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.