

Sin Lugar Para Esconderse

La Creciente Amenaza Para Las Bases Aéreas

CORONEL SHANNON W. CAUDILL, USAF

MAYOR BENJAMÍN R. JACOBSON, USAF

VISTIENDO UNIFORMES del ejército estadounidense, los atacantes atravesaron las defensas de la base aérea ocultos por la oscuridad de la noche. Armados de rifles, lanzagranadas propulsadas por cohete, y chalecos suicidas, el grupo de 14 hombres inició su misión mortal contra una base aérea en la Provincia de Helmand, Afganistán, una base con personal de la Fuerza Internacional de Asistencia de Seguridad (ISAF) de la Organización del Tratado del Atlántico Norte (OTAN). El combate duró varias horas, y el amanecer reveló la destrucción de seis aviones a reacción AV-8B Harrier y daños a otras dos aeronaves; además, “sufrieron daños seis hangares”, y “quedaron destruidas seis estaciones de reabastecimiento de combustible”.¹ En el ataque, murieron 14 insurgentes y dos infantes de marina estadounidenses mientras que ocho miembros militares y un contratista de la coalición fueron heridos. En septiembre de 2012, esta operación insurgente constituyó el ataque terrestre más exitoso hasta la fecha contra activos aéreos de la ISAF de la OTAN en el conflicto de Afganistán.

El General italiano Giulio Douhet dijo una vez que “es más fácil y más efectivo destruir el poderío aéreo del enemigo atacando sus nidos y huevos en el suelo que cazar sus aves voladoras en el aire”.² La observación de Douhet es aún válida, como se demostró con el ataque antes mencionado contra la base aérea Helmand. De hecho, las bases aéreas deficientemente defendidas seguirán siendo susceptibles a los asaltos por tierra. Con anterioridad, a arremetida más exitosa contra una base aérea después de la guerra de Vietnam había ocurrido durante la guerra civil en El Salvador en 1982, donde unos 100 rebeldes atacaron una base de la Fuerza Aérea Salvadoreña, destruyendo cinco aeronaves Ouragan, seis UH-1B y tres C-47 a la vez que dañaron otras cinco plataformas. Evidentemente, esta “operación bien planeada y ejecutada . . . demostró la superioridad táctica” de los insurgentes contra la fuerza gubernamental de defensa de la base.³

En el futuro, la complejidad y el costo de proteger bases aéreas y los activos del aire y el espacio crecerán exponencialmente debido a las nuevas tecnologías, la abundancia de información de dominio público, y el desarrollo de la capacidad del adversario. Las amenazas tradicionales como asaltos aerotransportados, fuego indirecto (IDF) mediante cohetes y morteros, y ataques directos con escuadrones suicidas continuarán siendo las opciones básicas de la acción enemiga. En consecuencia, debemos examinar las amenazas emergentes que hacen posible nuevos modos de ataque a bases aéreas, incluyendo el desarrollo de municiones de precisión, la propagación de vehículos a control remoto (RPV), la proliferación de misiles superficie-aire (SAM) disparados desde el hombro que son una creciente amenaza interna, y otras variantes de una nueva bonanza tecnológica para terroristas e insurgentes. La defensa de los activos aéreos se volverá aún más problemática frente a un espectro de amenazas habilitadas por la tecnología y una aceleración de la amenaza interna. Este desarrollo y proliferación de tecnologías permitirá que los grupos pequeños logren una ventaja aún mayor contra los defensores de bases y operadores aéreos.

Evidentemente, los Aerotécnicos deben considerar seriamente la alta probabilidad de estas amenazas emergentes y los costos asociados de garantizar las operaciones continuas. Anteriormente, un hombre y un rifle cubrían una brecha en un sector de defensa de la base. Las bases aéreas bien defendidas obligan al enemigo a explorar medios alternativos de afectar las operaciones aéreas. Naturalmente, cualquier actor racional quiere lograr el camino al éxito más rá-

pido y de menor costo después de seleccionar el objetivo. Si no está buscando un ataque espectacular diseñado para producir bajas e imágenes dramáticas de televisión (como fomentan los grupos tipo al-Qaeda), posiblemente deseará impedir la continuidad de las operaciones aéreas y desgastar a la base mediante un acoso que produzca víctimas en transcurso del tiempo.

Sin embargo, al examinar la amenaza, debemos preguntarnos constantemente qué es lo que el enemigo decidirá atacar, ya que no será necesariamente aeronaves en tierra. Los blancos y objetivos dependen de los atacantes, quienes pueden ser desde grupos terroristas hasta fuerzas convencionales y operaciones especiales, y de los objetivos políticos y la capacidad real que puedan utilizar contra la base aérea. En Vietnam, las fuerzas enemigas se dieron cuenta que los ataques terrestres contra los aeródromos representaban un drenaje de sus recursos. En consecuencia, se adaptaron a perturbar las operaciones aéreas en lugar de atacar directamente a los aeródromos, porque “si que las incursiones dañaban aeronaves, instalaciones o pistas de aterrizaje, el resultado era una disminución de las tasas de vuelo. Las armas de ataque a distancia [IDF en el léxico actual], así como otras formas de explosivos detonados por mando, pronto se convirtieron en las armas preferidas entre los muchos beligerantes involucrados en conflictos desde la década de 1960”.⁴

La amenaza del terrorismo ha dado lugar a que la mayoría de operaciones de defensa de la base se centren en derrotar a los dispositivos explosivos improvisados que se transportan en vehículos (VBIED). Los grupos terroristas principales siempre han querido realizar ataques espectaculares que causen muchas imágenes visuales, impacto traumático y alto número de muertos. Las imágenes del cuartel de la Infantería de Marina en Beirut, Líbano, o de las Torres Khobar de la Fuerza Aérea en Khobar, Arabia Saudita, se convirtieron en el resultado deseado de los ataques del adversario. Se ve la misma intención en la detonación de un camión explosivo del Talibán en el décimo aniversario de los ataques terroristas del 11 de septiembre de 2001, un ataque que hirió a 89 personas, incluyendo 77 soldados.⁵ Este artículo examina algunas de las amenazas más alarmantes—como los VBIED, que creemos que el enemigo usará en ataques futuros—y la tecnología emergente que podría permitirle atacar nuestras bases aéreas.

La creciente precisión del fuego indirecto

El IDF se ha convertido en la opción preferida entre los insurgentes para ataques a bases aéreas. Activado a distancia y con frecuencia manipulado para que se active después que el atacante se ha alejado, ofrece cierto grado de supervivencia. En Vietnam, las fuerzas norvietnamitas y del Vietcong atacaron las bases aéreas estadounidenses en 475 ocasiones entre 1964 y 1973, usando principalmente el IDF, destruyendo 99 aeronaves estadounidenses y survietnamitas, y dañando 1.170.⁶ En Irak, los insurgentes usaron el IDF para acosar a las bases aéreas, pero no fue eficaz debido al deficiente adiestramiento del enemigo y las defensas de base externas activas. En Afganistán el enemigo empleó el IDF no solo para acosar a las fuerzas de la coalición sino también para enmascarar y cubrir ataques de tierra. El 22 de agosto de 2012, las fuerzas enemigas se las arreglaron incluso para dañar el avión visitante del Presidente del Estado Mayor Conjunto.⁷

La efectividad de los morteros y cohetes, apuntados a una base por alguien que tiene información limitada del blanco, depende de la pericia técnica del operador—un factor que dificulta su eficacia total. Sin embargo, ha llegado una nueva era en sistemas de armas IDF de precisión. El 31 de marzo de 2011, los soldados de la Cuarta Brigada de Combate dispararon un proyectil de mortero con guía de precisión de 120 mm desde la Base de Operaciones de Avanzada de Kushamond, en Afganistán, impactando a unos cuatro metros del blanco.⁸ Normalmente un mortero dispara un proyectil “tonto”—que no tiene un sistema de guía integrado. Con el tiempo es probable que esta tecnología la adquieran los grupos insurgentes y terroristas, mejorando su capaci-

dad de elegir blancos con extraordinaria precisión y aumentando la vulnerabilidad de las aeronaves y las instalaciones importantes.

Para derrotar a este tipo de sistema de armas es necesaria una defensa tecnológica verdaderamente integrada. Tanto Estados Unidos como Israel han sido pioneros en sistemas defensivos diseñados para contrarrestar la creciente precisión de las armas IDF. En Irak, la Base Conjunta Balad y otras bases usaron un sistema de Mortero Anticohete manejado por personal conjunto para defenderse contra el IDF enemigo. En el futuro, el sector de defensa tendrá que asegurar un sistema de defensa completo porque los disparos de precisión harán que el ataque a una base sea más simple y las fuerzas defensoras tengan menos margen de error. Además, la capacidad de esta tecnología de defensa está mejorando. Por ejemplo, durante el conflicto israelí de noviembre de 2012 con Hamas en Gaza, los militantes lanzaron más de 1.500 cohetes contra Israel, pero la Cúpula de Acero (Iron Dome) de ese país, un “sistema anticohetes portátil desarrollado para derribar misiles de corto alcance”, interceptó unos 400 de ellos.⁹ Este sistema puede ofrecer un modelo de sistema de defensa portátil para operaciones aéreas. Si los disparos de IDF de precisión pasan a ser parte del entorno operativo, nuestros Aerotécnicos no tendrán el lujo de un enemigo incompetente que dispare proyectiles tontos.

Vehículos a control remoto

El personal que contemple la defensa de una base aérea debe considerar la amenaza que representan los vehículos a control remoto (RPV) mediante la formulación de un plan para enfrentar una gama de amenazas remotas, desde tierra y aerotransportadas. ¿Quién tiene autoridad para utilizar tales vehículos y con qué armas? Para vehículos basados en tierra, la respuesta está más claramente definida y concuerda con las contingencias establecidas para los VBIED; sin embargo, puede existir una brecha defensiva en la defensa contra las amenazas aerotransportadas. El hecho de que aún se tenga que explorar totalmente los protocolos para estas defensas deja una brecha que un enemigo con conocimientos tecnológicos podría explotar. Debemos desarrollar sistemas de modelado, simulación y defensa para tomar en cuenta las nuevas amenazas antes de que un grupo de protesta interrumpa las operaciones de vuelo o—peor aún—antes de que una organización terrorista utilice los RPV para reconocimiento o ataques contra nuestros activos aéreos.

El uso de estos vehículos (RPV, robots, vehículos teledirigidos, etc.) ya no se restringe al uso militar exclusivo. Después de todo, los civiles han volado aeroplanos a control remoto desde la década de 1930. Sin embargo, en la actualidad la sofisticación, el alcance y su capacidad de video permiten que los civiles accedan a tecnología que antes estaba reservada solo para organizaciones militares y de inteligencia. Pongamos el caso de un grupo de protesta denominado SHARK (Showing Animals Respect and Kindness) que propugna respeto y compasión por los animales. Este grupo planeó usar un Mikrokopter (vehículo teledirigido) para grabar un video de cómo se cazaban palomas vivas como medio de disuadir e interferir con una excursión de caza legal. El 21 de febrero de 2012, el grupo SHARK se instaló en Broxton Bridge Plantation cerca de Ehrhardt, Carolina del Sur. Agentes de la policía y un abogado local trataron de impedir que el grupo de protesta vuela su Mikrokopter, pero lo hicieron de todas maneras, solo para que lo derriben los cazadores en la escena.¹⁰

Esta misma tecnología es capaz de llevar armas o realizar reconocimiento para grupos que intenten atacar un aeródromo—de hecho, ya se ha hecho. Por ejemplo, aunque en años recientes los legisladores estadounidenses se han preocupado más por al-Qaeda, Hezbollah ha demostrado tener alcance global y capacidad de aguante. Es reconocido como el primer grupo terrorista en usar terroristas suicidas como arma de destrucción masiva, dirigiendo vehículos explosivos grandes a blancos estratégicos.¹¹ Hezbollah ha mostrado recientemente su destreza

tecnológica utilizando RPV con cargas explosivas y tecnología de misiles, logrando incluso incapacitar un barco de guerra israelí.¹² El éxito de la organización viene del respaldo financiero y logístico que recibe de Siria e Irán, éste último le suministra armas avanzadas y equipo de reconocimiento.

A partir de noviembre de 2004, Hezbollah asombró a los israelíes lanzando un avión de vigilancia a control remoto, el Misrad 1, que voló sobre poblados israelíes y volvió intacto a Líbano. En una manifestación de Hezbollah, el líder de la organización, Hassan Nasrallah, declaró, “Ustedes pueden cargar el avión Misrad con 40 ó 50 kilos de explosivos y enviarlo a su objetivo. . . . ¿Quieren una planta eléctrica, una planta de agua, una base militar? ¡Lo que sea!”¹³ Sin duda, con el tiempo, esta tecnología se difundirá a otros grupos terroristas y de protesta.

Para resaltar este punto, examinemos el caso de Rezwán Ferdaus, un ciudadano estadounidense de 26 años de edad. Fue arrestado el 28 de septiembre de 2011, acusado de planear el ataque al Pentágono y al Congreso Estadounidense con “aviones grandes a control remoto cargados con explosivo plástico C-4” y suministrar “apoyo material y recursos a una organización terrorista extranjera, específicamente a Al Qaeda”.¹⁴ Según la Oficina Federal de Investigaciones, Ferdaus planeaba complementar su “ataque aéreo” de tres vehículos teledirigidos con un ataque por tierra que incluía “seis personas armadas con armas automáticas divididas en dos equipos”. Ferdaus explicó que “con este ataque aéreo, podemos eliminar efectivamente lugares claves del edificio P [el Pentágono], después podemos añadir otras cosas para anular todo lo demás y dejar un área como lugar restringido solamente donde los individuos quedarían aislados, allí serán vulnerables y los podemos dominar”.¹⁵

Proliferación de misiles superficie-aire disparados desde el hombro

Un escuadrón de vuelo puede lograr éxito en la misión solo generando vuelos de aviones, sin importar las amenazas del entorno operativo. La protección de las aeronaves contra misiles SAM durante el despegue, la fase más vulnerable del vuelo, es sumamente difícil debido a las restricciones de maniobrabilidad causadas por el peso y la baja altitud. En consecuencia, las aeronaves de transporte pesado y su valiosa carga, posiblemente municiones y/o pasajeros, presentan blancos sumamente tentadores durante el despegue. Inversamente, los aviones que se aproximan tienen poco combustible y deben mantener velocidades y trayectorias de vuelo predecibles. En cualquiera de los dos casos, los misiles SAM representan una amenaza para tales aeronaves. Por ejemplo, los rebeldes en el actual conflicto sirio supuestamente poseen entre “quince y treinta sistemas de defensa aérea portátiles SA-7 [MANPADS]” y “aparentemente han derribado al menos cinco aeronaves de ala rotatoria y seis de ala fija”, cuando menos uno de ellos fue derribado por un MANPADS.¹⁶ De acuerdo con el Centro de la Fuerza Aérea de los Estados Unidos Contra la Proliferación,

Actualmente, 27 grupos terroristas, incluyendo Al Qaeda, han confirmado o reportado la posesión de MANPADS. Desde 1994, ha habido diez intentos de alto perfil para atacar aviones comerciales y se ha derribado cuatro, incluyendo uno que llevaba a los presidentes de Ruanda y Burundi. Además, los MANPADS se adaptan perfectamente al modo de operación de Al Qaeda y son relativamente fáciles de usar, de transporte conveniente, ampliamente disponibles, de poco costo, y definitivamente mortíferos.¹⁷

A medida que avanzan y proliferan las tecnologías desarrolladas por competidores extranjeros, las tácticas, técnicas y procedimientos para la defensa integrada tendrán que ponerse a la par con su empleo. Recientemente el MANPADS SA-24 “Grinch” de fabricación rusa pasó a Venezuela, Libia y Siria.¹⁸ Por cierto, el gobierno de Libia ha sido derrocado, y al momento de esta redacción Siria se mantiene en un estado de guerra civil. La seguridad de los MANPADS en los países en guerra es dudosa debido al potencial desarrollo de mercados negros y la inestabilidad que atrae elementos perversos. La amenaza de MANPADS para las fuerzas estadounidenses y de la coali-

ción, así como para las operaciones de las aerolíneas civiles probablemente aumentará a medida que estos sistemas se hagan más accesibles en el terreno fértil de la guerra civil y la insurgencia.

La creciente “amenaza interna”

En el futuro previsible, las fuerzas estadounidenses y de la coalición se desenvolverán en medio de amenazas internas. Desde 2007 hasta 2011 en Afganistán, las estadísticas del Pentágono revelan un total de 42 ataques realizados por miembros de las Fuerzas de Seguridad Nacional de Afganistán contra personal estadounidense o de la OTAN, causando la muerte de 70 soldados de la coalición e hiriendo a otros 110.¹⁹ Uno de los casos más graves y horribles de una amenaza interna ocurrió en la mañana del 27 de abril de 2011, cuando un capitán de la Fuerza Aérea Afgana asesinó a ocho aerotécnicos y un contratista en el Aeropuerto Internacional de Kabul.²⁰ Otro incidente demostró cómo un terrorista suicida decidido y astuto pudo infiltrar una base de la Agencia Central de Inteligencia (CIA) en el este de Afganistán y mató a ocho estadounidenses.²¹ Esta perturbadora tendencia se intensificó en 2012 cuando fuerzas de seguridad afganas uniformadas realizaron 46 ataques internos contra fuerzas de la coalición en las que perdieron la vida 60 miembros de la OTAN.²²

Aún más preocupante es la creciente amenaza dentro de las filas del personal estadounidense. El 11 de mayo de 2009, cinco de sus miembros militares fueron asesinados por un soldado estadounidense en un centro de consejeros en Camp Liberty, Bagdad.²³ En un tiroteo realizado por un psiquiatra del Ejército de los Estados Unidos el 5 de noviembre de 2009 en Fort Hood, Texas, resultaron muertas 13 personas y heridas otras 32.²⁴ Evidentemente, al Departamento de Seguridad Nacional le preocupa la amenaza que podrían crear los veteranos en el territorio nacional, teniendo en cuenta que éstos al volver de Irak y Afganistán podrían ser reclutados por los radicales de extrema derecha.²⁵

Es importante recordar que una persona puede causar un daño enorme, lo atestigua el número de incidentes “lobo solitario” que han ocurrido. Por ejemplo, el 22 de julio de 2011, Anders Breivik, un noruego, hizo explotar un coche bomba cerca de edificios del gobierno en Oslo, causando la muerte de ocho personas, y después masacró 69 personas en un campamento de jóvenes en la cercana isla de Utoeya.²⁶ El 20 de julio de 2012, el estadounidense James Holmes entró en un cine repleto de espectadores cerca de Denver y comenzó a disparar; asesinó a 12 e hirió a 58.²⁷ Los miembros militares estadounidenses capacitados y con experiencia y los veteranos podrían causar estragos aún mayores. Sea dentro del país o en ultramar, los comandantes deben asegurarse de proporcionar y ejecutar un plan de seguridad interior completo—uno que incluya un programa agresivo de evaluación psicológica para identificar las amenazas internas.

Obtención de mapas de las bases aéreas

Anteriormente, cuando las fuerzas enemigas planeaban un ataque terrestre contra una base aérea, se apoyaban en colaboradores con acceso a la base seleccionada para facilitar el mapeo del terreno y las instalaciones claves, y también para obtener distancias que hagan posible los ataques con fuego indirecto. Hoy, las autopistas de la información ofrecen acceso a imágenes satelitales y otras informaciones de dominio público que facilitan el trabajo del potencial atacante. Uno de esos sitios web, el de la Federación de Científicos Estadounidenses (FAS), se auto-describe como “un grupo de reflexión independiente, no partidario y registrado como organización con membresía sin fines de lucro 501(c)(3) . . . dedicado a proporcionar análisis rigurosos y objetivos basados en evidencia y recomendaciones de política práctica sobre asuntos de seguridad nacional e internacional conectados a la ciencia y tecnología aplicadas”.²⁸ GlobalSecurity.org, una ramificación de FAS fundada por John Pike, uno de sus ex miembros, se atribuye ser “la

fuerza principal de información de referencia y noticias recientes en los campos de defensa, espacio, inteligencia, armas de destrucción masiva [WMD], y seguridad nacional”.²⁹ Su sitio web contiene imágenes satelitales de bases militares alrededor del mundo, muchas de las cuales el gobierno estadounidense considera clasificadas. Otros sitios web, como Google Maps, ponen a disposición imágenes y mapas de calles. En resumen, ahora hay una multitud de formas de adquirir mapas detallados de bases aéreas que facilitarían ataques contra esas instalaciones.

Medios sociales: Turbas relámpago, terrorismo, y uso de la conexión en red para ataques a las bases

Las comunicaciones instantáneas mejorarán dramáticamente las operaciones de información del enemigo y los ataques a las bases, permitiéndoles aprovechar elementos favorables de una población local para crear situaciones que avergüencen al liderazgo de una base aérea o agobien las defensas. Por lo tanto, inteligencia y las autoridades policiales deben estar un paso por delante de un enemigo cada vez más ágil, mejorando la eficiencia de sus esfuerzos de recopilación de información. La tecnología básica, como los teléfonos celulares, ha afectado a la sociedad en formas insólitas creando medios sin precedentes para la comunicación y coordinación de las acciones. Pensemos por ejemplo el fenómeno en la “turba relámpago”, un grupo de gente convocada por teléfonos celulares, medios sociales y correos virales con el fin de realizar alguna clase de acto en un lugar específico. La Web e incluso los comerciales de las empresas de telecomunicaciones están repletos de imágenes de turbas relámpago benignas que aparecen en un lugar público para llevar a cabo alguna clase de acto inusual o artístico, como congelarse en un lugar o realizar una rutina de baile coordinado. Aunque hacen esto en nombre del entretenimiento, ¿qué sucede cuando alguien utiliza esta misma tecnología para fines nefastos?

En el verano de 2011, por ejemplo, en Filadelfia se produjo una epidemia de turbas relámpago organizadas para llevar a cabo robos, asaltos, saqueos, y caos. Este incidente incluyó golpizas a peatones al azar, alborotos en una tienda Sears, y reuniones de cientos de personas en lugares designados para estrangular el tráfico. Margaret Rock, editor de Multimedia.com en Chicago, dijo lo siguiente: “No se por qué, pero lo que comenzó como algo que se puede usar para el bien ha mostrado su lado oscuro”.³⁰ Posteriormente en ese mismo verano, ocurrieron disturbios en Londres, Birmingham, Manchester, y otros lugares, causando gran preocupación en los oficiales de seguridad. Scotland Yard identificó y arrestó cerca de 3.000 personas sospechosas de cometer excesos físicos o incitar a la violencia a través del país usando BlackBerry Messenger, Twitter, y Facebook.³¹ Según un texto, “Si quiere ganarse un dinero, estamos a punto de gastar mucho en el este de Londres”.³² David Cameron, Primer Ministro Británico, observó que “lo que observan estas acciones horribles quedarán sorprendidos al saber cómo se organizaron mediante los medios sociales. . . . Por eso estamos trabajando con la policía, los servicios de inteligencia y la industria para determinar si sería correcto impedir que estas personas se comuniquen por estos sitios web cuando sabemos que están tramando violencia, desorden y criminalidad”.³³

La rapidez del avance tecnológico ha llegado a todas las esquinas del mundo. Los teléfonos celulares son ahora potentes computadoras por derecho propio, conectándose en red con otros dispositivos de manera global. En ningún lugar es esto más evidente que en los países en desarrollo que tienen comunicaciones deficientes debido al costo de cablear la infraestructura para las líneas de tierra. Los teléfonos celulares le restan validez a ese gasto ya que las torres y los satélites permiten que esos países se conecten a la red global de comunicaciones. En 2008, el 80 por ciento de la población mundial tenía acceso a una red celular, y para fines de 2006, los países en desarrollo compraron el 68 por ciento de los teléfonos móviles del mundo.³⁴

La misma tecnología que habilita el intercambio y avance de la información global también permite la conexión en red de los grupos terroristas y criminales. Según un nuevo estudio de la Universidad de Haifa en Israel, Al-Qaeda, Hamas, Hezbollah, y otros similares han invertido en los medios sociales como Facebook y Twitter para reclutar, recolectar fondos y reunir inteligencia. El profesor Gabriel Wiemann, autor del estudio, sostiene que “en la actualidad, cerca del 90 por ciento del terrorismo organizado en Internet se lleva a cabo a través de los medios sociales” y que esto último está “permitiendo que las organizaciones terroristas tomen iniciativas haciendo pedidos de ‘amigos’, colgando videos cortos y similares, y ya no tienen que conformarse con las herramientas pasivas disponibles en los sitios web regulares”.³⁵

¿Cómo afectarán esta tecnología y las redes sociales a la seguridad de las bases en el futuro? Fácilmente se podría convocar a manifestantes, turbas y grupos terroristas sin previo aviso para la inteligencia militar o la policía, y reunirse rápidamente cerca del punto de entrada o el perímetro de una base para protestar, crear desórdenes o atacar. En muchos casos, tales áreas tendrían solo un puñado de vigilantes disponibles para contrarrestar a los grupos reunidos—un escenario que fácilmente podría abrumar al escaso personal en la escena e intensificarse más allá de su capacidad para sofocar tal acción.

Ciberataques: Un potencial “botón fácil” para ataque a una base aérea

Los avances tecnológicos han dado lugar a que los militares estadounidenses se apoyen en una “ciberfuerza” que depende principalmente de una red de computadoras y enlaces de comunicaciones, para asegurar no solo el uso efectivo de las fuerzas durante las operaciones de contingencia sino también la misión cotidiana de preparación y capacitación de la fuerza. Hasta ahora, los insurgentes han carecido de la capacidad y capacitación para llevar a cabo ciberataques en gran escala contra instalaciones militares. Sin embargo, es probable que eso cambie cuando las organizaciones terroristas auspiciadas por estados y las fuerzas insurgentes se asocien para derrotar a un enemigo común. La utilización de un ciberataque que afecte las operaciones aéreas o los sensores y cámaras de defensa de la base con el fin de facilitar un ataque cinético puede ser una opción económica y eficiente.

Los ataques a través del ciberespacio podrían degradar las operaciones de vuelo, tal como ocurrió en el Aeropuerto Internacional Indira Gandhi, cuando un código malicioso que utilizaba comandos específicamente diseñados para explotar la debilidad de ese sistema, desactivó los mostradores de facturación y las puertas de embarque afectando tremendamente las operaciones.³⁶ Un ataque similar podría interrumpir los nodos de control de tráfico aéreo, programas de mantenimiento en red, y operaciones de capacitación, y también amenazar a los RPV con armas o sin armas operados por la Fuerza Aérea y otras agencias del gobierno. Considere por ejemplo el reciente hackeo de un vehículo teledirigido del Departamento de Seguridad Nacional como parte de una apuesta entre un profesor de un instituto superior de Texas y sus alumnos. Con menos de \$1.000 dólares, estos individuos “engañaron” con éxito al RPV, “cambiándole efectivamente de misión”.³⁷ Esta broma académica de poco costo demuestra la facilidad con que un grupo adversario o terrorista podría cambiar de misión de los RPV y convertirlos en misiles volantes contra una base aérea u otro blanco.

Red Flag, el ejercicio de entrenamiento para combate de la Fuerza Aérea que incluye fuerzas estadounidenses y aliadas, ha integrado elementos cibernéticos y del espacio del Comando Espacial de la Fuerza Aérea para abordar efectos asociados con ataques contra activos cibernéticos o del espacio. En el ejercicio Red Flag de marzo de 2011, un oficial de la Fuerza Aérea comentó, “Sabemos de muchas amenazas alrededor del mundo que trabajan diligentemente para acceder, degradar o negarnos el uso de [sistemas de computadoras clasificados y no clasificados]”.³⁸ Los

activos y el personal asociado con los sistemas de defensa integrados pueden también convertirse en blancos. Además, los adversarios podrían intentar interrumpir o manipular el uso creciente del ciberespacio para las comunicaciones, incluyendo transmisiones de radio cifradas, mensajería clasificada y no clasificada, y sistemas de identificación biométrica en nuestras puertas de acceso. Una investigación del *Washington Post* encontró que ciertos tipos de plataformas de software usadas por el gobierno y el sector privado—incluyendo un sistema de la empresa Tridium llamado Niagara—son más vulnerables que otros. Marc Petock, vicepresidente para mercadeo y comunicaciones globales de Tridium, señaló que “algunas instalaciones del Departamento de Defensa en los Estados Unidos también dependen de Niagara. Eso incluye el gigantesco Almacén del Ejército de Tobyhanna en Pennsylvania” y algunas instalaciones militares de “alta seguridad”.³⁹

La rápida evolución del ciberdominio promete muchos beneficios: necesidad reducida de personal, mayor eficiencia, mejor selección de objetivos y facilidad de acceso/uso. No obstante, estas mismas tecnologías presentan importantes oportunidades para que un adversario ingenioso y determinado cree una puerta trasera a través de la cual puede penetrar e inutilizar la totalidad del sistema de seguridad.

Combinación de la tecnología moderna con las fuerzas especiales

No hace mucho tiempo, los planificadores en las bases de la OTAN se concentraban en los planes de la URSS para atacar bases aéreas. Durante la Guerra Fría, los soviéticos exploraron muchas formas de atacar e inhabilitar bases, principalmente empleando la Spetsnaz (fuerzas especiales). Una revisión de los perfiles de ataque contra aeródromos de la Spetsnaz en informes desclasificados de la Agencia Central de Inteligencia (CIA) del tiempo de la Guerra fría podría resultar útil porque ofrecen perspectivas sobre los métodos de ataque directo contra estos blancos. Estos incluían el lanzamiento en paracaídas de 30 operadores especiales en las cercanías de una base aérea, quienes se separarían en “cuatro equipos de operaciones, cada uno con responsabilidades específicas incluyendo capturar vehículos y personal con el fin de infiltrar el objetivo [base aérea]”, usando misiles SAM y dispositivos explosivos para destruir aeronaves.⁴⁰ Además,

en un segundo método, una compañía de Spetsnaz (aproximadamente 10 equipos de cinco a doce miembros) operaría contra un aeródromo fuertemente defendido. La compañía no podía acercarse a menos de 2 ó 3 kilómetros del objetivo. Durante la primera noche situarían Block Strelas [lanzamisiles SAM de tres tubos montados en trípode] lo más cerca posible de uno de los extremos del campo, y después se iniciarían ataques contra sistemas de tuberías, líneas de transmisión, líneas de comunicación, personal de seguridad, y las cuadrillas que se dirigían al aeródromo.⁴¹

Esto interrumpiría las operaciones del aeródromo, crearía la impresión de que había una fuerza soviética más grande en el área, y atraería más tropas de la OTAN para la defensa y lejos de las líneas de fuego. Imagínense fuerzas especiales enemigas bien capacitadas que dispongan de muchos de los avances tecnológicos antes mencionados. La defensa de la base se volvería increíblemente difícil, y la complejidad del contrarresto de la amenaza aumentaría significativamente.

Conclusión

El entendimiento y contrarresto de estas crecientes amenazas jugará un papel muy importante en la capacidad de proyectar poderío aéreo de forma efectiva en el futuro. Una solución—poner la base de las aeronaves lo más lejos posible de las hostilidades—impone en las aeronaves y sus tripulaciones tiempos de vuelo más largos. Sin embargo, esto no resuelve el requisito probable de que las aeronaves de movilidad aterricen cerca de o en la zona de combate para apoyar las operaciones de tierra. Ni tampoco las bases remotas responden a los medios tecnológicos de ataque a través del ciberespacio, terroristas tecnológicamente habilitados, o fuerzas especiales

que atacan una base aérea supuestamente segura. Por lo tanto, los Aerotécnicos deben realizar un verdadero análisis de amenaza de espectro total y tomar en consideración estas potenciales vulnerabilidades en el planeamiento de protección de la fuerza.

Las aeronaves son sumamente frágiles. Un proyectil de mortero bien puesto puede inutilizar aeronaves por valor de varios cientos de millones de dólares o destruir las barracas ocupadas por personal esencial, como pilotos o técnicos de aeronaves. Las fuerzas de la Fuerza Aérea y de la coalición tendrán que tomar decisiones difíciles sobre defensa de la base teniendo en cuenta los requisitos de la misión, las restricciones económicas, y la creciente amenaza que presenta un enemigo decidido habilitado por alguna de las tecnologías antes mencionadas. Los Aerotécnicos y los líderes conjuntos deben mantenerse al tanto de estos problemas durante el período entre guerras o arriesgar la eliminación y degradación de los activos aéreos al comienzo de la próxima campaña importante. □

Notas

1. Barbara Starr, Chris Lawrence y Joe Sterling, "ISAF: Insurgentes en ataque mortal en Afganistán vestían uniformes del ejército de los Estados Unidos", Cable News Network, 15 de septiembre de 2012, <http://www.cnn.com/2012/09/14/world/asia/afghanistan-fatal-attack/index.html>.

2. Giulio Douhet, *The Command of the Air (El Comando del Aire)*, trans. Dino Ferrari (1942; nueva impresión, Washington, DC: Oficina de Historia de la Fuerza Aérea, 1983), 53–54.

3. James S. Corum y Wray R. Johnson, *Airpower in Small Wars: Fighting Insurgents and Terrorists (Poderío Aéreo en las Guerras Menores: Combatiendo a Insurgentes y Terroristas)* (Lawrence: University Press of Kansas, 2003), 334–35.

4. Mayor Michael P. Buonaugurio, USAF, "Air Base Defense in the 21st Century: USAF Security Forces Protecting the Look of the Joint Vision (Defensa de la base aérea en el siglo 21: Fuerzas de seguridad de la USAF protegen el aspecto de la visión conjunta)" (tesis de maestría, Marine Corps Command and Staff College, 2001), 8, <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA401262>.

5. Jeremy Kelly, "Base militar de la OTAN atacada por terrorista suicida en Afganistán," *Guardian*, 11 de septiembre de 2011, <http://www.guardian.co.uk/world/2011/sep/11/us-base-suicide-bomber-afghanistan>.

6. Alan Vick, *Snakes in the Eagle's Nest: A History of Ground Attacks on Air Bases (Serpientes en el Nido del Ágila: Una Historia de los Ataques Terrestres Contra Bases Aéreas)* (Santa Monica, CA: RAND, 1995), 68, http://www.rand.org/content/dam/rand/pubs/monograph_reports/2006/MR553.pdf.

7. Barbara Starr, "Esquirlas impactan avión del Presidente del Estado Mayor en una base afgana" Cable News Network, 21 de agosto de 2012, http://articles.cnn.com/2012-08-21/asia/world_asia_afghanistan-dempsey-plane_1_fight-against-afghan-green-on-blue-afghan-man-afghanistan.

8. Sargento Tercero Todd Christopherson, "Soldados disparan el primer mortero con guía de precisión en Afganistán", Ejército de los Estados Unidos, 7 de abril de 2011, <http://www.army.mil/article/54502/>.

9. Jennifer Rizzo, "Estados Unidos continúa apoyando la cúpula de acero de Israel", Cable News Network, 17 de mayo de 2012, http://articles.cnn.com/2012-05-17/us/us_israel-missile-system_1_anti-rocket-iron-dome-missile-defense?s=PM:US; y Ernesto Londoño, "Para Israel, el sistema de defensa contra misiles Cúpula de Acero representa un gran avance", *Washington Post*, 2 de diciembre de 2012, http://www.washingtonpost.com/world/national-security/for-israel-iron-dome-missile-defense-system-represents-breakthrough/2012/12/01/24c3dc26-3b32-11e2-8a97-363b0f9a0ab3_story_1.html.

10. Rebecca Boyle, "Después que activistas hacen seguimiento con vehículo teledirigido de caza de palomas, los cazadores de palomas lo derriban," *Popular Science*, 21 de febrero de 2012, <http://www.popsci.com/technology/article/2012-02/after-pigeon-hunt-thwarted-shooters-take-down-activist-groups-spy-drone>.

11. Capitán Daniel Helmer, "Hezbollah's Employment of Suicide Bombing during the 1980s: The Theological, Political, and Operational Development of a New Tactic (Empleo de terroristas suicidas por Hezbollah durante la década de 1980: El desarrollo teológico, político y operativo de una nueva táctica)", *Military Review*, Julio-Agosto de 2006, http://www.army.mil/professionalWriting/volumes/volume4/november_2006/11_06_1.html.

12. Associated Press, "Israel: Tropas iraníes ayudan en ataque de Hezbollah", *NBC News*, 16 de julio de 2006, <http://www.nbcnews.com/id/13875121/>.

13. Lisa Myers, "Vehículo teledirigido de Hezbollah amenaza a Israel", *NBC News*, 12 de abril de 2005, <http://www.msnbc.msn.com/id/7477528/ns/nbcnightlynews/t/hezbollah-drone-threatens-israel/>.

14. "Residente de Massachusetts es acusado de planear ataque contra el Pentágono y el Capitolio de Estados Unidos e intentar el suministro de apoyo material a una organización terrorista extranjera", comunicado de prensa, Oficina

Federal de Investigaciones, 28 de septiembre de 2011, <http://www.fbi.gov/boston/press-releases/2011/massachusetts-man-charged-with-plotting-attack-on-pentagon-and-u.s.-capitol-and-attempting-to-provide-material-support-to-a-foreign-terrorist-organization>.

15. *Ibíd.*

16. Eddie Boxx y Jeffrey White, “Respuesta al uso del poderío aéreo de Assad en Siria”, Washington Institute for Near East Policy, 20 de noviembre de 2012, <http://www.washingtoninstitute.org/policy-analysis/view/responding-to-assads-use-of-airpower-in-syria>.

17. James C. “Chris” Whitmire, *Shoulder Launched Missiles (a.k.a. MANPADS): The Ominous Threat to Commercial Aviation (Misiles disparados desde el hombro (o MANPADS): La ominosa amenaza contra la aviación comercial)*, Documentos Contra la Proliferación, Serie Future Warfare No. 37 (Maxwell AFB, AL: Centro de la Fuerza Aérea de los Estados Unidos Contra la Proliferación, Universidad del Aire, diciembre de 2006), 1, <http://cpc.au.af.mil/PDF/monograph/manpads.pdf>.

18. David Fulghum y Robert Wall, “SA-24 ‘Grinch’ de Rusia cae en manos insurgentes”, *Aviation Week and Space Technology*, 12 de marzo de 2012, http://www.aviationweek.com/Article.aspx?id=/article-xml/AW_03_12_2012_p27-433282.xml&p=1.

19. Anna Mulrine, “¿Infiltrados del Taliban en Afganistán? El Pentágono advierte sobre la ‘amenaza interna’”, *Christian Science Monitor*, 1 de febrero de 2012, <http://www.csmonitor.com/USA/Military/2012/0201/Taliban-infiltrators-in-Afghanistan-Pentagon-warns-of-insider-threat>.

20. Jill Laster, “Motivo del tiroteo de Kabul sigue siendo esquivo”, *Air Force Times*, 17 de enero de 2012, <http://www.airforcetimes.com/news/2012/01/air-force-motive-in-kabul-shooting-deaths-remains-elusive-011712/>.

21. Joby Warrick, “Terrorista suicida ataca base de la CIA en Afganistán, dando muerte al menos a 8 estadounidenses”, *Washington Post*, 31 de diciembre de 2009, <http://www.washingtonpost.com/wp-dyn/content/article/2009/12/30/AR2009123000201.html>.

22. “¿Qué hay detrás de los ataques internos en Afganistán?”, British Broadcasting Corporation, 11 de marzo de 2013, <http://www.bbc.co.uk/news/world-asia-19633418>.

23. Timothy Williams, “Soldado estadounidense asesina a 5 de sus compañeros en Irak”, *New York Times*, 11 de mayo de 2009, http://www.nytimes.com/2009/05/12/world/middleeast/12iraq.html?_r=2.

24. Joseph I. Lieberman y Susan M. Collins, *A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government’s Failure to Prevent the Fort Hood Attack (Una bomba de tiempo: Lecciones antiterrorismo de la falla del gobierno de los Estados Unidos para prevenir el ataque de Fort Hood)*, informe especial (Washington, DC: Comisión del Senado de los Estados Unidos sobre Seguridad Nacional y Asuntos del Gobierno, febrero de 2011), <http://www.hsgac.senate.gov/download/fort-hood-report>.

25. Associated Press, “Líderes de Seguridad Nacional defienden memo sobre veteranos de guerra”, *USA Today*, 19 de abril de 2009, http://usatoday30.usatoday.com/news/washington/2009-04-19-homeland-memo_N.htm.

26. “Anders Breivik describe la masacre en isla de Noruega”, BBC, 20 de abril de 2012, <http://www.bbc.co.uk/news/world-europe-17789206>.

27. M. Alex Johnson y Pete Williams, “Policía: Se realizaron semanas de planeamiento para los tiroteos en la proyección de Batman en Colorado”, *NBC News*, 20 de julio de 2012.

28. “Acerca de la FAS”, Federación de Científicos Estadounidenses, consultado el 29 de enero de 2013, <https://www.fas.org/about/index.html>.

29. “Historia de la empresa”, GlobalSecurity.org, consultado el 13 de marzo de 2013, <http://www.globalsecurity.org/org/overview/history.htm>.

30. John Timpane, “Violencia de las turbas relámpago levanta preguntas importantes”, Philly.com, 14 de agosto de 2011, http://articles.philly.com/2011-08-14/news/29886718_1_social-media-flash-mob-facebook-and-other-services.

31. Neil Lancefield, “3,000 arrestos en investigación de disturbios en Londres”, *Independent*, 7 de octubre de 2011, <http://www.independent.co.uk/news/uk/crime/3000-arrests-in-london-riots-investigation-2366933.html>.

32. Timpane, “Violencia de las turbas relámpago”.

33. Josh Halliday, “David Cameron considera prohibir que los agitadores sospechosos entren en los medios sociales”, *Guardian*, 11 de agosto de 2011, <http://www.guardian.co.uk/media/2011/aug/11/david-cameron-rioters-social-media>.

34. Sara Corbett, “¿Puede el teléfono celular ayudar a terminar con la pobreza global?”, *New York Times*, 13 de abril de 2008, <http://www.nytimes.com/2008/04/13/magazine/13anthropology-t.html?pagewanted=all>.

35. “Grupos terroristas utilizan los medios sociales para reclutar”, Canadian Broadcasting Corporation News, 10 de enero de 2012, <http://www.cbc.ca/news/technology/story/2012/01/10/tech-terrorist-social-media.html>.

36. Rahul Tripathi, “Ciberataque dio lugar a la paralización del Aeropuerto Indira Gandhi”, *Indian Express*, 25 de septiembre de 2011, <http://www.indianexpress.com/news/cyber-attack-led-to-igi-shutdown/851365/>.

37. “Instituto Superior de Texas hackea vehículo teledirigido del gobierno frente al Departamento de Seguridad Nacional”, Organización autónoma sin fines de lucro (“TV-Novosti”), 27 de junio de 2012, <http://rt.com/usa/news/texas-1000-us-government-906/>.

38. Sargento Segundo Scott McNabb, “Red Flag Cyber Operations: Part I—Isn’t Red Flag a Flyer’s Exercise? (Operaciones cibernéticas Red Flag: Parte I—¿No es Red Flag un ejercicio de vuelo?)”, Comando Espacial de la Fuerza Aérea, 1 de marzo de 2011, <http://www.afspc.af.mil/news/story.asp?id=123244481>.

39. Robert O’Harrow Jr., “Tridium’s Niagara Framework: Marvel of Connectivity Illustrates New Cyber Risks (Marco teórico de Niagara de Tridium: Maravilla de conectividad ilustra nuevos riesgos cibernéticos)”, *Washington Post*, 11 de julio de 2012, http://www.washingtonpost.com/investigations/tridiums-niagara-framework-marvel-of-connectivity-illustrates-new-cyber-risks/2012/07/11/gJQARJL6dW_story.html.

40. Director de Inteligencia Central, *Warsaw Pact Nonnuclear Threat to NATO Airbases in Central Europe (Amenaza no nuclear del pacto de Varsovia para las bases aéreas de la OTAN en Europa Central)*, NIE 11/20-6-84, 25 de octubre de 1984, 35, http://www.foia.cia.gov/sites/default/files/document_conversions/89801/DOC_0000278545.pdf. Este documento ha sido desclasificado.

41. *Ibíd.*, 36, 39.



El Coronel Shannon W. Caudill, USAF (BS, Norwich University; MS, Central Michigan University; MMS, Marine Corp University) es estudiante en el Programa de Gran Estrategia de la Escuela Superior de Guerra de la Fuerza Aérea y ex vicepresidente del Departamento de Liderazgo y Estrategia, Escuela Superior de Comando y Estado Mayor, Base Aérea Maxwell, Alabama. Antes de ocupar su puesto actual, el Cnel. Caudill estuvo al mando del 532º Escuadrón Expedicionario de Fuerzas de Seguridad (los Leones), Base Conjunta Balad, Irak. En calidad de oficial de carrera en las fuerzas de seguridad, se ha desempeñado a niveles de unidad, comando principal y estado mayor conjunto; ha estado al mando de tres escuadrones de fuerzas de seguridad; servido en cuatro asignaciones en ultramar y acumulado 18 horas de experiencia en combate en Irak. El Cnel Caudill ha escrito varios informes blancos y artículos sobre terrorismo, liderazgo interinstitucional y cumplimiento de la ley que han sido publicados en el *Air and Space Power Journal*, *Joint Force Quarterly*, *American Diplomacy* y *The Guardian*—la publicación sobre antiterrorismo del Estado Mayor Conjunto. El Coronel es egresado de la Escuela Superior para Oficiales de Escuadrón, de la Escuela Superior de Comando y Estado Mayor del Cuerpo de Infantería de Marina y de la Escuela Superior de las Fuerzas Conjuntas.



El Mayor Benjamin R. Jacobson, USAF (BS, University of Idaho; MBA [con énfasis en Justicia Criminal], Touro University; MMOAS, Escuela Superior de Comando y Estado Mayor) es director adjunto del Curso de Estudios Aéreos, Espaciales y de Poder Cibernético, Departamento de Liderazgo y Estrategia, Escuela Superior de Comando y Estado Mayor, Base Aérea Maxwell, Alabama. Antes de ocupar su puesto actual, el Mayor Jacobson estuvo al mando del 96º Escuadrón de Entrenamiento en Combate Terrestre, Base Aérea Eglin, Florida. En calidad de oficial de carrera en las fuerzas de seguridad, el Mayor Jacobson se ha desempeñado a niveles de unidad, ala y comando principal y ha servido en dos asignaciones en ultramar. El Mayor Jacobson es egresado del Curso Básico Aeroespacial, de la Escuela Superior para Oficiales de Escuadrón y de la Escuela Superior de Comando y Estado Mayor.