrenan el ritmo de las operaciones. En un final, el esfuerzo principal también dicta la eficacia de los electrones.

El ámbito cibernético es un entorno operacional en el que la eficacia del individuo es ampliada a causa de la automatización, la agilidad de grupos pequeños y la difusión del conocimiento a lo largo de las geografías. Un individuo operando en cualquier parte del mundo con una conexión a la *Internet* puede estar al mando de un *botnet* (un grupo de computadoras controladas clandestina y remotamente) grande y a menudo involuntario para llevar a cabo ataques de negación de servicio. Un individuo también puede crear un programa que se reproduce y extiende por sí solo, a través de la misma vulnerabilidad. En vista de que la transmisión de conocimiento ahora es prácticamente gratuita, los individuos en redes de cooperación pueden aprender rápidamente las técnicas de ataque más eficaces y aprovecharse de vulnerabilidades anteriormente desconocidas. Esas redes de cooperación y redes de redes comienzan a dar muestras de inteligencia emergente, reproduciendo acciones dirigidas centralmente cuando no existe ese tipo de autoridad. Esto significa que individuos tales como el grupo *Anonymous,* empleando un *botnet*, puede tener el mismo impacto que los operativos de computadora que desactivaron grandes cantidades de redes estonianas públicas y privadas en el 2007.[9]

Por último, la asimetría entre los recursos, costos, valores, intereses y organización de grupos tales como *Anonymous* en comparación con organizaciones gubernamentales tales como el Comando Cibernético de Estados Unidos estriba de un medio ambiente que está más dispuesto a la insurgencia virtual que a la guerra convencional.[10] En vista del diseño abierto del ámbito ciberespacial, la defensa es intrínsecamente más costosa y toma más tiempo que la ofensiva. Además, armas cibernéticas costosas y sumamente técnicas creadas por gobiernos se pueden rediseñar fácil y económicamente por otros en el ámbito ciberespacial. La asimetría en el ámbito ciberespacial por lo general favorece a actores más pequeños y más ágiles. A menudo esos actores no cuentan con una dirección física permanente y pueden enmascarar sus direcciones virtuales. Este es un punto clave que las burocracias grandes tienen que adoptar para poder crear estrategias eficaces de mitigación.

Clausewitz Cibernético

La primacía de la política en la ejecución de cualquier tipo de guerra significa que en un final la guerra es una contienda de voluntad política. Cuando las estrategias se crean correctamente, los objetivos políticos serán la meta final de la ciberguerra. Algunos comentarios sobre la ciberguerra se enfocan en las características singulares del ámbito cibernético, a la vez que pasan por alto la idea de que la guerra es una extensión de la política. En los argumentos de si un "Pearl Harbor cibernético" es o no inevitable, los comentaristas rara vez toman en cuenta la idea que dicha acción extrema sería emprendida para fines políticos.[11] De manera similar, cuando se discute el ciberterrorismo, un "11-S cibernético" se describe como imposible o inevitable.[12]

Un "Pearl Harbor cibernético" probablemente no ocurrirá a menos que los beneficios de tomar dicha acción superan los costos para un estado. Por ejemplo, la integración de las economías estatales aumentan los costos de la acción unilateral. Algunos parecen pensar que el plural de los ataques cibernéticos es la guerra cibernética pero no debemos olvidar que la guerra exige

un objetivo político. Inclusive los actos terroristas están concebidos para lograr algún tipo de objetivo político o religioso, ya sea desmoralizar una población u obligar a un gobierno a negociar, no solamente destruir por destruir. Entender las intenciones de los adversarios es primordial al igual que lo es reconocer hasta el punto al cual un adversario dependería de otros actores en el sistema. En el mundo hiperintegrado en el que vivimos, no tomar en cuenta la dependencia nos conduce a obviar el factor clave en la probabilidad o poca probabilidad de que estalle una guerra. Por último, la ciberguerra no tiene que ocurrir en las partes extremas del espectro de la capacidad. Enfocarse en la discusión de escenarios extremos solo sirve para polarizar argumentos y ofuscar los peligros verdaderos que existen.

La situación real actual

¿Ya hemos presenciado la ciberguerra?[13] Las acciones rusas pretendidas durante el conflicto con Estonia en el 2007 son el primer ejemplo y a menudo el más mencionado. Algunos expertos creen que el uso de las tácticas cibernéticas durante la disputa con Estonia en el 2007 fue más semejante a un conflicto cibernético, que no está a la altura del umbral de la guerra.[14] Sin embargo, en el 2007 ni los estados ni las poblaciones dependían tanto del ámbito cibernético como dependen ahora. La informática de nube apenas estaba comenzando y su dependencia en la *Internet* para el comercio y la banca era infinitamente diferente.

Las vulnerabilidades intrínsecas en el ámbito cibernético, junto con el desarrollo de las capacidades de varios actores (algunos con intenciones malignas) significa que la ciberguerra es una posibilidad muy real en el futuro. Cualquier estrategia nacional cibernética que busque lidiar con el medio ambiente cibernético debe tomar en cuenta los riesgos si no se tratan las vulnerabilidades. Con base en nuestro nivel de dependencia en el ámbito cibernético tanto para las capacidades de seguridad nacional como el funcionamiento de la vida cotidiana, los riesgos son grandes.[15]

Pero, ¿cuál es el nivel actual de la amenaza? Esto es difícil de definir por varias razones, aunque podemos decir con certeza que durante los dos últimos años, los ataques a redes y sistemas principales han crecido consistentemente, tanto en situaciones públicas como en el sector privado.[16] Resulta difícil recopilar y analizar estadísticas exactas con respecto a los ataques, y un enfoque en las estadísticas del ataque pasa por alto la amenaza más insidiosa de ataques no detectados y vulnerabilidades no explotadas en el *software* y *hardware*.[17] Organizaciones y sectores diferentes pueden albergar intereses provincianos con respecto a exagerar o disminuir el panorama de la amenaza.[18] Ya sea que esos intereses sean burocráticos o impulsados por las ganancias, los análisis de la amenaza deben juntarse y destilarse para lograr un entendimiento más holístico e imparciales de la situación real actual. También es posible que ataques a gran escala se vean muy diferentes de lo que se ha experimentado anteriormente.[19]

Cuando se trata de ciberguerras hay un espectro de amenazas y tácticas, desde negación de servicio a interrupción hasta la destrucción de *hardware* físico conectado vía los sistemas de control industrial. Este espectro de amenazas llega a todos los demás ámbitos de la guerra—terrestre, marítima, aérea y espacial.[20] La dimensión económica también es tremenda—el General Keith Alexander, jefe del Comando Cibernético de EE.UU. y de la Agencia de Seguridad Nacional de EE.UU., expresó que las amenazas y los ataques cibernéticos existentes constituyen la mayor "transferencia de riqueza en la historia".[21] Para una institución de defensa estadounidense que depende tanto de una ventaja económica y material abrumadora, esto equivale a una "muerte segura".[22]

Una conclusión razonable es que podría sufrir una amplia gama de ataques posibles, especialmente en un conflicto mundial real que tiene lugar a lo largo de otros ámbitos.[23] Es probable que el ciberterrorismo se convierta más en un conocimiento acerca de propagaciones de siste-

mas de control industrial mientras que las vulnerabilidades seguirán sin tratarse. Por último, ha habido cierto movimiento hacia los ataques cibernéticos de precisión, programas complejos de computadoras que funcionan para lo que fueron concebidos podría resultar en consecuencias catastróficas no intencionales a falta de la interacción humana.[24]

En conclusión: Educar, entrenar y coordinar

Si se permite que nuestras vulnerabilidades cibernéticas continúen sin tratarse, estamos dejando bajar el puente levadizo virtual.[25] Nuestra labor ahora es mejorar el intercambio de información, los esfuerzos de inteligencia y los mecanismos para coordinar la seguridad de manera que podamos evitar, adaptarnos y reaccionar en caso de que llegue el momento en que se comprometan la infraestructura crítica u otras redes importantes. Debemos actuar ahora porque la infraestructura crítica le da poder a nuestra economía y a nuestro aparato de seguridad nacional.

Avanzando, continuar educando a todos los interesados civiles y militares es de suma importancia, además de asegurar las redes y nódulos en sí. Un problema que se avecina es que la cantidad de norteamericanos que se están entrenando, educando y desarrollándose dentro de Estados Unidos (inclusive estudiantes universitarios especializándose en ciencias computacionales y campos afines) no está aumentado correctamente para igualar la amenaza creciente. También es importante educar a los ciudadanos en general acerca de mejorar la seguridad en sus computadoras y redes. Un método híbrido para administrar la amenaza cibernética, la respuesta en casos de incidentes y las medidas defensivas preplanificadas se debe adoptar para poder crear una arquitectura defensiva más resistente.[26]

En el futuro cercano veremos más *software* para recopilar inteligencia en nuestras redes, experimentaremos más ataques generalizados de distintos tipos y debemos esperar enfrentarnos a consecuencias imprevistas e interrupciones que aún no se han visto. Si bien en la mayoría de los casos la naturaleza de los ataques puede que sea impredecible, la historia será una guía confiable para otros. Lo que sí sabemos es que distintos tipos de adversarios—individuos, grupos parias y organizaciones sofisticadas—ya radican en redes y pueden penetrarlas a su antojo en muchos casos.

Hasta cierto punto hemos sido afortunados. En algunas ocasiones los ataques en la infraestructura crítica y otros sistemas importantes han sido frustrados y esa información se ha compartido con el público.[27] Esos episodios disipan el mito que no hay motivo para que los agresores ataquen esos sistemas. La resistencia de los modelos es eficaz en planificar la recuperación y respuesta, particularmente a causa de la naturaleza asimétrica del ámbito y la probabilidad de patrones de ataque complejos y de muchas fases. Una educación exitosa en este campo debe incluir entrenamiento en resistencia, prácticas de respuesta en un escenario al igual que ingeniería técnica y social. El diseño de módulos de entrenamiento que se puedan desplegar rápidamente podría ser sumamente útil. En muchos casos, el proceso de obtener permiso para ofrecer programas de educación y entrenamiento puede ser un obstáculo por derecho propio, evitando que personal a todos los niveles obtengan destrezas muy necesarias que pueden ser útiles para identificar y combatir ataques cibernéticos.

En un final, la complejidad y las propiedades intrínsecas del entorno cibernético no nos deben detener de trazar estrategias y planificar.[28] Mientras que la inmensidad del ámbito cibernético abruma nuestra infraestructura vertical no integrada gubernamental, nuestro entendimiento colectivo mejora cada año aunque la amenaza continúa creciendo. Pero al incorporar la resistencia al sistema y distribuir la responsabilidad defensiva a todos los usuarios finales, llevar a cabo una guerra en el ámbito cibernético se tornará más costosa y menos eficaz para el agresor. Puede que la ciberguerra aún no haya ocurrido, pero es verdaderamente una amenaza futura que los gobiernos, empresas privadas e individuos deben tomar en serio. La amenaza está au-

mentando y al tomar medidas ahora para aumentar la seguridad, disminuimos el riesgo de ser sorprendidos desprevenidamente. ❑

Notas

1. En la *Joint Publication* (Publicación Conjunta) 1-02 se define el ciberespacio como "un ámbito global en el entorno de información que consta de la red independiente de infraestructuras de tecnología de la información, inclusive la *Internet*, redes de telecomunicaciones, sistemas de computadoras y procesadores y controladores incorporados". *United States Department of Defense, Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms* (Diccionario de Términos Militares y Afines del Departamento de Defensa), (Washington D.C.: 8 de noviembre de 2010), págs. 79-80; consultado en: <http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf>.

2. Por publicarse: Sarah Granger, Lorelei Kelly, *"Cybersecurity and Modern Grand Strategy"* (Ciberseguridad y la gran estrategia moderna), Institute for the Study of Diplomacy, Georgetown University School of Foreign Service, 2012; pág. 1.

3. Ver: United States Army Training and Doctrine Command, *"TRADOC Pamphlet 525-5-500: Commander's Appreciation and Campaign Design"* (Folleto TRADOC 525-5-500: Evaluación del Comandante y diseño de la campaña), 28 de enero de 2008, págs. 5-7; consultado en: <http://www.tradoc.army.mil/tpubs/pams/p525-5-500.pdf>.

4. Ver: Pingdom, *"Internet in 2011 in numbers"* (La Internet en cifras en el 2011), Royal Pingdom, 17 de enero de 2012; consultado en : <http://royal.pingdom.com/2012/01/17/internet-2011-in-numbers/>. Jon Brodkin, *"Mobile internet devices will outnumber humans this year, Cisco predicts"* (Cisco predice que los dispositivos móviles de *Internet* sobrepasarán la cifra de seres humanos este año), Ars Techica, 14 de febrero de 2012; consultado en: <http://arstechnica.com/business/2012/02/mobile-internet-devices-will-outnumber-humans-this-year-cisco-predicts/>; IDC, "The 2011 Digital Universe Study: Extracting Value From Chaos" (Estudio del universo digital 2011: Extrayendo valor del caos), junio de 2011; consultado en: <http://www.emc.com/collateral/demos/microsites/emc-digital-universe-2011/index.htm>.

5. En un estudio JASON de MITRE sobre la seguridad cibernética se alega que, "No hay "leyes de naturaleza" intrínsecas para la seguridad como las hay, por ejemplo, en física, química o biología. La ciberseguridad es esencialmente una ciencia aplicada que es informada por los conceptos matemáticos de la ciencia computacional tales como teoría autómata, complejidad y lógica matemática". JASON, "Science of Cyber Security" (La ciencia de la ciberseguridad), MITRE Corporation, noviembre de 2010, pág. 4; consultada en: <http://www.fas.org/irp/agency/dod/jason/cyber.pdf>.

6. Ver: Paul A. Strassaman, *"The Internet's Vulnerabilities Are Built Into Its Infrastructure"* (Las vulnerabilidades de la *Internet* están incorporadas a su infraestructura), AFCEA, Signal Online, noviembre de 2009; <http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=2109&zoneid=3>.

7. Para un ejemplo de los peligros de la convergencia ver: Robert O'Harrow Jr., *"Tridium's Niagara Framework: Marvel of Connectivity Illustrates New Cyber Risks,*(Estructura Niágara de Tridium: Maravilla de conectividad ilustra nuevos riesgos cibernéticos)" *Washington Post,* 11 de julio de 2012, consultado en: <http://www.washingtonpost.com/investigations/tridiums-niagara-framework-marvel-of-connectivity-illustrates-new-cyber-risks/2012/07/11/gJQARJL6dW_story.html>.

8. Ver: Keith Stouffer, Joe Falco, and Karen Scarfone, *"Guide to Industrial Control Systems"* (Guía para los sistemas de control industriales), National Institute of Standards and Technology", NIST Special Publication 800-82, pág. 2-1; consultado en: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800.82.pdf>. Supervisory Control and Data Acquisition Systems (SCADA) (Los sistemas de supervisión de control y adquisición de datos [SCADA]) son una clase de sistemas de control industrial. Programas como *SCADAscan* detectan redes SCADA conectadas a la *Internet*. Ver también: Bill Brenner, *"#BSidesSF: Why SCADA security is such an uphill struggle"* (#BSidesSF: Por qué la seguridad SCADA es una ardua batalla), CSO Online, 27 de febrero de 2012; consultado en: <http://blogs.csoonline.com/critical-infrastructure/2044/bsidessf-why-scada-security-such-uphill-struggle>.

9. Se sospecha que piratas cibernéticos rusos o pro rusos han perpetrado ataques de negación de servicio contra sitios del gobierno estoniano y del sector privado durante un conflicto sobre la reubicación de un monumento de guerra. Ver: William C. Ashmore, "Impact of Alleged Russian Cyber Attacks" (Impacto de presuntos ciberataques rusos), US Army School of Advanced Military Studies, mayo de 2009, págs. 5-8; consultado en: <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA504991>.

10. Para una discusión sobre asimetría y la ciberguerra ver: Michael Breen, Joshua A. Geltzer, *"Asymmetric Strategies as Strategies of the Strong"* (Estrategias asimétricas como estrategias del fuerte), Parameters, primavera 2011, págs. 48-49; consultado en: <http://www.carlisle.army.mil/usawc/parameters/Articles/2011spring/Breen-Geltzer.pdf>. También ver: Quinn Norton, *"How Anonymous Picks Targets, Launches Attacks, and Takes Down Powerful Organizations"* (Cómo anónimos seleccionan blancos, lanzan ataques y destruyen organizaciones poderosas), Wired, 3 de julio de 2012, consultado en: <http://www.wired.com/threatlevel/2012/07/ff_anonymous/all/>.

11. Un "Pearl Harbor cibernético" en nuestro cálculo sería un ataque debilitante masivo, intencional e inesperado a la infraestructura crítica y capacidades de defensa de EE.UU. Ver: Jake Tapper, *"Leon Panetta: A Crippling Cyber Attack Would Be An Act of War"* (Leon Panetta: Un ciberataque de consecuencias catastróficas sería un acto de guerra), ABC News, 27 de mayo de 2012; consultado en: <http://abcnews.go.com/blogs/politics/2012/05/leon-panetta-a-crippling-cyber-attack-would-be-act-of-war/>.

12. Sunlen Miller, *"Despite Threat of 'Cyber 9/11', Lawmakers Punt Cyber Security Bill"* (A pesar de la amenaza de un 11-S cibernético, los encargados de formular leyes desaprueban proyecto de ley sobre ciberseguridad), ABC News, 2 de agosto

de 2012; consultado en: <http://abcnews.go.com/blogs/politics/2012/08/despite-threat-of-cyber-911-lawmakers-punt-cyber-security-bill>.

13. Este es un debate que ha ocurrido varias veces durante los últimos diez años. Ver: Intelligence Squared, *"The Cyber War Threat Has Been Greatly Exaggerated"* (La amenaza de la ciberguerra se ha exagerado demasiado), 8 de junio de 2010; consultado en: <http://intelligencesquaredus.org/debates/past-debates/item/576-the-cyber-war-threat-has-been-grossly-exaggerated>. Ver también: David Betz, "'Cyberwar' is not coming" (La ciberguerra no ocurrirá), Infinity Journal, Volume 1 Issue 3.

14. Contraalmirante (ret.) Michael McConnell, "Cyber-Power and Cyber-Security" (Poder cibernético y seguridad cibernética), Aspen Security Forum, 1 de julio de 2012; consultado en: <http://www.aspenideas.org/session/cyber-power-and-cyber-security>. Thomas Rid alega que el umbral que la ciberguerra debe cumplir es que "tiene que ser potencialmente violento, con una finalidad y tiene que ser político". Aquellos que alegan que la ciberguerra no ha ocurrido creen que la falta de violencia y la destrucción física hacen que la acción cibernética no sea del orden de una guerra cibernética. Thomas Rid, "Think Again: Cyberwar" (Piensen nuevamente: Ciberguerra), *Foreign Policy,* marzo/abril de 2012, consultado en: <http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=full>.

15. Un aspecto crítico del cual civiles y militares dependen es el sector de generación de potencia. Ver: Reuters, *"Senators to hear pitch for tougher cyber security"* (Los senadores escucharán oferta para seguridad cibernética más fuerte), 12 de marzo de 2012, consultado en: <http://www.reuters.com/article/2012/03/07/us-usa-cybersecurity-congress-idUSTRE82621W20120307>.

16. David Sanger, Eric Schmitt, *"Rise is Seen in Cyber Attacks Targeting U.S. Infrastructure"* (Se ve aumento en ciberataques que se concentran en la infraestructura de EE.UU.), *The New York Times,* 26 de julio de 2012, consultado en: <http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html>. Ver también: James A. Lewis, *"Significant Cyber Events"* (Eventos cibernéticos significativos), Center for Strategic and International Studies, última actualización mayo de 2012; consultado en: <http://csis.org/publication/cyber-events-2006>.

17. Conocidas anteriormente pero existentes, las vulnerabilidades incluyen vulnerabilidades de *hardware y de software* conocidas como explotaciones de "día cero". La dificultad en atribuir el ataque (saber quién lo hizo) es también una preocupación importante en el ámbito cibernético. Ver también: Sergei Skorobogatov, Christopher Woods, *"In the blink of an eye: There goes your AES key"* (En un abrir y cerrar de ojos: Ahí va su clave AES), 28 de mayo de 2012, consultado en: <http://eprint.iacr.org/2012/296.pdf>.

18. Para una discusión sobre este tema, ver: consultado en: Peter Maass, Megha Rajagopolan, *"Does Cybercrime Really Cost $1 Trillion?"* (¿En realidad el crimen cibernético cuesta $1 trillón de dólares), Propublica, 1 de agosto de 2012; <http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion>.

19. Frank Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Conflicto en el siglo XXI: El surgimiento de las guerras híbridas), consultado en: <http://www.potomacinstitute.org/index.php?option=com_content&view=article&id=77:-conflict-in-the-21st-century-the-rise-of-hybrid-wars&catid=40:books&Itemid=62>.

20. Danny Steed, *"Cyber Power and Strategy: So What?"* (Poder y estrategia cibernética: ¿Y qué?), *Infinity Journal,* Vol. 1 Issue 2, consultado en: <http://www.infinityjournal.com/article/11/Cyber_Power_and_Strategy__So_What?>.

21. Michael Riley y Dune Lawrence, *"Hackers Linked to China's Army Seen from E.U. to D.C."* (Piratas cibernéticos conectados con el Ejército Chino vistos desde la UE hasta DC), Bloomberg, 26 de julio de 26, 2012; consultado en: <http://www.bloomberg.com/news/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.html>.

22. Cheryl Pellerin, *"Cyber Operations Give Leaders New Options, Official Says"* (Según funcionarios, las operaciones cibernéticas les ofrecen nuevas opciones a los líderes), American Forces Press Service, 12 de abril de 2012; consultado en: <http://www.defense.gov/news/newsarticle.aspx?id=67918>. Tanto James Lewis de CSIS y Richard Clarke también han empleado esta analogía.

23. Para una discusión de la presunta carrera armamentista cibernética, ver: Michael Riley, Ashlee Vance, Cyber Weapons: The New Arms Race (Armamento cibernético: La nueva carrera armamentista), *Bloomberg Businessweek,* 20 de julio de 2011, consultado en: <http://www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html#p1>

24. Por ejemplo, ver el impacto del comercio automatizado de alta velocidad en Wall Street. Nathaniel Popper, *"Knight Capital Says Trading Glitch Cost it $440 Million",* (Knight Capital alega que el percance del comercio le costó $440 millones de dólares), The New York Times, 2 de agosto de 2012, consultado en: <http://dealbook.nytimes.com/2012/08/02/knight-capital-says-trading-mishap-cost-it-440-million/>.

25. Stewart Baker, Natalia Filipiak, Katrina Timlin, *"In the dark: Crucial industries confront cyberattacks"* (En la oscuridad: Industrias cruciales enfrentan ciberataques), McAfee, Center for Strategic and International Studies, 2011; consultado en: <http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf>.

26. El estratega norteamericano T. X. Hammes declara que lidiar con "grupos pequeños sumamente fortalecidos" requiere una "respuesta de toda la sociedad" y que ese modelo está presente en "la defensa de la Internet". Ver: Jim Zirin, *"Will the war in the 21st Century be fought in cyber space?"* (¿Se librará la guerra del siglo XXI en el ciberespacio?), Digital Age, 25 de noviembre de 2007, 20:26-20:28; consultado en: <http://www.youtube.com/watch?v=j1_QG0NIwdE>. Charles Billo, Welton Chang, *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States,*(Ciberguerra: Un análisis de los medios y motivaciones de naciones estados exclusivas), Institute for Security Technology Studies, (Hano-

ver, NH: Dartmouth College, diciembre de 2004), pág. 133; consultado en: <http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf>.

27. Mark Clayton, *"Report: Cyberattacks on critical US targets surge"* (Informe: Aumentan ciberataques en blancos críticos estadounidenses), *Christian Science Monitor,* 29 de junio de 2012, consultado en: <http://www.csmonitor.com/USA/2012/0629/Report-Cyberattacks-on-critical-US-targets-surge>. La operación Dragón Nocturno fue un grupo de ataques publicados contra compañías de energía. La operación Shady Rat atacó, según informes, 70 víctimas gubernamentales, del sector privado y sin fines de lucro en 40 países. Ver: Dmitri Alperovitch, *"Revealed: Operation Shady RAT"* (Revelada: Operación Shady RAT), McAfee, versión 1.1, 2012, consultado en: <http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf> y McAfee, *"Global Energy Cyberattacks: Night Dragon"* (Ciberataques a la energía global: Dragón Nocturno), 10 de febrero de 2011, consultado en: <http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf>.

28. Michael J, Gallagher, Joshua A. Geltzer, y Sebastian L.V. Gorka, "The Complexity Trap" (La trampa de la complejidad), *Parameters,* primavera de 2012, consultado en: <http://www.carlisle.army.mil/usawc/Parameters/Articles/2012spring/Gallagher_Geltzer_Gorka.pdf>. También ver: Sarah Granger, Lorelei Kelly, *"Cybersecurity and Modern Grand Strategy",* Institute for the Study of Diplomacy, Georgetown University School of Foreign Service, 2012.

El Sr. Welton Chang es un analista en el Departamento de Defensa. Fue el asesor principal civil en el 2011 en la Célula de Inteligencia Nacional de Iraq. Desde el 2005 al 2012 Welton se desempeñó como oficial del servicio activo y de la reserva del Ejército. Durante ese tiempo fue desplegado a Iraq y Corea del Sur. En el 2005, Welton egresó cum laude del Darmouth College con altos honores de la facultad. Mientras asistió a Darthmouth, Welton trabajó en el Institute for Security Technology Studies (Instituto de Estudios de Tecnología de Seguridad) donde fue coautor y publicó una monografía muy mencionada sobre la guerra cibernética. En la actualidad es candidato para una Maestría en el Programa de Estudios de Seguridad de la Georgetown University. Además es un becado de Truman National Security Project (Proyecto Truman de Seguridad Nacional).

La Srta. Sarah Granger es la fundadora del Center for Technology, Media & Society (CFTMS)(Centro de Tecnología, Medios de Comunicación y Sociedad). Actualmente es becada del Truman National Security Project, donde es co-presidenta de su grupo de ciberseguridad. Comenzó su carrera trabajando en ciberseguridad para el Lawrence Livermore National Laboratory, seguido por trabajo como asesora de seguridad en la red varios años antes de fundar CFTMS. Sarah fue autora colaboradora de Ethical Hacking, y ha editado varios libros sobre seguridad móvil, criptografía y biométrica. Además, ha escrito para Spectrum, Security Focus, y Forbes Russia. Pueden seguirla en Twitter @sarahgranger.

Las opiniones expresadas en este artículo son las de los autores y no reflejan ni la política oficial ni la postura de la Agencia de Inteligencia de la Defensa, ni del Departamento de Defensa, ni de ninguna agencia del gobierno de Estados Unidos.

Pautas para Diseñar Estructuras Adaptativas de Mando y Control (C2) para las Operaciones Ciberespaciales

Teniente Coronel Jeffrey B. Hukill, USAF-Ret

EL MANDO Y CONTROL (C2) eficaz de las operaciones ciberespaciales, al igual que otras formas de operaciones militares, es esencial para lograr el éxito en el entorno dinámico operacional anticipado del futuro.[1] A pesar de la imposibilidad de que los pronósticos sean infalibles, hay un consenso general entre los estudios con respecto a la naturaleza del entorno militar operacional del futuro. La opinión es que los próximos 25 años retarán a las fuerzas militares con amenazas y oportunidades a lo largo de la gama de las operaciones militares extendiéndose desde guerras regulares e irregulares, hasta ayuda y reconstrucción en zonas de crisis, y compromiso cooperativo en el espacio común global.[2] Confrontar esas amenazas y oportunidades exigirá que las operaciones se lleven a cabo en un entorno integrado, conectado a redes y distribuido bajo un comandante de fuerza conjunta. En vista de que estas operaciones sirven una mezcla de objetivos militares y civiles, el éxito en esas operaciones exige la integración de capacidades de todas las agencias gubernamentales, servicios y socios de la coalición. Dicha integración recalca la necesidad de contar con un método C2 adaptativo para las operaciones espaciales basado en la acción unificada que conduce a la unidad de esfuerzo.[3] Para guiar a un comandante en el desarrollo de una estructura C2 adaptativa se necesitan dos elementos claves: un entendimiento claro del estado final o meta general y una identificación de las variantes claves que pudiesen influenciar el diseño final. Ambos elementos fueron identificados durante un estudio exhaustivo sobre C2 fomentado por el Jefe de Estado Mayor de la Fuerza Aérea. Este estudio sobre C2 fue organizado y llevado a cabo por el Instituto de Investigaciones de la Fuerza Aérea (AFRI, por sus siglas en inglés) en la Base Aérea Maxwell, Alabama.[4] Si bien la finalidad de este artículo es enfocarse en las operaciones ciberespaciales, el estudio del AFRI concluyó que las pautas C2 que aquí se presentan también pueden aplicarse a todas las formas de las capacidades militares.

Meta del mando y control adaptativo para las operaciones ciberespaciales

Los investigadores que llevaron a cabo el estudio C2 analizaron recientes operaciones militares y humanitarias de EE.UU. que son similares en naturaleza al entorno operacional esperado durante los próximos 25 años.[5] En el análisis se identificaron los siguientes rasgos comunes necesarios para el desarrollo del C2 adaptativo para las operaciones ciberespaciales: enfocarse en la unidad de esfuerzo al igual que en la unidad de mando, integración de las funciones de mando y control al nivel más bajo apropiado, la necesidad de crear agilidad y la necesidad de realzar la velocidad de acción. Combinados, estos rasgos proveen una descripción precisa del estado final general o la meta principal del diseño de C2 adaptativo ciberespacial. La meta principal es la creación de la unidad de esfuerzo mediante la integración al nivel de organización apropiado más bajo, logrando la agilidad y velocidad de acción en proveer los efectos deseados.[6]

La unidad de esfuerzo recalca la coordinación y cooperación hacia objetivos comunes por participantes que no necesariamente forman parte del mismo comando u organización. Para la mayoría de las misiones a lo largo de la gama de las operaciones militares, un comandante necesitará integrar las capacidades ciberespaciales que radican con otros servicios militares, interinstitucionales, multinacionales y gubernamentales, al igual que con socios no gubernamentales. Algunos individuos opinan que esa interdependencia es riesgosa porque el éxito depende de las

capacidades que un comandante puede que no controle directamente. Sin embargo, las capacidades necesarias para apoyar misiones a lo largo de la gama de las operaciones militares y el tamaño y estructura probables de la fuerza ciberespacial hacen que esta situación sea una realidad. Los comandantes no necesitan "ser dueños de o controlar" los recursos de los socios para garantizar el acceso a sus capacidades. Las estructuras C2 adaptativas ciberespaciales deben crear sinergia mediante la colaboración horizontal basada en la confianza mutua entre todos los socios de combate en lugar de sencillamente recalcar la característica tradicional de interacción vertical de la jerarquía militar. La falta de confianza entre los socios da lugar al deseo de "ser dueño" de todos los recursos necesarios para una operación; esto tiene como consecuencia el control excesivo y evita la sinergia. Un diseño C2 para las operaciones ciberespaciales que se concentra en la unidad de esfuerzo permitirá una mentalidad de un equipo, una contienda y aumentará el acceso eficaz a una variedad más amplia de capacidades.[7]

Otro aspecto clave de la meta general del C2 ciberespacial implica maximizar la agilidad y velocidad de acción que un comandante necesita para decidir y actuar más rápido que un adversario. Descentralizar el C2 de las operaciones ciberespaciales al nivel apropiado más bajo capaz de integrar recursos es la mejor manera de aumentar la aptitud de un comandante de actuar con rapidez. Las estructuras C2 demasiado centralizadas incorrectamente puede que pierdan agilidad y menoscaben la iniciativa, resultando en el fracaso de la misión. Las pautas, intención y prioridades claras de un comandante, al igual que el riesgo aceptable y la autoridad apropiada para el nivel de responsabilidad deben acompañar el proceso de descentralización. Además, las relaciones de mando que permiten la colaboración horizontal eficaz entre los socios pueden realzar tanto la agilidad como la velocidad de acción.[8]

El reto más grande en lograr la meta del C2 adaptativo para las operaciones ciberespaciales es determinar el nivel de organización apropiado más bajo para integrar recursos. En otras palabras, ¿cuál es el equilibrio de centralización correcto versus descentralización dentro del diseño C2 necesario para lograr la unidad de esfuerzo, agilidad y velocidad de acción? El diseño actual para lograr la meta de C2 ciberespacial adaptativo variará de situación en situación. El diseño C2 más eficaz es aquel que se puede ajustar a las realidades operacionales. Un comandante debe comprender qué ocasiona esas variaciones o qué incide en los elementos fundamentales de C2.

Variables que impactan el diseño de mando y control de las operaciones ciberespaciales

David Alberts y Richard Hayes (*Power to the Edge: Command and Control in the Information Age* [Poder a la organización: Mando y control en la era de la información]*)* describen tres elementos fundamentales a tomar en cuenta al diseñar cualquier estructura C2.[9] Los elementos fundamentales son la asignación de decisiones, intercambio de información y patrones de interacción. La asignación de los derechos de decisión tiene que ver con otorgarles a individuos designados la autoridad y responsabilidad de tomar decisiones entre opciones posibles, empleando relaciones de mando para definir claramente la autoridad de decisión y responsabilidad de un comandante. Los patrones de interacción especifican quién debe interactuar (por ejemplo, comandantes, plana mayor y empleados), cómo interactúan (por ejemplo, cara a cara o por medio de vídeo teleconferencias) y qué tipos de transacciones (por ejemplo, decisión, asesoramiento y conocimiento de la situación) ocurren durante la interacción. El intercambio de información consiste en los diferentes medios y maneras de compartir información para informar a todos los socios involucrados en una operación. Esto incluye compartir información a otros servicios, servicios conjuntos, coalición, otros gobiernos y agencias no gubernamentales.

Alberts y Hayes continúan exponiendo que en un mundo perfecto la manera más eficaz de realizar la unidad de esfuerzo y velocidad de acción durante una operación, logrando por ende la meta principal del C2 adaptativo para las operaciones ciberespaciales, implica decisiones descentralizadas, intercambio de información y exhortar la interacción al nivel de organización más

bajo.[10] Sin embargo, en realidad ciertas variables—algunas *comunes* y otras *singulares* a las aptitudes ciberespaciales—limitan la descentralización completa de estos tres elementos fundamentales de mando y control.

Aunque variables innumerables pueden influenciar el diseño C2, las *variables comunes* claves identificadas a lo largo de los ejemplos operacionales analizados en el estudio del AFRI incluyen la naturaleza de una operación, los recursos disponibles, capacidades de las unidades subordinadas, grado de confianza y riesgo político.[11] Además de las *variables comunes,* las *aptitudes singulares* de los recursos ciberespaciales, velocidad, alcance, flexibilidad y versatilidad, también inciden en el diseño C2.

El nivel de impacto de todas estas variables será diferente según la situación. La tensión constante existe entre los comandantes de las fuerzas militares conjuntas durante el proceso de determinar el grado para controlar centralmente las capacidades ciberespaciales. Por lo tanto, al diseñar un método C2, un comandante debe evaluar cómo estos elementos influirán una operación. Convertir las variables *comunes* y *capacidades singulares* en una serie de preguntas y emplear las descripciones que se dan a continuación para ayudar a responder las preguntas, ofrecen una manera práctica de ayudar a los comandantes en el "arte" de diseñar C2 adaptativo para las operaciones ciberespaciales.

¿Cuál es la naturaleza de la operación? Operaciones diferentes conducen a equilibrios diferentes de centralización entre los tres elementos fundamentales. Por ejemplo, las operaciones globales tales como un ataque ciberespacial estratégico, por lo general requieren un grado elevado de centralización para poder dirigir la secuencia de la operación y hacer ajustes durante la ejecución. En cambio, las operaciones ciberespaciales que apoyan las fuerzas terrestres en una contienda terrestre distribuida son más eficaces cuando se llevan a cabo con un grado elevado de descentralización, en vista del deseo de retener la respuesta táctica. Otras operaciones, tales como la defensa de la red de computadoras, se benefician de una mezcla de centralización y descentralización. La centralización permite la dirección de prioridades en general mientras que la descentralización permite un ritmo de operaciones más rápido durante la ejecución.[12]

¿Cuál es la capacidad de los recursos disponibles versus el requerimiento? La oferta y demanda sencilla son factores determinantes significativos al identificar el grado de centralización correcto entre los elementos fundamentales del C2 ciberespacial. Si suficientes recursos ciberespaciales, inclusive equipo y personal, están disponibles para entregar el efecto deseado, entonces uno puede descentralizar en gran medida el mando y control de esos recursos. No obstante, recursos escasos ameritan un método de mando y control más centralizado para poder llevar a cabo los procesos empleados para determinar la priorización y asignación contra los requerimientos en competencia.[13]

Las prioridades preestablecidas de los recursos con una oferta limitada pero demanda elevada, que se llevan a cabo en una manera centralizada, permitirán que los encargados de tomar decisiones descentralizadas ajusten rápidamente los recursos a las realidades de la ejecución. La priorización eficaz les permite a los comandantes aprovecharse de la velocidad, alcance, flexibilidad y versatilidad singulares de las capacidades ciberespaciales. Por ejemplo, si un evento crea la necesidad de un cambio al nivel táctico durante la ejecución de la misión, los nódulos de control de niveles inferiores no necesitan esperar aprobación de niveles más elevados para alterar el plan de comunicaciones ciberespaciales o entregar recursos ciberespaciales limitados a otras organizaciones. La priorización eficaz y comunicada claramente de las capacidades apoya la descentralización de la integración mejorando la velocidad de acción.

¿Cuáles son las capacidades de las unidades subordinadas? Puede que otras variables permitan mayor descentralización de la autoridad de decisión, intercambio de información e interacción pero puede que las capacidades de la unidad no permitan esta forma de mando y control. Para desempeñar exitosamente la función de mando y control, las unidades deben estar organizadas, entrenadas y equipadas correctamente—un proceso que exige direcciones claras con res-

pecto a los tipos de autoridad de decisión de una unidad y esto exige la elaboración correcta de la infraestructura de las comunicaciones que da lugar a la interacción e intercambio de información eficaz.

¿Cuál es el grado de confianza entre los socios? ¿Se puede cambiar? En general, mientras mayor sea la confianza entre los comandantes, subordinados y socios, es más probable la descentralización de los elementos fundamentales de mando y control ciberespacial. La presencia de la confianza con respecto a la aptitud y acciones de los demás fomenta mayor disponibilidad para otorgar autoridad de decisión e intercambiar información con otros. La confianza se puede desarrollar a través de la interacción, por medio de la cual los socios deben planificar para alcanzar esa virtud y reforzarla continuamente. Al diseñar un método C2 para las operaciones ciberespaciales, uno debe entender que la confianza comienza con experiencias compartidas e interacción cara a cara. En virtud de la naturaleza perecedera de la confianza, esas cualidades se establecen mejor en persona, no virtualmente, y debe esforzarse por proteger esa confianza, la cual es difícil recuperar una vez que se pierde.

¿Cuál es el riesgo político? En general, la arquitectura C2 debe permitirles a los comandantes de la línea del frente a tomar decisiones rápidas en el lugar, especialmente durante la ejecución de operaciones complejas y que se desarrollan rápidamente. Sin embargo, a medida que los comandantes y las planas mayores crean planes para las operaciones, las consideraciones políticas puede que dicten un método C2 más centralizado. Por ejemplo, puede que inquietudes políticas significativas surjan a causa de la posibilidad de daños colaterales, o la creación de un efecto a nivel estratégico con armamento ciberespacial probablemente dictaría un enfoque centralizado. Resulta indispensable mantener al mínimo esas ocasiones. La tecnología de información moderna podría persuadir a los comandantes a mandar y controlar las operaciones centralmente inclusive cuando esas operaciones no ameritan dicho control. A pesar de las grandes mejoras en la tecnología, una sola persona no puede lograr un conocimiento completo de la situación durante operaciones con compromisos múltiples y simultáneos a lo largo de una zona de operaciones grande. Los comandantes superiores deben balancear la ejecución de la campaña en general frente a la necesidad de flexibilidad táctica. El equilibrio correcto de la centralización y descentralización con respecto a la autoridad de decisión, intercambio de información e interacción debe hacer posible la capacidad de un subordinado para apoyar la intención del comandante y cumplir con los objetivos de la campaña.[14]

¿A cuál escalafón de la organización deben radicar las autoridades y dónde debe llevarse a cabo la planificación y ejecución para aprovecharse de la velocidad, alcance, flexibilidad y versatilidad de las capacidades ciberespaciales? Las *capacidades singulares* del ciberespacio exigen una consideración especial para el diseño de C2. El aprovechamiento de las *capacidades singulares:* velocidad, alcance, flexibilidad y versatilidad conducen a un método más centralizado para la toma de decisiones, intercambio de información e interacción.[15] Coordinar e integrar operaciones globales, en el teatro y en teatros secundarios; administrar recursos escasos frente a una demanda elevada; llevar a cabo reasignación de tareas de la misión en tiempo real y crear simultáneamente efectos a nivel de estratégico a táctico hacen que el método centralizado sea deseable. Un método de mando y control centralizado le permite a un comandante responder a los cambios en el entorno operacional y aprovecharse de oportunidades fugaces. El reto para un comandante es equilibrar el deseo de centralizar una estructura C2 para aprovecharse de las *capacidades singulares* del ciberespacio con las otras variables de diseño C2. El equilibrio correcto creará unidad de esfuerzo mediante la integración al nivel de organización correcto más bajo, logrando así la agilidad y la velocidad de acción en entregar los efectos deseados.

Conclusión

Un comandante debe diseñar una estructura C2 optimizada para dirigir, planificar y emplear capacidades ciberespaciales para apoyar operaciones que logran los objetivos en general de un comandante de fuerza conjunta, todo en apoyo a los intereses de seguridad nacional. Con el fin de poder operar eficazmente en el entorno operacional emergente, las operaciones militares modernas se tornarán cada vez más conjuntas, de coalición, distribuidas, complejas, intensas y globales. Esas condiciones exigen C2 adaptativo de las capacidades ciberespaciales con la autoridad de decisión al nivel de mando más apropiado. Crear agilidad para aprovecharse de las oportunidades en este entorno dinámico exige la descentralización de decisiones, intercambio de información e interacción entre comandantes y planas mayores al nivel de organización apropiado más bajo capaz de integrar recursos. Entender las influencias en el diseño C2 ocasionadas por *variables comunes* y balancearlas con el deseo de aprovechar las *capacidades singulares* del ciberespacio ayudará a los comandantes a determinar el nivel de organización apropiado más bajo para promocionar la autoridad de decisión, intercambio de información e interacción. A veces el nivel más bajo está al nivel de mando nacional. En otras ocasiones, las operaciones eficaces necesitan la presencia de comandantes que tienen autoridad para tomar decisiones, poseen la información requerida e interactúan a niveles de la organización por debajo del comandante más antiguo—individuos que pueden ofrecer un grado de control, unidad de mando y flexibilidad táctica óptima. Esas operaciones también ameritan distribuir planificadores y elementos de control a los escalafones correctos de los socios y otorgarles acceso a información y la autoridad para tomar decisiones. Enfocarse en la meta fundamental de C2 adaptativo y entender, con base en la operación específica, la influencia de las *capacidades ciberespaciales singulares y comunes* conducirá al C2 eficaz de las capacidades ciberespaciales mediante el control flexible, con autoridad de decisión, intercambio de información y patrones de interacción centralizada al escalafón de mando apropiado. ❑

Notas

1. Para fines de este escrito, la *United States Joint Military Doctrine* (Doctrina Militar Conjunta de EE.UU.) se emplea para definir los términos *Operaciones Ciberespaciales* y *Mando y Control*. El término *operaciones ciberespaciales* se define como "el empleo de capacidades ciberespaciales en las que la finalidad principal es lograr objetivos e o a través del ciberespacio. El término *mando y control* se define como "el ejercicio de autoridad y dirección de un comandante correctamente designado sobre fuerzas asignadas y adscritas en el logro de la misión. Las funciones de mando y control se llevan a cabo mediante un arreglo de personal, equipo, comunicaciones, instalaciones y procedimientos empleados por un comandante al planificar, dirigir, coordinar y controlar fuerzas y operaciones en el logro de la misión". Joint Publication (JP) (Publicación Conjunta) 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Diccionario de Términos Militares y Afines del Departamento de Defensa), 8 de noviembre de 2010 (según enmendado al 15 de julio de 2012), 56, 80, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

2. El siguiente documento capta los puntos principales de otros documentos en los que se discute el entorno de operaciones militares futuras. Si bien este documento está redactado desde el punto de vista de Estados Unidos, en él se describen operaciones que la mayoría de los países podrían enfrentar. *United States Joint Forces Command* (Comando de Fuerzas Conjuntas de EE.UU.), *The Joint Operating Environment, 2010* (El entorno de operaciones conjuntas 2010) (Suffolk, VA: *Joint Futures Group [J59], United States Joint Forces Command*, 18 de febrero de 2010), 4, http://www.jfcom.mil/newslink/storyarchive/2010/JOE_2010_o.pdf.

3. El término *unidad de esfuerzo* se define como la "coordinación y cooperación hacia objetivos comunes, inclusive si los participantes no necesariamente forman parte del mismo comando u organización—el resultado de acciones unificadas exitosas". El término *acción unificada* se define como "la sincronización, coordinación o integración de las actividades de entidades gubernamentales y no gubernamentales con operaciones militares para lograr la unidad de esfuerzo". Joint Publication (JP) (Publicación Conjunta) 1, *Doctrine for the Armed Forces of the United States* (Doctrina de las Fuerzas Armadas de Estados Unidos, 2 de mayo de 2007, incorporando el cambio 1, 20 de marzo de 2009, GL-11.

4. *Research Paper 2012-5* (Documento de Investigación 2012-5), *Air Force Command and Control: The need for Increased Adaptability* (Mando y Control de la Fuerza Aérea: La necesidad de contar con mayor adaptabilidad), Air Force Research Institute, Air University Press, Maxwell AFB, Alabama, julio de 2012.

5. Las operaciones analizadas fueron Operación Fuerza Aliada, la fase de combate más importante de la Operación Libertad para Irak, la fase de combate más importante de la Operación Libertad Duradera, la fase de guerra irregular de

la Operación Libertad para Irak, la fase de guerra irregular de la Operación Libertad Duradera, y las operaciones de ayuda humanitaria después del Huracán Katrina.

6. Una variedad de documentos de lecciones aprendidas recalca esta idea, inclusive *United States Joint Forces Command* (Comando de Fuerzas Conjuntas de Estados Unidos), *Joint Operations: Insights and Best Practices* (Operaciones Conjuntas: Discernimientos y Mejores Prácticas), 3rd ed. (Suffolk, VA: Joint Training Division, Joint Warfighting Center, United States Joint Forces Command, 12 de enero de 2011), 6, https://jko.harmonieweb.org/coi/JointTrainingDivision/Documents/Insights_3rd_edition_Jan_12_2011.pdf.

7. Unites States Joint Forces Command, *Joint Operations: Insights and Best Practices* 6, 24.

8. Ibid., 6, 20.

9. David S. Alberts y Richard E. Hayes, *Power to the Edge: Command and Control in the Information Age* (Washington, DC: Command and Control Research Program, 2003), 75.

10. Alberts and Hayes, *Power to the Edge: Command and Control in the Information Age.*

11. Las influencias comunes fueron creadas de un análisis de la Operación Fuerza Aliada, la fase de combate más importante de la Operación Libertad para Irak, la fase de combate más importante de la Operación Libertad Duradera, la fase de guerra irregular de la Operación Libertad para Irak, la fase de guerra irregular de la Operación Paz Duradera, las operaciones de ayuda humanitaria después del Huracán Katrina y operaciones espaciales al igual que de otras fuentes, incluyendo el escrito del Tte Cnel Clint Hinote, *Centralized Control and Decentralized Execution: A Catchphrase in Crisis?* (Control Centralizado y Ejecución Descentraliza: ¿Una frase de moda en crisis?, Documento de Investigación 2009-1 (Maxwell AFB, AL: Air Force Research Institute, March 2009), 59–64, http://aupress.au.af.mil/digital/pdf/paper/Hinote_centralized_control_and_decentralized_execution.pdf; AFDD 1, *Air Force Basic Doctrine, Organization, and Command* 14de octubre de 2011, capítulos 2–5, http://www.e-publishing.af.mil/shared/media/epubs/AFDD1.pdf; and United States Joint Forces Command, *Joint Operations*, 17.

12. Hinote, *Centralized Control and Decentralized Execution*, 59–60.

13. Ibid., 61.

14. AFDD 1, Air Force Basic Doctrine, Organization, and Command 14 de octubre de 2011, capítulos 2–5, http://www.e-publishing.af.mil/shared/media/epubs/AFDD1.pdf, 39.

15. Para una descripción detalla de cada una de estas características singulares, ver, Ibid, capítulos 4 y 5 y AFDD 2, Operations and Organization (Operaciones y Organización), 3 de abril de 2007, capítulos 1 y 2, http://www.e-publishing.af.mil/shared/media/epubs/AFDD2.pdf.

El Teniente Coronel Jeffrey Hukill, USAF-Ret (Licenciatura, Norwich University; Maestría, Gonzaga University; MMIS, Auburn University) pasó a formar parte del Instituto de Investigaciones de la Fuerza Aérea (AFRI, por sus siglas en inglés) el 8 de marzo de 2008 y se ha desempeñado en calidad de jefe de la División de Investigaciones y como profesor de investigaciones de seguridad nacional. Entre sus intereses de investigación principales se encuentran el mando y control de fuerzas conjuntas, integración de las operaciones aire/tierra, presentación de la fuerza, y método basado en efectos a las operaciones. Antes de unirse al AFRI, se desempeñó como analista superior de defensa militar en el Curtis E. LeMay Center for Doctrine Development and Education, enseñando y escribiendo sobre una variedad de temas relacionadas con el poder aéreo y espacial, tales como el proceso de fuerzas expedicionarias aéreas y espaciales, estrategias anti acceso, y relaciones de mando conjunto y de la Fuerza Aérea. Durante su carrera de 22 años en la Fuerza Aérea desempeñó puestos operacionales, de mando y educativos, inclusive asignaciones como comandante de instalación, presidente del Departamento de Estudios de Poder Aeroespacial y Teoría de Guerra al igual que decano de Aprendizaje a Distancia en la Escuela Superior de Comando y Estado Mayor, y oficial de guerra electrónica en el B-52G. Fue líder de grupo y coautor de un estudio encomendado por el Jefe de Estado Mayor de la Fuerza Aérea titulado "*U.S. Air Force Command and Control: The Need for Increased Adaptability*" (Mando y Control de la Fuerza Aérea de EE.UU: La necesidad de contar con mayor adaptabilidad), y coautor del artículo "*Developing Flexible Command and Control of Airpower*" (Creando Mando y Control Flexible del Poderío Aéreo) (Air and Space Power Journal, 2º trimester 2011). Además, el Tte Cnel Hukill ha contribuido en una variedad de revistas tales como *Armed Forces Journal*, *Defense Analysis*, *Joint Force Quarterly*, y el *Air and Space Power Journal* (Ediciones en Inglés, Español, Chino y Portugués).

CURSO DE CONTROL DE CORROSIÓN DE LA IAAFA

Dentro de los muchos cursos enseñados en la IAAFA, el curso de Control de Corrosión es bastante popular. Está diseñado para menos de diez alumnos, dura aproximadamente ocho semanas e incluye 180 horas de clase. Los instructores son especialistas en Estructuras Aeroespaciales y Control de Corrosión. Poseen una amplia gama de experiencia y conocimiento en aeronaves y equipos de apoyo para todo tipo de funciones. Enfocan el aprendizaje en los tipos de corrosión, características geográficas, fundamentos de un programa efectivo de control de corrosión, detección, inspección, reparación, y equipos.

El curso cuenta con equipos de punta en tecnología para enriquecer el aprendizaje en la clase. A su disposición cuentan con un laboratorio con sistema circulatorio de filtración de aire, sistema contenido de horneado para revestimientos orgánicos, pistolas de pintura de alto volumen y baja presión (HVLP), y sistemas de respiración de aire forzado. Además, cuentan con el único sistema virtual de pintura disponible. Este simulador móvil se puede usar en cualquier sitio de entrenamiento y trae un suministro ilimitado de pintura "virtual" que ahorra dinero y ofrece lo máximo en un ambiente de adiestramiento. Con esta cantidad ilimitada de pintura virtual, los instructores enfatizan la técnica correcta de pintado, reiteran la importancia del uso eficaz a fin de reducir gastos de pintura, y hacen hincapié en evitar corrosión en las aeronaves y todo su equipo relacionado. El laboratorio y el simulador permiten que los instructores combinen al máximo su experiencia a través de tecnología del siglo 21 para darles a los estudiantes una educación de la más alta calidad en la aplicación de revestimientos orgánicos.

El propósito de este curso es mejorar el conocimiento del estudiante haciéndole consciente de la gran importancia de un programa eficiente de control de corrosión. La meta del curso es aumentar las prácticas estudiantiles con las técnicas, herramientas y equipo actuales de la USAF o en residencia o a través de un equipo móvil preparado para las necesidades específicas de la unidad o misión del país amigo. Para solicitar cursos en IAAFA, favor de contactar al representante del Grupo Militar en su país quien coordinara con su respectivo Gerente de País por medio de la Unidad de Adiestramiento de Seguridad de la Fuerza Aérea (AFSAT). Para más información sobre los cursos de IAAFA, favor de contactar al Señor Gregorio Delgado, Director, de la Escuadrilla de asuntos estudiantiles, 210-671-4802 (gregorio.delgado@us.af.mil) o el Señor Ralph Sánchez, Oficina del registro de la IAAFA, 210-671-5593 (ralph.sanchez.1@us.af.mil). También, nos puede visitar en http://www.37trw.af.mil/units/interamericanairforcesacademy(iaafa)/index.asp o búsquenos en facebook bajo La Academia-Interamericana de las Fuerzas Aéreas.

En la foto, el estudiante se prepara para aplicar la base con el fin de asegurarse de que la capa se adhiera a la superficie correctamente. Durante el Curso de Control de Corrosión, los estudiantes pasan por cada paso del proceso de revestimientos orgánicos simulando trabajo hecho en estructuras de aeronaves (Foto cortesía del 318avo escuadrón de entrenamiento).

ASPI

EDICION EN ESPAÑOL
DE LA REVISTA PROFESIONAL
DE LA FUERZA AEREA DE
LOS ESTADOS UNIDOS

UNITED STATES CYBER COMMAND

AU PRESS
http://aupress.au.af.mil

AIR UNIVERSITY