



<http://www.af.mil>



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



<http://www.au.af.mil>

General Mark A. Welsh III

Jefe del Estado Mayor, Fuerza Aérea, EE.UU.

General Edward A. Rice Jr.

Comandante, Comando de Educación y Entrenamiento Aéreo

Teniente General David S. Fadok

Comandante, Universidad del Aire

General John A. Shaud, USAF-Retirado

Director, Air Force Research Institute

Editor, Edición en Español

Tte. Cnel. Luis F. Fuentes, USAF-Retirado

Asistente Editorial

Sra. Drina L. Marmolejo

Producción

Sra. L. Susan Fair, *Ilustradora*

Sr. Daniel Armstrong, *Ilustrador*

Sra. Vivian D. O'Neal, *Diagramación*

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

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

DSN: 493-6382

Fax: (334) 953-1626

E-mail: aspjspanish@maxwell.af.mil

aspjspanish@gmail.com (Alternativa)

AIR & SPACE POWER

JOURNAL
en ESPAÑOL

Volumen 23, N° 4

CUARTO TRIMESTRE 2012



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

Editorial	3
La Fuerza Aérea Colombiana en Red Flag Coronel Kristian D. Skinner, USAF-Ret	5
El Espectro de una Guerra no Evidente Dr. Martin C. Libicki, PhD	19
Creando un Comando Nuevo en el Ciberespacio General Keith B. Alexander, USA	29
Requisitos de las Organizaciones Terroristas con Capacidad Internacional Mayor Michael Haack, USAF	36
Diseñando Colisiones de Satélites en la Guerra Cibernética Encubierta Dr. Jan Kallberg, PhD	46
Sendero Luminoso y el Narcotráfico en el VRAEM Comandante Ismael Iglesias L., FAP-Ret	55
Crimen y Gobernabilidad en una Honduras Contemporánea Dra. Mary Fran T. Malone, PhD	63
La Contribución de la Fuerza Aérea Colombiana en el Surgimiento de Colombia como el Nuevo Catalizador Regional Capitán Rodrigo Mezú Mina, Fuerza Aérea Colombiana	82
Diez Mil Pies y Diez Mil Millas: Reconciliación de la Cultura de Nuestra Fuerza Aérea con los Aviones de Control Remoto y la Nueva Naturaleza del Combate Aéreo Mayor Dave Blair, USAF	89
Reseña de Libros	95
Medalla Militar, San Miguel Arcángel	96



El entrenamiento militar conocido con el nombre de Red Flag es quizás el ejercicio de combate aéreo más realista y de mayor precisión, pero también el de mayor dificultad para los pilotos de la Fuerza Aérea de los Estados Unidos y sus aliados. Desde sus inicios, en noviembre de 1975, este ejercicio se realiza varias veces al año en la Base Aérea de Nellis en Nevada, en una área de entrenamiento militar con una extensión de espacio aéreo de 12.000 Kilómetros cuadrados y de 2.9 millones de hectáreas de tierra, de acuerdo a la narración hecha por el Coronel Kris Skner en su artículo “La Fuerza Aérea Colombiana en Red Flag”. A la fecha, solo 31 de los países aliados suficientemente capacitados y más cercanos a los Estados Unidos, han sido invitados a participar en este arduo entrenamiento, entre los cuales en Latinoamérica figuran las fuerzas aéreas de Brasil, Chile, Colombia y Venezuela. Es de resaltar que la exitosa participación de la Fuerza Aérea Colombiana en Red Flag fue la demostración más valiosa de su profesionalismo, al mismo tiempo que con ella colmó el sueño de muchos de sus pilotos y logró alcanzar varios hitos, entre ellos el de constituirse en la Fuerza Aérea Latinoamericana que por vez primera y sin asistencia externa consiguió desplegar un escuadrón de cazas y tanqueros a Red Flag que la hace merecedora de nuestro reconocimiento por el éxito alcanzado.

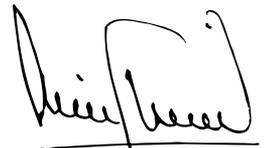
Siguiendo una línea de continuidad con nuestra pasada edición (Tercer Trimestre 2012), en la cual centramos nuestra atención en el tema del ciberespacio y, en particular, de la ciberguerra y las actividades criminales que podrían causar una catástrofe de magnitud mundial, hacemos referencia a través de esta edición, a tres interesantes artículos que relatan los peligros y retos que se derivan del ciberdominio. El primero de ellos, titulado “El espectro de una guerra no evidente” y escrito por el Dr. Martin Libicki, presenta un análisis sobre la adecuada respuesta que los estados víctima pueden dar a la amenaza de guerra no evidente, teniendo en cuenta los adelantos tecnológicos en el ciberdominio. A su vez, un segundo artículo titulado “Diseñando colisiones de satélites en la guerra cibernética encubierta”, escrito por el Dr. Jan Kallberg, narra los peligros a los cuales muchas naciones ven expuestos sus satélites, utilizados primariamente con fines pacíficos, a ataques cinéticos directos e indirectos con los que los adversarios con fines políticos, económicos o militares buscan causar daño desestabilizando sus sistemas. Por último, un tercer artículo “Creando un comando nuevo en el ciberespacio” escrito por el General Keith Alexander, USA, describe la historia y los pasos defensivos iniciados por los Estados Unidos en el ciberdominio con la creación de un Comando Ciberespacial.

Otra de las amenazas para la seguridad y la paz mundial se deriva de los ataques asimétricos perpetuados por individuos u organizaciones internacionales. Para sustentar esta tesis, el Mayor Michael Haack en su artículo “Requisitos de las organizaciones terroristas con capacidad internacional”, hace un análisis sobre las causas y los métodos empleados en algunos de los últimos ataques terroristas que le permiten emitir sugerencias respecto a estrategias a seguir, para poder combatir el terrorismo y antiterrorismo, a la vez que enumera una serie de características de estos grupos a los cuales Estados Unidos debe contrarrestar mediante la implementación de políticas enmarcadas en la prevención, predicción y acción contra los grupos terroristas ya existentes.

Consciente del enorme desafío que actualmente enfrenta el gobierno peruano ante el resurgir del conocido movimiento “Sendero Luminoso”, de ideología marxista-maoísta, derrotado hace más de una década, el Teniente Coronel Ismael Iglesias enfoca su análisis en los esfuerzos del Gobierno, la Policía Nacional y las Fuerzas Armadas peruanas por impedir que remanentes

de los rebeldes maoístas se consoliden políticamente en alianza con el narcotráfico. Haciendo historia, el Teniente Coronel Iglesias, en su artículo titulado “El Sendero Luminoso y el Narcotráfico en el VRAEM,” se remonta a sus orígenes en la década de los 80’s cuando se inicia como un movimiento político marxista que en su afán por constituirse en un estado comunista deja un saldo de más de 70.000 muertes, pero que es derrotado finalmente a comienzos de 1990. En una nueva etapa, un proceso de reencarnación comienza a fortalecerse por parte de los remanentes del Sendero Luminoso que lo transforman en un poderoso movimiento guerrillero narcotraficante que controla el cultivo y la distribución de drogas en los valles cocaleros del sudeste peruano entre los ríos Ene-Apurímac, denominado VRAEM. Como resultado, Perú se ha convertido ahora en el mayor productor de cocaína del mundo, con más del 50% de la producción mundial.

Enfocándonos finalmente en la problemática de Centro América, podemos concluir afirmando que la inseguridad, la corrupción y la violencia son las principales fuentes de inestabilidad de esta región, en donde la situación de Honduras azotada por el flagelo del crimen y de la violencia se constituye en un reflejo viviente de esta realidad y que al presentar las tasas más altas de homicidio del mundo, le confiere la infame distinción de ser la capital mundial del asesinato. Su situación es aún más compleja si nos remitimos a las altas tasas de pobreza y de desigualdad que la señalan negativamente en el contexto del hemisferio occidental, con el ingrediente de desconfianza existente en los estamentos de la Policía, de las Fuerzas Armadas y de su clase política. Y ante el impacto que produce la delincuencia sobre el apoyo ciudadano a la democracia y sus normas en Honduras, la Señora Mary Malone se pronuncia en su artículo “Crimen y gobernabilidad en una Honduras Contemporánea”, citando datos de numerosas entrevistas plasmadas en el Proyecto Latinoamericano de Opinión Pública (The Latin American Public Opinion Project -LAPOP 2012).



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

La Fuerza Aérea Colombiana en Red Flag

CORONEL KRISTIAN D. SKINNER, USAF-RET



La primera noche

La formación de cuatro Kfir C-10, designada “Rocket 41”, se desprende de su órbita en la oscuridad de la noche a mediana altura y a una velocidad casi supersónica. Acabaron de dejar atrás su tanquero del cual cada piloto llenó sus tanques externos. No hay luna. Solo la luz de las estrellas ilumina el escenario en sus equipos de visión nocturna mientras mantienen su formación visual. Los pilotos tienen mucha experiencia en ataque nocturno, pero esta noche algo es distinto. Experimentan un estrés adicional por ser su primera misión en este ambiente y encuentran amenazas nuevas. Su blanco es defendido no solamente por los misiles tierra-aire (SAMs por sus siglas en inglés) y artillería anti-aérea (AAA por sus siglas en inglés), sino también por los ‘Agresores’ de la Fuerza Roja, equipados con misiles de guía de radar de largo alcance; un escenario bien difícil. Su meta es colocar su carga de bombas de 500 libras sobre el blanco designado y escaparse exitosamente sin trabar combate con la Fuerza Roja; disparar con precisión y letalidad manteniéndose todo el tiempo invisible a sus adversarios. Aumentándoles el estrés a medida que se acercan al blanco, comienza la interferencia en la radio (*jammer*). En su radio frecuencia, totalmente inesperado, Britney Spears comienza a cantar en voz alta: “*Hit me baby, one more time . . .*” El líder de la formación, Mayor Sergio “*Yahdai*” Perdomo, persiste a pesar del caos y pro-

cede a identificar su blanco. Con una descarga de adrenalina “*Yahdai*” tira su avión en picada y lanza su ordenanza sobre el blanco, utilizando su sistema de tiro computarizado “CCIP”. Los demás, manteniéndose en formación visual, maniobran el ataque detrás de su líder, cada uno sobreponiendo su simbología letal sobre el blanco. Con precisión descargan su ordenanza. El blanco queda destruido. Sin embargo, inesperadamente, el detector del radar enemigo del Rocket 43 se prende como si fuera un árbol de navidad, indicándole que está siendo rastreado por un SAM. Segundos después, como de Dios mismo, una voz anuncia por la radio: “Rocket 43, estás muerto.”

Habiendo disparado sus bombas, la formación Rocket 41, menos el número 3, se reúne para el egreso. Sin vacilar, “*Yahdai*” escoge el rumbo y la altura. Los pilotos restablecen su formación y responsabilidades de búsqueda justo cuando el *jammer* cambia la música de Britney Spears a la de los Beach Boys. Son momentos vulnerables para los pilotos mientras recuperan su conocimiento situacional, el requerimiento más crítico al éxito del piloto de caza. Su experiencia y dedicación al entrenamiento les han servido. Saliendo del blanco recobran su búsqueda de radar a tiempo para detectar un posible Agresor dentro de 10 millas náuticas a la una, definitivamente un factor para su ruta de egreso. No perdiendo tiempo, “*Yahdai*” entabla al ‘*bogey*’ con su radar y le pide al AWACS identificación. El controlador del AWACS rápidamente confirma que se trata de un Agresor. Con la suerte que normalmente fluye de la destreza, “*Yahdai*” ha detectado primero al Agresor. Mientras el Rojo vira para entablar combate, “*Yahdai*” lanza su misil.

Durante el *debriefing* de la primera misión nocturna hecha por pilotos de la Fuerza Aérea Colombiana (FAC) en *Red Flag*, el Mayor Perdomo y los integrantes de Rocket 41 observan la reconstrucción de su misión. Sistemas sofisticados de rastreo y evaluación revelan que su formación le dio a su blanco y logró ‘matar’ a un Agresor durante el egreso, con la pérdida de un Rocket 43 por un SAM. La misión fue del tipo soñado por todo piloto de caza y representó un comienzo prometedor para los pilotos del Comando Aéreo de Combate Número. 1 (CACOM-1) de la FAC en su primera participación en el mejor ejercicio aerotáctico del mundo, *Red Flag*, patrocinado por la Fuerza Aérea de los EE. UU. (USAF) conducido en la Base Aérea Nellis en la ciudad de Las Vegas, Nevada. ‘Kfir’ es el nombre hebreo para ‘león joven’ y “*Yahdai*” y los pilotos de Rocket 41 fueron fieles a esta imagen durante su primera misión nocturna de *Red Flag*. El despliegue de ocho Kfirs y dos tanqueros a *Red Flag* 12-4, del 14 al 28 de julio de 2012, marcó la primera vez que un escuadrón de América Latina se había desplegado por sus propios recursos para participar en *Red Flag*.

Historia de la FAC

La FAC fue organizada después de la Primera Guerra Mundial. La Escuela de Oficiales de la FAC se fundó en 1920 y, desde entonces, ha venido preparando a oficiales de la FAC. Durante las décadas después de la Primera Guerra Mundial, la FAC se granjeó en Colombia la confianza de los líderes gubernamentales y siguió incrementando su personal, aviones, e instalaciones.

La época del avión jet empezó para la FAC en los años 50 con la incorporación del F-86 ‘Sabre’. La FAC entró en la era supersónica cuando en los 70 se adquirió el Mirage-V de Francia. En los 90 la flota de Mirage fue complementada con varios aviones Kfir de Israel.

A mediados de los 50, organizaciones guerrilleras armadas en Colombia empezaron a amenazar el poder y legitimidad del gobierno. La FAC se adaptó a la situación, entrenándose y equipándose para la guerra interna. Como resultado, las tripulaciones de la FAC han obtenido mucha experiencia en operaciones de contrainsurgencia, fusión de inteligencia, combate nocturno, y ataque con precisión. Por necesidad la FAC dispone de los sistemas de armas apropiados para tales misiones: el OV-10 ‘Bronco’, A-37 ‘Dragonfly’, T-27 ‘Tucano’, A-29 ‘Super Tucano’, y AC-47 ‘Fantasma’.

Durante su prolongada guerra interna, la contribución de la FAC ha sido importante: misiones de transporte aéreo de ala fija y ala rotaria, búsqueda y rescate en combate (CSAR por sus siglas en inglés), inteligencia, y apoyo cercano. Sin embargo, en los últimos seis años la intervención de la FAC hacia la derrota de la guerrilla ha sido decisivo, logrando la mezcla perfecta de inteligencia, entrenamiento, y experiencia operacional que toda fuerza aérea busca en sus operaciones. El resultado es la liquidación de numerosos altos líderes guerrilleros a través de ataques aéreos. Estos ataques han debilitados significativamente al movimiento insurgente y les han permitido a las tropas del Ejército, Armada, y Policía Nacional recuperar el control de todo el territorio nacional.

La FAC es el servicio militar más pequeño de Colombia con aproximadamente una nómina de 13.500 efectivos, entre ellos 3.000 oficiales, 3.300 suboficiales, 4.700 reclutas, y 2.400 civiles. En comparación, el Ejército dispone de 235.000 miembros, la Armada tiene 35.000 (incluyéndose los Marines), y la Policía Nacional 144.000. Comparándose con los demás servicios del Ministerio de Defensa, sus números tan diminutivos no indican ni la extensión ni el alcance de la FAC. Ha desarrollado una infraestructura impresionante de operaciones, mantenimiento, y logística. La FAC ha crecido hasta incluir seis Comandos Aéreo de Combate (CACOM) regionales, tres Grupos Aéreos más pequeños, una base de transporte aéreo estratégico, una base de mantenimiento estratégico, y Escuelas de Oficiales y Suboficiales. Tanto con aviones de ala fija igual como ala rotatoria, el apoyo continuo y eficaz de la FAC para el Ejército, Armada, y Policía Nacional se puede dar por hecho.

Comando Aéreo de Combate #1

El Comando Aéreo de Combate #1 (CACOM-1) es el comando aéreo principal de la FAC. Se ubica en el centro de Colombia en una aldea llamada Palanquero a la orilla del río principal del país, el Río Magdalena. La unidad fue establecida en 1933 y fue el primer CACOM en recibir aviones de caza jet: F-86, Mirage, y Kfir. Es conocido en la FAC como “La Casa del Piloto de Caza”. Solo ‘la crema’ de los pilotos de la FAC, los más experimentados en aviones de caza, son asignados a Palanquero. Se disponen de dos escuadrones de combate, un escuadrón de transporte, y un escuadrón de entrenamiento. Para ser destinado a volar Kfir o Mirage en CACOM-1, un piloto tiene que haber volado otro avión de combate varios años. Lo normal es que sus pilotos tengan experiencia previa en el A-37, OV-10, o A-29.

En el 2007, el Ministro de Defensa aprobó la adquisición de 24 Kfir C-10/12 modernizados por la *Israeli Aircraft Industries* (IAI) para ser basados en Palanquero. En el acuerdo, la FAC le devolvió toda su flota de Mirage-V y Kfir a IAI para que ésta le entregara a la FAC 24 Kfirs modificados a la configuración C-10 o C-12; el C-10 completo con radar integrado y misiles modernos de guía de radar e infrarrojo (IR por sus siglas en inglés). La adquisición de los nuevos Kfirs representó un paso gigantesco hacia adelante para la FAC y un desafío logístico y de entrenamiento enorme para CACOM-1. En el 2009 recibieron los primeros Kfir modernizados. Para los primeros meses del 2011 la entrega fue completa.

Génesis de la idea de participar en Red Flag

Participar en *Red Flag* ha venido siendo el sueño de los pilotos de la FAC por dos generaciones de pilotos de caza. Sin embargo, la idea de que la FAC realmente pudiera asistir fue propuesta por primera vez en el 2009 en conversaciones entre el Comandante de la FAC (COFAC), Mayor General Jorge Ballesteros y el liderazgo de la Misión Aérea de los EE.UU. en Colombia (MUSAF), el Coronel USAF Kris Skinner y el Teniente Coronel (Tcnel) Chuck Gerstenecker. La idea era que CACOM-1 pudiera realizar el potencial máximo de los nuevos Kfirs a través de prepara-

ción y participación en el ejercicio *Red Flag*. Con los nuevos Kfirs, dotados con radar integrado y misiles modernos de guía de radar e IR, la FAC estaba entrando al mundo de aviones de caza de la cuarta generación. Preparándose, desplegándose, y participando exitosamente en *Red Flag* con otros aviones de la cuarta generación le traería beneficios duraderos y hasta transformacionales a la FAC; aumentándole la capacidad operacional e incrementando su interoperabilidad con aliados.

Aunque el sueño de *Red Flag* era muy incierto en el 2009, la propuesta requería consideración seria de los varios desafíos. Había por lo menos tres: 1) Un programa de entrenamiento operacional masivo sería necesario para preparar a los pilotos para *Red Flag* con fuerzas aéreas que por años han dispuesto de aviones de la cuarta generación. 2) Dado los requerimientos muy estrictos de conocimiento del idioma inglés impuestos por *Red Flag*, se tendría que montar una campaña intensiva de instrucción del idioma inglés para que los pilotos participantes pudieran alcanzar la nota mandataria de “85” en el examen de inglés de la USAF. 3) Considerando las demandas de la guerra actual en Colombia, asegurar el presupuesto necesario de entrenar para *Red Flag*, luego desplegar más de cien efectivos de la FAC (pilotos y técnicos), ocho aviones Kfir, y dos tanqueros de Colombia a la Base Nellis en EE.UU. debería requerir un milagro.

Aunque los presupuestos fueran apretados y los requerimientos del inglés fuertes, la preparación operacional parecía el reto más formidable. *Red Flag* es intencionalmente diseñado para que las tripulaciones confronten una amenaza intensiva en el aire y en la tierra. Dos escuadrones de aviones de combate de la USAF en Nellis, volando el F-15 y el F16, se dedican a ser Agresores y simulan amenazas de la cuarta generación. Además, *Red Flag* cuenta con docenas de emplazamientos en tierra que simulan sistemas de SAM y AAA, los cuales, trabajando en conjunto con los Agresores, son expertos en defender su espacio Rojo contra los invasores visitantes de la Fuerza Azul. ¿Podrían los pilotos del CACOM-1 entrenarse lo suficiente como para operar en este ambiente?

La evolución del avión de caza se ha desarrollado en varias generaciones según la sofisticación de los sistemas abordo y la amenaza presentada por sus adversarios. Cada generación demandaba al piloto tener destreza con nuevos sistemas, manipular más sensores, e incrementar el nivel del conocimiento situacional.

Aviones de la primera generación se dotaban con cañones y bombas manuales, sin radar. Así eran los aviones de caza durante la Primera Guerra Mundial y hasta los años 50.

La segunda generación traía misiles de guía IR de aspecto de cola durante los años 50 y 60. El piloto podía atacar al adversario fuera del alcance del cañón, pero solo desde la cola.

En los años 70 y 80, la tercera generación vio la incorporación del radar de búsqueda y rastreo integrado, misiles IR de todo aspecto, misiles guiados por el propio radar del avión, misiles guiados aire-tierra, y receptores de radar para alertar al piloto del rastreo del radar del enemigo. Estos sistemas nuevos le aumentaron bastante el trabajo al piloto, sin embargo le ofrecieron conocimiento situacional aumentado y lo hicieron sumamente más eficiente.

En los años 90 aparecieron aviones de la cuarta generación con misiles guiados por su propio radar, bombas guiadas por satélite, conexiones entre pilotos y controladores por ‘*data link*’, y fusión de información.

En el 2009, a medida que recibían sus nuevo Kfirs (aviones de la cuarta generación) y a pesar de su vasta experiencia en combate, los pilotos del CACOM-1 todavía operaban sólidamente en la segunda generación. ¿Podrían estos pilotos efectuar el salto de la segunda generación hasta un *Red Flag* de la cuarta generación en el tiempo disponible? ¿Estarían dispuestos a dedicarse al programa de entrenamiento necesario, mejorar su inglés, y todo el tiempo cumplir con las demandas de las operaciones corrientes? ¿Podría el COFAC obtener el presupuesto necesario para realizar todo esto? Había dudas.

El Estado Mayor de la FAC analizó estas preguntas con la debida seriedad. Todos los Generales de la FAC estaban motivados a enfrentar los retos. Se tomó la decisión de proceder. El COFAC

oficialmente solicitó a la USAF la oportunidad de participar en *Red Flag*. La USAF aprobó la participación de la FAC para el ejercicio *Red Flag* 12-4 en julio de 2012; con la condición de que la FAC pasara una evaluación operacional administrada por la USAF. La fecha fue marcada. El compromiso fue hecho. ¡Se empezó la carrera!

Una gran variedad de aviones de combate con distintas misiones participarían en *Red Flag* 12-4. Además de los Kfirs y tanqueros de la FAC, la USAF enviaría un escuadrón de F-15C para el rol aire-aire, dos escuadrones de F-16CJ para supresión de las defensas aéreas enemigas (SEAD por sus siglas en inglés), un escuadrón de F-15E, unos bombarderos B-1B, y B-52H en el rol de ‘*striker*’ (bombardear el blanco), unos KC-135 para reabastecimiento aéreo, y un E-3C para comando y control en el aire (AWACS). La Armada de EE.UU. aportaría unos EA-6B para supresión electrónica. La Fuerza Aérea de los Emiratos Árabes Unidos tendría varios F-16C, también en el rol de ‘*striker*’. Los Kfirs colombianos participarían también como ‘*strikers*’. En total, 62 aviones de combate formarían la Fuerza Azul. Defendiendo el espacio de *Red Flag*, de 12.000 millas cuadradas, contra el ataque de los Azules sería la misión de 16 Agresores (F-15C y F-16) de la USAF pintados de colores camuflados.

El COFAC montó una campaña de ‘*lobby*’ impresionante al Ministro de Defensa para asegurar los fondos para *Red Flag*. Los puntos claves para venderle la idea eran: la oportunidad para aumentarle el prestigio y confianza de las tripulaciones de la FAC, demostrarle al mundo la capacidad operacional de la FAC, y mejorar la interoperabilidad con aliados importantes. El Ministro le dio luz verde y se comprometió proveer los fondos requeridos. Para finales del 2009, el General Tito Pinilla, Jefe de Operaciones de la FAC, mandó desarrollar un plan de entrenamiento para *Red Flag*.

En noviembre de 2010, el Brigadier General Carlos Bueno fue ascendido a Comandante del CACOM-1. El Gen Bueno, uno de los pilotos de combate más experimentados de la FAC, fue el oficial apropiado para llevar CACOM-1 a *Red Flag*. Evaluó a sus pilotos, de acuerdo a la experiencia en vuelo y pericia en inglés. Tomó la decisión difícil de seleccionar su equipo de pilotos de *Red Flag* y ordenó que estos pilotos se dedicaran exclusivamente al entrenamiento de *Red Flag* y mejorar el idioma inglés.

En septiembre de 2011, el General Pinilla fue confirmado como el nuevo COFAC, con el General Flavio Ulloa como Vice Comandante. Ambos, pilotos de caza y ex-comandantes del CACOM-1, dieron su apoyo total a la participación en *Red Flag*.

La USAF también se puso a la orden para ayudar en las preparaciones. Según las reglas de la USAF, aquellas fuerzas aéreas aliadas que deseen participar en *Red Flag* tienen que pasar por una certificación operacional. Administrar la certificación era responsabilidad de la Duodécima Fuerza Aérea (12th AF) ubicada en la Base Aérea Davis-Monthan en Tucson, Arizona. Le tocaba a la MUSAF en Bogotá ayudarle a CACOM-1 a prepararse para la certificación operacional. Su



Brigadier General Carlos Bueno, FAC

nuevo jefe, el Coronel (USAF) Hans Palaoro, quien tenía bastante experiencia con *Red Flag*, coordinó el apoyo de la USAF con CACOM-1 y la 12th AF. Estableció el plan de apoyo de la USAF que incluía los siguientes elementos: entrenamiento en inglés, preparación en los procedimientos estándares para las tripulaciones de tanqueros, adiestramiento para los pilotos en las reglas de entrenamiento de *Red Flag* y operaciones con controladores aéreos (GCI) y procedimientos específicos de la línea de vuelo de *Red Flag* para técnicos de mantenimiento. El Coronel Palaoro coordinó las visitas a Palanquero de una docena de equipos de entrenamiento móvi-

les de la USAF y ayudó con la planificación de tres ejercicios del empleo aéreo realizados por CACOM-1 en preparación para la certificación operacional.

Todo personal de la FAC, el Ministro de Defensa, y hasta el señor Presidente se contagiaron con la “fiebre *Red Flag*”. En la primera semana de noviembre del 2011, la semana antes de la celebración anual del “Día de la Fuerza Aérea”, después de más de dos años de preparación, CACOM-1 completó la certificación requerida para participar en *Red Flag*. No solamente pasaron el examen, sino que lo hicieron en forma impresionante.

El día 8 de noviembre el Presidente de la República, Juan Manuel Santos, manifestó durante la celebración:

“El día de ayer se celebró un examen también muy riguroso, y en ese caso el examen se le hizo a nuestra Fuerza Aérea: resulta que en Las Vegas se celebra un concurso, una competencia, de las mejores fuerzas aéreas del mundo entero. Los escuadrones de combate de esas fuerzas aéreas son invitados a concursar en esa competencia. Pero no todo el mundo puede ir. Tienen que cumplir con unos requisitos mínimos para ser aceptado en la competencia. Se llama Red Flag. Resulta que por primera vez en la historia de la Fuerza Aérea Colombiana, la Fuerza Aérea fue invitada a concursar en esa competencia. Pero antes tenía que pasar unos exámenes. Y aquí vinieron oficiales de la Fuerza Aérea de los Estados Unidos a hacerles el examen. Y el resultado, y no me sorprende, de ese examen en todos sus frentes, y la calificación que le dieron a la Fuerza Aérea Colombiana, fue sobresaliente.”

Preparación para Red Flag



“Somos la Fuerza, Red Flag 2012”

En Palanquero diseñaron un nuevo parche para ser usado por todo personal de la unidad, no importa si formaban parte o no del equipo Red Flag. El parche, símbolo del trabajo en equipo requerido para el éxito en *Red Flag*, tenía un tanquero rodeado por cuatro Kfirs en formación, todo bajo la inscripción: “Somos la Fuerza, *Red Flag* 2012.” El parche serviría para motivar a la gente. No obstante, necesitarían mucho más que un nuevo parche para inspirar al personal a asumir la carga tan ardua que tenían por delante.

Los desafíos para el General Bueno, nuevo Comandante de la unidad, le pesaban.

1. Preparar 18 pilotos de Kfir, seis pilotos de tanqueros, y más de 80 técnicos de mantenimiento y logística para desplegar ocho aviones Kfir y dos tanqueros en un vuelo intercontinental de siete horas a los EE.UU.
2. Establecerse en su nuevo hogar y operar bajo reglas y procedimientos desconocidos.
3. Despachar una formación de cuatro Kfirs y un tanquero dos veces al día (uno de día y la otra de noche), cumpliendo 19 misiones con otros aviones de combate de la cuarta generación, dentro del ambiente táctico arduo con la amenaza más alta que habían visto, bajo reglas de entrenamiento estrictas y recuperar los aviones al final de la misión.
4. Extraer el máximo aprendizaje posible para los pilotos y técnicos.
5. Lograr todo lo anterior en un idioma extraño, inglés.

Desarrollaron una estrategia de entrenamiento que se concentraba en tres áreas principales: inglés, preparación para los pilotos de Kfir, y preparación para las tripulaciones de tanquero.

Las reglas de la USAF dictan que todas las tripulaciones de fuerzas aéreas aliadas tienen que lograr una nota mínima de “85” en el venerable examen *English Comprehension Level* (ECL por

sus siglas en inglés). Para mejorar su nivel de inglés, con la ayuda de la MUSAF, la FAC consiguió doce puestos en el curso de ‘Terminología Especializada de Aviación’ en el *Defense Language Institute, English Language Center* de la USAF (DLI por sus siglas en inglés) en la Base Aérea Lackland en San Antonio, Texas. En noviembre de 2009, se enviaron doce pilotos, dos a la vez. Para acelerarle el mejoramiento, instructores civiles de inglés de DLI y de la MUSAF se desplegaron a Palanquero para trabajar tiempo completo con los pilotos. No cabía duda de que los pilotos y los controladores aéreos tomaban muy en serio el reto del inglés. El General Bueno declaró la política “solo inglés” para su equipo *Red Flag* durante el año entero antes de *Red Flag*. Comenzando en mayo de 2011, todos los *briefings* de vuelo, *debriefings*, y comunicaciones en vuelo tenían que efectuarse solo en inglés.

El entrenamiento de vuelo era aun más riguroso que lo del inglés. Cada piloto de Kfir cumplió un curso de seis fases. Tres pilotos de caza de la USAF, instructores y especialistas en el entrenamiento táctico de caza, se desplegaron secuencialmente a Palanquero para ayudar a los pilotos con el curso. Vino el Tte Cnel Patrick “*Ichi*” Karg, de mayo a septiembre de 2011. El Tte Cnel James “Red” Barron de la 12AF, de octubre de 2011 a marzo del 2012. Finalmente, el Mayor James “Crashin” Byrne, de abril a julio de 2012 y luego acompañó al equipo *Red Flag* a la Base Nellis. Los tres dictaban clases y volaban en la cabina trasera de los Kfir. Fueron claves en ayudarles a los pilotos a dominar su nuevo radar y sistemas de misiles en los roles de aire-aire y aire-tierra que iban a tener que ejecutar en *Red Flag*. Además de los tres pilotos instructores, otros especialistas de mantenimiento y logística visitaron a Palanquero para adiestrar a los técnicos en los procedimientos de la línea de vuelo de *Red Flag*.

Los pilotos de CACOM-1 tenían bastante experiencia en la misión aire-tierra. Pero eran novatos en cuanto a la misión aire-aire. Aprender a usar la terminología y procedimientos de radar de la USAF les fue un tremendo reto. Con cientos de frases y pasos para asimilar en corto tiempo, tanto los pilotos como los instructores frecuentemente se sentían frustrados. El Tte Cnel “*Ichi*” perseveró. El Mayor Hedin “*Tornado*” Vargas de la FAC describió su frustración y su éxito:

“Cuando empezamos a volar, para nosotros todo esto era una locura, nos sentimos en el piso, perdidos. Cuando llegamos a la casa en la noche pasábamos horas estudiando y repasando. Jamás se nos hubiera pasado por la cabeza que hubiese tanta información en este tipo de entrenamiento. Sin embargo, ” Ichi” nos persistía. Entonces, la primera vez que hubo un enfrentamiento positivo en una misión, y pudimos entablar con el radar, y pudimos cumplir con el ‘timeline’, “Ichi “nos dijo: ‘¡No lo puedo creer!’. Dos lágrimas salieron de sus ojos.

Un aspecto crítico para *Red Flag* es la necesidad de que los pilotos trabajen en equipo con los controladores aéreos (GCI por sus siglas en inglés). En vista de que el espacio aéreo del norte de Colombia facilita mejor la coordinación con GCI, en enero de 2012 los pilotos y los controladores del CACOM-1 se desplegaron a la base del CACOM-3 en Barranquilla y pasaron allá los últimos seis meses entrenándose antes de ir a *Red Flag*. En el espacio aéreo adyacente a la base, con la ayuda del personal de la MUSAF, quienes conocen el espacio aéreo de *Red Flag*, arreglaron lo que llamaban el espacio aéreo “*Nellis North*”, completo con los GCI, con el fin de simular el espacio aéreo de *Red Flag*.

Otro aspecto muy exigente de *Red Flag* son los procedimientos de tierra, despegue, salida al área de trabajo, y regreso a la base. La Base Nellis es muy congestionada y los pilotos participantes de *Red Flag* al regresar a la base normalmente tienen necesidad urgente de aterrizar por bajo nivel de combustible. Es preciso que todos cumplan con procedimientos rígidos en su navegación de ida y vuelta al área de entrenamiento ubicada unos minutos al norte de la base. Sacándole provecho a la última tecnología informática, los cadetes de la Escuela de Oficiales de la FAC en Cali fabricaron simulacros de vuelo y carreteo para la Base Nellis y el espacio aéreo de *Red Flag*. Los pilotos del equipo *Red Flag* pasaron varios días practicando los procedimientos de la

Base Nellis de prender motores, carreteo, salida, y aproximación; simulando en inglés comunicaciones con los controladores aéreos. Gracias a los cadetes de la FAC tan tecnológicamente avanzados, el equipo *Red Flag* fue bien preparado para cumplir con todos los procedimientos de la Base Nellis y el resultado fue que no cometieron ninguna desviación durante *Red Flag 12-4*.

Los tripulantes de tanqueros de la FAC tenían considerable experiencia reaprovisionando a aviones de combate sobre Colombia durante años de operaciones reales. No obstante, para realizar reaprovisionamiento en vuelo durante *Red Flag*, un requisito en cada misión, los tripulantes de los tanqueros serían obligados a cumplir con el estándar de la OTAN. Este estándar se encuentra dentro del Manual de la OTAN ATP-56, un libro colosal de 500 páginas escrito en inglés técnico. Enviarían ambos de sus tanqueros a *Red Flag 12-4*: el venerable KC-137 “Zeus”, que había servido muchos años en un sinfín de misiones, y el recién adquirido KC-767 “Júpiter”, que transportaría la mayoría del equipo logístico a Nellis. A pesar del difícil inglés técnico del Manual de la OTAN y el choque de cultura ocasionado por la necesidad de adaptarse a la manera que la OTAN trabaja en situaciones en las que ya son expertos, los seis pilotos de tanqueros estudiaron largas horas y asimilaron exitosamente el Manual ATP-56. Sus esfuerzos fueron recompensados cuando, juntos con los pilotos de Kfir, pasaron la certificación de la USAF la primera semana de noviembre de 2011.

Finalmente, para mostrarse listos para ir a *Red Flag*, los pilotos de los tanqueros Júpiter y Zeus llevaron al grupo entero a un despliegue de ensayo en marzo de 2012. Durante el llamado “*fighter drag*” los tanqueros reaprovisionaron a los ocho Kfirs múltiples veces durante un vuelo de seis horas de Palanquero rumbo norte sobre el Caribe, luego al sur por Panamá y de vuelta a Cali, donde desempacaron los equipos y se establecieron como si hubieron llegado a la Base Nellis. Junto con pasar la certificación de noviembre de 2011, el “*fighter drag*” les dio a todos una sensación de confianza.

El programa de preparación fue suficientemente difícil por si solo sin las complicaciones agregadas por la Madre Naturaleza. El personal del CACOM-1 sufrió un desastre natural extraordinario en medio de sus preparaciones para *Red Flag*. El Rio Magdalena tiene una historia larga de inundaciones. La base en Palanquero fue construida pocos metros por encima del nivel normal del rio. En noviembre de 2008 lluvias torrenciales provocaron que el rio inundara la base. El sistema de diques y muros del que se disponía para detener el agua fue sobrepasado. Después de recuperarse, en el 2009, CACOM-1 reforzó el sistema con diques más profundos y muros más altos. Sin embargo, en abril de 2011, con el personal afanadamente involucrado en el programa de *Red Flag*, las inundaciones peores de toda la historia azotaron a Palanquero. En la zona de vivienda de la base todo fue perdido. Se sumergió la pista, la mayoría de la zona operacional fue inundada, y la base estuvo fuera de servicio varias semanas. En medio de prepararse para realizar su sueño, a varios pilotos se les perdió todo. Afortunadamente, no hubo heridos. Pese al golpe de la Madre Naturaleza, el personal no se detuvo. Cuando el agua se retiró, la preparación para *Red Flag* comenzó de nuevo arduamente.

Otro desafío afrontado por CACOM-1 fue su falta de personal. La FAC, como muchas fuerzas aéreas, no dispone de todo el personal requerido para cumplir con las exigencias impuestas sobre ella. El piloto típico desempeña varios cargos adicionales no relacionados con el vuelo. Sin embargo, el General Bueno le ordenó a su equipo *Red Flag* a dedicarse exclusivamente a la preparación para *Red Flag*. Esto les obligó a los oficiales y suboficiales logísticos y administrativos cargar responsabilidades anteriormente asignadas a los pilotos del equipo *Red Flag*. La selección del equipo *Red Flag* efectivamente dividió la unidad en dos grupos: los que iban y los que no iban. Se creó resentimiento dentro de la unidad, especialmente porque el peso de las operaciones diarias del CACOM-1 tuvo que ser realizado por un grupo de oficiales y suboficiales más pequeño que antes: los que no iban a *Red Flag*. Pero aún, muchos de los pilotos más experimentados no fueron seleccionados debido a su bajo nivel de inglés. El General Bueno acabó con el resentimiento entre su personal enfatizándoles que *Red Flag* representaba un compromiso por

todo el personal del CACOM-1; los que iban y los que no iban. La buena reputación de la unidad estaba en jaque y todos deberían trabajar juntos para asegurar el éxito del CACOM-1 y de la FAC.

En noviembre de 2011 cuando superaron la certificación, el General Bueno para celebrar este acontecimiento ofreció una fiesta para toda la base. Extremadamente orgulloso de su gente por su tremendo esfuerzo, el General delineó varios objetivos para el despliegue a *Red Flag*. No sería una cuestión de ‘ganar’ *Red Flag*, si no se trataría de aprender interoperabilidad, nuevas tácticas, y demostrar el profesionalismo de la FAC. Enfatizó a sus pilotos que, a pesar de su afán de exponer sus destrezas con los sistemas de armas de la cuarta generación, también tendrían que ser profesionales en su empleo. Demostrarían buen juicio en todo momento, en la tierra y en el aire. Operarían sus aviones siempre de manera segura. Tampoco incurrirán casos de fratricidio ni violaciones de las ‘reglas de entrenamiento’ de *Red Flag*. Al final, el General tenía toda confianza en sus pilotos.

La experiencia de Red Flag

La flotilla de dos tanqueros, ocho Kfirs, y 130 efectivos partieron de Palanquero el 29 de junio de 2012. El 2 de julio llegaron a la Base Davis-Monthan en Tucson, Arizona. Permanecieron en Tucson seis días mientras los pilotos recibían instrucciones finales de los procedimientos de *Red Flag*. El viernes 13 de julio, llegaron a la Base Nellis. Descargaron los equipos de “Júpiter” y “Zeus”, estacionaron los Kfirs en la rampa de *Red Flag*, y se posesionaron de sus instalaciones operacionales y logísticas.

El Mayor Oscar “Zero” Sánchez fue seleccionado como líder de la formación para la primera misión de la FAC, llevando el ‘callsign’ del CACOM-1, “Rocket 41”. Normalmente, en *Red Flag*, la meteorología normal es de cielos despejados con visibilidad ilimitada. Con tantos aviones involucrados, el mal tiempo crea confusión y obliga a los líderes de formaciones ejercer buen juicio. El primer día de *Red Flag* 12-4 fue uno de los días de mal tiempo. Afortunadamente, “Zero” dirigió Rocket 41. Iban a ser los primeros de la Fuerza Azul en llegar al blanco. A pesar de tener un plan muy preciso, las cosas comenzaron a cambiar para Rocket 41 antes del despegue. El tanquero Júpiter se canceló debido a un problema del motor. El Comandante de la Fuerza Azul anunció un ‘rolex’, una demora de varios minutos. “Zero”, después de calcular su combustible, llevó su formación al aire confiado en su habilidad de hacer funcionar el plan del Comandante a pesar de los cambios. Al llegar al espacio aéreo de *Red Flag* encontró un tiempo peor de lo que se esperaba. Escuchó por la radio que el avión controlador, AWACS, había regresado a la base. Dándose cuenta de que confrontaba combustible escaso, mal tiempo, y ausencia del AWACS, “Zero” se acordó de la directiva del General Bueno sobre el buen juicio. Tomó una decisión de mando: retornó su formación temprano a Nellis donde aterrizaron sanos y salvos. Los demás pilotos de la Fuerza Azul que continuaron hacia el área del trabajo fueron obligados a abortar sus misiones minutos después. La decisión de “Zero” de regresar temprano impresionó al Estado Mayor de *Red Flag*. Consideraban que “Zero” mostró una madurez pocas veces vista entre pilotos participando por primera vez en *Red Flag*.

El Mayor Hedin “Tornado” Vargas fue seleccionado para liderar a Rocket 41 la próxima tarde. “Tornado”, comandante de uno de los escuadrones de combate del CACOM-1, estuvo en el grupo original de pilotos que se calificó en el nuevo Kfir. Debido a su experiencia en el avión y su conocimiento del inglés, resultó ser fácil seleccionar a “Tornado” para el equipo *Red Flag*. Fue el primero enviado a DLI para el curso de inglés de aviación. Se graduó con notas altas y al regresar a Palanquero trabajó con sus compañeros para mejorarles el inglés. Había sido seleccionado para el Curso de Comando y Estado Mayor de la FAC en el 2010, curso que duraba un año. El curso es obligatorio para el acenso a Teniente Coronel. A pesar de la posibilidad de perder el

ascenso, “*Tornado*” rechazó el curso a favor de quedarse en Palanquero entrenándose con sus compañeros del equipo *Red Flag*. Fue una excelente decisión.

El día antes de la misión “*Tornado*” dirigió la formación Rocket 41 por el proceso de planeamiento: estudiar fotos del blanco, reunirse con el comandante de la misión y el *pre-briefing*. El día de la misión el *briefing* principal empezó tres horas antes del primer despegue. Asistieron más de 300 personas en el famoso auditorio principal de *Red Flag*. Estuvieron presentes las tripulaciones, controladores, monitores de seguridad, operadores de los sistemas de rastreo y miembros del siempre vigilante Estado Mayor de *Red Flag*. Las paredes estaban llenas de las placas de cientos de escuadrones de vuelo de los EE.UU. y países aliados participantes de ejercicios de *Red Flag* anteriores. Durante el *briefing* principal el Comandante de la Fuerza Azul recalcó el plan táctico. Más de 60 aviones de la Fuerza Azul se desprenderían de sus órbitas en el este, irían a atacar docenas de blancos en el oeste, y luego regresarían a su zona segura en el este. El plan dependía de la sincronización de todos los elementos de la Fuerza Azul: tanqueros, contra-aire, SEAD, escolta, y ‘*strikers*’. Rocket 41 iba lejos, al lado extremo oeste del territorio Rojo. Serían los primeros ‘*strikers*’ en salir de la órbita y atacarían tanques enemigos detrás de la línea de batalla, lanzando bombas de 500 libras. Los tanques estaban camuflados para el desierto. No serían fáciles de descubrir. Los integrantes de Rocket 41 salieron del *briefing* entendiendo el plan y con confianza en su capacidad de ejecutar su parte.

Prendieron motores y carretearon según el plan. “*Tornado*” prestó atención completa al plan de rodaje para asegurar que colocara a Rocket 41 en la posición correcta. Si una formación carretea fuera de la posición especificada, la consiguiente confusión puede afectar el plan entero. Había que ser preciso en todo. Los diferentes acentos de inglés que tenían los pilotos en la radio le dificultaban el trabajo a “*Tornado*”. Él se esforzó para entender todo y mantener el conocimiento situacional.

Rocket 41 carreteo a tiempo y en el orden correcto. Pasaron por el chequeo final donde se armaron las bombas y recibieron autorización para tomar la pista. Se alinearon en formación escalón en la pista, listos para decolar. Autorizados, los pilotos despegaron individualmente con 30 segundos de separación. Rugieron sus posquemadores mientras los Kfirs, tan pesados con bombas y combustible, saltaron al aire caliente del desierto. “*Tornado*” dirigió su formación a su punto de órbita, ubicó a sus pilotos en formación, y esperó para el momento de desprenderse.

Una falla súbita de comunicaciones a bordo del AWACS hizo que todos los de la Fuerza Azul operaran en la misma frecuencia de radio. Había tanta bulla en la frecuencia que “*Tornado*” no podía entender, a pesar de haber dominado la terminología requerida durante sus años de preparación para *Red Flag*. Se mantuvo tranquilo e hizo salir a Rocket 41 del punto de órbita a tiempo, con rumbo al oeste, cruzando las 100 millas náuticas de desierto, montañas, SAMs, AAA, y Agresores que separaban su formación de su blanco.

A media ruta “*Tornado*” bloqueó un ‘*bogey*’ con su radar: a las doce por 15 millas náuticas, probablemente un Agresor. Sin una identificación positiva “*Tornado*” resistió la tentación de atacar y no le disparó, recordando la directiva del General Bueno de evitar el fratricidio. Sesenta segundos después, pasó a toda máquina un Agresor bajo la formación y en sentido opuesto. No había tiempo para preocuparse. Estaban aproximándose al blanco.

Después de 15 minutos del ingreso, que parecieron una eternidad, “*Tornado*” picó su Kfir desde 15.000 pies hacia el blanco. Por cinco segundos largos buscaba la línea de tanques enemigos en el desierto cuyas fotos había escudriñado por más de una hora el día antes. Tan pronto como los pudiera identificar pondría su mira “*CCIP death dot*” encima del centro del tanque. Lamentablemente, los tanques estaban invisibles, camuflados contra el desierto. Al acabarse los cinco segundos con su Kfir en picada, “*Tornado*” por fin los detectó. ¡Era demasiado tarde! En vez de arriesgar sobre picar su avión y entrar en una situación peligrosa, pasó en seco. Recuperando su Kfir marcó el blanco por la radio para sus compañeros detrás. Sin pensarlo en el momento, “*Tornado*” había cumplido la directiva primordial de su jefe, demostrando la madurez de un avia-

dor táctico experimentado. Al pasar en seco evitó una situación peligrosa clásica que ha atrapado muchos pilotos de caza. Pilotos menos experimentados en la misma situación, afanados de lanzar sus bombas, han forzado sus aviones hasta actitudes peligrosas y muchos han pagado con sus vidas.

Saliendo del blanco, de inmediato la formación Rocket 41 encontró un *'furball'* a las doce por 10 millas náuticas; una colección de aviones, amigos y enemigos, todos enfrentados en una pelea. Con la radio totalmente saturada, *"Tornado"* no pudo obtener la identificación necesaria para determinar quién era quién, y aunque fue tentado, no disparó sus misiles, evitando otra vez el posible fratricidio. En vez de detenerse a pelear, *"Tornado"* dirigió su formación a máxima velocidad para su zona segura, desviando el *'furball'*. Un líder menos experimentado, de pronto hubiera atacado, probablemente resultando en la pérdida de uno o más de sus integrantes.

"Tornado" llevó a Rocket 41 de vuelta a Nellis donde los pilotos se dirigieron a la pista y aterrizaron. Después de una misión tan intensiva, en la cual le parecía que se habían esforzado todos los músculos y células cerebrales para mantener su conocimiento situacional con el fin de liderar sus compañeros de ida y vuelta con seguridad, *"Tornado"* se relajó en la cabina mientras su Kfir rodaba al final de la pista. Sentía una tremenda satisfacción en darse cuenta que había logrado, con éxito y seguridad, lo que anhelaba poder hacer durante dos años y medio en entrenamiento fuerte. ¡Había cumplido todos los procedimientos, entendido las comunicaciones, y evitado el fratricidio! Se le formó una lágrima en sus ojos mientras salía de la pista. ¡Había realizado su sueño!

¿Cómo les fue a los Pilotos del CACOM-I?

Durante los primeros dos días del ejercicio, cuatro pilotos lideraron las misiones: *"Yahdai"*, *"Zero"*, *"Tornado"*, y el Mayor William *"Falcón"* Bello, otro comandante de escuadrón en Palenquero. Mostraron profesionalismo, buen juicio, y destreza táctica. La pauta que dejaron continuó por el resto de las dos semanas. Como el General Bueno había exigido, no hubo violaciones de las reglas de entrenamiento. Hubo cumplimiento 100% con los procedimientos, tanto en la tierra como en el aire. Tal ejecución es muy rara entre los escuadrones de la USAF con experiencia en *Red Flag* y es sin precedente entre unidades participando por primera vez, especialmente las fuerzas aéreas aliadas. El profesionalismo y madurez de los pilotos del CACOM-I impresionaron al Estado Mayor de *Red Flag*. El Coronel USAF Tod Fingal, Jefe del Estado Mayor de *Red Flag* expresó lo siguiente:

"La participación de la Fuerza Aérea de Colombia en Red Flag 12-4 fue un enorme éxito. Sus casi tres años de entrenamiento y preparación para este ejercicio seguramente rindió. Los colombianos fácilmente encontraron su ruta en este estresante entrenamiento de combate para lograr interoperabilidad con más de 1.800 participantes de tres países distintos. Son estimados compañeros y amigos".

Además del profesionalismo, los pilotos y técnicos del CACOM-I manifestaron destreza y efectividad en las operaciones y la logística. Con el apoyo dedicado de los 70 técnicos, la unidad montó un total de 63 salidas de Kfir con solo tres misiones canceladas, y 15 salidas de tanqueros con solo dos canceladas. *"Júpiter"* y *"Zeus"* juntos suplieron un total de 89.000 libras de combustible a los Kfirs, efectuando 180 eventos de reaprovisionamiento en vuelo. De los blancos asignados a Rocket41 durante el ejercicio, el 80% fue destruido. Los pilotos de Kfir lograron derribar nueve de los Agresores, un logro que nadie hubiera esperado antes del ejercicio. Durante las dos semanas se perdieron nueve Kfirs a los SAM y AAA, mientras cuatro fueron derribados por los Agresores. Todo esto resultó en un inmenso aprendizaje táctico para los pilotos. El Mayor USAF *"Crashin"* Byrne, quien los acompañó a *Red Flag*, estuvo tan complacido que exclamó:

“Estoy más orgulloso de ustedes que cuando vi a mi propio hijo dar sus primeros pasos!”

Red Flag 12-4 aumentó enormemente la confianza de los pilotos del CACOM-1. Se habían desplegado a Nellis y afrontado el reto de participar en el primordial ejercicio aéreo del mundo. Realizaron otro logro significativo también en el campo de interoperabilidad. El Coronel Palaoro, Jefe de la MUSAF, lo describió a la revista *“Dialogo”* (27 de julio de 2012).

“Durante su preparación para Red Flag los tripulantes de la FAC aprendieron y adoptaron el estándar internacional de la OTAN para el reabastecimiento aéreo, permitiendo la interoperabilidad en tanqueros con nosotros, una realidad. Adoptaron estándares de la USAF de la línea de vuelo y de reglas de entrenamiento en misiones aire-aire, y verdaderamente han demostrado su capacidad de operar de manera segura y efectiva con nosotros – totalmente integrados – dentro del ejercicio aéreo del empleo de fuerza más difícil del mundo. No podría estar yo más orgulloso de lo que han logrado, y esto representa el comienzo de una nueva fase de nuestras relaciones que ya son fuertes.”

Ahora toca considerar la cuestión de cómo los pilotos del CACOM-1 lograron hacer el ‘salto’ de operaciones de la segunda generación de aviones de combate a la participación en *Red Flag* al nivel de la cuarta generación. ¿Cómo es posible que pudieran realizar tanto progreso en sus habilidades tácticas en poco más de dos años? Su éxito se atribuye a cinco factores.

1. Los mejores pilotos de la FAC se encuentran en CACOM-1. Antes de ser asignados al CACOM-1 han logrado la excelencia en otros aviones. Lo mismo les aplica a los pilotos de tanqueros; los mejores pilotos de transporte vuelan “Júpiter” y “Zeus”.
2. Experiencia de combate. Como casi todos los pilotos de la FAC, los del CACOM-1 son veteranos de numerosas misiones de combate. Muchos han liderado paquetes de aviones de caza en misiones contra la guerrilla en Colombia. Aunque la guerrilla no representa la misma amenaza simulada en *Red Flag*, cualquier piloto confirmará que no hay nada como el combate para convertir a un piloto no experimentado en piloto experimentado. El combate obliga al piloto a ejercer buen juicio en el aire. Además, operaciones de combate en Colombia requieren reglas de entrenamiento muy estrictas para evitar los daños colaterales ya que la guerrilla muchas veces se mezcla con la población civil. Esto hizo que no les fuera tan difícil a los pilotos del CACOM-1 cumplir con las reglas de entrenamiento de *Red Flag*. Además, el General Pinilla especificó cuatro factores relacionados con el combate que ayudaron a preparar a sus pilotos.
 - a. Tecnología. El combate le ha necesitado a la FAC la adquisición y empleo de sistemas de armas cada vez más avanzados tecnológicamente: equipos de visores nocturnos, sistemas de entrega aire-tierra computarizados, y bombas de precisión.
 - b. Entrenamiento. El combate obliga a los pilotos de la FAC tomar muy en serio sus cursos de entrenamiento. Cada piloto sabe que al graduarse lo podrían enviar directamente al combate donde su vida estaría en peligro.
 - c. Fusión de operación es con inteligencia. El combate les ha enseñado a las tripulaciones de la FAC el valor de la inteligencia.
 - d. Trabajo conjunto. El combate les ha verificado a todos los servicios militares de Colombia (Armada, Ejército, Fuerza Aérea, y Policía Nacional) la importancia de operar en manera conjunta, apoyándose el uno al otro.
3. Enfoque al entrenamiento. Los pilotos del CACOM-1 entrenaron intensivamente más de dos años para realizar su sueño de participar en *Red Flag*. Diseñaron un plan de entrenamiento excelente y se dedicaron a él. Sus líderes, desde los altos niveles hasta el escuadrón, constantemente motivaban a la gente a seguir adelante. Con indisputable persistencia su-

peraron los desafíos del inglés y del entrenamiento operacional. También se le debe reconocer enormemente al personal, pilotos y no pilotos, que no fueron seleccionados a ir a *Red Flag*. Son los héroes no reconocidos que asumieron cargos adicionales para que sus compatriotas pudieran enfocarse al entrenamiento. Ojalá, que todos ellos tengan la oportunidad de participar en un *Red Flag* en el futuro.

4. Cooperación con la USAF. El Coronel Palaoro y su gente de la MUSAF, al igual que los oficiales de la 12th AF, aportaron un servicio invaluable. Abogaron para recursos de la USAF y coordinaron despliegues de personal de la USAF a Palanquero. Agradecimiento especial se les debe dar a los tres pilotos instructores de la USAF. Sin la instrucción diaria, tanto en la sala de *briefings* como en la cabina trasera ocupada por el Tte Cnel “*Ichí*” Karg, el Tte Cnel “*Red*” Barron, y el Mayor “*Crashin*” Byrne, no se habría realizado el sueño.
5. Los técnicos. Se les debe felicitar a los técnicos que preparaban, despachaban, armaban, y mantenían los aviones en vuelo, permitiéndoles a los pilotos emplearlos. La pericia de los técnicos del CACOM-1 en arreglar aviones fue obvio, al igual que su capacidad de operar en condiciones adversas e integrarse con los técnicos de la USAF. La temperatura en la rampa durante la tarde a veces alcanzaba los 50° C. El éxito de los pilotos fue fundado sobre el trabajo duro y sacrificio de los técnicos de mantenimiento y logística. El General Bueno describió su trabajo

“La otra parte bien importante son los técnicos quienes han trabajado muy duro. Les expliqué lo que estaba pasando y en que consistía el escenario. Les dije que los demás están mirando de qué está hecho un técnico colombiano, y si tiene la capacidad de sacrificio para cambiar un tanque de combustible en un sol de 50 grados. Todo el mundo le metió un corazonazo y no más orgulloso me puedo sentir.”

El valor de Red Flag 12-4 – El futuro

Con CACOM-1, la FAC realizó su sueño de participar en *Red Flag*. Sin embargo, para la FAC y el CACOM-1, *Red Flag* será más que tan solo un sueño, será transformacional. Resultará en una nueva visión, más amplia para la FAC. El Mayor “*Falcón*” Bello dio eco a los sentimientos de sus colegas, resumiendo la importancia transformacional del ejercicio para la FAC dijo:

La participación de la FAC en Red Flag 12-4 “...es una forma de transmitir un mensaje... que Colombia tiene una fuerza aérea profesional, una fuerza aérea que se ha venido inicialmente construyendo en su conflicto interno y que gracias a esta interacción con la Fuerza Aérea de los EE.UU. hemos llegado a una madurez para poder integrarnos con una coalición. El aprendizaje de todos los que estamos acá es de transformar nuestra fuerza porque realmente Red Flag es un punto de transformación. Al igual que todos, me siento muy orgulloso y comprometido a que en el futuro cercano no solamente el escuadrón de los Kfirs esté a este nivel, sino que toda la Fuerza Aérea en todas sus misiones de transporte, de combate, de CSAR, esté bajo estos estándares de integración y sincronización.”

El General Bueno resumió la esencia de lo que la FAC tomó de *Red Flag*:

“Red Flag no se trata de un campeonato, no es de ganar o perder, sino de aprender, aprender todo lo más que se pueda, de volar con seguridad, de que nuestros pilotos descubran este inmenso mundo de posibilidades que tiene la aviación de combate que es un arte, una ciencia, que requiere mucha dedicación y que todo lo que nosotros podamos extraer de esa experiencia es poco. Se trata de sobresalir. Sobresalir en la ejecución de normas y procedimientos en los que fuimos seguros, profesionales y respetuosos. Nuestra fuerza aérea con el escuadrón Kfir y el escuadrón de tanqueros buscó estar a la altura de las mejores

fuerzas aéreas del mundo para garantizar en el futuro la interoperabilidad y que esas fuerzas aliadas se sientan orgullosas y confiadas de trabajar con nosotros.”

Refiriéndose a sus pilotos y su futuro rol como líderes de la FAC el General agregó:

“Estos pilotos son los futuros líderes de la FAC. Como resultado de su participación en Red Flag tendrán una visión global, no solamente una visión regional.”

Hablando de visión, el General Pinilla, como COFAC, ofrece una visión para lo que su fuerza aérea puede ser. Sus tres metas:

1. *“Ser capaces de ganar nuestra guerra interna.”*
2. *“Ser una de las fuerza aéreas más operacionales de América Latina.”*
3. *“Ser interoperables con nuestros amigos.”*

El General Pinilla cree que esta primera participación en *Red Flag* contribuirá significativamente a sus metas. Está justificablemente orgulloso de lo que ha hecho su gente. Enfatiza los logros de su equipo de tanqueros: *“Puedo contar que ya hoy la FAC es interoperable en tanqueros. Debido a la preparación para Red Flag ya tenemos certificación en la regla de la OTAN sobre ‘air refueling’ ATP-56, el requerimiento de operar en las grandes ligas de los tanqueros.”*

El General Pinilla está seguro que *Red Flag 12-4* es meramente el punto de partida para la colaboración continua de la FAC con fuerzas aéreas aliadas de la región. Espera que la FAC participe en otros ejercicios aéreos de empleo de fuerza en la región, como: “*Salitre*” en Chile, “*CruzEx*” en Brasil, “*Maple Flag*” en Canadá, y “*Green Flag*” en los EE.UU. También, espera que la FAC regrese a *Red Flag* en un futuro muy cercano.

El 30 de julio de 2012 los primeros Kfirs llegaron de vuelta a Palanquero, gracias a varios abastecimientos aéreos de “*Júpiter*” y “*Zeus*”, con el General Bueno dirigiendo la formación. Con todo éxito el General había liderado a CACOM-1 durante el primer despliegue operacional al extranjero de la FAC. Antes de aterrizar, los Kfirs hicieron varias pasadas triunfales sobre la audiencia que los esperaba abajo. En la tierra los pilotos fueron recibidos como héroes por líderes militares y gubernamentales. Tomaron tiempo para gozar de su significativa hazaña con sus familias y amigos. Se dieron cuenta de que por participar en *Red Flag 12-4* no solamente realizaron el sueño de todos los pilotos de la FAC, sino que también dieron un paso gigantesco hacia el cumplimiento de la visión del General Pinilla. □



El Coronel Kris Skinner, (USAF-Ret.) se retiró el 1ro de junio del 2012 después de treinta años de servicio activo. Recibió su comisión en la USAF en 1981. Fue piloto de F-16 por más de veinte años. Se graduó del Colegio de Guerra Aérea de la Fuerza Aérea de Venezuela (FAV) en 1996 y fue piloto de intercambio en el F-16 con la FAV hasta 1998. Fue comandante del 56th Escuadrón del Apoyo Operacional en la Base Aérea Luke en Arizona de 1998-2000 y comandante del 98th Grupo de Operaciones en la Base Aérea Nellis en Nevada de 2003-2005. El Coronel Skinner fue Jefe de la Misión Aérea de la USAF (MUSAF) en Bogotá, Colombia de 2001-2003 y Director del Elemento de Coordinación del Componente Aéreo de la USAF (ACCE) en Bogotá, Colombia del 2005-2010. En su última asignación se desempeñó como Secretario General del Sistema de Cooperación entre las Fuerzas Aéreas Americanas (SICOFAA) desde enero del 2010 hasta abril del 2012.

El Espectro de una Guerra no Evidente

DR. MARTIN C. LIBICKI, PHD*

LAS INNOVACIONES, tanto tecnológicas como organizativas, en las últimas décadas han creado un potencial de una guerra no evidente,¹ en la que la identidad del lado combatiente e incluso el mero hecho de la guerra son completamente ambiguos.

El gusano informático Stuxnet es solamente el ejemplo más reciente hecho público extensivamente. Se cree que este gusano ha infiltrado la instalación de centrifugas Natanz de Irán, haciendo que los equipos se destruyan a sí mismos en un período de semanas y produzcan la reducción prematura del 10 por ciento de la capacidad de enriquecimiento de uranio de Irán. Varios meses después de la divulgación pública del gusano (septiembre de 2010), las fuentes de inteligencia occidentales anunciaron que la fecha más próxima en la que Irán podía construir una bomba se había retrasado varios años. Hasta que se descubrió y examinó el gusano, los mismos iraníes no estaban seguros de la razón por la que sus equipos se desgastaban tan deprisa. De hecho, cuando se preguntó a Irán públicamente acerca de la posibilidad, primero negaron que había ocurrido dicho ataque, y dos meses más tarde dijeron lo contrario con rodeos.

Aunque la ciberguerra es el mejor ejemplo de guerra no evidente,² los estados pueden atacarse unos a otros de muchas maneras sin que la víctima sepa exactamente quién lo hizo o incluso qué se hizo. Algunas guerras, como la guerra electrónica (contra objetivos no militares) y la guerra espacial, aún no se han materializado de ninguna forma significativamente estratégica. Otros, como las minas navales/terrestres o el sabotaje, tienen largos antecedentes históricos. Lo que comparten es la ambigüedad. Entre una lista corta de tipos de guerra que *podría* llevarse a cabo plausiblemente de una manera no evidente se incluyen las siguientes

- ciberguerra;
- guerra espacial;
- guerra electrónica;
- guerra de drones;
- sabotaje, operaciones especiales, asesinatos, y minas;
- ataques de fuerzas sustitutas;
- armas de destrucción masiva; y
- respaldo de inteligencia para operaciones de combate.

La guerra no evidente ofrece un contraste claro, por ejemplo, con la invasión de carros de combate que tuvo lugar en la frontera entre Alemania y Polonia, un acontecimiento que con muy poca probabilidad planteara preguntas como, ¿qué carros de combate son esos, . . . y por qué están aquí? Por el contrario, los *usos* de guerra no evidente son limitados. Es bastante difícil capturar la capital de otro país de forma anónima (las fuerzas sustitutas pueden hacerlo pero a

*El Dr. Martin C. Libicki, PhD es un científico de gestión superior de RAND Corporation, que se concentra en los impactos de la tecnología de información en seguridad doméstica y nacional. Ha publicado *Conquest in Cyberspace: National Security and Information Warfare and Information Technology Standards: Quest for the Common Byte (Conquista en el ciberespacio: Seguridad nacional y Guerra de información y normas de tecnología de información)*, así como numerosas monografías. Anteriormente trabajó en la Universidad de Defensa Nacional, estado mayor de la Armada y la División de Energía y Minerales de GAO. El Dr. Libicki tiene un título de maestría y un doctorado de la Universidad de California–Berkeley. Este artículo fue anteriormente publicado en nuestra revista *Strategic Studies Quarterly*, Vol. 6, No. 3, Fall 2012.

esas alturas dejan de ser sustitutas y evolucionan hasta convertirse en dependientes o incluso independientes). La guerra defensiva es llevada a cabo casi siempre por el que posee lo que se defiende. Incluso la coacción requiere una autoidentificación *si* el “me” en—“no me pises”—no se comunica de forma adecuada. Pero hay algunos tipos de guerra que no se pueden llevar a cabo de forma satisfactoria o incluso de forma más ventajosa si hay duda de quién hizo qué. Nuevamente, Stuxnet constituye un ejemplo. Demorar el programa nuclear iraní benefició a Israel, tanto si alguien sabe o no con certeza si Israel (o alguien más) lo hizo. Además, si la finalidad de la guerra es hacer cambiar de ideas en la capital de la víctima, la incertidumbre puede concentrar la reflexión subsiguiente en lo que dice un ataque así sobre la seguridad y la potencia (reducida) de la víctima en vez de sobre la malevolencia del atacante sin determinar.

De forma correspondiente, este artículo explora el tema en varios pasos. Lo primero es desarrollar un sentido de lo que significa no ser evidente. Lo segundo es delinear varias formas de guerra que, en ciertas circunstancias, pueden ser no evidentes y por qué. Lo tercero es especular sobre cómo los estados (y los actores que no son estados) podrían hacer uso de la guerra no evidente. Lo cuarto es especular sobre cómo los estados víctima pueden responder a la amenaza de guerra no evidente.

¿Cuándo no es evidente la guerra?

La ambigüedad es la base de la falta de evidencia. Si la víctima no está segura de quién llevó a cabo una operación, puede tener dudas acerca de responder de la misma manera que si fuera cierto. De forma alternativa, el resto del mundo podría tener dudas incluso si la víctima tiene certeza, haciendo que la víctima se sienta insegura de responder como lo haría si *otros* estuvieran muy seguros de lo que pasa.

La falta de evidencia aumenta si los acontecimientos en cuestión pueden cuestionarse por sí mismos. Algunos podrían ser accidentes o misterios absolutos, por ejemplo, la falla inexplicable de un satélite. Otros podrían ser delitos, como robos a bancos por grupos con inclinación política, o actos de espionaje—muchos acontecimientos denominados ciberataques son realmente intentos de sustraer información. No obstante, algunos incidentes bélicos no evidentes serían claramente actos de guerra si fueran evidentes—en cuyo caso, la ambigüedad clave es el actor y no el acto.

Algunas formas de guerra no son evidentes porque la relación entre el atacante y un estado no es clara; por ejemplo, ¿en qué medida trabaja Hizbulá para sus propios fines, y en qué medida es una marioneta manipulada por Teherán? En algunos casos los perpetradores pueden ser empleados del estado que no están necesariamente trabajando, o al menos no probablemente, bajo el mando y control del propio estado. ¿El hecho de que alguien cercano a la estructura política rusa se atribuyera haber organizado ataques a instituciones estonias en Rusia significa que fue un ataque de Rusia?³ Se ha acusado a la agencia de inteligencia ISI de Pakistán de haber protegido a jefes militares talibanes; así pues, ¿está Pakistán en guerra con Afganistán? Si ambas preguntas pueden responderse con un “sí”, entonces estos los dos ejemplos anteriores son ejemplos de guerra no evidente.

Por último, muchas formas de guerra no evidente no presentan ningún riesgo personal para los combatientes—que tendrían que hacerlo, casi por definición, ya que la captura o identificación del perpetrador puede hacer que la fuente del ataque sea evidente. Pero nadie puede llegar a la conclusión de que los *estados* que empleen dichos combatientes estén desligados simplemente porque lo estén sus combatientes. Un método de guerra sin huellas digitales puede ser el siguiente paso lógico después de un método sin huellas de pisadas, pero los dos siguen siendo bastantes diferentes.

La falta de evidencia no es absoluta, y el umbral de respuesta dinámica para el estado víctima variará enormemente. El criterio principal es el grado de confianza que siente la víctima de que cierto estado llevó a cabo un ataque—sí, ciertamente, lo que ocurrió realmente *fue* un ataque. Esta probabilidad percibida va a ser casi siempre distinta de cero. Hay pocos estados que crean realmente que ningún otro estado quiera dañarles. Incluso lo que más adelante se demuestra que son accidentes (por ejemplo, la explosión del barco de EE.UU. *Maine*) se culpa a menudo a otros estados (por ejemplo, España). Si hay una crisis (por ejemplo, intento de España de sofocar una insurgencia cubana), la tendencia a creer que cualquier suceso dañino e inusual es un ataque será mucho más elevada.

Así pues, el atacante que atacara con impunidad debe preguntarse si la confianza con que la víctima cree que se llevó a cabo el ataque es probablemente mayor o menor que la confianza que requiere la víctima para responder al ataque. Todo depende de cuál es el umbral de la respuesta, y puede haber muchos tipos de respuestas. La evidencia suficiente para lograr una condena criminal en un tribunal de EE.UU. “fuera de toda duda razonable” es pocas veces el caso, aunque similarmente unos altos niveles de confianza pueden, de hecho, ser necesarios antes de que la víctima decida ir a la guerra. Por otra parte, la mera sospecha puede bastar para reducir o desaprobar presuntos planes de cooperación como ejercicios militares conjuntos, investigación conjunta o relaciones de redes homólogas. En el caso de algunas formas de guerra no evidente, el objetivo puede no estar seguro en lo que se refiere al patrocinio del estado pero puede convenirse a sí mismo de que dicho estado tiene que responsabilizarse de parte de la culpa si pudiera haber detectado y detenido u obstaculizado razonablemente dicho ataque y se hubiera negado a hacerlo.

También variará de qué forma aproximada el estado objetivo adquirirá la confianza de que otro estado específico llevó a cabo un ataque, pero uno no puede equivocarse mucho al considerar los medios, los motivos y la oportunidad. La oportunidad—en forma de algún vehículo de suministro identificable—a menudo distingue mejor la guerra evidente de la no evidente. Pero la oportunidad representa solamente un tercio. Considere, por ejemplo, cómo reaccionaría Estados Unidos ante la detonación de una llamada arma nuclear de maletín alrededor de, digamos, 1962. El maletín se incineraría, dejando poca evidencia forense. Pero en esa época, solamente otros tres estados disponían de los *medios* para llevar a cabo un ataque nuclear, y de esos tres, solamente uno, la URSS, tenía un *motivo* para hacerlo. En dichas circunstancias, la falta de un vehículo de suministro visible habría mellado poco la confianza de EE.UU. de creer que la URSS lo había hecho. De forma similar, para muchos tipos de guerra no evidente, dichos ataques a naves espaciales, la lista de sospechosos sería muy corta, ya que el número de naciones que navegan por el espacio es limitado (aunque, en ese caso, la víctima también debe distinguir con credibilidad entre accidentes y ataques).

Tipos de guerra no evidente

¿Qué es lo que hace que distintas formas de guerra evidente sean de hecho no evidentes? Examinémoslas una por una.

Ciberguerra

Los piratas pueden estar sentados en cualquier lugar y atacar sistemas de todo el mundo, alterando su funcionamiento, corrompiendo la información que tienen y los algoritmos que utilizan, y, según mostró Stuxnet, incluso descomponiendo máquinas al enviarles comandos dañinos desde sistemas pirateados. La atribución es particularmente difícil para un ciberataque. Los unos y ceros que constituyen el ataque no dejan los residuos físicos de sus operadores (especialmente si estos unos y ceros se copiaron de herramientas de otros). Los sistemas atacados con éxito, casi

por definición, no pueden distinguir un ataque de entradas completamente benignas en el momento (con un ataque de denegación de servicio distribuido, lo que importa es el volumen, no el contenido; los bytes de ataque generalmente proceden de máquinas “inocentes” que son manipuladas para bombardear a la víctima con mensajes no solicitados). Los métodos forenses como la identificación del ataque hasta sus orígenes pueden frustrarse fácilmente haciendo rebotar el ataque a través de suficientes portales, usando los servicios de una máquina inocente o pasando a una tercera conexión Wi-Fi. Las dificultades de atribución pueden ser inherentes al medio y es poco probable que mejoren en los años venideros. Los estados que deseen adivinar quién les atacó se dan cuenta de que deben fiarse de los medios y del motivo. Los medios ofrecen solamente poca ayuda en caso de un ataque poco refinado, ya que más de 100 países han investigado la ciberofensiva y la lista de piratas incluye grupos del crimen organizado, actores que no son estados e individuos. Por lo general, se cree que solamente un estado podría haber efectuado un ataque refinado como el de Stuxnet, con sus cuatro vulnerabilidades de días cero y dos certificados robados. Irán puede haber averiguado, una vez que se dio cuenta de que *había* sido atacado, que solamente Israel y Estados Unidos tendrían la razón y el talento para llevar a cabo un ataque de este tipo. Sin embargo, no es completamente imposible que Rusia o China hayan querido retrasar la carrera de armas nucleares de Irán.

Nadie sabe todavía si los ciberataques llevados a cabo de una manera no evidente demostrarán ser ventajosos para los que lo llevan a cabo. No está claro ni mucho menos que los ataques de Rusia (o rusos) a Estonia o Georgia le hicieran mucho bien. Si Israel atacara a Irán en el ciberespacio, lo que parecería un éxito podría considerarse como el principio de un nuevo conjunto de operaciones militares, o, de forma alternativa, un caso muy especial que nadie puede ni necesita duplicar.

Guerra espacial

Los satélites normalmente pierden capacidad de vez en cuando en la inmensidad y oscuridad del espacio. Un ataque a un satélite sin que se descubra el vehículo de ataque puede convertirse casi en el crimen perfecto. Los estados tal vez deseen saber lo que ocurrió, pero sacar un satélite de su órbita tal vez no sea necesariamente algo para lo que el satélite se diseñó, puede hacerse imposible debido a la naturaleza del ataque y requerirá gastos de una cantidad sustancial de combustible. Aunque el análisis posterior a la recuperación indicaría probablemente lo que ocurrió, tal vez se siga sin saber quién lo hizo. Una vez observado eso, salirse con la suya después de atacar a un satélite presenta dificultades. Estados Unidos tiene la capacidad de averiguar la plataforma de lanzamiento de todos los misiles terrestres suficientemente grandes y supuestamente puede hacer el seguimiento de objetos espaciales del tamaño de llaves (los detalles exactos serían indudablemente secretos). Como tiene una idea bastante buena de lo que está haciendo cada satélite, los que se emplean de otra manera son descubiertos necesariamente, pero la llegada de microsátélites, nanosatélites y picosatélites puede complicar la detección por sustracción en los años venideros. Los sistemas terrestres pueden cegar los satélites, pero los satélites tienen que mirar a lo que sea que les esté cegando (es decir, indicar de dónde procede el láser). El número de estados que pueden comprar una plataforma de lanzamiento es mucho mayor que los pocos que pueden lanzar objetos al espacio.

Guerra electrónica

A medida que nuestro mundo interconectado se hace cada vez más inalámbrico, el potencial de interferencias electrónicas crece por al mismo ritmo. Los dispositivos radiantes genéricos pequeños emplazados o dispersos de forma clandestina pueden bloquear señales de GPS (al menos para receptores comerciales) y causar estragos en las comunicaciones, que van desde comunicaciones de teléfonos móviles y de emergencia a controladores de máquinas. A veces puede ser

bastante difícil localizar dichos dispositivos pero no caracterizarlos (es poco probable confundir por mucho tiempo las interferencias deliberadas con causas naturales o accidentes). El uso de dispositivos genéricos puede frustrar la identificación, pero lo difícil en el anonimato es no ser sorprendido en el emplazamiento de dichos dispositivos. Una vez que empiecen a operar los dispositivos, su vida útil es limitada, porque son descubiertos o porque se agotan sus baterías.

Drones

En una serie de circunstancias relativamente limitadas, se puede llevar a cabo un ataque de drones sin una atribución firme. Los requisitos son muchos. El drone tiene que evitar que se estrelle (o debe recuperarse si se estrella); de lo contrario, existe una buena probabilidad de identificar incluso hasta el último comprador de un drone genérico. El país objetivo tiene que tener una cobertura de radar relativamente deficiente o ser contiguo a territorios u océanos donde no haya cobertura de radar. Si el drone procede del océano, la lista de posibles atacantes puede limitarse a los que tienen barcos en el área en ese momento. El drone mismo tiene que ser bastante genérico—de modo que su perfil a una distancia sea coherente con el inventario de muchos países diferentes—o ser furtivo. Por último, la posibilidad de que el ataque de un drone pueda ser un ataque no evidente de Estados Unidos debe esperar al desarrollo de drones de ataque por países *distintos* de Estados Unidos—si eso no ocurre, se asumirá que cualquier drone es estadounidense. Para estados en dificultades con Estados Unidos, la combinación de motivo y medios puede bastar.

Operadores especiales, saboteadores y asesinos

Al igual que con los drones, la clave para mantener el anonimato en operaciones especiales es evitar ser sorprendido. Irónicamente, la capacidad de llevar a cabo *muchas* operaciones especiales sin ser sorprendido requiere tantas destrezas organizativas y profesionales que el número de países capaces de hacer esto es pequeño—hacer acusaciones es mucho más creíble. De aquí que, la perfección puede ser delatora, a menos que el atacante muestre una moderación considerable. Esta categoría incluye minado por transporte encubierto (por ejemplo, submarinos), que, al menos, le da una resonancia histórica, pero también una resonancia contemporánea, como en los daños misteriosos—y disputados—a una embarcación irlandesa preparada para romper el bloqueo de Gaza.⁴

Ataques con fuerzas sustitutas

Esta amplia categoría incluye terroristas, insurgentes, milicias y corsarios. La atribución se dificulta porque generalmente requiere la captura de los perpetradores (o el uso de un método de operación reconocible) pero en su mayor parte porque requiere relacionar al perpetrador con un actor importante. No obstante, en la práctica la relación entre grupos insurgentes y estados realmente es ambigua, y no necesariamente, por diseño; facultar a individuos con organización, ideología y armamento tiende a hacerles creer que sus objetivos son importantes por sí mismos. El Vietcong, por ejemplo, puede haber sido establecido y sostenido por Vietnam del Norte pero tenían prioridades ligeramente diferentes.⁵ África proporciona un caso más pertinente en el que varios países que patrocinaron insurgencias contra sus vecinos se las arreglaron para encontrarse sitiados por insurgentes propios, respaldados de forma similar.

Ataques usando armas de destrucción masiva

A la llamada bomba del maletín de la época de la Guerra Fría se les ha añadido el uso de agentes biológicos y químicos—de los que hay muchos tipos—todos los cuales ofrecen, al menos en

teoría, un método de matar a personas sin que un estado se vea sorprendido haciéndolo. Por regla general, como las armas de destrucción masiva son relativamente pequeñas, es posible que su uso no requiera una inserción forzosa, y los componentes electrónicos modernos permiten detonarlas de forma remota. No obstante, dichos ataques se consideran particularmente infames, y casi todos los estados han firmado uno o más tratados internacionales contra eso. Por esa razón, más de esos ataques pueden identificarse a su último origen que un ataque similarmente encubierto por altos explosivos. Por supuesto, los agentes infecciosos, particularmente los que se puedan inventar por técnicas de recombinación de ADN, pueden suministrarse de una manera muy encubierta. No obstante, a menos que los ciudadanos propios de un estado sean de alguna manera inmunes a sus efectos, no está claro lo que ganaría ese estado al usarlos o, si se usan en una modalidad de “tipo fin del mundo”, por qué a un estado le gustaría ser no evidente en lo que respecta al asunto.

Apoyo de inteligencia a las operaciones de combate

Aunque técnicamente no es una guerra, un estado con un mecanismo refinado a distancia de recopilación de inteligencia y procesamiento/distribución puede proporcionar datos que pueden ser de gran ayuda para sus amigos. Si la asistencia no es interceptada directamente y su distribución es limitada, entonces otros tendrían dificultad en distinguir el origen de forma certera (aunque los estados pueden sospechar que los oponentes por debajo de sus posibilidades pueden haber tenido cierta ayuda, solamente un puñado de países podrían suministrarlo y lo suministrarían). A diferencia de otras formas de guerra no evidente, la ayuda con información no es particularmente infame, y las negaciones—o al menos “ni confirmar ni negar”—son normales en el mundo de la inteligencia. No obstante es posible que el estado proveedor no muestre su participación en el conflicto para no ser acusado de ser beligerante o si tiene un rival que pueda justificar entonces *su propia* asistencia al otro bando.

Merece la pena repetir que a menos que el ataque parezca un accidente completo—y el objetivo sea completamente creíble—no existe un ataque que sea completamente no atribuible. Cada estado tiene sus enemigos o amigos que no son de fiar, y si pasa algo desagradable, se sacarán a relucir los sospechosos normales para el examen. Por el contrario, la capacidad de negación plausible importa solamente si el estado víctima realmente necesita algo aproximado a una prueba judicial para tomar medidas o si se siente aliviado de que la autoría del ataque no sea tan evidente que su negativa a responder no se considere una cobardía. Los perpetradores no tienen que ser sorprendidos con las manos en la masa para sufrir represalias en manos de los que pueden juntar medios, motivos y oportunidad para formar una base suficientemente robusta para llevar a cabo una acción.

Los usos de guerra no evidente

A menudo es más fácil afirmar lo que *no se puede* hacer con la guerra no evidente. Su falta de aplicabilidad para la conquista y la coacción específica ya se ha observado. Además, cualquier finalidad que requiera una serie sostenida de ataques no puede usar una técnica de guerra no evidente si la probabilidad de imputación de cada ataque no es cero y la probabilidad de imputar un acontecimiento es al menos algo independiente de la probabilidad de imputar otro. Esto descarta la guerra espacial, la guerra electrónica, los drones y las operaciones especiales. También puede descartar la ciberguerra pero es menos probable que se descarte la guerra de fuerzas sustitutas—donde la atribución debe inferirse en vez de descubrirse—y el apoyo de la inteligencia a la guerra.

Entonces, ¿qué se *puede* hacer con la guerra no evidente? Un uso es la coacción o disuasión generales. En vez de señalar, “si haces esto nosotros haremos eso”, la señal es, “si hace esto

entonces le pasarán cosas malas”. Como el acto de señalar mismo puede implicar al atacante, es útil si las señales proceden de alguien más. Otros pueden desear ayudar si hay múltiples estados con un interés común, como Vietnam, Indonesia y Filipinas que se oponen a la fanfarronería china en el Mar de China del Sur. Estos otros pueden ser también correligionarios o coideólogos (por ejemplo, “falten al respeto a nuestra religión y le pasarán cosas malas”). El uso de guerra no evidente para obligar es más complicado que dé resultado, ya que es más fácil que entidades dispares se pongan de acuerdo en lo que se va a condenar que en lo que se debe hacer.

Otro uso muy evidente es el sabotaje, tipo Stuxnet, llevado a cabo para denegar a su objetivo cierta capacidad. La dificultad es que el sabotaje es bastante ineficaz a menos que tenga lugar a gran escala o esté de alguna forma relacionado con una operación (si es una operación de combate, el objetivo puede asumir que los saboteadores trabajan para los combatientes). Incluso si los daños son permanentes, los estados pueden recuperarse en general. El ataque a las centrifugas iraníes tenía sentido debido al fuerte deseo sentido por algunos países en hacer renquear el programa nuclear de Irán y ganar tiempo. Otra justificación del sabotaje es empujar un objetivo más allá de un punto crítico cercano, incluso si esto tiende a ser visible solamente desde un punto de vista retrospectivo. De lo contrario, las consecuencias de llevar a cabo lo que podría ser un acto de guerra pueden sobreponerse a las ganancias, incluso si ser sorprendido es poco probable.

Un ataque no identificable de suficiente magnitud también puede debilitar el objetivo antes de un ataque armado o al menos distraer tanto al objetivo que no pueda asignar los recursos, como sensores, armas in situ o atención de gestión, requeridos para prever y preparar lo que en verdad es, un ataque abierto inminente. Claramente, si no se produce un ataque, el precursor dejará de ser un ataque no evidente desde un punto de vista retrospectivo (a menos que el objetivo tenga múltiples enemigos ansiosos, todos ellos buscando indicios de debilidad, en cuyo caso, lo que parece evidente puede seguir siendo erróneo). Las ventajas de empezar en una modalidad no evidente son dobles. Primero, si el ataque inicial fuera evidente el objetivo podría efectuar una jugada defensiva de forma que dificulte la realización del ataque. Puede saber adónde apuntar sus defensas, por así decirlo; podría estimular a otros a ejercer presión sobre el atacante; o podría incluso contraatacar. En segundo lugar, si el ataque no cumple con sus objetivos, el atacante puede cancelar el ataque abierto y permanecer en la anonimidad con la esperanza de eludir el castigo.

De forma correspondiente, un ataque no evidente puede ser una prueba para ver si cierta técnica da resultado, cuáles son las defensas del objetivo, y donde deben buscarse las mejoras. Sería una prueba costosa si el objetivo mismo averiguara algo sobre sus vulnerabilidades y por lo tanto tuviera una causa para corregirlas y evidencia sobre cómo hacerlo.

Las operaciones no evidentes también pueden ayudar a ganar las guerras de terceros. Dicha ayuda puede ser no evidente si el *hecho* de la ayuda no es evidente o si el *origen* de la ayuda puede ser de cualquier país o entidad como grupos insurgentes o mercenarios. Esto plantea la cuestión de por qué un estado así querría dejar huellas dactilares. Una razón es que los ataques tienen lugar en un país distinto a otro que quería ayuda (por ejemplo, Siria ataca a Irak, y Estados Unidos ataca objetivos en Siria), convirtiéndose así en un acto de guerra por derecho propio y una excusa para que el país atacado llame a *sus* amigos para que le ayuden (por ejemplo, ataque a Irak). Sin embargo, lo más probable es que la asistencia respalde operaciones dentro del estado que está siendo atacado, ya sea por otro estado o por insurgentes, de modo que estos factores no entran en juego. Sin embargo, lo que *importa* es el aspecto de compromiso y cómo impide asumir un compromiso para tratar de obtener una victoria o perder crédito. La intervención y después la retirada prematura plantea dudas sobre la importancia del fin e incluso de la integridad del estado, incluso si dicho estado nunca se comprometió explícitamente a seguir como hasta ahora.

La guerra no evidente también puede llevarse a cabo para lograr un efecto narrativo. Normalmente, en la guerra, el atacante y el objetivo forman parte de la narrativa, y a menos que las

acciones del atacante sean totalmente infundadas, la disputa sobre las narrativas es probable que tenga dos vertientes donde los dos lados apoyan a su propio bando. No obstante, si el atacante es desconocido, o al menos no está claro, entonces el enfoque de la historia es necesariamente el objetivo, y el tema es probable que se concentre en por qué es atacado el objetivo—y puede muy bien extenderse en lo que el objetivo hizo para merecer el ataque o por qué el objetivo no pudo protegerse. Eso, de hecho, puede ser el motivo del atacante: crear una crisis de confianza en el estado objetivo, ya sea debilitándolo inmediatamente, creando fisuras en su cuerpo político, o al menos hacerle más proclive a hacer concesiones.

Por último, si un atacante puede persuadir al objetivo de que fue impactado por un tercero, puede catalizar el conflicto de modo que sea ventajoso para el atacante. Por ejemplo, un cibera-taque taiwanés no evidente a Estados Unidos durante una crisis con China podría poner a Estados Unidos en oposición creciente a China y de esta forma apoyar más probablemente a Taiwán. Un atacante que instigue una guerra entre dos socios comerciales anteriores podría forzar a ambos a comprar del otro país neutral relevante, el atacante. Por supuesto, si se sigue la atribución, el atacante se habrá hecho con un enemigo que no necesitaba y quizás también con un segundo enemigo—el país que el atacante esperaba que fuera acusado.

Las opciones de respuesta del objetivo

En algunos casos, la ambigüedad da resultado para ventaja del objetivo al dar una excusa para evitar la respuesta; afirma incertidumbre sobre quién lo hizo o lo qué de hecho se hizo. No saber ayuda a protegerse contra llamadas populares a combatir y redimir su honor. En algunos casos, el atacante mismo tal vez no piense necesariamente lo peor del honor del objetivo si no se produce una respuesta; en otros casos, se convencerá a sí mismo de que el objetivo sabía pero mentía para evitar una confrontación. Considere, de forma análoga, el arsenal nuclear fantasma israelí. Una vez que otros estados poderosos de Oriente Próximo reconozcan que Israel tiene armas nucleares, deben responder a la razón de por qué no las tienen ellos. Ningún gobierno resulta engañado, pero tampoco humillado.

No obstante, en su mayor parte, los objetivos querrán que se acaben dichos ataques —pero, ¿cómo hacerlo? La defensa es claramente una opción que lógicamente cobraría una mayor importancia cuanto menos pueda apoyarse en no responder, ya que no hay seguridad sobre quién lo hizo. Otra opción es ayudar a ejercer presión desde la comunidad mundial para terminar la posesión de la tecnología de ataque requerida, pero la mayoría de éstas no pueden prohibirse de forma efectiva. Las ciberarmas son en gran medida el anverso de las vulnerabilidades del sistema, es trivial ocultar el código de ataque y se requieren tecnologías de ataque básicas para la ciberdefensa. Las interferencias electrónicas son inherentes en su capacidad de generar energía de radiofrecuencia. El apoyo de la inteligencia a terceros es idéntico al apoyo de la inteligencia a operaciones militares en general. Las armas de sabotaje, las operaciones especiales y las insurgencias son armas pequeñas. Por el contrario, las armas de destrucción masiva y las minas terrestres (no las navales) ya están prohibidas por tratado. Las únicas armas no cubiertas por los tratados y que podrían prohibirse concebiblemente son las armas antisatelitales y los drones; ambas tienen finalidades militares legítimas (abiertas). Generalmente, es más cómo se usan dichas armas en vez de las armas mismas lo que determina las características de la guerra no evidente.

Una variante del segundo método es desarrollar un consenso global de que el uso encubierto de la guerra es mucho más infame que su uso abierto. Así, si dichas armas *se* usan—algo que no siempre es aparente—la comunidad mundial apoyaría los esfuerzos para ejercer presión sobre los usuarios potenciales para permitir investigaciones que clarificarían qué estado tiene la culpa. Después de todo, la mayoría de las formas de guerra son consideradas universalmente crímenes si son llevadas a cabo fuera de las fuerzas armadas; así, incluso el estado acusado debe tener

interés en localizar y extirpar a sus criminales peligrosos, suponiendo que desearan atribuir la culpa. En los casos en que el estado use fuerzas sustitutas y dichos actos *sean* crímenes, pueden sentir presión para cooperar con las investigaciones de la policía internacional. No obstante, la satisfacción para la parte afectada, supone que las acciones de la policía puedan establecer niveles razonables de certidumbre. Y lo que es más problemático, cuanto más se acerquen las vías de investigación a las puertas de los establecimientos militares o de inteligencia, mayor será la renuencia de los estados a que prosigan. Dicha renuencia no sería sin fundamento—si las supuestas acciones de guerra no evidente permiten a los investigadores escudriñar las operaciones encubiertas, los estados pueden en gran medida interpretar la necesidad de evidencia de forma que también les permitan descubrir los secretos de sus rivales.

El último recurso es que los estados víctima y sus aliados respondan a los estados combatientes sospechosos como si ciertamente lo hubieran hecho. Al hacer eso, deben tener en cuenta el grado de certidumbre de *otros* de que la acusación es correcta y, en cierta medida, si el supuesto estado atacante cree que es culpable. Muchas técnicas de guerra no evidente pueden ser llevadas a cabo por elementos descontrolados. Según se observó, algunas respuestas, como las malas relaciones entre el objetivo y el supuesto atacante, no requieren nada que se aproxime a una prueba conclusiva; la mera inquietud basta. Otras respuestas, como las represalias, requieren normalmente altos niveles de confianza. Al final, el estado víctima tiene que sopesar los riesgos relacionados con negativos falsos (no hacer nada ante la agresión) y positivos falsos (represalias contra inocentes). Observe además que la “denegación plausible” es apenas un absoluto en este caso. A menos que el estado víctima solamente pueda responder a través del sistema de tribunales—y los estados no puedan ir a juicio, solamente sus líderes—el balance entre responder y no responder pueden inclinarse mucho antes de que el medidor de confianza llegue al 100 por cien. Un estado relativamente pacifista rodeado por todas partes por amigos (por ejemplo, Bélgica) y que forme parte de alianzas puede desear una certeza casi absoluta y tal vez no reaccione incluso en ese caso; un estado ansioso bien armado rodeado por todas partes por adversarios potenciales (por ejemplo, Israel) puede ser menos quisquilloso.

La víctima también puede efectuar una represalia usando guerra no evidente usando guerra no evidente ella misma. Ostensiblemente, el compromiso mutuo de ambos lados para modular sus respuestas entre sí podría limitar el potencial de una guerra abierta, y por tanto, más destructora—siempre que ambos lados tengan cuidado de no descubrirse. Esto puede crear un conjunto de incentivos extraños donde las comunidades de ambos lados involucradas en una guerra no evidente se esfuercen en no revelar las actividades de sus contrarios no sea que el poder y la influencia en ambos bandos se desplacen a comunidades cuyos métodos bélicos sean bastantes evidentes. Por el contrario, la percepción de que es aceptable intensificar las hostilidades de una manera no evidente en vez de llamar al otro bando puede hacer que aumente el costo destructor de la guerra no evidente hasta sus límites. Si los asuntos se hacen entonces evidentes, el nivel de guerra que forma la base del siguiente conjunto de amenazas empieza a un nivel mucho más elevado.

Evaluación y conclusiones

¿Sería buena la propagación de la guerra no evidente? Incluso si se esgrimiera únicamente para lograr buenos fines, dichas técnicas corroen tanto los valores militares como las normas diplomáticas. La guerra no evidente, casi por definición, tiene que ser el trabajo de pequeños equipos que deben aislarse de la comunidad más grande, de forma muy parecida a las agencias de inteligencia, por sí se descubren sus aventuras. Los esfuerzos de los equipos pequeños de guerra no evidente dejarían a la masa del establecimiento de seguridad nacional bastante

insegura acerca de lo que exactamente estaba pasando y quién estaba exactamente detrás de todas esas actividades (solamente algunas de ellas parecerían accidentes).

La guerra no evidente también se ajusta mal a los estados democráticos pero se adapta mucho mejor a estados autoritarios o en decadencia en los que la comunidad de inteligencia se haya desacoplado de su estructura de gobierno legítimo. Es probable que los estados que tengan que gestionar reputaciones a largo plazo vean la desventaja de tener que mentir sobre las actividades bélicas cuando se vean preguntados.

La adopción universal o incluso amplia de la guerra no evidente probablemente produciría un mundo más sospechoso. Una vez que los ataques se hagan de forma que parezcan accidentes, se empezará a sospechar que muchos accidentes son ataques. Las naciones reaccionarían (incluso más que ahora) antes sospechas en vez antes la realidad; se podría atribuir/culpar a los atacantes de mucho más de lo que realmente merecen. En demasiados países, *cualquier* cosa que parezca rara se culpa a Estados Unidos (o a Israel) y a sus agencias de inteligencia ubicuas y omnipotentes. Parte de la madurez de sus gobiernos consiste en mejoras en su capacidad de distinguir realidades de fantasías; la evidencia de que dicha fantasía contenga un núcleo de verdad apenas facilitaría el proceso de madurez. De hecho, en circunstancias de crisis, es concebible que pueda iniciarse un conflicto aun cuando el acusado no haga nada.

Y por supuesto, una crisis podría empezar cuando un estado use dichas técnicas pensando en que nunca le iban a descubrir—y sea descubierto. □

Notas

1. El término *no evidente* tuvo una manifestación anterior en el producto de extracción de datos de Jeff Jonas, Non-Obvious Relationship Analysis (Análisis de relaciones no evidentes).

2. El término *guerra*, usado aquí, comprende operaciones llevados a cabo para fines políticos por estados con el objeto de destruir, corromper o alterar de forma significativa haberes o intereses relacionados con el uso por parte de otros estados de medios que generalmente se consideran ilegales si no los llevan a cabo los estados. Nuestro debate se limita a los estados, porque los actores no estatales no siempre tienen remites ni siquiera identidades que no sean siempre ambiguas, y los individuos incluidos pueden estar sujetos a medidas legales en formas que los estados no pueden estar.

3. Sergei Markov, un diputado de la Duma estatal del Partido Rusia Unificada a favor del Kremlin, afirmó, “Acerca del ciberataque a Estonia . . . no se preocupen, ese ataque fue llevado a cabo por mi asistente. No les voy decir su nombre, porque entonces es posible que no pueda conseguir visados”. “Behind the Estonia Cyberattacks” (Detrás de los ciberataques a Estonia), *Radio Europa Libre/Radio Libertad*, 6 de marzo de 2009, http://www.rferl.org/content/Behind_The_Estonia_Cyberattacks/1505613.html.

4. Robert Mackey, “Irish Flotilla Activists Show Damage to their Boat” (Activistas de la flotilla irlandesa muestran daños en su barco), *The Lede: Blogging the News*, 1º de julio de 2011, <http://thelede.blogs.nytimes.com/2011/07/01/what-flotilla-activists-videos-look-like/>.

5. Qué se quedó en casi nada después de que los rangos originales se redujeran considerablemente en la ofensiva Tet de 1968.

Creando un Comando Nuevo en el Ciberespacio

GENERAL KEITH B. ALEXANDER, USA*

Nota del Editor: En marzo de 2011, el General Keith B. Alexander hizo declaraciones ante el Comité de Servicios Armados de la Cámara de Representantes sobre Amenazas Emergentes y Capacidades y el progreso en establecer el Comando Cibernético de EE.UU. Este comentario refleja su declaración en esa ocasión. Este artículo fue publicado anteriormente en nuestra revista *Strategic Studies Quarterly*, Summer 2011.

LA CIBERSEGURIDAD es vital para nuestra nación. Parte de nuestra tarea en el Comando Cibernético de Estados Unidos es garantizar que nuestra nación entienda qué es lo que la Casa Blanca, el Congreso y el Departamento de Defensa nos han encomendado y por qué es tan importante que se haga bien. Crear un comando nuevo a la vez que se llevan a cabo las operaciones es un reto, especialmente en tiempos de cambios rápidos tecnológicos y en la política. Pero este comando nuevo ha producido resultados que han hecho que nuestra nación sea más fuerte y segura y ya ha habido dividendos de ciberseguridad en las inversiones de tiempo y recursos dedicados a esta creación.

El camino hacia la capacidad operacional completa

El Comando Cibernético de EE.UU. logró su capacidad operacional completa (FOC, por sus siglas en inglés) el 31 de octubre de 2010 como un comando sub-unificado bajo el Comando Estratégico de EE.UU. (USSTRATCOM, por sus siglas en inglés). El camino hacia la FOC culminó aproximadamente según el calendario del secretario de defensa cuando él ordenó el establecimiento del comando en junio de 2009. Originalmente se proyectó que la capacidad operacional inicial (IOC, por sus siglas en inglés) se alcanzase en octubre de ese año, pero la fecha se retrasó a mayo de 2010 cuando su nombramiento para desempeñarse como su primer comandante fue confirmado por el Senado. Hicimos buen uso de los meses entre octubre de 2009 y mayo de 2010, sin embargo, crear un estado mayor consolidado para unir las dos organizaciones heredadas, el Comando Conjunto de Componentes Funcionales para la Guerra en la Red (JFCC-NW, por sus siglas en inglés) y la Fuerza de Tarea Conjunta de Operaciones en la Red Global (JTF-GNO), las cuales juntas se convirtieron en el Comando Cibernético. Además, esbozamos las tareas necesarias que nos conducirían a una FOC una vez que el reloj echase a andar. Aunque el intervalo entre la capacidad inicial en mayo y lograr la capacidad operacional completa en octubre fue de solamente cinco meses en lugar de los 12 que se habían planificado, pudimos alcanzar varias metas. Además, lo hicimos acelerando el ritmo de las operaciones diarias que la JTF-GNO y la JFCC-NW habían establecido.

A pesar del horario comprimido, el estado mayor consolidado en el Comando Cibernético logró mucho para octubre de 2010. Establecimos un centro de operaciones conjuntas, transferimos control operacional de la misión de la JTF-GNO al Fuerte Meade, Maryland, y desactivamos el centro de vigilancia 24/7 de la JTF-GNO en Arlington, Virginia; estas medidas ayudaron al USSTRATCOM a disolver la JFCC-NW y la JTF-GNO. La última tarea tomó una cantidad consi-

*El General Keith B. Alexander, Ejército de los EUA, es el *Comandante del Comando Cibernético de Estados Unidos, Director de la Agencia de Seguridad Nacional, y Jefe del Servicio de Seguridad Central*

derable de tiempo planificarla y una orquestación cuidadosa porque las actividades y la fuerza laboral de la JTF-GNO había que trasladarlas del norte de Virginia al Fuerte Meade, a la vez que se garantizaba que el funcionamiento diario de las redes de información del DoD se mantenían intactas. Establecimos procesos eficaces de mando y control operacional para los conjuntos de misiones consolidadas. Se estableció un centro conjunto de operaciones de inteligencia. Los componentes cibernéticos de nuestro servicio fueron asignados oficialmente al USSTRATCOM, y continuamos forjando relaciones con socios claves. Integramos oficiales de enlace en los comandos combatientes y establecimos las condiciones para ampliar su presencia en elementos de apoyo cibernético más grandes. Desplazamos equipos expedicionarios para apoyar las operaciones en Irak y Afganistán. Además, logramos progresar en nuestro apoyo a la planificación operacional por parte de los comandantes combatientes y en crear procesos para que ellos emitieran requerimientos de apoyo cibernético. El comando logró todo esto sin impactos negativos a la misión, manteniendo seguras las operaciones del departamento a la vez que hacía transparente la transición a los usuarios de sus sistemas informáticos.

Se proyecta que el presupuesto del comando para el año fiscal 2012 sea de \$159 millones de dólares, y se espera que para ese entonces la fuerza laboral sea de 464 efectivos y 467 civiles, un total de 931 empleados. La misión general de este equipo es planificar, coordinar, integrar, sincronizar y conducir actividades para dirigir las operaciones en la defensa de redes de información específicas del DoD y estar preparado, cuando se le ordene, para llevar a cabo el espectro total de las operaciones militares ciberespaciales con el fin de habilitar las acciones en todos los ámbitos, garantizar la libertad de acción en el ciberespacio para EE.UU. y sus aliados y negarle lo mismo a nuestros adversarios. Por último, el Comando Cibernético de EE.UU. continúa creando sinergia con la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés) con el fin de aprovecharse de la infraestructura y experiencia de la NSA, que continúan siendo cruciales para nuestro progreso. Nuestra cobicación con la NSA le permite al gobierno maximizar nuestros talentos y capacidades colectivas.

Perspectivas actuales

Nuestros líderes, desde el Presidente Obama y sucesivamente, han hablado sobre la importancia para nuestra nación de conservar nuestra seguridad en el ciberespacio y mantener nuestra libertad de acción en este ámbito nuevo, singular y fabricado por el hombre. Al hacerlo enfrentamos muchos retos, especialmente en virtud de los últimos acontecimientos.

La amenaza cibernética continúa evolucionando, constituyendo peligros que sobrepasan las fallas en el 2008 de nuestros sistemas clasificados que el Subsecretario de Defensa, William Lynn, describió en su artículo en la revista *Foreign Affairs* en el otoño de 2010 como un momento decisivo para nuestra seguridad cibernética. Ahora, nuestra nación depende del acceso al ciberespacio y los datos y capacidades que radican ahí; somos colectivamente vulnerables a una gama de amenazas que van desde inestabilidad en la red, actividades criminales y terroristas, hasta capacidades auspiciadas por el estado que están progresando desde explotación a interrupción a destrucción. Si bien no hemos sufrido daños desastrosos o irreparables en el ciberespacio de ninguna de esas categorías de riesgo, debemos estar preparados para contrarrestar esas amenazas.

Tanto los actores externos como las amenazas internas constituyen retos significativos para nuestra ciberseguridad. Por supuesto, ningún actor estatal ha admitido haber lanzado ciberataques perjudiciales a otro estado. Sin embargo, han ocurrido incidentes que se asemejan mucho a esos ataques. Los ciberasaltos en Estonia en el 2007 incitaron a Estados Unidos y nuestros aliados de la OTAN a reflexionar sobre qué constituiría un “ataque armado” en el ciberespacio a un miembro de la alianza que provocase las provisiones del Tratado del Atlántico Norte sobre la defensa colectiva. El año siguiente, la invasión de Georgia coincidió con ciberataques planificados con precisión, marcando una de las primeras veces que hemos visto esos “ataques apoyados

por la cibernética”. La coincidencia fue tan perfecta que observadores independientes llegaron a la conclusión de que no hubo tal coincidencia—que los piratas informáticos (*hackers*) que habían imposibilitado temporalmente la reacción y las comunicaciones del gobierno georgiano con el mundo exterior habían practicado sus asaltos y respondieron a indicios oficiales cuando los montaron de verdad.

Recientemente hemos visto el acceso a la *Internet* manipulado o restringido por los gobiernos para contener e interrumpir hasta las protestas pacíficas de sus propios ciudadanos. Además, creemos que los actores estatales han creado armamento cibernético para paralizar los blancos de la infraestructura en maneras equivalentes a asaltos cinéticos; algunos de esos armamentos podrían posiblemente destruir *hardware* al igual que datos y *software*. Las posibilidades de efectos cibernéticos destructivos, hace tiempo reconocidos como teóricos en su mayoría, ahora se han producido afuera del laboratorio y se están proliferando hacia los arsenales nacionales y posiblemente más allá, moviéndolos un paso más cerca al uso intencional o la liberación accidental. Segmentos de la infraestructura crítica de nuestra nación no están preparados para lidiar con este tipo de amenaza.

Además, contemplamos con inquietud las capacidades cada vez mayores de los actores no estatales. Las amenazas que vemos aquí son asimétricas, lo que significa que actores comparativamente nuevos o menores pueden causar efectos acordes con acciones auspiciadas por el estado. Aunque individuos con destrezas en computación han mostrado independientemente que esos ataques los puede lanzar un solo actor con una computadora portátil y un motivo, estamos enfocados principalmente en terroristas y criminales cibernéticos bien organizados. Éstos continúan tornándose más hábiles para usar la *Internet* como un medio para reclutar, coordinar y llevar a cabo otras actividades, y cada vez se tornan más sofisticados al hacerlo. Los criminales cibernéticos están más interesados en robar y sacarle provecho a información sensitiva que pueden darles ganancias, ya sea directamente a través del fraude o robo de identidad o indirectamente a través de la piratería de capital intelectual. De hecho, el verano pasado observadores tales como el Senador Sheldon Whitehouse y un grupo de colegas bipartitas le llamaron a esto “la transferencia de riqueza más grande en la historia de la humanidad a través del robo y la piratería”—una transferencia que significativamente ha reducido el costo para que posibles adversarios cierren y contrarresten nuestra ventaja tecnológica. Por supuesto, esa actividad es un delito y pertenece más correctamente a la policía que a los militares, pero cuando el blanco principal es nuestra base industrial de defensa, nosotros en el Departamento de Defensa tenemos que desempeñar un papel en la respuesta. También sabemos que actores estatales y terroristas pueden sacarle provecho a las infracciones y herramientas fabricadas por criminales, al igual que un agente patógeno peligroso emplea, de manera oportunista, un vector de enfermedades para penetrar las células huésped. De hecho, a veces los actores estatales y no estatales colaboran en asuntos de interés mutuo.

Retos de seguridad significativos también emanan de la higiene cibernética deficiente, mal uso inadvertido y actos maliciosos. Después de todo, incluso el más astuto de los actores cibernéticos maliciosos—aquellos que pueden entrar en prácticamente cualquier red a la que en realidad quieren intentar penetrar—por lo regular están buscando blancos de oportunidad. Ellos buscan vulnerabilidades fáciles en la seguridad de nuestro sistema y luego se aprovechan de ellas. Parches de *software* que no se han aplicado, *firewalls* desatendidas y *suites* de antivirus que nunca se actualizan inclusive en la milicia estadounidense, nos causan problemas graves, especialmente cuando un riesgo para uno es un riesgo compartido por todos. Ahora, multiplique esos problemas a lo largo del gobierno y del sector privado, y comprenda que hemos interconectado nuestras vulnerabilidades a la vez que hemos segmentado nuestras defensas entre los ámbitos .mil, .gov, .com, .edu de la *Internet*. Cada ámbito (y a menudo cada sistema) ha sido abandonado para que se las arregle como pueda contra actores cibernéticos que no están interesados

en distinciones jurídicas o límites organizacionales. Y, por último, hay una amenaza interna; algunas de las violaciones de seguridad más grandes en la historia han originado desde adentro.

La creación reciente del Comando Cibernético se ha granjeado mucho interés por parte de militares extranjeros y los gobiernos que los supervisan. Con frecuencia vemos informes de prensa sobre países que están contemplando crear sus propios “comandos cibernéticos”. Esto parece ser una señal no necesariamente de una “militarización” del ciberespacio sino más bien un reflejo del nivel de inquietud con la que líderes civiles y militares alrededor del mundo contemplan los problemas actuales. Muchos de esos pasos son esencialmente defensivos, y si tantos países están interesados en mejorar sus defensas, estarían más dispuestos a discutir sobre las maneras como pueden disminuir las amenazas comunes. Al nivel estratégico del ciberespacio hay una disuasión *de facto* peligrosa. Aunque nadie sabe cómo se desarrollaría una ciberguerra, hasta los actores estatales más capaces parecen reconocer que no está en el interés de nadie enterarse a la mala. Esta inquietud ha provocado cierto grado de restricción por estados que consideramos son capaces de ocasionar efectos cibernéticos muy graves. A menos que el optimismo oculte las amenazas verdaderas, debemos destacar que no contamos con una capacidad segura de refrenar el comportamiento de extremistas radicales, no estatales.

En resumen, nuestros adversarios en el ciberespacio son sumamente capaces. Nuestra economía y sociedad se han tornado dependientes, directa o indirectamente, en el acceso a y la libertad de movimiento en el ciberespacio—y de hecho nuestra milicia depende igual de ese acceso—y, por lo tanto, no podemos estar a gusto con una situación en la cual a veces somos nuestro peor enemigo.

Trabajando hacia el futuro

La finalidad de los esfuerzos y la planificación del Comando Cibernético de EE.UU. es garantizar que el DoD ha hecho todo lo que puede para defenderse en contra de y disuadir adversarios, mitigar amenazas peligrosas y tratar las vulnerabilidades persistentes de manera que inclusive nuestros opositores más capaces sabrán que interferir con las propiedades de nuestra nación en el ciberespacio es una mala inversión.

Nuestro comando enfrenta serios retos a medida que se prepara para llevar a cabo trabajos en el ciberespacio que se necesitan urgentemente. Su establecimiento refleja la necesidad del departamento de administrar los riesgos cibernéticos, asegurar la libertad de acción y garantizar el desarrollo de capacidades integradas. Nuestra intención es superar los retos que enfrentamos mediante los esfuerzos concertados de implementar la recién aprobada estrategia para el ciberespacio del departamento. Continuaremos buscando la solución a los problemas de capacidad, recursos y eficiencias de la tecnología de informática que enfrentamos mediante las cinco iniciativas estratégicas de esa estrategia. Nuestra intención es:

- tratar el ciberespacio como un ámbito para fines de organizar, capacitar y equipar, de manera que el DoD pueda aprovechar completamente su potencial en las operaciones militares, de inteligencia y de negocios;
- emplear nuevos conceptos operacionales de defensa, inclusive ciberdefensas activas tales como vigilar la seguridad del tráfico de los sistemas de informática, hasta proteger las redes y los sistemas del DoD;
- colaborar de cerca con otras agencias y departamentos del gobierno de EE.UU. y el sector privado para permitir una estrategia integral por parte del gobierno y un método nacional integrado hacia la ciberseguridad;
- forjar relaciones robustas con los aliados y socios internacionales de Estados Unidos para permitir que se comparta la información y se fortalezca la ciberseguridad colectiva; y

- sacarle provecho a la ingeniosidad de la nación reclutando y reteniendo una fuerza laboral cibernética excepcional y dar lugar a la innovación tecnológica rápida.

Nuestro primer deber es garantizar que las redes del DoD estén seguras. Hacerlo es crítico para proteger nuestros datos, mantener nuestro potencial bélico y en un final defender nuestra nación. Hasta hace poco, todos opinábamos que nuestras redes eran un gran multiplicador de fuerza—la magia que nos permite colocar pertrechos en el blanco y enviar aeronaves, tropas y buques a donde se necesitaban, cuando tenían que estar ahí. Sin embargo, hoy comprendemos que esas redes representan una vulnerabilidad grave y tememos a la idea que alguien logre destruirlas o, peor aún, haga unos cuantos cambios sutiles a la integridad de nuestros datos de manera que paralizaría todas nuestras operaciones militares. Sin el flujo de datos rápido, garantizado y seguro no podremos combatir nuestros adversarios en la manera como nosotros, en calidad de estadounidenses, pensamos que se deben combatir. No estamos necesariamente cerca de perder esa ventaja, pero los posibles adversarios comprenden dónde radica y, de hecho, están contemplando maneras de debilitarla en cualquier conflicto en el futuro.

El Comando Cibernético de EE.UU. está trabajando de muchas maneras para conservar esa ventaja de información. Estamos dirigiendo las operaciones de las redes de informática del departamento, que unen siete millones de dispositivos de computadoras a lo largo de quince mil redes. El reciente traslado de la Agencia de los Sistemas de Información de la Defensa (DISA, por sus siglas en inglés) a una nueva instalación en el Fuerte Meade ha dado lugar a una mayor colaboración entre nuestras dos organizaciones. Esa labor incluye el mantenimiento de sensores para detectar y bloquear la actividad del adversario en esas redes, la inspección de ámbitos y prácticas de seguridad y la investigación de incidentes reales o sospechosos. Juntas estamos progresando en todas esas áreas, fomentando nuestra capacidad para detener intromisiones y adaptarnos a los cambios en las prácticas casi tan rápido como evolucionan. Las capacidades de sensor nuevas que estamos desplazando y el régimen de inspección dinámico que estamos preparando mejorarán aún más nuestra situación.

También planificamos—en asociación con la NSA—la defensa de sistemas de información específicos del DoD, a sabiendas de que tenemos que mantenernos a la delantera de la amenaza cibernética en términos tecnológicos. En este aspecto, el Comando Cibernético de EE.UU. y nuestros socios están buscando maneras de cambiar a una arquitectura diferente y más defendible para ofrecer servicios de informática a los usuarios. De aquí a un año debemos estar bien encaminados en contar con una arquitectura templada comprobada, desplazada y que ofrece un nivel nuevo de ciberseguridad. La idea es reducir las vulnerabilidades innatas en la arquitectura actual y aprovechar las ventajas de *“cloud” computing* (computación en nube) y redes *thin-client* (estrechas), moviendo los programas y los datos que los usuarios necesitan lejos de los miles de computadoras de mesa que ahora usamos—cada una de las cuales hay que asegurar individualmente—a una configuración centralizada que nos otorgue una disponibilidad de ampliaciones más amplia y datos combinados con un control más estricto en cuanto a accesos y vulnerabilidades y más mitigación oportuna de estas últimas. Cambiar a una arquitectura *cloud* tiene las ventajas de producir economías de escala y reducir los costos de la tecnología de información del departamento. Además, a primera vista pareciera que esta arquitectura es vulnerable a las amenazas internas—de hecho, ningún sistema que los seres humanos usan está inmune al abuso—pero estamos convencidos que los controles y herramientas que se incorporen al *cloud* garantizarán que las personas no podrán ver ningún dato más allá de los que necesitan para sus trabajos y se les identificará rápidamente si intentan el acceso no autorizado a los datos.

Durante el año próximo esperamos “poner en marcha” las redes de nuestro departamento. Desde luego, continuaremos haciéndolo respetando plenamente y protegiendo la privacidad y las libertades civiles de todos los estadounidenses, al igual que en cumplimiento con todas las leyes y regulaciones pertinentes. La idea es transformar los sistemas de información del DoD de

algo que es protegido pasivamente a un conjunto de capacidades que les ofrece a nuestros comandantes y líderes superiores oportunidades para ajustar nuestras defensas. Si aquellos que buscan hacernos daño en el ciberespacio aprenden que hacerlo es costoso y difícil, creemos que sus patrones de conducta cambiarán. La tecnología está preparada.

En el documento de misión de nuestro comando se declara que coordinamos, integramos y sincronizamos actividades para dirigir las operaciones y la defensa de las redes de DoD. En práctica, esto significa que invertimos mucho tiempo hablando con los líderes y expertos en el departamento, el gobierno estadounidense, la industria privada al igual que con otros países. Por supuesto, este esfuerzo comienza con los componentes de servicio cibernético del Comando Cibernético de EE.UU., que proveen las fuerzas que implementan nuestros planes y ejecutan nuestras directrices—Comando Cibernético del Ejército, Comando Cibernético de las Fuerzas de Infantería de Marina, Comando Cibernético de la Flota y el Comando Cibernético de la Fuerza Aérea. Aún estamos perfeccionando las maneras como nosotros y ellos interactuaremos para apoyar y ser apoyados por los comandos combatientes geográficos en distintas situaciones. Nuestra misión también depende de la labor de la NSA, que provee inteligencia y experiencia que son indispensables para comprender lo que está sucediendo en el ciberespacio. Además, estamos constantemente comprometidos con DISA y nuestra relación con esta agencia probablemente cambiará sustancialmente y cada vez será más estrecha en el futuro cercano.

También hemos fortalecido nuestra asociación con el Departamento de Seguridad Interna (DHS, por sus siglas en inglés) según el acuerdo reciente celebrado por los Secretarios Robert Gates y Janet Napolitano. Un funcionario superior de DHS ahora trabaja con nosotros en la NSA, está al frente de un elemento de coordinación conjunta DHS-DoD que también fue establecido por el acuerdo y asiste a muchas de las reuniones de los líderes. Varias agencias gubernamentales también son representadas 24 horas al día en nuestro centro de operaciones conjuntas. Esas medidas, junto con las medidas complementarias en el DHS y otros socios, deben proporcionar una concienciación en todo el gobierno de lo que todos pueden apreciar de manera que podamos planificar y ejecutar acciones conjuntas autorizadas y coordinadas en caso de una emergencia. Por último, somos participantes activos en las discusiones productivas del Departamento de Defensa entre el gobierno y la industria sobre cómo compartir información relacionada con las amenazas comunes y las posibles maneras de mitigarlas. La gran mayoría de la información de nuestra milicia viaja en infraestructura comercial, y por lo tanto necesitamos crear discernimientos compartidos en esas dependencias para fines de asegurar la misión.

La segunda parte de nuestra misión en el Comando Cibernético es estar preparados para llevar a cabo operaciones militares ciberespaciales de todo tipo. Como mencioné anteriormente, los actores estatales y no estatales ya han experimentado con maneras de hostigar o atacar gobiernos rivales, ya sea para plantear un punto estratégico o en combinación con ataques cinéticos. Sería desacertado que nuestra milicia y nuestra nación diesen por sentado que hemos visto los últimos de esos ataques. Estamos preparados, cuando se nos ordene y en cumplimiento total con las leyes pertinentes, a responder cuando nosotros o nuestros aliados seamos amenazados o sometidos al uso de la fuerza en el ciberespacio. El Presidente ha recalcado que nuestra infraestructura digital es un recurso nacional estratégico y ha insistido que preparar a nuestro gobierno para la tarea de proteger los recursos nacionales estratégicos en el ciberespacio es una prioridad de seguridad nacional. Nuestros esfuerzos para hacerlo están concebidos para lograr dos metas:

- Primero, protegemos en el ciberespacio la libertad de acción de EE.U. y los aliados. Ya no es posible concebir que nuestra nación funcione correctamente o inclusive se defienda sin la capacidad de crear, transmitir y asegurar montones de datos digitalizados. Hacer imposible, o siquiera problemático, nuestro acceso al ciberespacio representaría una amenaza estratégica a los intereses vitales de Estados Unidos—uno que a nuestro comando se le ha establecido y encomendado evitar con respecto a las operaciones del DoD en el ciberespacio.

Además, nuestra seguridad cibernética está inextricablemente unida con la de nuestros aliados, y nuestros intereses en el ciberespacio también pueden coincidir con aquellos de otros estados con los cuales tenemos lazos menos formales. La falta de fronteras geográficas en el ciberespacio significa que una amenaza a uno puede constituir una amenaza a todos, lo que nos ofrece un incentivo verdadero para compartir concienciación situacional y las mejores prácticas que ayuden a proteger a nuestra milicia, gobierno y redes privadas y datos.

- Segundo, cuando se nos ordene, necesitamos negarles a nuestros adversarios la libertad de acción en el ciberespacio. Al igual que con todas las actividades que el DoD emprende, las operaciones solamente se ejecutan con una misión clara y bajo autoridades claras, y son gobernadas por todas las leyes pertinentes, inclusive la ley del conflicto armado. No nos podemos dar el lujo de permitir que el ciberespacio sea un santuario en el que adversarios reales y posibles puedan organizar fuerzas y capacidades para usarlas contra nosotros y nuestros aliados. Este no es un peligro hipotético; en las zonas de conflicto donde las fuerzas estadounidenses están trabadas en combate hemos visto, de hecho, que la *Internet* se emplea para reclutar, recaudar fondos, adiestramiento operacional y otras actividades dirigidas en contra del personal de nuestro servicio y los socios de la coalición. En el Comando Cibernético gran parte del enfoque está en ayudar a nuestras tropas en campaña a que limiten las vulnerabilidades en y desde el ciberespacio. Este esfuerzo refleja la probabilidad de que, a partir de ahora, todos los conflictos tendrán un aspecto cibernético, y nuestros intentos para comprender esta evolución serán cruciales para la seguridad futura de Estados Unidos.

Conclusión

El Departamento de Defensa dio un paso importante para nuestra nación al crear el Comando Cibernético de EE.UU. y declararlo completamente operacional. En el Comando Cibernético tenemos una misión de administrar activamente las redes de información del departamento—no solo defenderlas sino también utilizarlas como una herramienta conservando su libertad de acción—y estar igual de preparados para utilizar nuestras capacidades para interrumpir cualquier uso del ciberespacio por parte de nuestros enemigos en contra de los intereses de Estados Unidos. El comando busca:

- aumentar la capacidad de la fuerza laboral cibernética;
- implementar y sacarle provecho, en una asociación sólida con la NSA, la transformación de las redes del departamento;
- trabajar con los comandos combatientes para sincronizar procesos y planificar para entregarles los efectos conjuntos que requieren;
- extender las capacidades de defensa cibernética a lo largo de las redes del gobierno de EE.UU. a través del apoyo de asociaciones con la NSA y el DHS a medida que se esfuerza por asegurar los sistemas de seguridad federales, civiles y no nacionales y,
- con el DHS, incrementar el diálogo del gobierno con los socios privados en cuanto a la protección de la infraestructura crítica de nuestra nación.

El Comando Cibernético de Estados Unidos funciona respetando las libertades civiles y en cumplimiento con las leyes que rigen la privacidad de nuestros compatriotas y según las directrices de la autoridad de mando nacional, y en combinación con los socios de misión en los Departamentos de Defensa, Seguridad Interna, la policía, la comunidad de inteligencia, la industria y el mundo académico. Nosotros no consideramos la seguridad de nuestra nación y la protección de las libertades civiles y la privacidad como un “equilibrio”, más bien, creemos que debemos defender ambas. Confío que juntos tendremos éxito. □

Requisitos de las Organizaciones Terroristas con Capacidad Internacional

MAYOR MICHAEL HAACK, USAF

MUCHO SE ha escrito desde el 11 de septiembre de 2001 sobre el terrorismo y sus causas. Este documento no analizará las ‘causas principales’ del terrorismo internacional no estatal usualmente percibidas, como la pobreza o el fracaso del estado, ni se centrará en la ideología extremista islámica muy difundida hoy. Más bien, buscará aspectos comunes entre los grupos terroristas no estatales que han demostrado capacidad para realizar ataques internacionales exitosos durante un período de varios años. Quizás estos grupos terroristas no hayan logrado sus metas políticas, pero fueron capaces de realizar múltiples ataques terroristas internacionales. Comparando al-Qaeda en la Península Arábiga (AQAP), el Ejército Rojo Japonés (JRA), y otros grupos, demostraré que hay cuatro factores claves comunes de su éxito limitado. Estos factores son 1) ideología internacional, 2) liderazgo exiliado, 3) santuario geográfico y conectividad, y 4) apoyo externo.¹ Con estos factores en mente, Estados Unidos y otras naciones con ideas afines pueden asignar mejor los recursos para los esfuerzos de contrarresto y antiterroristas en todo el mundo. Antes de ahondar en los requisitos, es necesario hacer un poco de historia.

AQAP es una organización franquicia de al-Qaeda con base en Yemen y Arabia Saudita. AQAP es un resultado de la unión formalizada en 2009 entre al-Qaeda en Yemen y los miembros desplazados de al-Qaeda de Arabia Saudita.² La historia de AQAP es larga y destacada. Muchos de los actuales miembros de alto rango trabajaron con al-Qaeda en Afganistán antes de la caída del Talibán, y el grupo fue vinculado también a varios ataques entre los años 2000 y 2003 en Yemen. Éstos incluyen el intento de ataque contra el *USS The Sullivans* y los ataques exitosos contra el *USS Cole* y el tanquero francés *The Limburg*.³ Después que se dio muerte o capturó a dos líderes importantes, el grupo encontró mayor resistencia en Yemen y trasladó sus esfuerzos a Arabia Saudita entre 2003 y 2006 mientras que muchos yihadistas yemenitas se filtraron en Irak. El 3 de febrero de 2006, varios de los futuros líderes escaparon durante una fuga de una prisión en la capital de Sana’a.⁴ Esta fuga coincidió con el aumento de presión de las fuerzas del orden sobre los miembros en Arabia Saudita, lo que facilitó un cambio en personal. Después de este cambio en personal, los ataques comenzaron a redirigirse a intereses occidentales en Yemen, incluyendo varios ataques contra grupos de turistas, la embajada italiana, y la embajada estadounidense que causó la muerte de más de 34 personas.⁵

En 2007, AQAP entró en una nueva fase cuando comenzó a proyectar su poderío en las costas de Estados Unidos y Europa. Se le ha vinculado en el infructuoso ataque a Fort Dix, el ataque a Ft. Hood en 2009, el infructuoso intento de explotar una bomba en un avión cerca de Detroit (el llamado ‘bombardero de los calzoncillos’), y un infructuoso carro bomba en Times Square.⁶ Los ataques en estos casos se inspiraron en Anwar al-Awlaki, el clérigo *online* de AQAP, o fueron asesorados por él. Más recientemente, el grupo fue responsable de dos infructuosos intentos de explotar bombas a bordo de un avión de carga en el Reino Unido y los EAU en octubre de 2010.⁷ Desde este episodio, los eventos en Yemen han mantenido el grupo en el ámbito local y es difícil decir a qué facción se puede atribuir la violencia dentro del país. Es seguro asumir que AQAP está detrás de parte de la violencia reciente contra el gobierno de Yemen, y que buscó socavar la reciente elección para reemplazar al Presidente Saleh.⁸

En los últimos 12 años se han producido numerosos ataques exitosos, pero el ataque al *USS Cole* y Ft. Hood sobresalen por al alto número de bajas estadounidenses, 17 y 13 respectiva-

mente.⁹ Incluso los fracasos de alto perfil de AQAP ayudan a destacar su causa y provocan respuestas militares y no militares de Estados Unidos, lo que ha servido para debilitar al régimen yemenita en opinión de algunos.¹⁰ AQAP ha ayudado también a desestabilizar a Yemen con numerosos ataques contra el gobierno y objetivos occidentales, pero queda por verse si puede lograr una posición de liderazgo entre las tribus. Finalmente, AQAP ha ampliado con éxito la franquicia al-Qaeda, que probablemente contribuyó a la recientemente anunciada alianza de al-Shabaab y al-Qaeda.

El JRA fue parte del movimiento terrorista de izquierda que ganó notoriedad en la década de 1970. Se inició como consecuencia del movimiento político comunista japonés en la década de 1960, y no se dedicó al terrorismo hasta el secuestro de un avión el 30 de marzo de 1970.¹¹ Después del incidente, el liderazgo local del JRA cometió una serie de errores en Japón que dieron lugar a que su líder, Shigenobu Fusako, busque formas de impulsar una agenda más internacional.¹² A principios de 1971, Shigenobu en última instancia abrió el camino del JRA a Líbano e inició su relación con el PLO y el FPLP.¹³ El grupo restante quedó sujeto a presión política y lucha partidaria lo que eventualmente dio lugar a la virtual erradicación del grupo en Japón a principios de 1972.

Entretanto en Líbano, Shigenobu había creado un refugio seguro para los miembros del JRA, y éstos realizaron rápidamente un ataque mortal contra el aeropuerto Lod en Tel Aviv en el que murieron 28 y quedaron heridos 78 el 30 de mayo de 1972.¹⁴ Después de ese ataque, el JRA y el FPLP secuestraron un avión 747 de Japan Air Lines que partió de París y finalmente llegó a Libia después de una odisea de 3 días a través de Dubai y Siria.¹⁵ No murió ningún rehén, pero el avión fue destruido. Después de operaciones en Singapur y Países Bajos, el grupo logró su primera liberación de prisioneros en 1975 después de la toma de rehenes en el consulado estadounidense y la embajada sueca en Kuala Lumpur, Malasia.¹⁶ El JRA convenció nuevamente al gobierno japonés para que libere prisioneros en 1977 después de secuestrar un avión en Bombay, India y obligarlo a aterrizar en Bangladesh.¹⁷

Para la década de 1980, el JRA centró su atención en objetivos estadounidenses. Veían al gobierno japonés como marionetas de Estados Unidos, y resentían la política exterior ‘imperialista’ de Estados Unidos y sus bases en Japón. En 1986 y 1987, el JRA realizó una serie de ataques con explosivos contra las embajadas estadounidense y japonesa en Yakarta, la embajada estadounidense en Madrid, y las embajadas de Estados Unidos y del Reino Unido en Roma.¹⁸ Los últimos ataques importantes del JRA coincidieron con el segundo aniversario del bombardeo aéreo estadounidense de abril de 1986 en Libia, e ilustran su foco en el imperialismo estadounidense como el nuevo enemigo. Detonaron bombas en un club USO en Nápoles, Italia, donde murieron 5 personas, y fallaron un segundo ataque en la Ciudad de Nueva York cuando un policía alerta observó que Kikumura Yu actuaba de manera sospechosa y lo arrestó.¹⁹ Después de 1988, se escuchó muy poco del JRA, y en 2000 Shigenobu Fusako fue arrestado en Japón, produciéndose el desbande del grupo en 2001.²⁰

La primera semejanza entre el JRA y AQAP está en la creencia en un ideología de orientación internacional. La meta principal de AQAP es coherente con la visión de al-Qaeda de establecer un califato islámico. Busca eliminar el régimen local en Yemen, al que consideran una marioneta de una “alianza de Cruzados y Sionistas”.²¹ En este sentido, AQAP ha tratado de alinearse políticamente con las poderosas tribus de Yemen. AQAP apoya a los movimientos Houthi del norte y anti gobierno del sur, pero debido a que los Houthi son chiítas, AQAP no los ve como un posible aliado.²² Además de un cambio en el gobierno, AQAP también busca expulsar a los no musulmanes de la Península Arábiga y adquirir zonas seguras para adiestramiento y operaciones en Yemen.²³ AQAP ofrece también luchar contra la alta tasa de desempleo (35%), alta tasa de crecimiento (3,2%/año) y reservas de petróleo decrecientes de Yemen, que son problemas económicos principales.²⁴ La visión de AQAP se centra en los aspectos internacionales de instalar un gobierno islámico en todo el califato, comenzando en Yemen. Como parte de un movimiento

extremista islámico más amplio, el aspecto internacional de la ideología de AQAP proporciona parte del motivo para ampliar sus operaciones al ámbito internacional.

El JRA intentó derrocar al gobierno japonés e instalar una revolución comunista internacional.²⁵ Aunque inicialmente se formó en Japón, el grupo estaba sujeto a fuerte presión en su propio país cuando comenzó entrar en contacto con otros grupos izquierdistas hacia 1970. En una extraña ironía del destino, varios grupos palestinos se encontraban en la transición a Líbano después de la campaña de ‘Septiembre negro’ en Jordania.²⁶ Esto dio lugar a la alianza del JRA y el Frente Popular para la Liberación de Palestina (FPLP), un grupo simpatizante del marxismo. El JRA aprovechó las oportunidades de adiestramiento con el FPLP y cementó su relación con un ataque devastador contra el aeropuerto de Lod en Israel, su primer esfuerzo importante en el ámbito internacional.²⁷ Además de la revolución marxista, varios de los eventos de toma de rehenes por el JRA en la década de 1970 fueron también intentos de negociar la liberación de prisioneros en Japón.²⁸ Sin embargo, en el fondo el JRA buscaba provocar la revolución marxista internacional, lo que hizo que amplíe su espectro de objetivos potenciales. De manera muy similar a AQAP con su afán de un califato islámico, el JRA también tenía una ideología de orientación internacional.

Para ilustrar el requisito para una ideología internacional, es útil analizar dos grupos terroristas similares con menores ambiciones. Los Dinamiteros Fenianos realizaron ataques contra el Imperio Británico durante la década de 1870 en Canadá y Australia mientras recibían apoyo y refugio de la diáspora irlandesa en los Estados Unidos.²⁹ Su meta declarada era la independencia irlandesa atacando al enemigo en “Irlanda, en India, y en Inglaterra misma donde se presente la ocasión”.³⁰ En cambio, el Ejército Republicano Irlandés (IRA) de un siglo después luchó contra un Imperio Británico bastante más pequeño, y no tenía una ideología internacional de expansión. El grupo recibía fondos externos y refugio, pero debido a que carecía de una agenda internacional de expansión, sólo 3 de sus 2,670 ataques ocurrieron fuera de Europa Occidental.³¹ Aunque los dos grupos tenían metas nacionalistas similares, el IRA no atacó objetivos internacionales porque carecía de una ideología internacional. Si un grupo terrorista tiene metas que incluyen aspectos locales e internacionales, es más probable que logre ataques exitosos a través de las fronteras internacionales.

El segundo aspecto importante del terrorismo internacional es el liderazgo exiliado. El liderazgo de AQAP ha sido relativamente estable desde 2006. Antes de esa fecha hubieron varios cambios en el liderazgo debido a arrestos y acción militar. En 2006, Nasser al-Wahayshi escapó de prisión como parte de la fuga de Sana’a y rápidamente asumió la posición de líder de AQAP.³² Al-Wahayshi es yemenita y había sido secretario personal de Osama Bin Laden. Luchó en Afganistán en 2001, escapó a Irán y fue capturado en 2002, posteriormente fue extraditado a Yemen donde permaneció en prisión hasta su escape.³³ El segundo en el mando de Al-Wahayshi es un hombre con una historia parecida, Saeed al-Shihri.³⁴ Al-Shihri es un saudita que fue arrestado en Afganistán a fines de 2001 supuestamente por colaborar en la entrada de combatientes extranjeros al país. Permaneció en Guantánamo hasta 2007 cuando fue repatriado a Arabia Saudita y pasó por un programa de reintegración antes de su liberación.³⁵ Después de su liberación se unió a AQAP y asumió la función de segundo jefe. Abdullah al-Rimi es el comandante militar de AQAP.³⁶ Al-Rimi es buscado en conexión con el atentado con bombas al *USS Cole*. Fue arrestado en algún momento entre 2003 y 2004 y terminó en la prisión de Sana’a de donde escapó en 2006.³⁷ Después de su escape, asumió su función de comandante militar. Finalmente, Anwar al-Awlaki fue el clérigo *online* de AQAP hasta su muerte en septiembre de 2011.³⁸ Awlaki, y su asistente Samir Khan, eran ambos estadounidenses que vivían en Yemen.³⁹ Todos estos hombres fueron desterrados de su patria en el pasado, o viven actualmente en el exilio. Vivir en el exilio les proporcionó a estos hombres el motivo y los medios para realizar ataques internacionales.

El liderazgo del JRA vivió exclusivamente en el exilio durante su período de terror internacional. Shigenobu Fusako fue la principal líder de la facción del JRA que permaneció activa después

de la campaña del gobierno japonés. Estableció residencia en Líbano y permaneció en el extranjero hasta después de las acciones internacionales finales del JRA en 1988.⁴⁰ De hecho, cuando fue arrestada en Japón en noviembre de 2000, había estado de regreso en el país por menos de 6 meses después de huir de una campaña contra el JRA en Líbano.⁴¹ El número dos del JRA, Maruoke Osamu, también vivió en el extranjero gran parte de su vida. Luego de partir al Líbano en 1971, pasó tiempo en adiestramiento y operaciones desde Bengasi hasta Manila antes de su arresto en Japón en noviembre de 1987.⁴² Al momento de su arresto, se sospecha que estaba tratando de restablecer una presencia local del JRA en Japón en preparación para el esfuerzo de abril de 1988 contra las bases estadounidenses en ultramar. Otro líder principal del JRA, Wako Haruo, participó en muchos de los secuestros en la década de 1970 y también vivió en Líbano.⁴³ Fue arrestado en la campaña de marzo de 2000 en Líbano y extraditado a Japón.⁴⁴ El liderazgo del JRA vivió fuera de Japón debido a la acción policial contra éste, y el grupo no la pasó mal hasta que perdieron su refugio seguro en Líbano.

Vivir en el exilio es un aspecto común para algunos de los terroristas internacionales más notorios de los últimos 50 años. Osama bin Laden creció en Arabia Saudita antes de su exilio en Afganistán, Sudán y Paquistán.⁴⁵ Ayman al-Zawahiri era de Egipto antes de mudarse a los mismos países simpatizantes de al-Qaeda.⁴⁶ Abu Nidal nació en Jaffa, Palestina (hoy Tel Aviv) y vivió en el exilio alrededor del Oriente Medio después de la formación de Israel.⁴⁷ Antes de sus carreras activas en Jordania y Líbano, Yasser Arafat creció en Cairo, y Carlos 'El Chacal' vino de Venezuela. Obviamente vivir en el exilio no convierte a una persona en un terrorista internacional, pero hay una correlación en el hecho que los terroristas exportan sus acciones internacionalmente. La motivación para actuar en el ámbito internacional es mucho mayor cuando un líder principal del grupo tiene vínculos históricos a través de fronteras internacionales. Los grupos terroristas que actúan en una escala internacional, especialmente sobre distancias más grandes, necesitan motivación adicional. A menudo esta motivación la suministra el liderazgo exiliado que piensa en términos de una audiencia internacional, no solamente en una que es local.

Otro requisito importante para el terrorismo internacional es santuario geográfico y conectividad. En Yemen, la topografía actual no es tan importante como la existencia de zonas desgobernadas. AQAP se aprovecha de la debilidad del gobierno nacional para aliarse con los líderes tribales y obtener refugio.⁴⁸ El gobierno nacional es incapaz de hacer cumplir la ley en ciertas zonas tribales, y tiene poco control de sus fronteras y puntos de tránsito. AQAP puede usar el refugio en Yemen para adiestrar y fomentar la yihad. En su caso, la conectividad con el resto del mundo se hizo difícil con las restricciones de viaje y las nuevas técnicas de control como el software de reconocimiento facial. El aeropuerto de Sana'a no es hoy día tan falto de gobierno como el resto del país. Sin embargo, Yemen ofrecía conectividad en otras formas que el gobierno difícilmente podía interrumpir. En Yemen hay 12 millones de teléfonos móviles y fijos, y otros 2,3 millones de usuarios de internet.⁴⁹ En cambio, Somalia tiene 748.000 teléfonos y 106.000 usuarios de internet.⁵⁰ Aunque los terroristas en Somalia todavía podían tener conectividad con los teléfonos satelitales, los números permiten seguridad y eficiencia. Las telecomunicaciones se propagan a través de una gran parte de la población yemenita, haciendo que sea muy difícil evitar o explotar los métodos que AQAP usa para conectarse con el mundo. Esta conectividad permitió que AQAP disemine su mensaje al terrorista 'Lobo solitario' que vive en algún otro lugar. La combinación de santuario y conectividad encontrada en Yemen es un habilitador geográfico muy importante para AQAP.

El JRA también explotó la geografía de una manera muy similar. En 1970 Líbano era un refugio seguro para muchas organizaciones terroristas, mayormente palestinas. El JRA usó este santuario para adiestrarse y evitar que las autoridades internacionales los capture. Aunque considerado 'desgobernado', Líbano aún mantenía acceso internacional con un aeropuerto internacional totalmente funcional en Beirut. De hecho, Estados Unidos no actuó para aislar al aeropuerto ni a las aerolíneas libaneses hasta después del secuestro de 1985.⁵¹ El Secretario de

Estado explicó el motivo para “prohibir el acceso internacional de ese aeropuerto hasta que el pueblo de Beirut haga lo mismo con los terroristas”.⁵² Como herramienta unilateral este movimiento fue más una maniobra diplomática que una medida de ejecución, pero demuestra la importancia de la conectividad para el terrorista internacional. Durante los buenos tiempos del JRA, disfrutaron acceso a un aeropuerto internacional con una seguridad menos que estelar, lo que les permitió difundir sus actividades terroristas a zonas cercanas y lejanas del mundo. La combinación esencial de santuario geográfico y conectividad es un aspecto vital del terrorismo internacional.

Varios otros ejemplos a través de la historia ilustran este fenómeno. Los estados que apoyan el terrorismo pueden hacerlo porque controlan su propio territorio y se conectan con la comunidad internacional. Se puede mirar a Libia en la década de 1980 e Irán desde 1979 como dos ejemplos de países que permitieron que los grupos terroristas sigan actuando. Las zonas no gobernadas como las Áreas Tribales Administradas Federalmente (FATA) en la frontera Afganistán-Paquistán y la parte sur de Somalia son semilleros para adiestramiento de terroristas. Estas zonas sin gobierno no siempre facilitan el terrorismo internacional porque a menudo carecen de conectividad. A principios de la Guerra Global contra el Terrorismo, el énfasis estuvo en el Área de las Tres Fronteras (TBA) de América del Sur, compartida por Argentina, Brasil y Paraguay.⁵³ Esta zona proporcionaba santuario (si se conocía a la gente adecuada), y es conocida como una zona de contrabando, pero los países aledaños pudieron impedir que los grupos terroristas internacionales se afinquen allí. Evidentemente hay varios grados de santuario y conectividad, y el TBA atrajo un alto nivel de vigilancia después del 11 de septiembre de 2001.⁵⁴ En particular, no ha habido actividad terrorista internacional importante proveniente de esta región desde aquel tiempo.

El último requisito habilitador para los terroristas internacionales es el apoyo externo. El apoyo proporciona la logística para la acción, mientras que la fuente externa proporciona la motivación para actuar en un ámbito más amplio. AQAP recibió mucho apoyo de al-Qaeda y sus benefactores en Arabia Saudita. El apoyo externo está bien documentado y es un gran problema, según documentos de gobierno revelados recientemente.⁵⁵ El apoyo externo es fundamental para la intención de AQAP de actuar internacionalmente porque proporciona contactos fuera de Yemen y motiva la acción para mantenerse en la atención del público y recaudar fondos. También hay un elemento de motivación que viene de donantes importantes que ejercen presión para que la organización actúe en áreas específicas. Por ejemplo, si estos donantes viven en Arabia Saudita les gustaría ver en algún momento acción en el territorio saudita. El apoyo externo es fundamental no sólo para los medios de los terroristas internacionales, sino también para el motivo.

El JRA también recibió apoyo externo durante gran parte de su existencia. Este apoyo comenzó en 1970 cuando Shigenobu formó una alianza con el PLO y el FPLP.⁵⁶ De esta alianza el JRA recibió adiestramiento y mucho apoyo de los palestinos. Este apoyo continuó durante comienzos de la década de 1980 cuando el JRA acudió al Coronel Gadafi en Libia.⁵⁷ Al final se estrecharon más las relaciones entre el JRA y sus patrocinadores estatales, pero nunca se pudo considerar al JRA como una organización auspiciada por un estado. Fueron cuidadosos en elegir aliados que estuvieran en la misma página política y que trabajen en dirección a la revolución marxista global. El requisito de apoyo externo significó que en algunos casos se podría manipular al JRA a la acción. El ataque contra el aeropuerto de Tel Aviv en 1972 fue un esfuerzo de solidificar la alianza con los palestinos. Posteriormente, los ataques de 1988 contra objetivos estadounidenses en Nueva York y Nápoles posiblemente fueron llevados a cabo a pedido de Gadafi en represalia por el ataque aéreo estadounidense. No ha habido evidencia que demuestre que el JRA se ofreció por contrato como Carlos o Abu Nidal, pero el grupo fue influenciado en la selección de sus objetivos debido a su apoyo externo.

El PLO y el FPLP también hicieron gran uso del apoyo externo. Los palestinos desterrados y los estados árabes proporcionaron fondos para el PLO.⁵⁸ Además, la KGB suministró armas y adiestramiento a los palestinos y otras organizaciones terroristas marxistas.⁵⁹ Entre estas fuentes de apoyo externo, ambas organizaciones tuvieron bastante motivación para actuar internacionalmente. Es interesante observar que los ataques del FPLP fuera del Oriente Medio pararon en 1991, el mismo año en que se desmembró la URSS. La Figura 1 muestra datos por año y región para el FPLP.⁶⁰ Este grupo es un excelente ejemplo en que el financiamiento externo tiene un papel directo en la selección de objetivos internacionales. Los datos no son definitivos ya que también pudieron cambiar otras circunstancias durante este período (como liderazgo, santuario o estrategia).

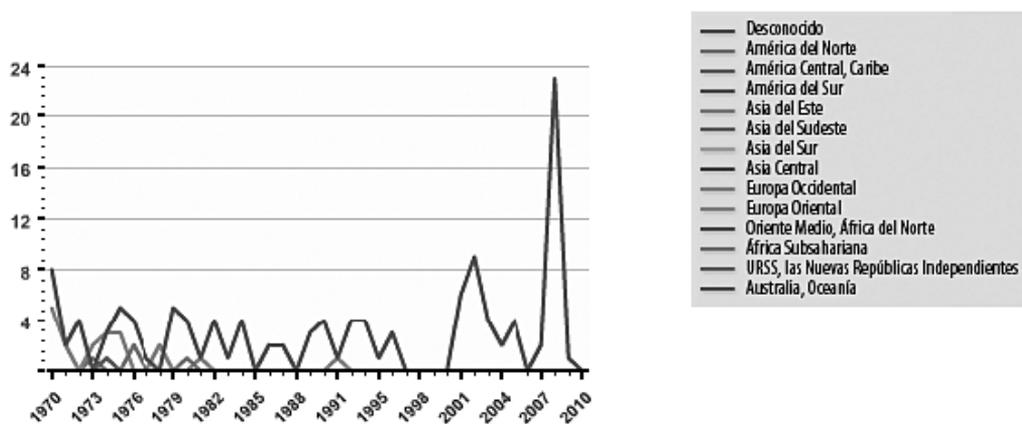


Figura 1. Ataques del FPLP por región

La conclusión lógica es centrar los esfuerzos estadounidenses contra el terrorismo y antiterroristas con este conocimiento a la mano. Primero debemos analizar los esfuerzos antiterroristas, o el uso de medidas para evitar el terrorismo mediante la acción indirecta. En lugar de enviar ayuda externa a todo estado fallido con posibles santuarios para terroristas, EE.UU. puede centrar esta ayuda en base a los factores restantes. Sin tener inteligencia específica sobre futuras organizaciones terroristas extranjeras, un predictor lógico del liderazgo exiliado es el número de refugiados aceptados por un país. Una proporción más alta de refugiados que viven dentro de un país debe tener correlación con la probabilidad de que los exiliados puedan recurrir al terrorismo. Además, como la mayoría de estados frágiles ofrecen oportunidades de viaje internacional que son difíciles de analizar (por ejemplo, por tierra), un buen predictor de la conectividad internacional es la proporción de la población que utiliza Internet. Sería difícil predecir qué grupos terroristas futuros odiarían tanto al Oeste como para producir una ideología de mentalidad internacional, o qué grupos recibirían apoyo externo en el futuro, por lo que un análisis rápido basado en estos factores (fallo de seguridad, usuarios de Internet, y refugiados) debe ser revelador.

La Figura 2 ilustra un grupo de países que son posibles destinos de la ayuda externa. El Índice de Seguridad FSI viene de ForeignPolicy.com y su índice de Estados fallidos de 2011. La gráfica muestra los 20 peores países de acuerdo con el índice del 'Aparato de seguridad'.⁶¹ El % de usuarios de Internet es el porcentaje de la población que tiene acceso a Internet.⁶² La estadística final de la UNHCR es la relación del número de refugiados en un país dividido por la población del país multiplicada por 1000.⁶³ Como se puede ver en los datos, varios países están cerca del mí-

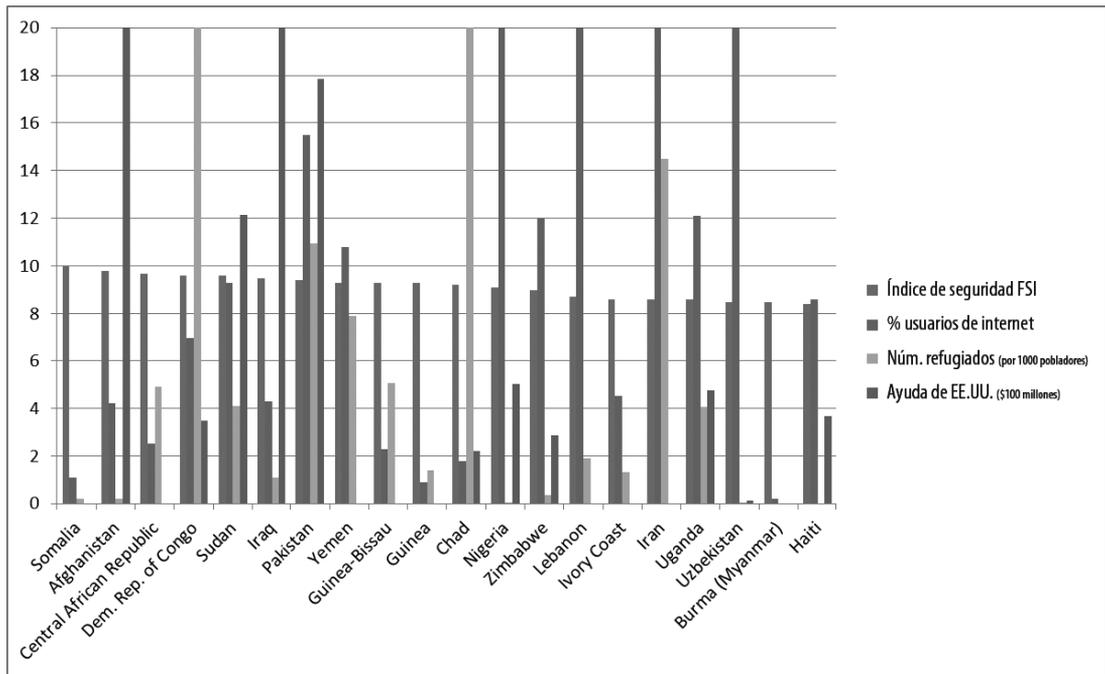


Figura 2. Grupo de Países que son Posibles Destinos de la Ayuda Externa

nimo en las tres categorías, incluyendo: Congo, Sudán, Pakistán, Yemen, Irán, y Uganda. Estos países tienen la más alta probabilidad de producir grupos terroristas con capacidad internacional porque es probable que tengan santuarios, conectividad internacional y exiliados que viven dentro del país. Estados Unidos y sus aliados deben centrar los esfuerzos de ayuda exterior y antiterrorista (es decir, adiestramiento militar, control de viajeros y monitoreo de Internet) en estos países. Como se desprende de los datos, muchos de los países no recibieron mucho en términos de ayuda estadounidense en 2009 (particularmente Congo, Yemen y Uganda).⁶⁴ Si el terrorismo es una prioridad alta en el ámbito de la seguridad nacional, estos países deberían recibir más atención.

En el ámbito contra el terrorismo, los servicios militares y de inteligencia de Estados Unidos deben centrar sus esfuerzos primero en los grupos o células terroristas extranjeros que cumplan los cuatro requisitos. El esfuerzo es menos efectivo cuando se utiliza sobre grupos que sólo poseen uno o dos de los requisitos. Después de identificar a estos grupos, se debe tomar medidas para eliminar uno o más de los requisitos. La acción directa se debe centrar en liquidar o capturar a los líderes exiliados. La presión diplomática se debe centrar en eliminar refugios seguros para los grupos identificados. La vigilancia se debe centrar en monitorear y bloquear los métodos de comunicación y viaje usados por los grupos especificados y en los lugares especificados. Los esfuerzos diplomáticos deben tratar de hacer difícil la transferencia de dinero a esos grupos y el viaje de su personal. Finalmente, se debe realizar campañas de información contra estas organizaciones para convencerlas a cambiar sus objetivos de internacionales a objetivos locales o regionales.

En conclusión, este análisis muestra los 4 requisitos de organizaciones terroristas con capacidad internacional y sugiere estrategias contra el terrorismo y antiterroristas para combatirlos. Estados Unidos debe preocuparse más sobre terroristas que tienen 1) ideología orientada al

ámbito internacional, 2) liderazgo exiliado, 3) santuario geográfico y conectividad, y 4) apoyo externo. Aunque todos los terroristas operan fuera del sistema internacional, es más probable que los grupos terroristas que reúnan estas características puedan montar con éxito ataques contra los Estados Unidos y sus aliados. La estrategia para contrarrestar a estos grupos debe centrarse en prevención, predicción y acción contra los grupos existentes. Estos esfuerzos se deben centrar cuando menos en uno de los cuatro requisitos. Se debe contrarrestar agresivamente a las organizaciones terroristas de este tipo porque una vez que reúnan los cuatro requisitos pueden causar problemas por décadas. □

Notas

1. Estos factores son una ligera variación de los requisitos de la insurgencia exitosa de Galula 1) causa, 2) debilidad del contrainsurgente, 3) condiciones geográficas, y 4) apoyo externo. David Galula, *Counterinsurgency Warfare: Theory and Practice (Guerra de contrainsurgencia: Teoría y práctica)*, (Westport, CT: Praeger Security International, 2006), 11-28.

2. Alistair Harris, *Exploiting Grievances: Al-Qaeda in the Arabian Peninsula (Explotación de los agravios: Al-Qaeda en la Península Arábiga)* (Washington, DC: The Carnegie Endowment for International Peace, mayo de 2010), 2.

3. Sarah Phillips, *What Comes Next in Yemen? Al-Qaeda, the Tribes, and State-Building (Qué viene después en Yemen: Al-Qaeda, las tribus, y el desarrollo del estado)* (Washington, DC: The Carnegie Endowment for International Peace, marzo de 2010), 3.

4. Harris, 3.

5. Harris, 4.

6. Richardson, 2.

7. Universidad de Maryland, Base de Datos del Terrorismo Global, <http://www.start.umd.edu/gtd> (consultado el 15 de febrero de 2012).

8. Reuters, "Militants kill Yemen officer, election official (Militantes asesinan a oficial electoral en Yemen)", 15 de febrero de 2012, <http://www.reuters.com/article/2012/02/15/us-yemen-militants-idUSTRE81E28220120215>.

9. Universidad de Maryland, Base de Datos del Terrorismo Global, <http://www.start.umd.edu/gtd> (consultada en 15 de febrero de 2012).

10. Phillips, 11.

11. William R. Farrell, *Blood and Rage, The Story of the Japanese Red Army (Sangre y furia, la historia del Ejército Rojo Japonés)* (Lexington, MA: Lexington Books, 1990), 81.

12. *Ibíd*, 103.

13. *Ibíd*, 125.

14. Universidad de Maryland, Base de Datos del Terrorismo Global, <http://www.start.umd.edu/gtd> (consultada el 1 de marzo de 2012).

15. Farrell, 153.

16. *Ibíd*, 165.

17. *Ibíd*, 185.

18. *Ibíd*, 208.

19. *Ibíd*, 211.

20. Universidad de Maryland, Base de Datos del Terrorismo Global, <http://www.start.umd.edu/gtd> (consultada el 1 de marzo de 2012).

21. Harris, 6.

22. Harris, 7.

23. Harris, 7-8.

24. Teniente Coronel Darren L. Richardson, *Al Qaida and Yemen – Is Our Current Policy Good Enough? (Al-Qaeda y Yemen – ¿Es suficiente nuestra política actual?)* (Carlisle Barracks, PA: U.S. Army War College, 2011), 7.

25. Universidad de Maryland, Base de Datos del Terrorismo Global, <http://www.start.umd.edu/gtd> (consultada el 1 de marzo de 2012).

26. Michael Burleigh, *Blood & Rage, A Cultural History of Terrorism (Sangre y furia, una historia cultural del terrorismo)* (New York, NY: Harper Perennial, 2010), 160.

27. Universidad de Maryland, Base de Datos del Terrorismo Global, <http://www.start.umd.edu/gtd> (consultada el 1 de marzo de 2012).

28. Farrell, 190.

29. Burleigh, 10.

30. *Ibíd.*
31. Universidad de Maryland, Base de Datos del Terrorismo Global, <http://www.start.umd.edu/gtd> (consultada el 12 de marzo de 2012).
32. También conocido como Abu Basir. Phillips, 4.
33. BBC News South Asia, "Al-Qaeda's remaining leaders (Líderes restantes de al-Qaeda)", *BBC.co.uk*, 30 de septiembre de 2011, <http://www.bbc.co.uk/news/world-south-asia-11489337>.
34. Harris, 2.
35. Robert F. Worth, "Freed by the U.S., Saudi Becomes a Qaeda Chief (Liberado por Estados Unidos, saudita se convierte en jefe de al-Qaeda)", *NYTimes.com*, 22 de enero de 2009, <http://www.nytimes.com/2009/01/23/world/middleeast/23yemen.html>.
36. También conocido como Qasim Yahya Mahdi al-Rimi. Naciones Unidas, "Al-Qaida Sanctions List (Lista de sanciones de al-Qaeda)", 21 de febrero de 2012, <http://www.un.org/sc/committees/1267/NSQI28210E.shtml>.
37. The Telegraph, "Al-Qaeda head in Yemen calls for killing of Saudi rulers (Jefe de al-Qaeda en Yemen insta a asesinar a gobernantes sauditas)", <http://www.telegraph.co.uk/news/worldnews/al-qaeda/8671051/Al-Qaeda-head-in-Yemen-calls-for-killing-of-Saudi-rulers.html> (consultado el 22 de febrero de 2012).
38. Martha Raddatz, Nasser Atta, y Brian Ross, "Al Qaeda's Anwar al-Awlaki Killed in CIA Drone Strike (Muere Anwar al-Awlaki, de Al Qaeda, en ataque con avión remoto de la CIA)", *ABCNews.com*, 30 de septiembre de 2011, <http://abcnews.go.com/Blotter/anwar-al-awlaki-killed-officials-yemen-confirm-al/story?id=14638303>.
39. *Ibíd.*
40. Farrell, 240.
41. BBC News, "Japanese Red Army leader arrested (Arrestado líder del Ejército Rojo Japonés)", *BBC.co.uk*, 8 de noviembre de 2000, <http://news.bbc.co.uk/2/hi/asia-pacific/1012780.stm>.
42. Farrell, 202.
43. Farrell, 190.
44. The Japan Times, "Police nab Red Army founder Shigenobu (Policía captura a fundador del Ejército Rojo Shigenobu)", 9 de noviembre de 2000, <http://www.japantimes.co.jp/text/nn20001109a1.html>.
45. PBS.org, "Who is Osama bin Laden and what does he want? (¿Quién es Osama bin Laden y qué quiere?)" <http://www.pbs.org/wgbh/pages/frontline/shows/binladen/who/> (consultado el 19 de marzo de 2012).
46. Gilles Kepel y Jean-Pierre Milelli, editores, *Al Qaeda in its Own Words (Al Qaeda en sus propias palabras)* (Cambridge, MA: The Belknap Press of Harvard University Press, 2008), 151.
47. Ewan MacAskill y Richard Nelsson, "Mystery death of Abu Nidal, once the world's most wanted terrorist (Muerte misteriosa de Abu Nidal, alguna vez el terrorista más buscado del mundo)", *The Guardian*, 19 de agosto de 2002, <http://www.guardian.co.uk/world/2002/aug/20/israel>.
48. Harris, 8.
49. CIA Factbook, <https://www.cia.gov/library/publications/the-world-factbook/geos/ym.html> (consultado el 1 de marzo de 2012).
50. CIA Factbook, <https://www.cia.gov/library/publications/the-world-factbook/geos/so.html> (consultado el 19 de marzo de 2012).
51. Bernard Gwertzman, "Israelis Set to Release 300; U.S. Opens Diplomatic Drive to 'Isolate' Beirut Airport (Israel listo para liberar 300; EE.UU. inicia campaña diplomática para 'aislar' el aeropuerto de Beirut)", *New York Times*, 2 de julio de 1985, 1.
52. *Ibíd.*
53. Teniente Coronel Philip K. Abbott, "Terrorist Threat in the Tri-Border Area: Myth or Reality? (Amenaza terrorista en el Área de las Tres Fronteras: Mito o realidad?)" *Military Review*, septiembre/octubre de 2004, http://www.army.mil/professionalWriting/volumes/volume3/january_2005/1_05_4.html.
54. *Ibíd.*
55. Eric Lichtblau y Eric Schmitt, "Cash Flows to Terrorists Evades U.S. Efforts (Flujo de dinero a los terroristas evade los esfuerzos estadounidenses)" *NYTimes.com*, 5 de diciembre de 2010, <http://www.nytimes.com/2010/12/06/world/middleeast/06wikileaks-financing.html?pagewanted=all>.
56. Farrell, 106.
57. Farrell, 219, 229.
58. Burleigh, 157.
59. Burleigh, 171.
60. Universidad de Maryland, Base de Datos del Terrorismo Global. http://www.start.umd.edu/gtd/search/Results.aspx?chart=regions&casualties_type=&casualties_max=&perpetrator=838. (consultado el 4 de abril de 2012).

61. El Índice de Estados Fallidos de 2011, ForeignPolicy.com, http://www.foreignpolicy.com/articles/2011/06/17/2011_failed_states_index_interactive_map_and_rankings. (consultado el 4 de abril de 2012).

62. InternetWorldStats.com, <http://www.internetworldstats.com/afrika.htm> y <http://www.internetworldstats.com/asia.htm> (consultado el 4 de abril de 2012).

63. The Guardian, “UNHCR 2011 refugee statistics: full data (Estadística de refugiados del UNHCR de 2001: datos completos)”, <http://www.guardian.co.uk/news/datablog/2011/jun/20/refugee-statistics-unhcr-data#data> (consultado el 4 de abril de 2012).

64. Oficina del Censo de los Estados Unidos, Resumen Estadístico de los Estados Unidos: 2012, “Table 1299. U.S. Foreign Economic and Military Aid by Major Recipient Country: 2001-2009 (Tabla 1299. Ayuda externa económica y militar estadounidense según principales países beneficiarios: 2001-2009)”. <http://www.census.gov/compendia/statab/2012/tables/12s1299.pdf>. (consultado el 19 de abril de 2012).



El Mayor Michael A. Haack, USAF, es un estudiante de la clase del 2012 del Air Command and Staff College, Base de la Fuerza Aérea de Maxwell, Alabama. Se graduó en la Academia de la Fuerza Aérea en 1999. Recibió adiestramiento de piloto en la Base de la Fuerza Aérea en Columbus, Mississippi, y en la Estación Aeronaval de Corpus Christi, Texas. Después completó misiones como comandante y piloto evaluador de aviones MC-130H en Hurlburt Field, Florida, y en la Real Fuerza Aérea en Mildenhall, United Kingdom. Durante estas misiones completó varios despliegues en Afganistán, Iraq, África del Norte, y Colombia. El Mayor Haack se desempeñó como jefe de planes de misiones especiales, para la Primera Ala de Operaciones Especiales en Hurlburt Field, Florida. Antes de su asignación al Air Command and Staff College, el Mayor Haack fue destacado a la Operación NUEVO AMANECER en Iraq y como comandante del Escuadrón de Operaciones Especiales.

Diseñando Colisiones de Satélites en la Guerra Cibernética Encubierta*

DR. JAN KALLBERG, PHD

EL ESPACIO EXTERIOR ha gozado después de la Guerra Fría de dos décadas de un desarrollo bastante pacífico, pero una vez más se hizo más competitivo y disputado con la mayor militarización. Por lo tanto, es importante que EE.UU. mantenga su superioridad espacial para asegurarse de que tenga las capacidades bélicas modernas para tener éxito en las operaciones. La diferencia con los períodos anteriores en el espacio¹ es que no es una carrera armamentística espacial² anunciada de forma flagrante sino un reto encubierto para los intereses de EE.UU. en mantener la superioridad, la resistencia y la capacidad. Hay un número finito de naciones que se consideran actores geopolíticos, pero mientras EE.UU. mantiene la superioridad espacial, esos estados deben comportarse según un conjunto de reglas escritas sin su consentimiento y sin ser forzados. Para los regímenes autoritarios, los haberes espaciales de EE.UU. supervisan sus acciones y buscan tener una influencia regional, lo que es muy inquietante. Para ellos, cualquier degradación o limitación de las capacidades espaciales de EE.UU. se consideraría como un resultado satisfactorio. La guerra cibernética de estos actores antagonistas ofrece la oportunidad de destruir directa o indirectamente los haberes espaciales de EE.UU. con un riesgo mínimo debido a una atribución y capacidad de identificación limitadas. El asunto de este artículo es cómo podrían lograr esta tarea. Uno debe empezar examinando la dependencia de Estados Unidos en el espacio antes de concentrarse en la obstrucción espacial y los medios que utilizaría un adversario. Mientras que la protección satelital es un reto, hay varias soluciones que EE.UU. debe tener en cuenta en los años venideros.

Dependencia de EE.UU. del espacio

La guerra concentrada en la red depende de la red de información global para capacidades de combate conjuntas.³ La capa fundamental crea la capacidad de combate global como la columna vertebral espacial de la red de información donde los haberes espaciales son el elemento decisivo. EE.UU. depende de las capacidades espaciales para su éxito y la seguridad nacional de EE.UU. se basa hoy en día en un número limitado de satélites muy utilizados. Estos satélites son cruciales para la disuasión estratégica, la vigilancia, la recopilación de inteligencia y las comunicaciones militares. Si la disuasión estratégica falla, los satélites forman parte integral de la defensa de misiles balísticos ofensivos y defensivos. Los satélites son fundamentales no solamente para la superioridad espacial de EE.UU., sino también para la superioridad de información—el motor en la maquinaria de combate bélico conjunta de canales múltiples que ha demostrado tener éxito en recientes conflictos. Las fuerzas estadounidenses pueden luchar globalmente debido al acceso al C4ISR apoyado por satélites. Los adversarios potenciales, de todos los tamaños e intenciones, entienden que las fuerzas militares de EE.UU. podrían estar estrechamente relacionadas con los haberes espaciales de EE.UU. Este enlace exclusivo entre los haberes espaciales y la seguridad nacional lo expresa bien el director Finch y el subdirector Steele de la Oficina del Subsecretario de Defensa para Política;

*Fuente: Publicado anteriormente en nuestra revista *Strategic Studies Quarterly*, Spring 2012

“Aunque otros estados utilizan cada vez más el espacio para fines económicos y militares, Estados Unidos es el país que mucho más depende de sistemas espaciales debido a sus responsabilidades globales y su método de combate de alta tecnología que aprovecha en gran medida los sistemas espaciales para la comunicación, la navegación, la inteligencia, la vigilancia y el reconocimiento. Esta asimetría crea un desequilibrio; cuanto más confíe una nación en sistemas espaciales, mayor será la tentación de que un posible adversario fije esos sistemas como objetivos”.⁴

Desde la caída de la Unión Soviética, la superioridad espacial de EE.UU. no ha sido retada extensivamente y hemos presenciado dos décadas de supremacía espacial de EE.UU. Los ataques contra los satélites de EE.UU. han sido una preocupación desde los años 70⁵ con un enfoque en interferencia de señales, rayos láser desde tierra⁶ y ataques de misiles directos antisatelitales cinéticos. William J. Lynn, III, anterior Subsecretario de Defensa de EE.UU., afirmó lo siguiente en el verano de 2011;

“La voluntad de los estados de interferir con satélites en órbita tienen implicaciones serias para nuestra seguridad nacional. Los sistemas espaciales permiten nuestra forma de guerra moderna. Permiten que nuestros combatientes ataquen con precisión, naveguen con exactitud, se comuniquen con certeza y vean el campo de batalla con claridad. Sin ellos, muchas de nuestras ventajas militares más importantes se evaporan”.⁷

Los comentarios de Lynn se deben en gran medida a la Estrategia Espacial de Seguridad Nacional de enero de 2011. La estrategia indica que el espacio está congestionándose, disputándose y haciéndose más competitivo. Claramente describe la importancia de proteger las capacidades espaciales de EE.UU.;

“La Estrategia Espacial de Seguridad Nacional se basa en todos los elementos del poder nacional y requiere un liderazgo activo de EE.UU. en el espacio. Estados Unidos buscará un conjunto de métodos estratégicos interrelacionados para cumplir con nuestros objetivos espaciales de seguridad nacional, a saber: estimular el uso responsable, pacífico y seguro del espacio; mejorar las capacidades espaciales mejoradas de EE.UU.; asociarse con naciones responsables, organizaciones internacionales y firmas comerciales; prevenir y disuadir la agresión contra la infraestructura espacial que respalda la seguridad nacional de EE.UU.; y prepararse para rechazar ataques y operar en un entorno degradado”.⁸

Lynn también observó el impacto de la cantidad creciente de residuos espaciales;

“El espectro de las interferencias no es la única nueva preocupación. La colisión de febrero de 2009 de un satélite de comunicaciones Iridium con un satélite soviético desactivado, y la anterior y deliberada destrucción de un satélite por China, produjeron miles de fragmentos residuales, cada uno de los cuales plantea una amenaza potencialmente catastrófica a la aeronave espacial operacional. En un instante, estos eventos, uno accidental, el otro premeditado, duplicaron la cantidad de residuos espaciales, haciendo que las operaciones espaciales sean más complicadas y peligrosas”.⁹

El ataque cinético y la destrucción deliberados de un satélite en desuso por los mismos chinos usando un misil antisatélite atrajo la atención no solamente al hecho de que los chinos probaran el misil antisatélite y el impacto de la política¹⁰, sino también la nube de residuos que produjo la explosión.

Un espacio muy congestionado

La cuestión de residuos espaciales se complica debido a la miríada de problemas que representan no solamente los obstáculos físicos para eliminar residuos sino también los asuntos legales e internacionales.¹¹ En consecuencia, el espacio se está congestionando más con unos 1.100 y 2.000 satélites inactivos en órbita.¹² Con el tiempo, la cantidad de residuos espaciales ha aumentado constantemente¹³ y la cantidad total de residuos rastreados asciende actualmente a 22.000 objetos. Los primeros pasos para crear una estrategia de mitigación de residuos se dieron a finales de

los años 70.¹⁴ Desde entonces, se han lanzado al espacio miles de satélites y la mayoría de éstos están inactivos o son de una generación de tecnología más antigua al final de su vida útil. EE.UU. ha liderado el esfuerzo de reducción de residuos para mitigar los riesgos diseñando activamente vehículos espaciales que podrían desecharse o eliminarse de forma segura por degradación orbital.¹⁵ El problema principal referente a los residuos espaciales es el interés mutuo en limitar los efectos de los residuos espaciales y en hacer un esfuerzo conjunto para disminuir la cantidad de residuos de modo que con el tiempo predominen la degradación orbital y la gravedad.

Para entender la potencia destructora de los residuos espaciales la velocidad tiene importancia. Un proyectil militar estándar de 5,56 mm se desplaza a 940 m/s cuando sale del cañón y puede penetrar fácilmente en un ser humano. Un proyectil de carro de combate de EE.UU. de 120 mm tiene una velocidad inicial de 1.740 m/s¹⁶ y puede atravesar un carro de combate de batalla de tamaño medio. Los residuos espaciales y la basura espacial que se desplazan a una velocidad orbital circular impactarán en un satélite a una velocidad de 3.000 a 7.600 m/s, dependiendo de la altitud. Los residuos, que se desplazan más de ocho veces más rápido que una bala de rifle de alta velocidad, ya sea una llave ajustable perdida hace mucho tiempo, de los años 70, con las letras CCCP estampadas, o una bala de acero dispersada intencionalmente, crea un impacto sin precedentes. La creación de residuos espaciales de forma deliberada e intencionada en órbitas específicas cambiaría radicalmente las probabilidades de impacto, incluso si la mayoría de los residuos se perdieran en otras direcciones o fueran afectados y eliminados por efectos físicos. Una colisión planeada o una nube grande de residuos en una órbita idéntica anularía la opción de sacar el objetivo del área fijada como objetivo. Los satélites son obras maestras frágiles de ingeniería electrónica, cables, conectores, paneles solares, circuitos integrados y antenas de alta frecuencia. Cada centímetro tiene una función especial. Cualquier objeto que se desplace a 7.600 m/s es una amenaza real para el satélite.

El síndrome de Kessler

El antiguo experto de la NASA en residuos espaciales, Donald J. Kessler, predijo la probabilidad de colisiones en el espacio y el riesgo de colisión que produciría una gran cantidad de residuos espaciales después del impacto de una colisión a alta velocidad.¹⁷ Una reacción en cadena, llamada síndrome de Kessler podría ser la consecuencia. El síndrome de Kessler se produce cuando los residuos u otro satélite colisionan con otro satélite (o basura espacial) con hipervelocidad, producen muchos más residuos debido al impacto hiperveloz y si la densidad del satélite (o basura espacial) es suficientemente alta podría surtir un efecto en cadena por el espacio. Kessler predijo el problema pero también indicó claramente, en los años 70, que la cantidad de basura espacial y satélites era demasiado pequeña para producir efectos en cadena en el espacio. Más adelante, ha reconfirmado la posición. La contribución de Kessler era identificar el problema y explicarlo. Desde que Kessler escribió sobre el problema en 1978, ha vuelto al tema para aclarar, ampliar la cuestión o presentar sus cálculos.¹⁸ El trabajo de Kessler se concentró en colisiones inintencionadas, aleatorias y descontroladas. De forma similar el debate sobre los residuos espaciales se concentra en la creación inintencionada de residuos espaciales al arrojar desperdicios desde estaciones espaciales, haciendo estallar propulsores espaciales y colisionando objetos.¹⁹ En términos reales, debido a la probabilidad limitada de una colisión aleatoria, el mayor riesgo se produce con creación intencionada y premeditada de nubes de residuos que se concentran en órbitas de satélites críticas de misiones de EE.UU. Si en vez de esto las colisiones son intencionadas, planificadas y controladas se multiplican los riesgos y se presenta al adversario la oportunidad de destruir equipos satelitales fundamentales de EE.UU. Para alcanzar un umbral en cadena, un adversario puede añadir residuos espaciales a través de acciones controladas e intencionadas. La forma más rápida de añadir residuos espaciales a la órbita es hacer colisionar la masa existente de satélites y los residuos espaciales que orbitan la tierra.

Si la masa que ya está en el espacio puede secuestrarse mediante ciberataques, traspasa la exposición al rastreo y a la atribución.

Tipo y medios de ataque

Para cualquier estado con intención de llevar a cabo operaciones en secreto, los satélites extranjeros son un problema importante. Los satélites llevan a cabo tareas de recopilación de inteligencia, vigilancia y reconocimiento, lo que puede ser muy importuno para estados que carecen de transparencia entre sus compromisos internacionales, su postura pública y lo que están haciendo entre bastidores. Normalmente, un adversario puede elegir entre dos tipos de ataques antisatelitales no cibernéticos: cinético directo y cinético indirecto. Aunque es posible un ataque de misiles antisatelitales cinético directo a un satélite de EE.UU., tendría una atribución directa al atacante que desembocaría en repercusiones. El propulsor y el calor del misil se identificarían y se atribuirían al país o a la aeronave que lanzaron el ataque. Un ataque cinético directo podría ser tentador pero el precio político es alto. Incluso si resultara atractivo atacar satélites, un adversario no podría atacar sin dejar un rastro de evidencia tangible. El uso de un misil antisatelital (ASAT) es un acto de guerra grave y solamente puede usarse razonablemente si el perpetrador anticipa y acepta una respuesta bélica.

Para un adversario potencial puede ser mucho más interesante aumentar la cantidad de residuos que obstruyen las órbitas específicas que resumen así el ataque indirecto. El aumento de residuos puede hacerse añadiendo activamente residuos a órbitas específicamente bien definidas, accidentes de diseño sistemáticos o colisiones en el espacio.

Durante el siglo XVIII, hasta la Segunda Guerra Mundial, las unidades de artillería tenían un proyectil especial si la infantería enemiga se acercaba demasiado a la posición de la batería —la metralla. La batería apuntaba hacia la infantería que se aproximaba y disparaba metralla que dispersaba miles de bolas de acero que creaban bajas masivas en las filas de la infantería. No importaba si las bolas de acero impactaban en un brazo, una pierna, el torso o una mano. El asalto de infantería hacia la posición de la batería perdía ímpetu y terminaba. Al aplicar la idea de metralla al espacio observamos una forma simplificada de aumentar radicalmente los residuos usando propulsores espaciales para alcanzar la órbita terrestre inferior (LEO) y después usar la energía cinética para dispersar miles de bolas de acero en una sección del espacio. Como propulsor espacial cualquier misil obsoleto o rudimentario, como el Shahab iraní o el Taepodong norcoreano, podría comportarse como un vehículo para transportar la carga al espacio. Una andanada de veinte propulsores espaciales rudimentarios que suministren una cantidad significativa de metralla prefragmentada o bolas de acero podría aumentar radicalmente la cantidad de residuos que se desplazan a hipervelocidad. La probabilidad de una colisión en el espacio entre un satélite en funcionamiento y los residuos es cuestión de números. Reducido a un ejemplo simplificado, si la presencia de 5.000 unidades residuales a una altura genérica específica genera un riesgo de impacto de satélite cada diez años, sin tener en cuenta los residuos adicionales generados por el impacto, unas 100.000 unidades residuales aumentarían considerablemente el riesgo. Para explicar el principio, veinte propulsores espaciales pueden lanzar 30 toneladas métricas de carga útil a la LEO—unas 400.000 bolas de acero—que se propagarían a hipervelocidad por las órbitas del satélite. El ataque es cinético pero indirecto, ya que los satélites objetivo no están fijados como objetivos individualmente sino que son atacados por un enjambre de residuos hiperveloces que impactan en los satélites deseados por penetración o destruyendo antenas, paneles solares u otros equipos. Este impacto generaría inicialmente más residuos aunque la degradación orbital contrarresta algunos de ellos moviendo residuos a una menor altitud que con el tiempo desaparecerían del espacio.

El ataque cinético directo e indirecto sería un acto de guerra y tendría la atribución necesaria para dar a EE.UU. un *casus belli* o motivo de guerra aprobado por al menos parte de la comuni-

dad internacional. En primer lugar, tanto el ataque cinético directo como indirecto se atribuiría a una nación que lanzara el ataque y las observaciones de satélites monitores espaciales serían suficientemente exactas para dar a EE.UU. un argumento sólido. En segundo lugar, la creación de cantidades sin precedentes de residuos espaciales no solamente sería peligroso para los satélites de EE.UU. sino también para otras potencias extranjeras. Si la nación inconformista X lanza un ataque cinético indirecto, afectaría a satélites rusos, europeos, chinos, indios, paquistaníes y de otras naciones. Dependiendo de la dispersión de estos objetos residuales, los daños podrían limitarse a pequeñas partes del espacio, pero seguiría siendo un territorio espacial no usado exclusivamente por EE.UU. La nación inconformista X evita tradicionalmente las repercusiones apoyadas por la ONU de la comunidad internacional cuando se hayan perjudicado los intereses de EE.UU. Probablemente Rusia o China, en particular, vetarían las acciones punitivas propuestas por EE.UU. en el Consejo de Seguridad de la ONU.²⁰ No obstante, en esta situación, la nación inconformista X no puede permitirse el lujo de ese apoyo dañando los haberes espaciales rusos y chinos como daños colaterales en un ataque a satélites de EE.UU. Los haberes espaciales chinos son muy limitados comparados con el inventario ruso y de EE.UU. Un ataque cinético indirecto contra haberes de EE.UU. podría causar daños importantes a intereses chinos, ya que los chinos carecen de elasticidad espacial. Ni los ataques cinéticos directos ni indirectos eran opciones adecuadas o viables para una nación inconformista que trate de dañar los satélites.

Ciberataque en el espacio

La vida útil de un satélite está comprendida entre cinco y treinta años, e incluso después puede seguir orbitando en el espacio con suficiente combustible propulsor para desplazarse por el espacio con comunicaciones funcionales que pueden activarse. El espacio contiene miles de satélites, activos y desactivados, lanzados por numerosas organizaciones y países con más de 5.000 transpondedores espaciales comunicándose con la tierra. Cada transmisión es una entrada potencial de un ciberataque. Los satélites viejos comparten similitudes con la oportunidad de ciberexplotar sistemas industriales para el control y el procesamiento. Los sistemas de control de supervisión y adquisición de datos (SCADA) dentro de nuestras municipalidades, instalaciones, infraestructura y fábricas están diseñados y construidos con tecnología y equipos más viejos, algunas veces diseñados hace décadas, y el software raramente se actualiza. Estos sistemas SCADA se consideran una vulnerabilidad estratégica y han atraído una atención creciente de la comunidad de ciberdefensa de EE.UU. en años recientes. Los satélites pueden basarse en hardware y tecnología de los años 80 por una razón muy sencilla—es poco probable que los satélites se actualicen después de haberse lanzado al espacio.

Los ciberataques terrestres son un “exploit” individual para miles, si no millones de sistemas idénticos y la amenaza se eliminará después en actualizaciones o modernizaciones. La diferencia entre satélites y “exploits” cibernéticos terrestres es que un satélite en muchos casos está hecho a la medida y el diseño de computación está patentado. En vez de eso, los ciberataques espaciales aprovechan un solo sistema, o un grupo limitado de sistemas, dentro de un grupo de satélites más numerosos. Estos haberes espaciales tienen una variedad de sistemas de operación, software integrado y diversos diseños de legados tecnológicos. A medida que más naciones participan en el lanzamiento de satélites con una variedad de refinamiento técnico, aumenta el riesgo de secuestrar y manipular mediante el uso de actividades encubiertas. La computadora abordo (OBC) del satélite puede permitir la reconfiguración y las actualizaciones de software, lo que aumenta la vulnerabilidad de los ciberataques. Un satélite vulnerable que orbite durante los próximos diez años puede prefijarse para el uso no autorizado cuando lo necesite un perpetrador cibernético.

Incluso con las capacidades forenses digitales más avanzadas para rastrear un ciberataque es complicado en sistemas de computadoras terrestres físicamente disponibles. Los sistemas espaciales no permiten el acceso físico y por ello la falta de acceso a un sistema de computadora anula

varias opciones de recopilación de evidencia forense. El único rastro del perpetrador son las transmisiones reales y los intentos inalámbricos para penetrar en el sistema. Si no se capturan estas transmisiones el rastro está perdido.

Además, si el adversario es habilidoso, es más probable de que la investigación de la atribución termine con un conjunto de actores inocentes engañados, cuyas identidades digitales han sido vehículos en el ataque, en vez de la atribución al perpetrador real. Una sospecha fundamentada impactaría las relaciones interestatales pero para crear un caso de represalias se necesita una atribución y un rastreo. La atribución puede graduarse pero depende de lo que se aceptaría como un ataque “atribuido”. El liderazgo nacional puede aceptar un menor nivel de una atribución tangible que la comunidad internacional, basándose en informes de inteligencia anteriores y *modus operandi* adversario pero está limitado para tomar medidas. China ha tenido un interés creciente en adquirir capacidades de guerra cibernética²¹ y es una de varias naciones que tendrían un interés sincero en degradar los haberes espaciales de EE.UU. Actualmente, las naciones están limitadas por las repercusiones políticas y económicas de un ataque atribuido. No obstante, la determinación de objetivos de guerra cibernética encubierta que fija como objetivos haberes espaciales de EE.UU. elimina la limitación de la atribución.

Un ciberataque que dé lugar a una colisión carecería de atribución e invitaría a nuestros adversarios encubiertos. Una colisión entre un satélite extranjero de movimiento súbito y un satélite de EE.UU. crítico para la misión no es ni coincidencia ni accidente. Pero sin atribución no importa si es evidente. Otras formas de ataques directos e indirectos corresponden a un atacante que podría tener repercusiones militares, económicas y políticas. En criminología sabemos que la consideración más importante principal de un perpetrador de actos premeditados es el riesgo de ser atrapado. La magnitud de las repercusiones, si se descubre, es secundaria. Si un ciberataque puede destruir o desactivar satélites de EE.UU., sin atribución ni identificación, es probable que sea considerado por aquellos que sean abiertamente nuestros adversarios y ciertamente los que de forma encubierta son nuestros adversarios. Desde una perspectiva de guerra cibernética esto crea una oportunidad para una tercera parte para atacar y secuestrar un satélite con la finalidad expresa de colisionar con un satélite de EE.UU. en misión crítica. El ataque podría ser una colisión directa o un ataque indirecto usando la nube de residuos de otra colisión. El satélite ariete puede proceder de cualquier otro país u organización internacional. La forma más sencilla de perpetuar este ataque sería secuestrar satélites de países menos avanzado técnicamente, sistemas menos protegidos o caídos en desuso.

El impacto en satélites fijados como objetivos

El impacto en satélites fijados como objetivos directa o indirectamente con la intención de destruir el objetivo por colisión con objetos hiperveloces. Según se ha hablado anteriormente, el adversario puede crear un ataque directo impactando satélites de EE.UU. fijados como blancos con vehículos espaciales usando comandos sin autorizar mediante medios cibernéticos. El objetivo del paso inicial en un ataque indirecto podría ser perfectamente otro satélite, parte de un vehículo de suministro, o desechos espaciales que crearían residuos significativos en el impacto. La colisión crearía cientos o miles de residuos espaciales que continuarían en el espacio a alta velocidad. La nube de residuos afectaría a otros satélites en la órbita de colisión e incluso pueden iniciar el síndrome de Kessler causando daños multiplicadores si se alcanza el umbral.

Resolución del reto espacial

Aunque los problemas y las vulnerabilidades en el espacio y los medios para atacar haberes espaciales son significativos, EE.UU. tiene opciones para mitigar los riesgos.

El impacto en satélites fijados como objetivos es más probable que ocurra si hay satélites obsoletos e inactivos abandonados en el espacio que puedan ser secuestrados para la determinación de blancos y la colisión. La eliminación después de la misión (PMD)²², el esfuerzo de la ONU e internacional de eliminar satélites después de su duración productiva, requeriría eliminar satélites del espacio 25 años²³ después de terminar su misión.²⁴ Naturalmente, podría ocurrir antes de 25 años pero también podría ser un proceso prolongado, ya que no hay sanciones tangibles por incumplimiento como hoy en día. Si un satélite tiene una duración de 10-20 años, los 25 años adicionales dejarían un número total de años cuando el satélite puede ser controlado remotamente a 35-45 años. Los satélites lanzados en 1977, 1987 y 1997 ya estaban técnicamente pasados de moda y varias generaciones atrasados. El tiempo entre el lanzamiento y el final de la operación para un satélite es la base de su vulnerabilidad cibernética. Es una buena decisión financiera usar un satélite en la máxima medida de su duración. Pero la cuestión se convierte en: ¿merecen la pena los riesgos? Debemos tener en cuenta el progreso técnico conseguido desde los primeros lanzamientos espaciales y qué vulnerabilidades podrían estar integradas cuando el espacio esté poblado por haberes de 25 a 45 años que todavía puedan navegar. Como la tecnología actual se desarrolla tan rápidamente, en realidad, la PMD aumenta el riesgo de un ciberataque por satélites secuestrados porque prolonga el tiempo que un satélite puede ser controlado de forma remota mediante señales de radio usando equipos de comunicación obsoletos y pasados de moda. Estados Unidos debe proponer el acortamiento del período de eliminación PMD e insistir en actualizaciones de comunicaciones para crear un control seguro para todos los haberes espaciales.

Si se pierde el uso pacífico y seguro del espacio, EE.UU. tratará de disuadir y rechazar la agresión contra la infraestructura espacial. El grado de preparación para rechazar ataques y operar en un entorno degradado requiere resistencia—la capacidad de absorber la pérdida de capacidad mientras siga en operación. Se puede usar un solo satélite para recopilar inteligencia, todos los niveles de comunicaciones militares y una plataforma para distintos sensores. Para los adversarios, un tipo o diseño específicos de satélites pueden tener una importancia crítica y un blanco de alto valor que destruir. Si un presupuesto insuficiente fuerza a EE.UU. a utilizar excesivamente los satélites también aumenta la dependencia en cada satélite individual para el combate y la inteligencia.²⁵ El riesgo evidente en una época de austeridad es que los recortes del presupuesto predominan sobre la dependencia en sistemas espaciales fundamentales.

La Política Espacial Nacional de 2010 requiere:

“Aumentar la seguridad y la resistencia de funciones esenciales para la misión activadas por aviación comercial, civil, científica y nacional e infraestructura de apoyo contra la alteración, degradación y destrucción, ya sean causas medioambientales, mecánicas, electrónicas u hostiles”.²⁶

Incluso en una época de austeridad federal será necesario reemplazar una flota envejecida de haberes espaciales de EE.UU., ya que estos haberes son cruciales para el éxito. Eso incluiría un mayor número de satélites incluso si la inversión creara una redundancia significativa. Esta redundancia es una salvaguardia contra la capacidad de operar en un entorno degradado y proporciona una resistencia vital.

Por último, EE.UU. debe adoptar una defensa activa y tantear los límites de la guerra cibernética en el espacio. Un factor limitador del éxito en defender los haberes espaciales contra el ciberataque son las limitaciones reguladoras en las operaciones de información llevadas a cabo por el Departamento de Defensa y agencias relacionadas. Es una decisión de política que requiere que los formuladores de políticas entiendan los fundamentos exclusivos del ciberespacio. El carácter exclusivo de la guerra cibernética requerirá restricciones en la guerra cibernética de prioridad. Si EE.UU. puede determinar qué satélites, activos o inactivos, pueden usarse para colisiones de diseñador debido a debilidades de comunicación y navegación, puede asegurar la

eliminación o retirada segura de estas vulnerabilidades. Al usar defensas activas, EE.UU. aumenta la probabilidad de detección de países extranjeros tratando de enviar ataques de satélites.

La mejor forma de poder determinar si la amenaza es real y si se pueden secuestrar haberes espaciales extranjeros es salir y hacerlo nosotros mismos—aunque sea solamente para determinar posibilidades. La seguridad no se crea esperando a que sus adversarios ejecuten sus opciones y se basan en una respuesta reactiva a un incidente; en vez de seguridad, se requiere mitigar el riesgo y determinar las vulnerabilidades. La única forma de establecer conocimientos sobre vulnerabilidades extranjeras es tantear digitalmente las defensas de los haberes. Adoptar una postura de defensa activa aumenta la oportunidad de atribuir y rastrear ciberataques que aumenta la incertidumbre entre los adversarios potenciales.

Conclusión

El ataque a satélites de EE.UU. puede ser una prioridad principal para cualquier adversario potencial o encubierto y la ventaja geopolítica de ataques encubiertos satisfactorios a haberes espaciales de EE.UU. es alta. Al mismo tiempo, el costo de entrada en la guerra cibernética es bajo, lo que permite a las naciones que no puedan retar la presencia regional de EE.UU. por medios convencionales adaptarse y llevar a cabo ciberataques sin atribuir contra haberes espaciales para degradar la capacidad combate de EE.UU.

Los haberes espaciales son críticos de la forma en que combate hoy EE.UU. y en un futuro previsible es probable que EE.UU. dependa aún más del uso de haberes espaciales para mantener y defender la superioridad de la información. Aun cuando los satélites no han sido atacados ni manipulados ni destruidos por adversarios, no verifican su intención de no hacerlo.

Los ciberataques son tradicionalmente un ataque de una vez porque explotan una vulnerabilidad que puede eliminarse después o corregirse por una tecnología más reciente. La realidad es que, con 3.000 satélites, activos e inactivos, en órbita es probable que los satélites ya estén condicionados para ser secuestrados si es necesario. Un satélite vulnerable que esté en órbita durante los diez años siguientes es una oportunidad que cualquier adversario aprovecharía. Un ciberataque que ofrece la opción de dañar satélites de EE.UU. de forma encubierta para un adversario que no esté ya en guerra con EE.UU.

La mejor solución es una defensa activa: recopilar información y tantear las vulnerabilidades de EE.UU. y satélites extranjeros, construir nuevos satélites de EE.UU. para reemplazar los haberes espaciales envejecidos, mantener un espectro de radio militar máximo para asegurar comunicaciones seguras, y aumentar el número de satélites para asegurar la resistencia en un entorno degradado. La renovación y expansión de los haberes espaciales de EE.UU. son críticas para la seguridad nacional en las décadas siguientes. □

Notas

1. Renaker, John. *Dr. Strangelove and the Hideous Epoch (El Dr. Strangelove y la época horrible)*. Claremont: Regina Books, 2000.
2. Moltz, James Clay. *The Politics of Space Security (La política de la seguridad en el espacio)*. 2ª edición. Stanford, CA: Stanford University Press, 2011.
3. Alberts, David S., John J. Garstka, Richard E. Hayes y David T. Signori. *Understanding Information Age Warfare (Cómo entender la guerra de la era informática)*. Washington, DC: Command and Control Research Program Publication Series, 2001.
4. Finch, James P. y Shawn Steele. *Finding Space in Deterrence Toward a General Framework for Space Deterrence (Cómo encontrar el espacio en la disuasión hacia una estructura general para la disuasión espacial)*. Strategic Studies Quarterly, Invierno 2011.
5. The Baltimore Sun. Soviet arms could destroy U.S. satellites, Brown says (Las armas soviéticas pueden destruir los satélites de EE.UU., dice Brown), 5 de octubre de 1977.
6. Chicago Tribune. *Russian laser 'blinds' U. S. 'spy satellite' (El láser ruso ciega un satélite espía de EE.UU.)*, 22 de noviembre de 1976.
7. William J. Lynn, III, *A Military Strategy for the New Space Environment (Estrategia militar para el nuevo entorno espacial)*, The Washington Quarterly, 34:3 pág. 7-16.

8. Departamento de Defensa. *National Security Space Strategy (Estrategia Espacial de Seguridad Nacional). Resumen sin clasificar*. Enero de 2011. http://www.defense.gov/home/features/2011/0111_nsss/docs/NationalSecuritySpaceStrategyUnclassifiedSummary_Jan2011.pdf.
9. Ibid.
10. Stefan A. Kaiser. *Viewpoint: Chinese Anti-Satellite Weapons: New Power Geometry and New Legal Policy (Punto de vista: armas antisatelitales chinas: una nueva geometría del poder y una nueva política legal)*. *Astropolitics* Tomo 6, Ejemplar 3, 2008.
11. Brearley, Andrew. *Faster than a Speeding Bullet: Orbital Debris (Más rápido que una bala veloz: residuos orbitales)*. *Astropolitics* Tomo. 3, Ejemplar 1, 2005.
12. NASA. *Orbital Debris Quarterly News*. Tomo 15, Ejemplar 4. Octubre de 2011.
13. J.-C. Liou y N.L. Johnson, *Risks in Space from Orbiting Debris (Riesgos en el espacio de los residuos orbitales)*, *Science*, Tomo 311, págs. 340-341, 20 de enero de 2006.
14. Kessler, D.J. *Sources of Orbital Debris and the Projected Environment for Future (Fuentes de residuos orbitales y el entorno proyectado para el futuro)*. *Spacecraft (Naves espaciales)*, Reunión internacional y exposición tecnológica de AIAA, AIAA-80-0855 (1980).
15. Johnson, N.L., *The Historical Effectiveness of Space Debris Mitigation Measures (La eficacia histórica de medidas de mitigación de residuos espaciales)*, *International Space Review*, Ejemplar 11, págs. 6-9, Diciembre de 2005.
16. American Ordinance. *Folleto de ventas KEW / KEWA1 / KEWA2*. <http://www.aollc.biz/pdf/120mmTankKEW.pdf>
17. Donald J. Kessler y Burton G. Cour-Palais. *Collision Frequency of Artificial Satellites: The Creation of a Debris Belt (Frecuencia de colisión de satélites artificiales: la creación de un anillo de residuos)*. *Journal of Geophysical Research* (1978) 83: 63.
18. Donald J. Kessler, Nicholas L. Johnson, J.-C. Liou y Mark Matney. *The Kessler Syndrome: Implications to Future Space Operations (El síndrome de Kessler: implicaciones para futuras operaciones espaciales)*. 33 CONGRESO ANUAL DE GUÍA Y CONTROL DE AAS. 6 - 10 de febrero de 2010. Breckenridge, Colorado.
19. Oficina de las Naciones Unidas para los asuntos del espacio exterior. *Space Debris Mitigation Guidelines of the Committee on the peaceful uses of outer Space (Guías de mitigación de residuos espaciales del comité para los usos pacíficos del espacio exterior)*. http://orbitaldebris.jsc.nasa.gov/library/Space%20Debris%20Mitigation%20Guidelines_COPUOS.pdf.
20. U.N. New Service. *Russia and China veto draft Security Council resolution on Syria (Rusia y China vetan el borrador de la resolución del Consejo de Seguridad sobre Siria)*. 2011. <http://www.un.org/apps/news/story.asp?NewsID=39935&Cr=syria&Cr1=>.
21. Wired. *Hackers Targeted U.S. Government Satellites (Los atacantes fijaron como objetivos satélites del gobierno de EE.UU.)*. <http://www.wired.com/threatlevel/2011/10/hackers-attack-satellites/>.
22. P.H. Krisko, N.L. Johnson, J.N. Opiela. *EVOLVE 4.0 orbital debris mitigation studies (Estudios de mitigación de residuos orbitales EVOLVE 4.0)*. *Advances in Space Research (Avances en la investigación espacial)* Tomo 28, Ejemplar 9, 2001, páginas 1385-1390.
23. Johnson, Nicholas L. *The Disposal of Spacecraft and Launch Vehicle Stages in Low Earth Orbit (La eliminación de las naves espaciales y fases de lanzamiento de vehículo a la órbita terrestre baja)*. NASA, 2007, http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20070021588_2007019149.pdf.
24. National Research Council. *Committee for the Assessment of NASA's Orbital Debris Programs (Comité para la evaluación de los programas de residuos orbitales de la NASA). Limiting Future Collision Risk to Spacecraft: An Assessment of NASA's Meteoroid and Orbital Debris Programs (Limitación del riesgo de colisión futuro con la nave espacial: evaluación de los programas de residuos meteoríticos y orbitales de la NSA)*. Washington D.C.: National Academies Press, 2011.
25. Office of the Under Secretary for Defense, *National defense budget estimates for FY 2012 (Estimaciones del presupuesto de defensa nacional para el año fiscal de 2012)*, http://comptroller.defense.gov/defbudget/fy2012/FY12_Green_Book.pdf (se accedió a la misma el 7 de noviembre de 2011).
26. El Presidente de Estados Unidos. *National Space Policy*. 2010. http://www.whitehouse.gov/sites/default/files/national_space_policy_6-28-10.pdf.



El Dr. Jan Kallberg, PhD es un abogado, científico político y escritor de opinión estadounidense de origen sueco. Recibió su doctorado en asuntos públicos y MA en ciencias políticas de la Universidad de Texas en Dallas y tiene un título de derecho de la Universidad de Estocolmo. Sus intereses de investigación incluyen asuntos de seguridad nacional como la disuasión estratégica y el campo de batalla de la Internet.

Sendero Luminoso y el Narcotráfico en el VRAEM

COMANDANTE ISMAEL IGLESIAS L., FAP-RET.

RECIENTEMENTE EN LA enmarañada selva de los Valles Cocaleros en el Perú, se capturó al llamado Camarada Artemio, cuyo verdadero nombre es Florindo Eleuterio Flores Hala, el último de los miembros en libertad del Comité Central de Sendero Luminoso y cabecilla de la principal organización narcoterrorista del Perú, era el hombre más buscado del país por las fuerzas de seguridad, operaba hace 30 años aproximadamente en el Valle del Huallaga, responsable de más de 500 atentados terroristas y 1,000 muertes entre militares, policías y civiles. La captura de este cabecilla en vida es de suma importancia en la lucha contra el narcoterrorismo, la información que maneja y que puede brindar es de mucho valor para la lucha contra el narcoterrorismo en los valles cocaleros. De igual forma, producto de un enfrentamiento con las fuerzas del orden, se abatió al terrorista conocido como el Camarada William, número tres (03) en la cadena de mando militar de dicha organización, y conocido por su actividad de francotirador, él es el que apostaba en las laderas de los cerros del VRAEM, con armamento personal de largo alcance a espera que un helicóptero de las fuerzas del orden, descienda para sembrar o recoger un patrulla, y apuntar certeramente nada menos que al mismo piloto, son varios los helicópteros y tripulantes derribados por el ahora muerto Camarada William.



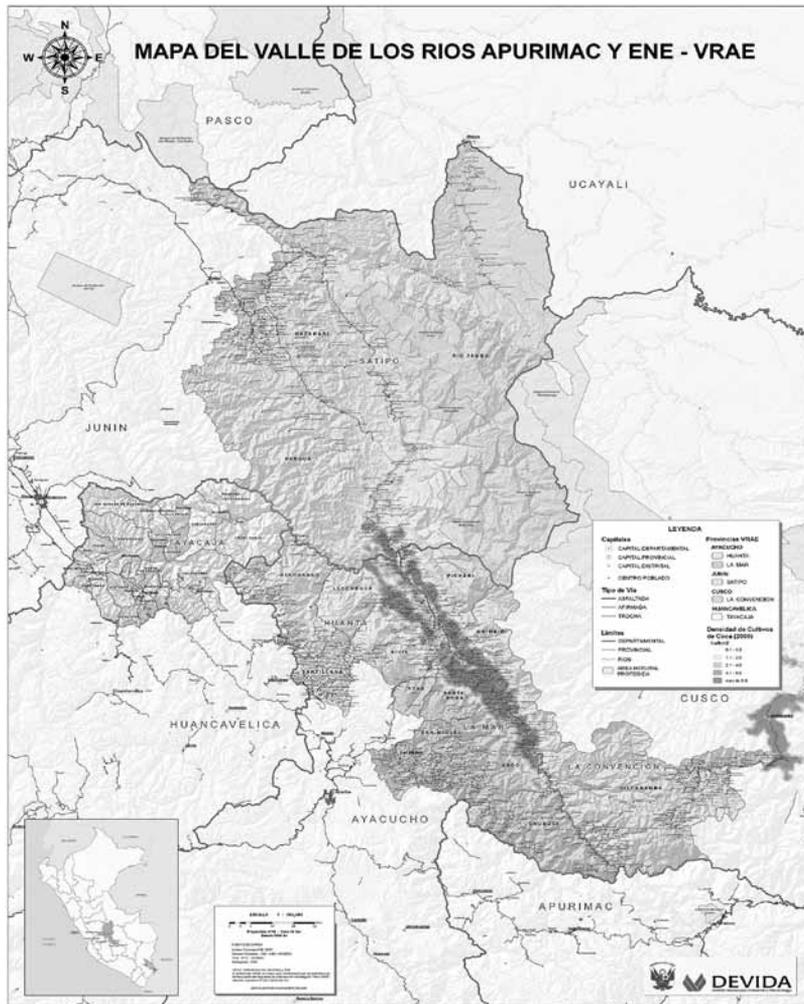
El Presidente Humala observa al máximo líder del brazo armado de Sendero Luminoso, el Camarada Artemio, capturado vivo.

Antecedentes

El Valle del río Marañón, acaba de ser incorporado a la zona declarada de emergencia, sumándose así a los valles de los ríos Apurímac-Ene, por lo que la nueva abreviatura pasa a ser VRAEM (Valles de los Ríos Apurímac, Ene y Marañón). ¿Cómo es que este territorio viene a convertirse en la zona de operación de Sendero Luminoso? ¿Desde cuándo? ¿Porqué? Son preguntas que debemos respondernos para hacer un correcto análisis y aplicar una estrategia adecuada en su combate y eliminación. Hace 20 años (el tiempo y las fechas nos dan el concepto de guerra prolongada que conciben los terroristas), con la captura del máximo líder de Sendero Luminoso, Abimael Guzmán Reynoso, el 12 de setiembre de 1,992, esta organización ingresa en una confusión inicial sobre qué hacer sin la guía del Camarada Gonzalo (Abimael Guzmán), más aún cuando en un reportaje televisivo abierto, originado por la inteligencia estatal de la época,

aparece éste con uniforme de guerrillero acompañado de su pareja la Camarada Miriam (Elena Iparraguirre), indicando a sus huéspedes la lucha por un acuerdo de paz, a través de negociaciones para buscar una “solución política a los problemas derivados de la guerra”, lo que debería incluir una “amnistía a los prisioneros”. Este hecho marca un quiebre o ruptura en Sendero Luminoso, por un lado los llamados “acuerdistas” seguidores de Abimael que buscaban una salida política al encarcelamiento de sus líderes, y por otro, la conocida como “línea proseguir”, es decir los que seguían sus acciones terroristas y de enfrentamiento a las Fuerzas Armadas y Policía Nacional, desconociendo de esta forma las indicaciones de Abimael Guzmán, aunque hay quienes afirman que esta “lucha entre dos líneas” es parte de una estrategia para presionar con acciones terroristas en el campo militar lo que se quiere ganar con negociaciones en el campo político.

Esta Línea Proseguir se instala en la zona del VRAE (antes no incluía el Valle del río Marañón), por diferentes razones tácticas y a su vez estratégicas, lo que incluye razones económicas y, para dar respuesta a las interrogantes arriba planteadas, podemos afirmar lo siguiente:



- El VRAEM es una zona de operación con una geografía totalmente accidentada, con muchas quebradas, de clima templado, en la región de la Selva Alta peruana, mezclada con partes de sierra.
- Por su accidentado terreno, las instituciones del estado como educación, salud, justicia, policía, etc. no llegaban a sus pobladores, hecho que fue aprovechado por Sendero Luminoso para ocupar el vacío que dejó el Estado.
- El VRAEM es una zona tradicionalmente cocalera, es decir, de sembríos de hoja de coca, sus pobladores se dedican en su mayoría a la siembra de este producto. Sendero Luminoso necesitaba más fuentes de financiamiento, y ve en la actividad cocalera de esta zona, una gran oportunidad para ello.

Situación actual: ¿Terroristas o narcotraficantes?

Hay quienes dicen que Sendero Luminoso está muy lejos de ser en la actualidad una organización político-partidaria, que busca la transformación de las estructuras de la sociedad para instaurar otras acordes con el marxismo-leninismo-maoísmo-pensamiento Gonzalo (fundamentalismo puro para justificar el terror), y que todo es una pantalla pero que bajo el manto de “guerrillero” se encuentra el cartel de narcotraficantes más grande del país. Esta apreciación sobre lo que es exactamente Sendero Luminoso, es a mi parecer, el origen que desencadena toda la estrategia para su combate, y que por lo tanto, una inadecuada caracterización o definición de Sendero Luminoso, nos lleva a errores estratégicos en su combate. Es cierto que su principal fuente de financiamiento es el narcotráfico, que inclusive tienen en sus bases y campamentos terroristas “cocinas” (laboratorios donde se elabora el clorhidrato de cocaína, es decir, droga pura), que la transportan hacia la costa y hacia Brasil, sus militantes son pagados monetariamente, reciben un sueldo mensual en dólares, lo cual para un joven campesino de la zona es atractivo. Sin duda es una organización narcotraficante, la más grande del país. Sin duda que sus líderes se enriquecen con esta actividad ilegal, pero también es cierto que utilizan este dinero para sus acciones terroristas en el campo militar, el terror no es moral, no tiene un juicio de valor respecto de lo legal o ilegal de una actividad, no tiene conciencia de la vida, menos la va a tener del rigor de una ley, por lo tanto, su lógica es más simple y objetiva, si el narcotráfico sirve y ayuda en sus fines político-ideológicos, bienvenido sea, si ayuda a comprar armamento, munición, y toda la logística militar necesaria, incluyendo el pago de salarios a sus nuevos reclutas, también bienvenido sea. Las últimas entrevistas televisivas concedidas en la clandestinidad en lugares de la agreste selva del VRAEM por sus principales líderes (los hermanos Quispe Palomino), confirman que sí existe una Convicción Ideológica-Partidaria. Las series de atentados realizados contra la infraestructura del Estado, los ataques a las fuerzas del orden, el reclutamiento de niños y adolescentes, la existencia de las llamadas Escuelas Populares, nos indica que Sendero Luminoso continúa con su proyecto político de llegar al poder (no importa cuando) a través de la violencia y el terror, para ello ha variado algunas técnicas como las de reclutamiento, los ataques a la población civil, etc., pero en su esencia siguen siendo el mismo Sendero Luminoso de antes, con el mismo proyecto político-ideológico y que para ello, no importa ser narcotraficantes.

Respecto a la actividad narcotraficante de Sendero Luminoso (por separarla de su actividad terrorista para efectos del análisis académico) se puede decir que controla y opera la principal cuenca cocalera del país: el Valle de los Ríos Apurímac-Ene y Marañón (VRAEM), donde se han alcanzado producciones de hasta 3.5 toneladas por hectárea de hoja de coca, principal insumo para la elaboración del clorhidrato de cocaína, considerando unas 20 mil hectáreas en el VRAEM, podemos hablar de una producción de 70 mil toneladas por cosecha, y se ha llegado a obtener, sobretodo en este Valle por sus condiciones de suelo y climáticas, de hasta 4 cosechas por año. A modo de referencia debemos saber que una hectárea de hoja de coca alcanza para producir 9.5

kilogramos de cocaína pura, por lo tanto el VRAEM produce aproximadamente 190 mil kilogramos de clorhidrato de cocaína, o simplemente cocaína como se le conoce. Esto equivale al 70% del total de cocaína que se produce en el Perú y al 50% del total de cocaína que se produce en el mundo, lo que convierte al Perú en el principal productor de cocaína en el mundo, esta producción anual alcanza por ejemplo para abastecer la mitad de la demanda de los consumidores en EEUU y la totalidad de la demanda de los consumidores en Europa anualmente.

Precio del Gramo de Cocaína en Dólares	
VRAEM	1.0
Lima	2.0
Argentina	5.9
Chile	26.6
España	83.2
Reino Unido	90.5
Francia	95.9
Estados Unidos	110
Noruega	150
Japón	190
Australia	250
Fuente: UNODC 2007: World Drug Report	

Este cuadro nos explica el porqué la mayoría de la población en el VRAEM se dedica al cultivo de la hoja de coca, las bandas de narcotraficantes, incluyendo a Sendero Luminoso, compran su producción y proceden a procesarla hasta convertirla en clorhidrato de cocaína, y por eso que los diferentes planes de sustitución de cultivos difícilmente tienen éxito porque mientras el café o el cacao les da una cosecha al año, la hoja de coca les da 3 y a veces 4 cosechas anuales, y con una rentabilidad muy superior. El VRAEM y el Valle del Huallaga abarcan el 75% de la producción de droga del país, y van apareciendo otras zonas emergentes cocaleras como el Valle de la Convención en el Cusco, así como la selva de Puno (Sandía y parte de Carabaya) donde, por ejemplo, existe el Caserío El Chocal (centro poblado menor de 500 habitantes), un pueblo alejado y olvidado mucho tiempo por el Estado, donde no hay agua ni desagüe, pero existen camiones 4x4 y televisión satelital con televisores modernos, el 80% de su población siembra hoja de coca.

Por el lado de sus acciones militares, Sendero Luminoso, ha realizado en el VRAEM, en el primer semestre del 2012, más de 100 acciones terroristas, algunas de gran trascendencia tales como el secuestro de 36 trabajadores de una empresa transportadora de gas natural, el derribo de un helicóptero de la Policía Nacional, ataque a patrullas, emboscadas, francotiradores, dando muerte a decenas de policías y militares, y se han capturado 224 terroristas en el último año (1), pero lo que más ha indignado a la sociedad peruana y a la comunidad internacional en general, es la difusión de videos y fotografías de la explotación y trata de niños por parte de esta agrupación demencial (2), donde se puede apreciar a estos pequeños lanzando arengas a su llamada revolución, al maoísmo y otras consignas terroristas. Estos niños son secuestrados de familias rurales del VRAEM y obligados a vivir en los campamentos terroristas, sometidos a rutinas y entrenamiento militar, en lo que los terroristas llaman escuelas populares". Las fuerzas del orden, en los últimos meses han logrado rescatar a 11 niños primero y luego a 3, incluyendo a uno de 8 meses, pero se estima que más de 100 niños arrancados de sus hogares, se encuentran aún en manos de los terroristas.



Poza de maceración en un laboratorio de droga en el VRAEM

La lucha frontal del estado peruano

La pacificación de VRAEM y la eliminación de los remanentes narcoterroristas que operan en esa región, no solamente competen a las Fuerzas Armadas y la Policía Nacional, sino que depende de una acción concertada y multisectorial entre el Gobierno Nacional, las regiones y las municipalidades afectadas por la subversión. Es decir, la estrategia militar debe ser reforzada con una estrategia integral en los demás campos como el político, el social y el económico. El estado viene buscando desarrollar el VRAEM, por tanto tiempo descuidado por el propio estado, actuando desde varios frentes, esto es, construyendo obras de infraestructura como carreteras, escuelas, impulsando programas de urgente atención médica y organizando a las localidades involucradas para su autodefensa, y últimamente integrando todos los programas de ayuda social del Estado en un Alto Comisionado para la zona con rango de ministro.

El VRAEM tiene unas características territoriales, étnicas y geográficas. Se trata de un extenso valle de selva alta que abarca más de 15 mil kilómetros cuadrados e incluye básicamente jurisdicciones de tres regiones: Ayacucho Cusco y Junín. Con la finalidad de incrementar la presencia del Estado en esas remotas poblaciones, el Gobierno ha destinado un fondo de más de 75 millones de nuevos soles, con los cuales se han puesto en marcha más de 220 proyectos en igual nú-



Niños secuestrados y en adoctrinamiento terrorista por Sendero Luminoso en el VRAEM

mero de comunidades. Esta suma no está incluida en las partidas destinadas a la construcción, rehabilitación y asfaltado de mil 500 kilómetros de carreteras con una inversión de 713 millones de nuevos soles. El Ministerio de la Mujer y Poblaciones Vulnerables, del Ambiente, Educación, Salud, Desarrollo e Inclusión Social, Agricultura, y Vivienda entre otras dependencias públicas, ya se encuentran concertando para la ejecución de programas especiales de desarrollo local con carácter prioritario. Aún así, el esfuerzo del gobierno central no basta, hace falta el compromiso y la participación de las autoridades regionales que comparten su territorio en el VRAEM, así como de las municipalidades provinciales y distritales.

Por su parte, el Comando Conjunto de las Fuerzas Armadas, también ha adecuado su accionar, su organización y su estrategia, para el combate y derrota de la narco guerrilla. La primera modificación a hacer es la nueva concepción del enemigo, ya no es tan solo un terrorista, sino que es una narco guerra con acciones terroristas, es una combinación de ambas tácticas, y para ello, la Policía y las Fuerzas Armadas responden a un solo Comandante en el VRAEM, quien tiene a su cargo las fuerzas combinadas, para ello los manuales se vienen actualizando y el entrenamiento se ha modificado teniendo en cuenta las particularidades de esta guerra. De hecho, la acción conjunta de las 3 instituciones de la Fuerza Armada (Ejército, Fuerza Aérea y Marina) se viene logrando con grandes éxitos. Los Comandantes Generales de cada Institución tienen como encargo la preparación y el entrenamiento de las fuerzas, entregándolas al Jefe del Comando Conjunto para su empleo y aplicación mediante los Comandos Operacionales, siendo uno de ellos el C-VRAEM o Comando Operacional del VRAEM, paralelamente la creación del Comando Operacional de Operaciones Especiales e Inteligencia, permite integrar las fuerzas especiales de las 3 instituciones, así como integrar todo el gran esfuerzo de la labor de inteligencia, que muchas veces no llegaba a los tomadores de decisiones, o éstos no le daban la real importancia, así como se evita la duplicidad de esfuerzos.

Igualmente, la Fuerza Aérea del Perú (FAP) continúa en un franco proceso de recuperación de la capacidad operativa en todos sus sistemas de armas, la que se orienta al combate y liquidación de los narcoterroristas en el VRAEM, y a la conexión de los pueblos remotos a la vida económica del país. Es en ese sentido, que la FAP ha recibido este año el primer avión de 12 contratados del DHC-6 Twin Otter con capacidades STOL. También ha recibido helicópteros Mi-17 y helicópteros de ataque Mi-35, los que han sido asignados al Comando Operacional del VRAEM, y junto



La Fuerza Aérea del Perú y la Policía Nacional en acción conjunta en el VRAEM

a aeronaves A-37B están realizando operaciones de apoyo táctico a las patrullas militares de la zona. Asimismo, viene desarrollando su primer UAV con tecnología FLIR y Guerra Electrónica.

Finalmente, el Gobierno Central ha recibido las facultades legislativas por parte del Congreso de la República a fin que pueda legislar por un periodo de 90 días en el tema concreto de Seguridad y Defensa Nacional. Según la información abierta que circula, los cambios a realizar incluyen:

- Fortalecimiento y reforma de los sectores Defensa e Interior, es decir los ministerios que tienen bajo su cargo a las Fuerzas Armadas y Policía respectivamente, siendo previsible que éstas también sean reformadas.
- Reforma del mismo Sistema de Seguridad y Defensa Nacional.
- Normas legales que establezcan las reglas de enfrentamiento cuando se determine la participación de las Fuerzas Armadas en el Orden Interno en apoyo de la Policía Nacional.
- Creación de un organismo central de compras de la Defensa Nacional.
- Reforma salarial de todos los militares y policías en actividad (146 mil efectivos) así como de las pensiones para los que están en retiro (105 mil pensionistas), estableciendo incentivos a los que están destacados y combatiendo en el VRAEM, zona de frontera, alta responsabilidad y otros actos meritorios. De igual manera, esta reforma de la escala salarial busca beneficiar en mayor parte desde el grado de comandante o teniente coronel hacia los grados inmediatos inferiores.
- Estrategia legal para el control de insumos químicos, los cuales son empleados para la elaboración de droga.

Conclusiones

- Sendero Luminoso ha sufrido importantes capturas de sus líderes principales, sobretodo de la línea militar, en los últimos meses por parte de las fuerzas del orden, incluyendo al Camarada Artemio y Camarada William, que totalizan 224 terroristas capturados solo en el último año (septiembre 2011-agosto 2012). Este hecho los ha obligado a replantear su estrategia a fin de mantener una presencia activa en el VRAEM.
- En la actualidad, Sendero Luminoso tiene dos frentes de lucha, uno clandestino dedicado a la línea militar y encargado de atacar a las fuerzas del orden, de realizar atentados terroristas a la infraestructura del estado, basado en su Fuerza Principal, conocido como el Ejército Revolucionario Popular, este primer frente podría estar actuando independientemente de la cúpula senderista en prisión; y el segundo frente, conformado por militantes políticos y ex prisioneros por terrorismo, quienes actúan de forma abierta buscando infiltrarse en diferentes organizaciones de la sociedad, sobre todo en movimientos sindicales, a fin de presionar por una salida política y la amnistía a sus líderes presos, la gran mayoría condenados a cadena perpetua en cárceles de máxima seguridad.
- El VRAEM es un territorio accidentado geográficamente, donde la mayoría de la población se dedica al cultivo de la hoja de coca, estas dos particularidades (zona agreste y cultivos de hoja de coca) son muy bien aprovechados por el brazo armado de Sendero Luminoso, no solo para combatir a las fuerzas del orden, sino también para realizar actividades ilícitas de narcotráfico, lo que convierte a Sendero Luminoso en el cártel de droga más grande del país. Este hecho pone en evidencia la condición actual de Sendero Luminoso de ser no solo una organización terrorista con ideología política-partidaria, sino también su condición de ser una organización delincencial dedicada al narcotráfico para financiar sus actividades terroristas y para el enriquecimiento de sus líderes.

- El VRAEM hoy en día se ha convertido en la principal zona productora de cocaína del país con el 70% de la producción nacional habiendo logrado producciones muy por encima de lo que se produce en otras zonas, es decir, han mejorado sus técnicas de cultivo, por lo tanto obtienen una mayor rentabilidad económica, que es el sustento de la logística necesaria para su brazo militar.
- La estrategia que ha adoptado actualmente el estado peruano para luchar integralmente contra el flagelo narcoterrorista, abarca todos los sectores, además del de Interior y Defensa, buscando llevar la presencia del estado a la zona del VRAEM, ganar el apoyo de la población brindándole todos los servicios básicos tales como educación, salud, agricultura, vivienda y todos los programas de ayuda social. Por el lado militar, las operaciones militares se realizan bajo el mando unificado del Comando Conjunto de las Fuerzas Armadas, que ha adaptado su organización a las exigencias del teatro de operaciones, así como su entrenamiento y las operaciones mismas.
- Las Fuerzas Armadas y la Policía Nacional están en un proceso de fortalecimiento y reforma institucional, el cual incluye desde una franca recuperación de su capacidad operativa hasta una reforma salarial y de las pensiones, con incentivos al personal combatiente dentro de una cultura de meritocracia.

Como conclusión general podemos decir que Sendero Luminoso sigue siendo una organización terrorista con ideología político-partidaria (marxismo, leninismo, maoísmo, pensamiento Gonzalo), que financia sus actividades con el narcotráfico que realiza en la zona del VRAEM y que además, existe un brazo abierto que busca principalmente la amnistía a sus líderes, entre ellos y principalmente a Abimael Guzmán, siendo necesario establecer si el brazo armado actúa independientemente del brazo abierto. Por su parte el estado peruano, consciente de esta nueva realidad narcoterrorista, viene adoptando una estrategia integral de combate a este flagelo, la misma que abarca todos los campos, y que para ello está haciendo los esfuerzos y cambios necesarios que deberán dar sus frutos en los próximos meses. □

Referencias:

- (1) <http://www.pnp.gob.pe/direcciones/dircote/logros.html>
- (2) <http://www.youtube.com/watch?v=XQERuc3wTU8>
- (3) <http://www.youtube.com/watch?v=eMzJls6aj6M>
- (4) <http://www.youtube.com/watch?v=FE0dxW5TCg0>



El Comandante Ismael Iglesias León Fuerza Aérea del Perú-Retirado, es graduado en: Inteligencia, CC. de la Administración Aeroespacial, Curso de Comando y Estado Mayor Conjunto. Postgrado en Alta Dirección y Gerencia, Administración de Empresas y Gerencia de Recursos Humanos, Maestría en Ciencia Política, Inteligencia Militar en EE.UU., Analista y Procesador de Imágenes Satelitales en Francia. Cursos Superior e Inteligencia Estratégica. Sirvió en Unidades Aéreas de Combate, Servicio de Inteligencia, Dirección de Inteligencia y en el Estado Mayor General, así como de Oficial de Enlace FAP - Congreso de la República. Cátedra en la Escuela de Inteligencia y Escuela de Oficiales. Secretario Permanente de las Reuniones Bilaterales de Inteligencia entre Fuerzas Aéreas. Columnista del diario La Industria de Trujillo, Revista Aviación y otras publicaciones. Actualmente estudia la licenciatura en Politología y el diplomado en Resolución de Conflictos.

Crimen y Gobernabilidad en una Honduras Contemporánea

DRA. MARY FRAN T. MALONE, PhD

“Estamos podridos hasta la médula. Estamos al borde de un abismo. Estas son organizaciones criminales por dentro y por fuera”

Gustavo Alfredo Landaverde, noviembre de 2011

GUSTAVO ALFREDO Landaverde, fundador del Partido Demócrata Cristiano y ex director de la Dirección de Lucha contra el Narcotráfico, hizo estas declaraciones dos semanas antes de ser asesinado desde un automóvil. Sus palabras enfatizan la desalentadora realidad de un Honduras contemporáneo, un país que ha recibido la distinción más infame de ser la capital del crimen en el mundo. Los titulares nacionales e internacionales confirman la magnitud de la crisis con subtítulos tales como “Asesinatos de estudiantes hondureños destacan preocupación sobre crímenes”, “Chanchullos, avaricia, caos convierten a Honduras en la capital del crimen en el mundo” e “Incendio en prisión recalca amplios problemas de seguridad en Honduras”.¹ Ciudadanos promedio en Honduras comparten preocupaciones sobre el deterioro de la seguridad básica en su país. En una reciente encuesta a la opinión pública, el crimen inclusive eclipsó las preocupaciones económicas, a medida que los ciudadanos identificaron el crimen y la corrupción como los problemas más graves que el país enfrenta (Proyecto Latinoamericano de Opinión Pública -LAPOP 2012).

Acontecimientos contemporáneos en Honduras plantean varias preguntas. ¿Cómo se generalizó tanto la violencia en Honduras? ¿Por qué han fracasado los intentos de controlar la violencia? Más importante aún, ¿qué impacto tendrán estas tendencias de violencia en el gobierno democrático y en la estabilidad política? En este artículo se tratan estas preguntas, enfocándose en particular desde la perspectiva de los ciudadanos en Honduras. Con este enfoque, en este artículo se define si las experiencias del ciudadano común con el crimen debilitan su compromiso con la democracia y sus normas. Dependiendo de los resultados de la encuesta de *Americas-Barometer 2012*, en este artículo se analizan las reacciones del pueblo común y corriente a la violencia y las respuestas del estado, y sus puntos de vista sobre el gobierno futuro y la estabilidad política.²

Reseña histórica

Durante gran parte de su historia, Honduras se escapó de la violencia generalizada que sumió a muchos de sus vecinos. Inclusive durante inicios del siglo XX, cuando las revueltas nacionalistas surgieron en países vecinos, Honduras estaba relativamente en calma. Tal como explica Booth, “Honduras, menos polarizada por los partidos políticos, menos integrada en la economía mundial y con menos concentración de riqueza que en cualquier parte en América Central, también experimentó menos líos políticos a inicios del siglo XX que sus vecinos” Booth 1998, 20). Las huelgas laborales eran comunes, pero relativamente hablando, Honduras empleó menos represión contra los trabajadores y las empresas hicieron más concesiones laborales. No fue sino hasta la década de los años cincuenta que la milicia hondureña comenzó a intervenir regularmente en la política. Esa década introdujo escasez de tierras, acompañada por tensiones entre las clases socio-económicas y la movilización de los campesinos rurales (Booth et al 2010). El

inicio de la Guerra Fría aumentó aún más la polarización política poniendo las antiguas disputas en una nueva perspectiva. Por ejemplo, los frecuentes disturbios laborales en las plantaciones bananeras ya no era cuestión de los trabajadores protestando por mejores salarios y condiciones laborales. Más bien, algunos actores políticos se preocuparon de que los comunistas pudiesen ver oportunidades políticas en estas protestas laborales. Estados Unidos respondió a esas inquietudes y aumentó dramáticamente la ayuda militar a Honduras durante la Guerra Fría, de un promedio anual de menos de medio millón de dólares en la década de los cincuenta a un promedio anual de más de \$57 millones de dólares para fines de la década de los ochenta (Booth et al 2010, 272).

Con esta nueva afluencia de fondos y entrenamiento extranjero, la milicia hondureña se tornó más ponderosa durante la Guerra Fría y empleó ese poder para intervenir en la política, comenzando con un golpe de estado del ejército en 1956. Mientras que los militares intensificaron su participación en la política durante las décadas de los sesenta y los setenta, durante ese tiempo no era tan represivos como las juntas de Guatemala, El Salvador y Nicaragua, actuando “más como árbitro entre otros grupos políticos que como un agente de una clase gobernante” (Booth et al 2010, 162). Para tratar el aumento en los disturbios y la movilización de campesinos, la milicia sí dependió de la represión, pero también empleó medidas populistas para reducir la pobreza, tal como la reforma agraria. La prensa conservó algunas de sus libertades y las violaciones a los derechos humanos nunca llegaron al mismo nivel de atrocidad como en Guatemala, El Salvador y Nicaragua. Sin embargo, para inicios de la década de los ochenta, el gobierno militar cambió dramáticamente. Los escuadrones de la muerte perseguían a los opositores políticos, y las desapariciones y asesinatos de políticos aumentaron, al igual que las cifras de la relativamente pequeña fuerza de la guerrilla. Aún así, a pesar del aumento en la represión y resistencia, Honduras evitó las guerras civiles abiertas de sus vecinos. Para mediados de la década de los ochenta la milicia comenzó a devolverle el poder a los civiles, aunque retuvo el poder de reprimir la disconformidad e influenciar las élites políticas.

A medida que la Guerra Fría terminó a fines de la década de los ochenta, el apoyo militar de Estados Unidos menguó y la milicia hondureña cada vez más le confió los asuntos políticos a los civiles. Comenzando en 1986, las elecciones presidenciales resultaron en el traslado pacífico de poder de un gobierno civil al próximo, y los abusos a los derechos humanos disminuyeron. En 1990, el nuevo comandante de la milicia redujo y castigó los abusos de poder y las infracciones a los derechos humanos, y subsiguientemente reconcilió a la milicia con las fuerzas de la oposición (Booth et al 2010, 170). Para 1996, las reformas constitucionales solidificaron el control civil de la milicia, el elemento final necesario para desmilitarizar completamente el sistema político.

La democratización y sus retos a la seguridad

Aunque bienvenida, la transición a la democracia no careció de problemas sustanciales. Durante el proceso de democratización, las instituciones políticas están en un estado de evolución a medida que los arreglos democráticos reemplazan los autoritarios. Particularmente en el caso de las instituciones judiciales como los tribunales y la policía, toma tiempo reformar leyes y códigos legales (o redactar nuevos del todo) y entrenar a jueces, abogados y funcionarios de la policía para defenderlos. Este es un proceso difícil en la democratización de cualquier país, no obstante en Honduras esos retos fueron aún más agudos. Si bien Honduras no experimentó la guerra civil en sí, su ubicación geográfica significaba que de todas maneras había heredado muchos de los problemas que heredaron los países después de un conflicto. En la década de los noventa, Honduras era el hogar de antiguos combatientes del conflicto en Nicaragua, muchos de los cuales no pudieron integrarse a la fuerza laboral y conservaban acceso a las armas. La política de EE.UU. exacerbó aún más los problemas después de la guerra, a medida que Estados

Unidos deportó numerosos miembros de pandillas salvadoreñas (particularmente de Los Ángeles) de regreso a un El Salvador después de la guerra, donde las posibilidades de trabajos legítimos eran remotas (Wolf 2011). A las pandillas les fue fácil organizarse en El Salvador y esas redes criminales comenzaron a expandirse a países vecinos como Honduras. Cuando las pandillas y el crimen organizado se aprovechan de las transiciones políticas, las tasas de crimen violento aumentan exponencialmente, particularmente cuando la transición sucede en un ambiente de soldados desmovilizados y desarme incompleto. Tal como Millet (2009) destaca:

El fin de los conflictos civiles con frecuencia deja miles de antiguos combatientes, que provienen de todos los bandos, sin trabajos, tierras o educación y acostumbrados a un estilo de vida violento. Intentos para incorporar esos individuos a la sociedad a menudo no son ni adecuados ni constantes, ofreciendo reclutas aprestos para las organizaciones criminales (Millet 2009, 252).

Además de la transición política a la democracia, Honduras (al igual que la mayoría de los países latinoamericanos) experimentó trastornos económicos importantes durante el mismo lapso de tiempo. La crisis de la deuda en la década de los ochenta provocó cambios económicos masivos en la región y, para la década de los noventa, surgió un consenso global que las políticas económicas neoliberales eran la mejor receta para economías renqueantes o rezagadas. Apodado con el nombre de Consenso de Washington (*Washington Consensus*), ese énfasis en las políticas económicas neoliberales significaba que países como Honduras necesitaban adoptar los principios de mercado libre para poder competir en la economía global y tener acceso a los mercados y préstamos internacionales. En un final, las reformas neoliberales aumentaron el poder del mercado, con respecto a los del estado. Al analizar la era después de la Guerra Fría, Naím (2005) observa que las fuerzas del mercado, inclusive las fuerzas del mercado ilícitas como los narcotraficantes, son mucho más poderosas que las del estado. Pérez coincide, destacando que las tendencias de liberalización e integración económicas contemporáneas han tornado más porosas a las fronteras y ofrecen “oportunidades excelentes para que empresarios ilícitos escondan sus ganancias entre los flujos lícitos” (Pérez 2000, 139). En resumen, si se unen, las transiciones políticas y económicas de la década de los noventa debilitaron el poder del estado y crearon oportunidades para que los actores no estatales ejercieran su influencia.

Los cambios políticos y económicos ofrecen oportunidades para los actores nuevos y, lamentablemente en el caso de Honduras, muchos de esos actores no tenían la buena gobernanza entre sus prioridades principales. Los elementos del crimen organizado pudieron aprovecharse del espacio creado por esas transiciones y establecerse en la política y la sociedad hondureña. La inseguridad pública comenzó a deteriorarse, tal como lo comprobó el incremento en las tasas de homicidios. Según se ilustra en la figura 1, a pesar del descenso en el 2003, las tasas de crimen violento aumentaron marcadamente durante la última década. Para el 2010, Honduras registró la tasa más alta de homicidios en el mundo—82,1 por cada 100.000. Como punto de comparación en el 2010 las tasas de homicidio en Nicaragua eran 13,2 y 4,6 en Estados Unidos (UNODC 2011).

Además del problema del crimen violento, la democracia hondureña también ha sido acosada por la corrupción. En la figura 2 se muestra al punto que la corrupción penetra a Honduras, dependiendo del Índice de Percepción de Corrupción (CPI, por sus siglas en inglés) de *Transparency International*. *Transparency International* califica la extensión a la que los gobiernos alrededor del mundo se pueden caracterizar según su transparencia o corrupción, en una escala del uno al diez. Países con los niveles más altos de transparencia (y, por lo tanto, los niveles más bajos de corrupción) obtienen calificaciones más cerca a la calificación perfecta de diez, mientras que países comprometidos por la corrupción reciben calificaciones más cerca al cero. Tal como se ilustra en la figura 2, durante la última década Honduras consistentemente ha sido calificada cerca de la parte inferior de esta escala.

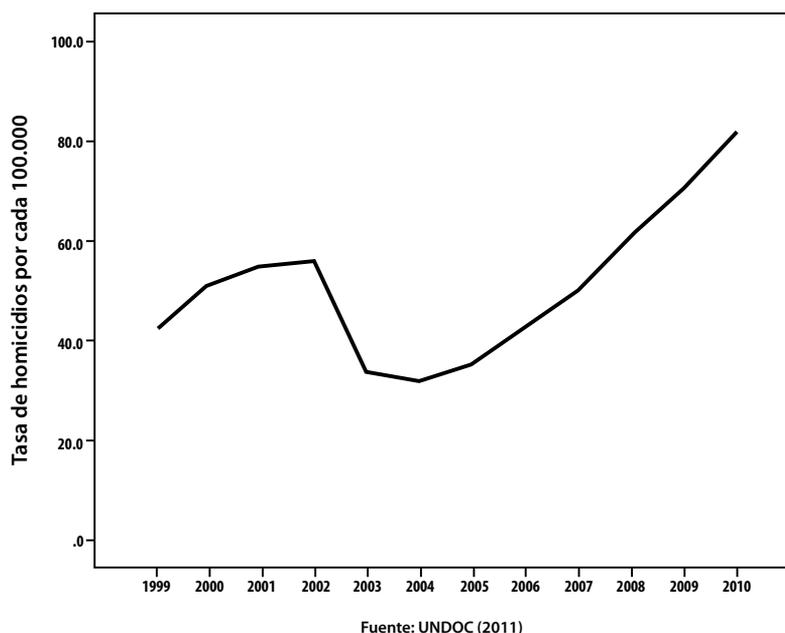


Figura 1. Tasa de homicidios por cada 100.000

Seligson y Booth (2010) destacan que para mediados de los años 2000, los ciudadanos promedio de Honduras expresaron altos niveles de descontento con el *statu quo*. De todos los países latinoamericanos, el pueblo en Honduras registró los niveles más altos de “triple descontento”, en los que el apoyo a la democracia, el apoyo a las instituciones nacionales y las evaluaciones de rendimiento económico del gobierno eran muy bajos. Para el 2008, los resultados de la encuesta identificaron a Honduras como “el único caso en América Latina con el nivel más alto de ciudadanos y triplemente descontentos, con relativamente bajo apoyo a la democracia, y un apoyo elevado a los golpes de estado, métodos políticos de confrontación y rebelión (Seligson y Booth 2010, 133).

La democracia era particularmente vulnerable en Honduras, y las élites políticas se aprovecharon de esta fragilidad en el 2009. El Presidente Zelaya y sus opositores chocaron en cuanto a los intentos de Zelaya de llevar a cabo un plebiscito y subsiguientemente destituir al jefe de la milicia. Ambas de estas movidas presidenciales fueron consideradas ilegales y la milicia respondió del mismo modo, pasando por alto la constitución para exilar a Zelaya a Costa Rica.³ El derrumbe de la democracia en Honduras desencadenó una tormenta internacional. Los líderes latinoamericanos estaban divididos en su apoyo al Presidente Zelaya, pero prácticamente unánimemente en su oposición a la intervención militar. La Organización de Estados Americanos (OEA) suspendió a Honduras de la organización, la primera vez que se tomaba esa acción desde la suspensión de Cuba en 1962. Las Naciones Unidas aprobó una resolución (cuyos patrocinadores incluían a Estados Unidos y Venezuela) por aclamación “después de aplausos sostenidos en el organismo de 192 integrantes”, condenando el golpe de estado y exigiendo la “restitución inmediata e incondicional” de Zelaya como presidente (Lacey 2009, A6). Zelaya no fue restituido como presidente, pero el 29 de noviembre de 2009 se celebraron nuevas elecciones para definir quién gobernaría el país como presidente. Porfirio Lobo ganó esas elecciones y fue inaugurado pacíficamente el 27 de enero de 2010. La OEA restituyó la membresía de Honduras el 1º de junio de 2011.

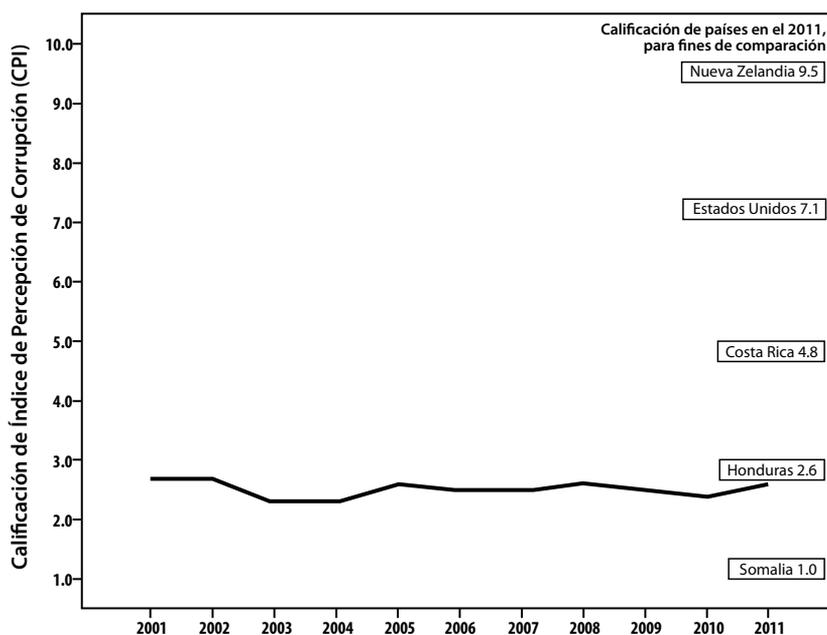


Figura 2. Calificación de Índice de Percepción de Corrupción (CPI)

El golpe de estado y su inestabilidad política correspondiente crearon más espacio para que los actores no estatales funcionaran. Muy en particular, el crimen organizado se aprovechó de la oportunidad para atrincherarse aún más en el tejido social, económico y político de Honduras. Tal como Bailey y Taylor (2009) explican, hay una diferencia importante entre los crímenes organizados y no organizados. Si bien los crímenes violentos constituyen problemas para el gobierno, el crimen organizado es un opositor aún más formidable, ya que tiende a ser una contraparte bien financiada y organizada con acceso inmediato a las armas y municiones. Cuando el crimen organizado puede desafiar sistemáticamente la monopolización de la fuerza del estado, también pone en peligro la legitimidad del gobierno.

El vacío de poder presentado por el 2009 creó una apertura política para el crimen organizado, pero las tendencias regionales también contribuyeron con el problema. En particular, la ofensiva anti droga mexicana empujó a que elementos criminales organizados se adentraran más en América Central. En el 2006, el 23% de los envíos de cocaína moviéndose hacia el norte atravesaban América Central. Para el 2011, esta cantidad subió al 84%, a medida que la ofensiva mexicana presionaba la actividad del cártel hacia el sur (Archibold y Cave 2011, A1). Honduras ha resultado ser un refugio particularmente atractivo para los traficantes de droga eludiendo las operaciones antidroga mexicanas contra los cárteles, ya que la costa del norte de Honduras “ofrece una selva tropical remota, no habitada en su mayoría que es perfecta para las aeronaves de un solo motor que utilizan los traficantes, y que luego esconden o incendian para esconder las pruebas” (Archibold y Cave 2011, A1). Las junglas densas y la extensa costa caribeña colocan a Honduras como “la primera esquina del triángulo, dando lugar a rutas comerciales que eventualmente llegan a México y Estados Unidos” (Shifter 2011, 51).

La respuesta del gobierno a la crisis del crimen

El gobierno hondureño ha reconocido los estragos del crimen en el gobierno democrático. Una serie de presidentes ha prometido refrenar el crimen y perseguir a los funcionarios corruptos que son cómplices con las actividades criminales. Hay una aceptación generalizada que se necesitan reformas adicionales en el sistema judicial y que el estado debe aumentar sus recursos para combatir el crimen. Sin embargo, ha habido menos acuerdo sobre cómo exactamente el gobierno debe interpretar esas metas abstractas en políticas tangibles. La realidad es que tan esperadas reformas toman mucho tiempo y requieren muchos recursos, y puede tomar años antes que esas reformas se conviertan en una fuerza policial y un sistema judicial que puedan confrontar el crimen exitosamente. Por lo tanto, muchos políticos han por lo menos buscado una solución rápida temporal, que tiende a tomar la forma de una serie de propuestas de “mano dura”.

Las reformas para revisar el sistema judicial comenzaron seriamente en 1996, justo cuando el gobierno civil estaba consolidando su control sobre el país y manteniendo a la milicia al margen del gobierno. La reformas constitucionales crearon una fuerza policial civil, seguida un año más tarde por nuevas leyes policiales y códigos de procesos penales en 1997 (Ungar 2009). No obstante, esas reformas duraron poco ya que políticos de mano dura las denunciaron porque le daban prioridad a los derechos de los criminales en lugar de los de las víctimas. Por ejemplo, cuando el Presidente Ricardo Maduro asumió el poder en el 2002, consideró que las reformas nuevas eran poco duras con el crimen (Ungar 2009). La indiferencia del Presidente Maduro por estas reformas resonó en un nivel personal con muchos votantes, ya que su hijo había sido asesinado en un secuestro mal logrado. El gobierno de Maduro se distanció de las reformas nuevas, optando en cambio por códigos penales que lucharían firmemente contra el crimen persiguiendo a miembros de pandillas, tal como la Provisión 332. La Provisión 332, una enmienda al código penal, castigaba la membresía en las pandillas con términos de encarcelamiento obligatorio de nueve a doce años (Ungar 2009). Otras leyes fueron incluso más lejos. La Ley de Policía y Convivencia Social aumentó los poderes discrecionales de la policía permitiéndoles “detener arbitrariamente a ‘vagabundos’—personas que no cuentan con medios honestos para ganarse su sustento o que se sospecha tienen la intención de participar en actividades criminales” (Ungar 2009, 98). Esas medidas han aumentado la población en las prisiones, provocando disturbios y las masacres subsiguientes en la prisión en el 2002 y 2004. Inclusive en ausencia de los disturbios, las prisiones abarrotadas sirven como base para las operaciones de pandillas, al igual que lugares de reclutamiento y entrenamiento para miembros nuevos (Arana 2005).

Tanto la Provisión 332 como la Ley de Policía y Convivencia Social ampliaron los poderes discrecionales de la policía sin proveerles recursos o entrenamiento adicional para luchar contra el crimen, esencialmente relegando a la policía a sus funciones como “guardias fronterizos” entre las clases sociales (Booth et al 2010). Además de aumentar los poderes de la policía, Honduras también se ha unido a la tendencia regional de desplegar militares para luchar contra el crimen. Bajo la Operación Guerra contra la Delincuencia, el Presidente Maduro envió aproximadamente 10.000 oficiales para patrullar las calles bajo el liderazgo de un funcionario militar (Booth et al 2010, 173). El Presidente actual, Porfirio Lobo, ha continuado esta tendencia, lanzando patrullas conjuntas de militares y policías para luchar contra el crimen bajo la Operación Relámpago.

Las medidas de mano dura coincidieron inicialmente con una caída en las tasas de asesinato a nivel nacional entre 2002-2004 (UNDP 2009, UNODC 2011). Según algunos cálculos, las medidas de mano dura resultaron también en “un descenso del 80% en secuestros y del 60% en la violencia entre jóvenes” (Ribando 2005). No obstante, para el 2004, la tasa de crímenes comenzó a subir a un ritmo constante, particularmente a medida que las maras se reagruparon y respondieron a las medidas enérgicas del gobierno con sus propias represalias violentas, abriendo fuego en autobuses y parques llenos de personas, particularmente en la zona de alto crimen de

San Pedro Sula. Políticos prominentes alegaron que la única manera de cambiar estas tendencias era ser más severos, pero los críticos han hecho acusaciones que las tácticas de mano dura no tan solo no son exitosas sino que también ponen en peligro el respeto hacia las libertades civiles y los derechos humanos. Ungar, por ejemplo, alega que las medidas mano dura de la administración de Maduro “exhortaron más uso de las redadas en masa, extendieron el encarcelamiento preventivo, obligaron confesiones y los asesinatos extrajudiciales de los mareros” (2009, 98). Booth et al documentan que entre 1998 y el 2002, “más de 1.500 jóvenes fueron asesinados, la mayoría hombres menores de dieciocho años” (2010, 173). Ante críticas severas de organizaciones como Amnistía Internacional y las Naciones Unidas, el gobierno investigó los asesinatos extrajudiciales y admitió que la policía y las fuerzas de seguridad habían desempeñado un papel en ellos. Sin embargo, este reconocimiento no resultó en condenas ya que el investigador que implicó a funcionarios de la policía y de las fuerzas de seguridad recibió amenazas de muerte después que el informe se hizo público.

Para tratar las inquietudes acerca de los derechos humanos, Honduras ha intentado mezclar las tácticas de mano dura con otras iniciativas, con varios niveles de éxito. Por ejemplo, en el 2002 el gobierno de Maduro lanzó un programa nacional de vigilancia comunitaria, Comunidad Más Segura, que se enfoca en estrategias preventivas como arreglar el alumbrado en las calles y reunirse regularmente con la comunidad para tratar inquietudes de la seguridad local (Ungar 2009). Algunas comunidades han reportado éxito bajo esos programas, lo cual se ha podido medir por los descensos en las tasas de homicidio local. Aún así, este modelo de vigilancia basado en la comunidad ha sido acosado por la violencia. Ungar relata que “el jefe de la policía comunitaria en un distrito fue arrestado en conexión a los asesinatos de jóvenes por parte de la policía y un miembro del grupo de policías ciudadanos dijo que lo utilizaron para atacar delincuentes sospechosos” (2009, 100). Este ejemplo sirve como recordatorio que la participación de ciudadanos no significa más respeto por los derechos humanos y civiles. Los mismos ciudadanos puede emplear esos foros para solicitar (y en este caso participar) en acciones extralegales que socaven el estado de derecho.

Por último, tanto el gobierno de Honduras como los mismos ciudadanos cada vez más han acudido a medidas de seguridad privadas para combatir el crimen. Típicamente, el estado cuida celosamente su monopolización de la fuerza y detesta cederles este monopolio a actores privados. No obstante, recientemente los estados en América Central han estado dispuestos a compartir esta función con actores privados. Por ejemplo, en Honduras en el 2006 el gobierno invitó a las fuerzas de seguridad privadas a unirse a la policía y la milicia en Operación Relámpago, una operación mano dura (Booth et al 2010). Esta invitación provocó la condena rápida de organizaciones de derechos humanos, especialmente del Comisionado de Derechos Humanos hondureño, Ramón Custodio, quien criticó al gobierno por no prestarle atención a la diferencia importante entre las fuerzas de seguridad privadas y las públicas, al igual que por no ofrecer seguridad a través de las instituciones jurídicas apropiadas, como el Ministerio de Seguridad (Mejía 2006). En vista del historial en materia de derechos humanos de Honduras durante esas campañas de mano dura, activistas de derechos humanos se han opuesto firmemente a añadir actores nuevos a la mezcla, particularmente cuando esos actores carecen de supervisión institucional y responsabilidad horizontal (Booth et al 2010). Aún así, aunque la privatización de la seguridad plantea numerosos obstáculos para el estado de derecho, resulta fácil ver por qué esas medidas son atractivas para un público temeroso, ya que muchos perciben la seguridad privada como la única cuerda salvavidas para salir de una situación nefasta. Para inicios de los años 2000, las fuerzas de seguridad privadas sobrepasaron en número a las fuerzas de seguridad públicas, ya que había 114 fuerzas de seguridad privadas por cada 100.000 habitantes, en comparación con una tasa de 91 por cada 100.000 para las fuerzas públicas (Silva 2003).

Impacto del crimen en el gobierno democrático

En vista del *statu quo* violento y la vulnerabilidad comprobada del gobierno democrático en Honduras, ¿qué impacto tendrá la crisis del crimen en el gobierno democrático y la estabilidad política en el futuro? Este estudio responde la pregunta al nivel micro, enfocándose en las experiencias de los ciudadanos con el crimen, al igual que sus evaluaciones de las instituciones políticas y del gobierno. El objetivo de este análisis empírico es determinar si las experiencias personales de las personas con el crimen disminuyen su apoyo a la democracia o los principios y las normas democráticas. Este análisis depende de los datos de la encuesta del 20120 de *AmericasBarometer*, llevado a cabo por Proyecto de Opinión Pública Latinoamericana (LAPOR, por sus siglas en inglés).

Para comenzar, este análisis empírico mide las experiencias personales de los encuestados con el crimen. En el 2012, la encuesta LAPOR le preguntó a los encuestados lo siguiente: “*Ahora, cambiando el tema, ¿ha sido usted víctima de algún tipo de crimen durante los últimos doce meses? O sea, ¿ha sido usted víctima de algún atraco, robo, fraude, extorsión, chantaje, amenazas o cualquier otro tipo de crimen en los últimos doce meses?*” Los datos de la encuesta revelaron que además del problema de los altos índices de homicidios, otros tipos de crímenes también figuran prominentemente en la vida diaria en Honduras. Tal como se revela en la figura 3, cuando se les preguntó acerca de las experiencias personales con el crimen, casi un quinto de los encuestados reportaron que habían sido víctimas de un crimen.⁴

Tal como se ilustra en la figura 4, el tipo de crimen más frecuente que los encuestados reportaron fue el robo.⁵ Mitad de las víctimas indicaron que había enfrentado robos a mano armada, y un 16% adicional indicó que habían enfrentado robos con la amenaza de fuerza. Catorce por ciento indicó que el robo no fue marcado ni por la violencia ni por amenaza de violencia. Todos los demás tipos de crímenes (por ejemplo, daño a la propiedad, extorsión, asalto) nunca sobrepasaron el 5% cada uno.

Lamentablemente, muchos hondureños no creen que los mecanismos legales para tratar estos tipos de victimización sean eficaces. En la figura 5 se analizan las respuestas de los encuestados a una pregunta en la encuesta que mide la confianza de que el sistema judicial puede responder adecuadamente a la victimización: “*Si usted fuese víctima de un robo o asalto, ¿cuánto confiaría en el sistema judicial para castigar al culpable? Lo confiaría (1) en lo absoluto (2) muy poco (3) algo (4) mucho*”. Tal como se ilustra en la gráfica, aproximadamente un cuarto de los encuestados no confían que el sistema judicial castigará al culpable en lo absoluto, y un 32,5% adicional registró solamente un poco de confianza. Por lo tanto, los niveles elevados de victimización se comparan con niveles bajos de confianza de que el sistema judicial castigará a los culpables.

Además de los niveles bajos de confianza que el sistema judicial castigará a los culpables, la mayoría de los hondureños registraron niveles bajos de confianza en la policía. En la figura 6 se comparan los niveles de confianza en una serie de instituciones, dependiendo de una variedad de preguntas en la encuesta diseñadas para medir la confianza del pueblo en instituciones políticas claves. A los encuestados se les preguntó lo siguiente: “*Hasta qué punto confía...*” en instituciones incluyendo las fuerzas armadas, el sistema judicial, el congreso, el presidente, los partidos políticos y la policía. Las respuestas variaron desde un puntaje bajo de uno (1) bajo hasta un puntaje alto de siete (7). En la figura 6 se ilustran las respuestas promedio a estas preguntas, y haya que la confianza del pueblo es más baja en la policía, pero significativamente más alta en la milicia.⁶ Cuando se comparó con todas las demás instituciones políticas nacionales en Honduras, la milicia excedió en categoría a todas las demás instituciones.

Un motivo por el cual los encuestados registraron bajos niveles de confianza en la policía está probablemente vinculado a las experiencias con la corrupción personal.⁷ En Honduras, los encuestados reportaron niveles muy elevados de corrupción en la policía. Según se ilustra en la figura 7, cuando se les preguntó si un oficial de la policía había solicitado un soborno en los últi-

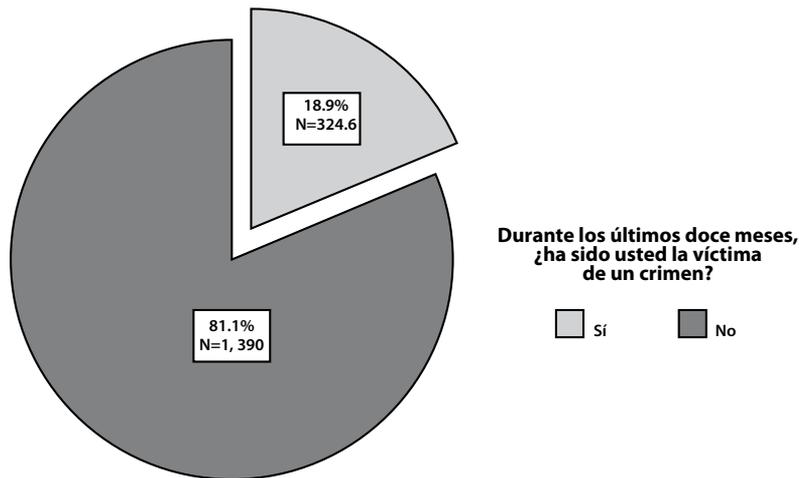


Figura 3. Victimización Autodenunciadas (LAPOP 2012)

mos doce meses, el 17% de los encuestados respondió afirmativamente. Este índice de sobornos está entre los más altos en la región en la encuesta del 2012. Un porcentaje significativamente más bajo de los encuestados reportó que miembros de la milicia y otros funcionarios públicos habían solicitado sobornos, pero resulta importante recordar que la persona promedio en Honduras tiende a tener menos contacto con miembros de la milicia y otros tipos de funcionarios públicos.⁸ En general, la policía tiende a ser los oficiales con quienes las personas promedio tienen más contacto. Lamentablemente, muchas de esas interacciones están contaminadas por la corrupción.

Tal como se indica en la figura 8, cuando se compara con otros países de América Central y México, la corrupción de la policía es particularmente elevada en Honduras. En esta comparación regional, Honduras es el tercer país en términos de corrupción policial, estadísticamente a la par con las tasas en Guatemala, y 4,5% más baja que en México. En contraste, El Salvador, Nicaragua, Costa Rica y Panamá reportaron índices que eran significativamente más bajos que en Honduras, por al menos 10%.

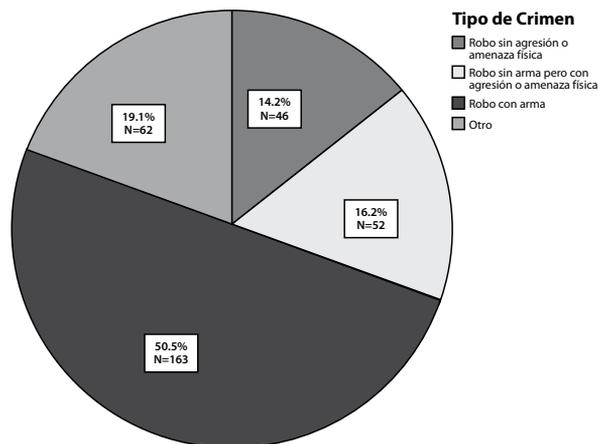


Figura 4. Tipo de Victimización Autodenunciada (LAPOP 2012)

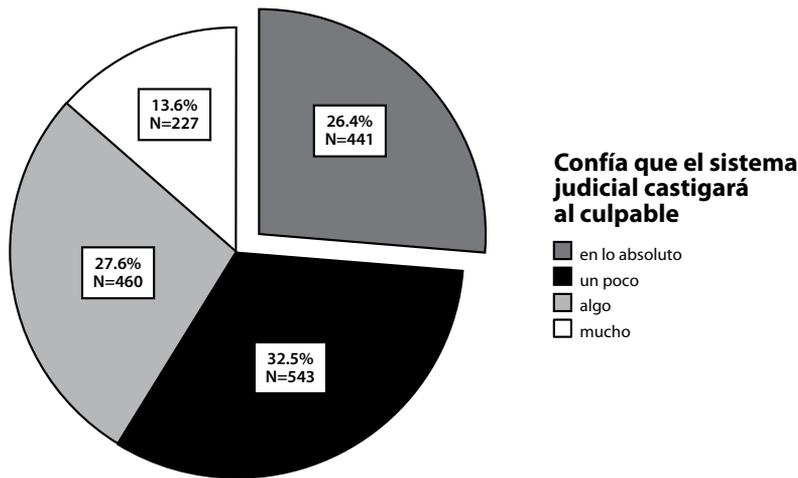
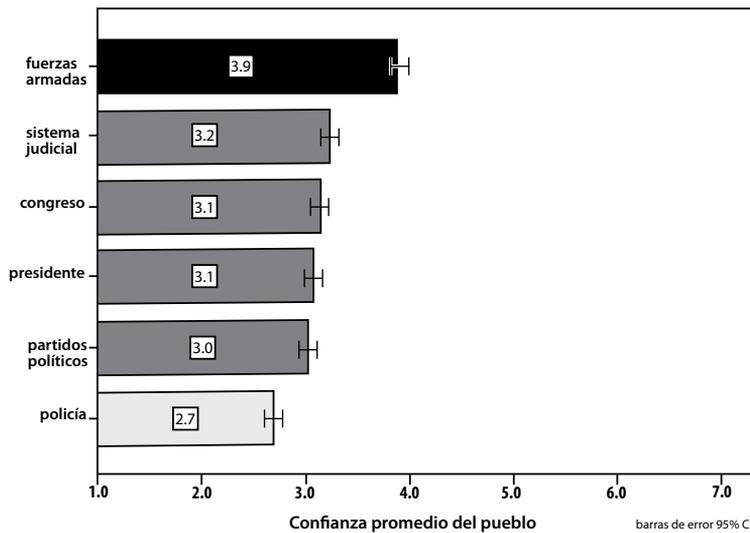


Figure 5. Confianza que el Sistema Judicial Castigará a los Culpables (LAPOP 2012)

Tal como nos recuerda la cita escalofriante de Gustavo Alfredo Landaverde en noviembre de 2012, el problema de la inseguridad pública está entrelazado con el problema de la corrupción hoy en día en Honduras. Cada vez más, el pueblo ha indicado niveles elevados de frustración con el rendimiento del gobierno en ambas áreas. En el LAPOP 2012 se le pidió a los encuestados que evaluaran el rendimiento del gobierno en los campos de lucha contra la corrupción y el crimen con las siguientes dos preguntas:

- ¿Cuánto diría usted que el gobierno actual lucha contra la corrupción en el gobierno? (1) en lo absoluto – (7) mucho.
- ¿Cuánto diría usted que el gobierno actual está mejorando la seguridad de los ciudadanos? (1) en lo absoluto – (7) mucho.



Figur 6. Confianza en las Instituciones en Honduras (LAPOP 2012)

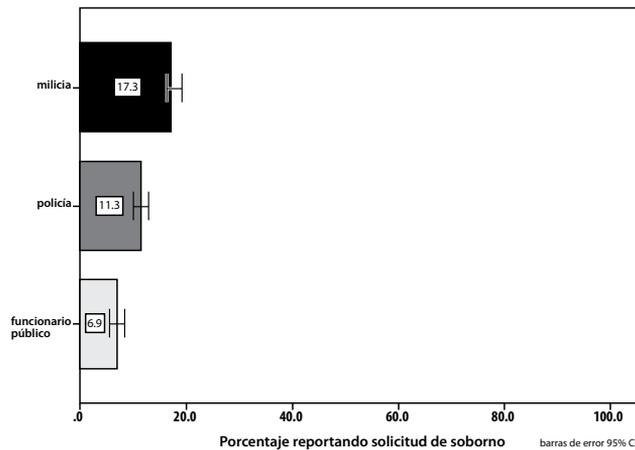


Figura 7. Experiencias Personales con la Corrupción en Honduras (LAPOP 2012)

En la figura 9 se ilustra que en promedio, las evaluaciones del pueblo sobre el rendimiento del gobierno en estas dos áreas son bastante bajas, concentradas en la parte inferior de la escala. Si bien el pueblo ha indicado claramente que el crimen y la corrupción son los problemas más apremiantes que Honduras enfrenta en la actualidad, cuenta con una evaluación pésima de los intentos del gobierno de tratar esos dos problemas. Como cabe esperar, esto abre la puerta para soluciones alternativas, tal como presionar a la milicia al servicio interno. Como se destacó anteriormente en este artículo, Honduras ha incorporado cada vez más a la milicia en sus políticas de la lucha contra el crimen. En este sentido, no es fuera de lo común para Honduras ya que la milicia ha incrementado su rol interno en varios países, más notablemente en México y Guatemala. La decisión de incorporar a la milicia resulta típicamente cuando los gobiernos consideran que sus fuerzas policiales nacionales son demasiado corruptas, no cuentan con suficiente entrenamiento y son ineficaces para confrontar la crisis del crimen (Ellingwood 2010). No obstante, tal como lo indican las evidencias de México, una vez que la milicia asume el rol interno de proveer seguridad, típicamente también está plagada con problemas similares de corrupción e ineficacia, a medida que elementos del crimen organizado merman la reputación de la milicia con ofertas de sobornos y amenazas de violencia. Tal como se discutió anteriormente en este artículo, cuando la milicia participa en operaciones de lucha contra el crimen interno, las violaciones a los derechos humanos con frecuencia aumentan, ya que las fuerzas militares típicamente están entrenadas para luchar contra insurgencias externas, y a menudo no están preparadas para operaciones extensas con la población civil.

Los datos de la encuesta del 2012 destacan esa tensión entre la incorporación de la milicia en iniciativas de lucha contra el crimen y el respeto por los derechos humanos. LAPOP le preguntó a los encuestados una serie de preguntas para medir las evaluaciones y las expectativas de las fuerzas armadas, particularmente en términos del papel que desempeña la milicia en los asuntos internos:

- “¿Hasta qué punto cree usted que las fuerzas armadas hondureñas están bien entrenadas y organizadas?”
- “La fuerzas armadas deben participar en combatir contra el crimen y la violencia en Honduras. ¿Cuánto está usted de acuerdo o en desacuerdo?”
- “¿Cuánto cree usted que las fuerzas armadas hondureñas respetan los derechos humanos de los hondureños en la actualidad?”

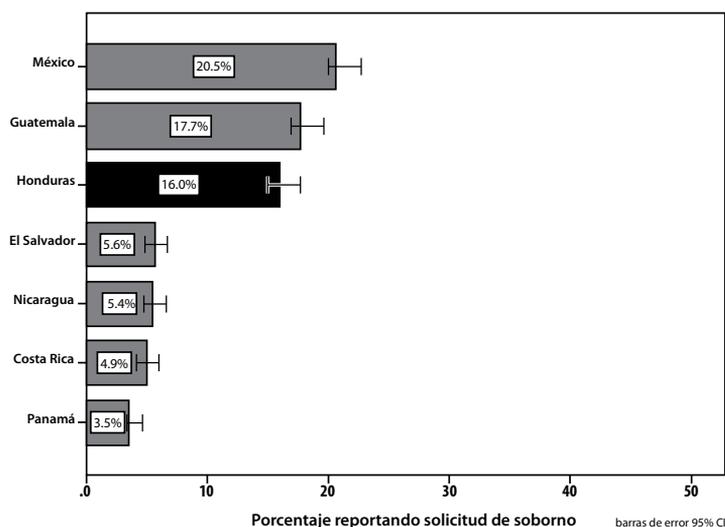


Figura 8. Experiencias Personales con la Corrupción en América Central y México (LAPOP 2012)

Las respuestas a estas tres preguntas variaron desde un puntaje bajo de uno (1) hasta un elevado de siete (7). Tal como se ilustra en la figura 10, hay un apoyo fuerte por la participación de la milicia en la lucha contra el crimen, aunque las percepciones de que la milicia está bien entrenada y organizada son significativamente más bajas (aunque aún están por encima del punto medio de la escala). Sin embargo, la milicia hondureña recibió la calificación más baja en las áreas de respeto a los derechos. En general, los encuestados registraron evaluaciones tibias sobre el rendimiento de la milicia en el campo de derechos humanos. Si bien los encuestados no piensan que el expediente de derechos humanos de la milicia en la actualidad es deficiente, tampoco le dan calificaciones elevadas. Esta es una preocupación si la milicia piensa ampliar su participación en actividades internas tales como el control del crimen.

Por último, en este artículo se analiza el impacto del crimen en el apoyo del pueblo a la democracia y sus normas. Los observadores han advertido que la epidemia del crimen podría socavar la democracia no tan solo en Honduras, sino también en los países aledaños en América Latina. Por ejemplo, en Guatemala, Seligson y Azpuru (2001) encuentran que la victimización y el temor al crimen disminuyen el apoyo a las instituciones democráticas, la confianza interpersonal y provoca que los ciudadanos prefieran cambios radicales. En un estudio de Ciudad México, Parás (2003) descubre tendencias similares, uniendo la victimización con un apoyo significativamente menos por la democracia. En un estudio comparativo de América Central, Pérez (2003) encuentra que el crimen puede crear presión para la “democratización” o acción enérgica por parte del gobierno, que puede resultar en medidas represivas y no democráticas.

Otros investigadores han encontrado que el crimen tiene el potencial de socavar la calidad de la democracia. Un componente de la democracia que es particularmente vulnerable es el estado de derecho, ya que las investigaciones han asociado que la inseguridad del pueblo apoya la justicia extra legal, y una disposición a ignorar la ley para poder atrapar a presuntos criminales más agresivamente. Por ejemplo, Diamond advierte que el crimen puede llevar a los ciudadanos a participar, o al menos apoyar, medidas extremas en conflicto con las normas democráticas, tales como los “pelotones vigilantes populares capaces de hacer justicia instantáneamente a presuntos infractores, tortura y asesinato de prisioneros y sospechosos por parte de la policía y pelotones de exterminio al mando de la policía” (1999, 91). En un análisis empírico, Parás y Coleman

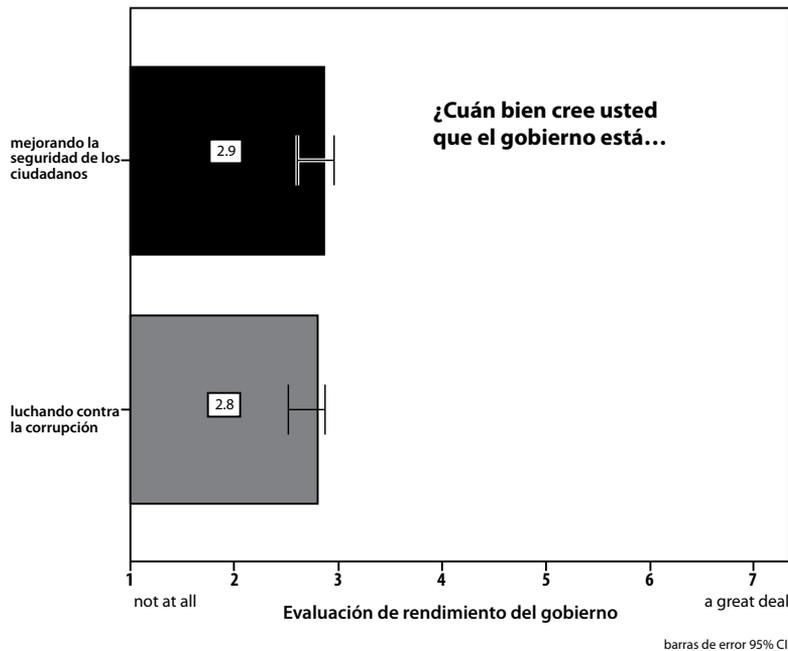


Figura 9. Evaluaciones sobre el Rendimiento del Gobierno (LAPOP 2012)

(2006) también encuentran una relación entre la victimización y el apoyo a las autoridades que eluden la ley.

En vista de esta prueba teórica y empírica, este análisis pone a prueba la capacidad del crimen de debilitar el apoyo a la democracia y sus normas en una Honduras contemporánea. En este análisis se examinan dos elementos clave en particular:

- Apoyo del pueblo por la democracia como la mejor forma de gobierno
- Apoyo del pueblo por el estado de derecho

Para determinar el impacto del crimen en el apoyo a la democracia y sus normas, este análisis depende de una herramienta estadística denominada Análisis de Variación (ANOVA, por sus siglas en inglés), que emplea la prueba F para significado estadístico para determinar si los medios de grupos diferentes son estadísticamente diferentes entre sí. En este caso, ANOVA puede determinar si las víctimas de un crimen registran diferentes niveles de apoyo a la democracia y sus normas que, por ejemplo, aquellos que no han sido víctimas.⁹ Para ilustrar esas diferencias entre los grupos, y si esas diferencias son significativas, este informe depende de una serie de gráficas que ilustran cada grupo en indicadores relacionados fuertemente con el gobierno democrático. En cada gráfica, las barras de error ilustran si la diferencia observada (de haberla) es estadísticamente significativa. Hablando claramente, si las barras de error en cada lado de la media no se traslapan, la diferencia observada es estadísticamente significativa.

Este análisis depende de ANOVA para determinar si aquellos que han sido personalmente afectados por el crimen, según lo midió la victimización personal en el pasado año, apoyan menos a la democracia o al estado de derecho. Por supuesto, esto es tan solo una prueba, midiendo la relación directa entre la victimización y las actitudes políticas claves. No mide otras maneras en la que el crimen podría incidir en el apoyo del pueblo por la democracia. Por ejemplo, puede que si un miembro de la familia o un amigo personal es victimizado por el crimen, las personas

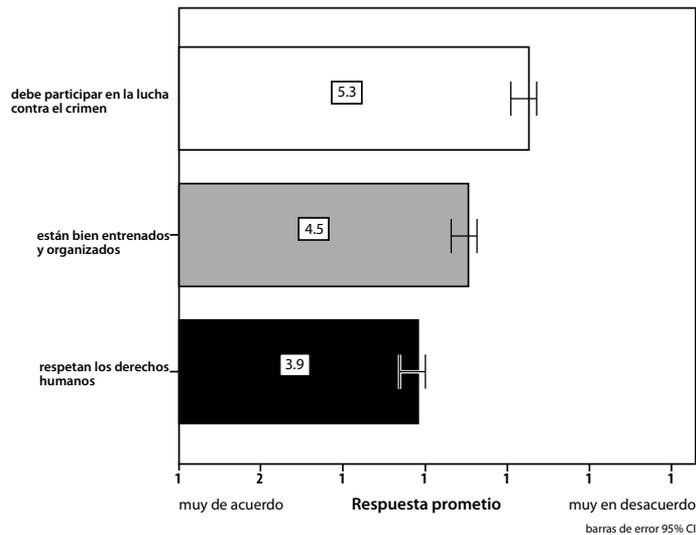


Figura 10. Evaluaciones y Expectativas de la Milicia (LAPOP 2012)

registren menos apoyo. El temor del pueblo por el crimen, no solamente la experiencia personal con el crimen en sí, también podría ser importante. Si bien la victimización personal no es el único factor relacionado con el crimen que podría estar unido teóricamente con el apoyo del pueblo por la democracia y sus normas, es un lugar importante para comenzar. Si la victimización está ligada a las actitudes hacia el gobierno democrático, los niveles elevados de crimen podrían llevar a las personas a apoyar medios no democráticos para luchar contra el crimen.

Apoyo a la democracia como la mejor forma de gobierno

En el primer análisis ANOVA se examina el apoyo del pueblo por la democracia. La democracia es estable cuando es “la única alternativa”. Cuando los ciudadanos están de acuerdo que la democracia es la mejor forma de gobierno (a pesar de todos sus problemas) ellos muestran un compromiso con el gobierno democrático y un rechazo a tipos de gobierno alternativos. En cambio, si los ciudadanos no están completamente comprometidos con el gobierno democrático y están dispuestos a contemplar otros tipos de gobierno, el sistema político podría estar en riesgo. La inestabilidad política puede resultar cuando los ciudadanos no apoyan claramente al gobierno democrático.

Para medir la cantidad de apoyo que el gobierno democrático genera en Honduras, a los encuestados se les preguntó cuánto están de acuerdo con la siguiente aseveración: “*Cambiando de tema nuevamente, puede que la democracia tenga problemas, pero ¿es mejor que cualquier forma de gobierno? ¿Hasta qué punto está usted de acuerdo o en desacuerdo con esta aseveración?*” Las respuestas variaron de un puntaje bajo de uno (1) a un puntaje elevado de siete (7). En la figura 10 se comparan las respuestas promedio de aquellos que reportaron haber sido victimizados durante el último año, y aquellos que no lo fueron. Tal como se muestra en la figura 11, no hay una diferencia significativa entre esos dos grupos. Las víctimas de crimen registraron niveles idénticos de apoyo a la democracia al igual que las no víctimas. En ambos casos, el apoyo a la democracia estaba ligeramente por encima del punto medio de la escala.

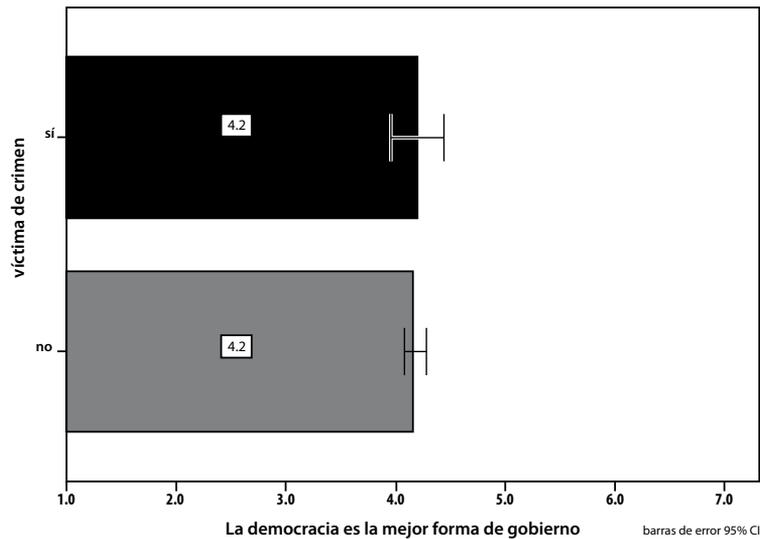


Figura 11. Apoyo a la democracia como la Mejor Forma de Gobierno según la Victimización (LAPOP 2012)

Apoyo por el estado de derecho

Además de evaluar el apoyo a la democracia, también es imprescindible explorar las actitudes de los ciudadanos hacia componentes específicos del gobierno democrático. Los ciudadanos pueden apoyar la “marca comercial” de democracia, pero el apoyo de algunos de sus componentes individuales podría ser menos entusiasta. Este análisis examina el apoyo a un componente clave de la democracia: el estado de derecho. Para que un país sea democrático, la ley debe respetar a todos los ciudadanos por igual, y debe regular eficazmente las relaciones entre los ciudadanos y entre los ciudadanos y sus gobiernos. Si bien el estado de derecho es un componente fundamental de la democracia, ha resultado ser un eslabón particularmente débil en muchas democracias latinoamericanas, particularmente Honduras. Los índices elevados de crimen pueden tentar a los ciudadanos a hacer caso omiso de algunas normas democráticas cuando son consideradas engorrosas. De hecho, en la actualidad hay numerosos ejemplos de la policía, la milicia, y grupos paramilitares sancionando extra judicialmente a sospechosos (Cruz 2008, Ungar 2009).

Para analizar el respeto de los ciudadanos por la ley, LAPOP incluyó una pregunta que mide la disposición de los ciudadanos de otorgarles a las autoridades más libertad de acción para perseguir a presuntos criminales, y actuar al margen de la ley: “Para poder atrapar criminales, ¿cree usted que las autoridades siempre deben obedecer la ley o que ocasionalmente pueden cruzar la línea?” Las respuestas fueron contestadas de manera dicotómica: (1) siempre deben obedecer la ley (0) ocasionalmente pueden cruzar la línea. Esta variante dicotómica fue transformada a una escala de 0-100.

Tal como se ilustra en la figura 12, las personas que reportaron haber sido victimizadas por crimen en el pasado año sí registraron niveles de respeto significativamente inferiores por el estado de derecho. Como promedio, 50,8% de las víctimas dijeron que las autoridades siempre deben respetar la ley, comparados con el 64,3% de aquellos que no habían reportado victimización. Esta diferencia de 13,5% es estadísticamente significativa e indica que la epidemia del crimen puede mermar el apoyo del pueblo al estado de derecho, una piedra angular del gobierno democrático.

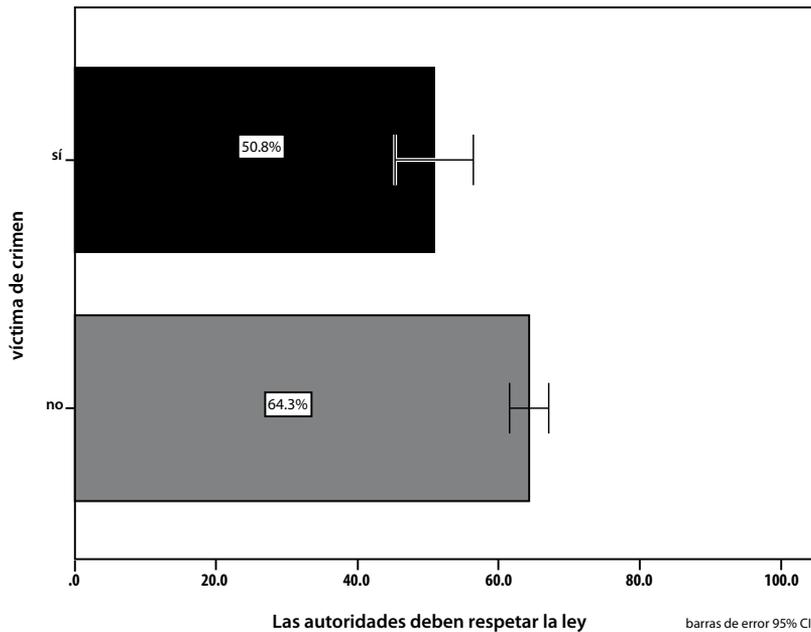


Figura 12. Respeto por la Ley según la Victimización (LAPOP 2012)

Conclusión

En este artículo se ha proporcionado una reseña a nivel macro del crimen y la corrupción en Honduras, al igual que evaluaciones de los ciudadanos de estas tendencias nacionales. El crimen y la corrupción han acosado al gobierno democrático en Honduras durante la última década, pero tal como se ilustra en la figura 1, la magnitud de la crisis del crimen ha aumentado de forma exponencial desde el 2006. Honduras ahora reporta las tasas de crimen más elevadas en el mundo, y los encuestados indican que ellos no creen que el gobierno esté haciendo una buena labor en confrontar la crisis. Tanto las fuerzas de seguridad privadas como de la milicia han sido llamadas a reforzar las fuerzas de la policía, pero esas “soluciones rápidas” no son infalibles. Mecanismos de supervisión para esas fuerzas suplementarias no están firmemente establecidos, y hay posibilidades que las libertades civiles y los derechos humanos se conviertan en víctimas de las medidas de mano dura contra el crimen.

Al mismo tiempo, este análisis de los datos de la encuesta de 2012 indica que ciudadanos atemorizados apoyen la suspensión de las libertades democráticas en nombre de la lucha contra el crimen. Si bien las experiencias personales con el crimen no llevó al pueblo a darle la espalda a la democracia como una forma de gobierno, si parece haber disminuido el apoyo al estado de derecho. Este es un hallazgo inquietante para una democracia en aprietos, particularmente cuando las organizaciones internacionales han expresado preocupación acerca del respeto por los derechos humanos en la batalla en curso contra el crimen. Además, el historial de la manera cómo las medidas de mano dura luchan contra el crimen están lejos de ser claras—a pesar de la serie de medidas enérgicas, los índices de asesinatos han continuado subiendo desde el 2005.

Este análisis se ha concentrado en el nivel micro, examinando las evaluaciones del crimen y el gobierno por parte de los ciudadanos. Si bien en el análisis se encontró que la experiencia personal con el crimen puede disminuir el apoyo al estado de derecho, esta, por supuesto, no es la única manera en la que el crimen pudiese tener un impacto en el gobierno democrático. Por

ejemplo, hay varias maneras en que el crimen pudiese afectar la democracia al nivel macro. Si la militarización de las cruzadas contra el crimen resultase en violaciones a los derechos humanos, esos incidentes obviamente socavarían la calidad de la democracia. Además, las campañas anti crimen pudiesen monopolizar los recursos del estado, tornándolo menos capaz para responder a las otras necesidades de los ciudadanos. Este análisis de la relación entre el crimen y el gobierno democrático al nivel macro es un área importante para las investigaciones futuras. □

Notas:

1. Estos titulares son de la *BBC* (2011), *Miami Herald* (2012) y *New York Times* (2012) respectivamente.
2. El Proyecto de Opinión Pública de American Latina (LAPOP) de la Vanderbilt University es dirigido por el Profesor Mitchell Seligson, y recibe apoyo de la Agencia de Estados Unidos para el Desarrollo Internacional, el Programa de Desarrollo de las Naciones Unidas y el Banco Interamericano de Desarrollo. Por más de tres décadas, LAPOP lleva a cabo entrevistas para medir las actitudes y comportamientos políticos en la región de América Latina. Información con respecto al muestreo, al igual que informes empleando los datos LAPOP están disponibles en <http://www.vanderbilt.edu/lapop/>.
3. Para una reseña clara y concisa de los eventos del golpe de 2009, consultar a Selgson y Booth (2009).
4. Según la encuesta LAPOP 2012 de los demás países centroamericanos y México, Honduras es el tercero después de México y Guatemala que ha tenido tasas de victimización del 23,1% y 20,9% respectivamente.
5. La pregunta de la encuesta rezaba: "Pensando sobre el último crimen del cual usted fue víctima, de la lista que le voy a leer, ¿qué tipo de crimen fue?"
6. Resulta interesante destacar que la confianza en el sistema judicial es más amplia y ligeramente más positiva que las evaluaciones del sistema judicial específicamente en el campo de castigar a los culpables (como lo indica una comparación entre las figuras 5 y 6)
7. Según una correlación de Pearson, hay una relación significativa y negativa más amplia entre la solicitud de un soborno y confianza en la policía.
8. En vista de los niveles de contactos típicamente más bajos entre el pueblo y la milicia, la tasa de soborno del 11% reportada en la figura 7 es bastante elevada.
9. Para calcular el significado, ANOVA compara la variante entre dos o más grupos, y luego determina si esa variante es mayor que la variante dentro de cada grupo. Si la variante entre los grupos (o sea, entre víctimas y no víctimas) es significativamente mayor que la variante entre los grupos (o sea, la variante dentro del grupo de víctimas y la variante dentro del grupo de no víctimas), podemos concluir que esos dos grupos de hecho registran diferentes resultados en el indicador seleccionado (por ejemplo, apoyo a la democracia).

Referencias

- Arana, Ana. 2005. "How the Street Gangs Took Central America" (Cómo las pandillas callejeras se han apoderado de América Central). *Foreign Affairs*, Mayo/Junio.
- Archibold, Randal y Damien Cave. 2011. "Drug Wars Push Deeper Into Central America" (Las guerras de las drogas penetra América Central). *The New York Times*. 23 de marzo de 2011, A1.
- Bailey, John y Matthew Taylor. 2009. "Evade, Corrupt, or Confront? Organized Crime and the State in Brazil and Mexico" (¿Evadir, corromper o confrontar? El crime organizado y el estado en Brasil y México). *Journal of Politics in Latin America* 2: 3-29.
- Booth, John, Christine J. Wade y Thomas W. Walker. 2010. *Understanding Central America: Global Forces, Rebellion, and Change (fifth edition)* (Comprendiendo América Central: Fuerzas globales, rebelión y cambio [quinta edición]). Boulder: Westview Press.
- Booth, John A. 1998. *Costa Rica: Quest for Democracy* (Costa Rica: En busca de la democracia). Boulder: Westview Press.
- Cruz, José Miguel. 2008. "Violence and Insecurity as Challenges for Democratic Political Culture in Latin America (Violencia e inseguridad como retos para la cultura política democrática en América Latina)." Consultado el 2 de junio de 2010 en <http://sitemason.vanderbilt.edu/files/iicjwk/Cruz.pdf>.
- Diamond, Larry (1999). *Developing Democracy: Toward Consolidation* (Democracia en desarrollo: Hacia la consolidación). Baltimore: Johns Hopkins University Press.

- Ellingwood, Ken. 2008. "Mexico Safety Chief's Tough Job: Policing the Police" (El trabajo difícil del jefe de seguridad en México: Vigilando a la policía). *Los Angeles Times*, 15 de septiembre de 2008.
- Lacey, Marc. 2009. "After Losing Honduras, Ousted Leader Wins International Support" (Después de perder Honduras, líder destituido recibe apoyo internacional). *The New York Times*, 30 de junio de 2009, A6.
- Latin American Public Opinion Project (LAPOP). 2010. *AmericasBarometer Survey*. <http://www.vanderbilt.edu/lapop/>.
- Mejía, Thelma. 2006. "A Violent Death Every Two Hours" (Una muerte violenta cada dos horas). *IPS News*. 27 de octubre de 2006. Consultado el 14 de junio de 2011 en <http://ipsnews.net/news.asp?idnews=35275>.
- Millet, Richard L. 2009. "Crime and Citizen Security: Democracy's Achilles Heel" (El crimen y la seguridad de los ciudadanos: El talón de Aquiles de la democracia). En *Latin American Democracy: Emerging Reality of Endangered Species* (Democracia latinoamericana: Realidad emergente de especies en peligro), editado por Richard L. Millet, Jennifer S. Holmes y Orlando J. Pérez. New York: Routledge. 252-264.
- Naím, Moisés. 2005. *Illicit: How Smugglers, Traffickers and Copycats are Hijacking the Global Economy* (Ílícito: Como los contrabandistas, los traficantes y los imitadores están secuestrando la economía global). New York: Doubleday.
- Pain, R (2000). "Place, social relations and the fear of crime: a review" (Puesto, relaciones sociales y temor del crimen: Un repaso). *Progress in Human Geography* 24(3): 365-387.
- Parás, Pablo y Ken Coleman (2006). The Political Culture of Democracy in Mexico (La cultura política de la democracia en México). Informe del *Latin American Public Opinion Project (LAPOP)*, dirigido por Mitchell Seligson, Vanderbilt University.
- Parás, Pablo (2003). Unweaving the social fabric: The impact of crime on social capital (Desenredando el tejido social: Impacto del crimen en el capital social). Proyecto sobre reforma de la administración de justicia en México, Center for US-Mexican Studies: University of California-San Diego.
- Pérez, Orlando J. (2003). Democratic legitimacy and public insecurity: Crime and democracy in El Salvador and Guatemala (Legitimidad democrática y la inseguridad pública: Crimen y democracia en El Salvador y Guatemala). *Political Science Quarterly* 118(4): 627-644.
- Pérez, Orlando. 2000. "Drugs and Post-Intervention Political Economy in Haiti and Panama" (Las drogas y la economía política después de la intervención en Haití y Panamá). En *The Political Economy of Drugs in the Caribbean* (La economía política de las drogas en el Caribe) editado por Ivelaw L. Griffith. New York: Palgrave: 138-161.
- Reuters 2010. "14 Killed on Sports Field in Honduras" (14 Muertos en campo deportivo en Honduras) *The New York Times*, 30 de octubre de 2010, A8.
- Ribando Seelke, Clare. 2011. "Gangs in Central America (updated)" (Las pandillas en América Central [actualizado]) Congressional Research Service (CRS), Washington, DC: The Library of Congress. Consultado el 2 de junio de 2011 en <http://www.fas.org/sgp/crs/row/RL34112.pdf>.
- Ribando, Clare. 2005. "Gangs in Central America" Congressional Research Service (CRS), Washington, DC: The Library of Congress. Consultado el 2 de junio de 2011 en <http://www.fas.org/sgp/crs/row/RS22141.pdf>.
- Seligson, Mitchell and John Booth. 2010. "Crime, Hard Times, and Discontent" (El crimen, tiempos difíciles y descontento). *Journal of Democracy* 21(2): 123-135.
- Seligson, Mitchell y Booth. 2009. "Predicting Coups? Democratic Vulnerabilities, The AmericasBarometer and The 2009 Honduran Crisis" (¿Prediciendo golpes? Vulnerabilidades democráticas, la *AmericasBarometer* y la crisis hondureña del 2009). *AmericasBarometer Insights*:

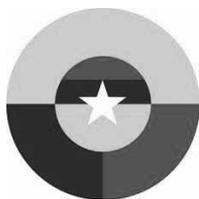
- 2009 *Special Report on Honduras*, <http://www.vanderbilt.edu/lapop/insights/I0821en.pdf> (última consulta el 28 de septiembre de 2012).
- Seligson, Mitchell y Dinorah Azpuru (2001). Las dimensiones y el impacto político de la delincuencia en la población guatemalteca. Población del istmo 2000: Familia, migración, violencia y medio ambiente. Luis Rosero Bixby. San José, Centro Centroamericano de Población.
- Shifter, Michael. 2011. "Central America's Security Predicament" (El dilema de la seguridad de América Central). *Current History* 110 (733): 49-53.
- Silva, José Adán. 2003. "Policía en Desventaja ante Seguridad Privada." *La Prensa*. 3 de marzo de 2003. Consultado el 14 de junio de 2011 en <http://archivo.laprensa.com.ni/cronologico/2003/marzo/03/nacionales/nacionales-20030303-18.html>.
- Smulovitz, Catalina (2003). Citizen Insecurity and Fear: Public and Private Responses in Argentina (Inseguridad y temor de ciudadanos: Respuestas públicas y privadas en Argentina). En Hugo Frühling, Joseph Tulchin y Heather Golding (editores.), *Crime and Violence in Latin America: Citizen Security, Democracy, and the State* (Crimen y violencia en América Latina: Seguridad de ciudadanos, democracia y el Estado). Washington, DC: Woodrow Wilson Center Press.
- United Nations Office on Drugs and Crime (Oficina de las Naciones Unidas para las drogas y el Crimen) (UNODC). 2011. *Global Study on Homicide* (Estudio global sobre el homicidio). http://www.unodc.org/documents/data-and-analysis/statistics/Homicide/Globa_study_on_homicide_2011_web.pdf (consultado por última vez el 28 de septiembre de 2012).
- Ungar, Mark. 2009. "La Mano Dura: Current Dilemmas in Latin American Police Reform" (La Mano Dura: Problemas actuales en la reforma de la policía latinoamericana). 2009. *Criminality, Public Security, and the Challenge to Democracy in Latin America* (Criminalidad, la seguridad pública y el reto a la democracia en América Latina), editado por Marcelo Bergman y Laurence Whitehead. Notre Dame: University of Notre Dame Press, 93-118.
- Walklate, S. L. (2001). Fearful communities? (¿Comunidades temerosas?) *Urban Studies* 38(5-6): 929-939.
- Wolf, Sonja. 2011. "Mano Dura: Gang Suppression in El Salvador" (Mano Dura: Represión de las pandillas en El Salvador). <http://sustainablesecurity.org/article/mano-dura-gang-suppression-el-salvador> (consultado por última vez el 8 de junio de 2011).



Dra. Mary Fran T. Malone, PhD. Es profesora adjunta en la facultad de ciencias políticas en la Universidad de New Hampshire. Sus investigaciones se enfocan en el estado de derecho, analizando el impacto de la epidemia del crimen actual en las evaluaciones de los ciudadanos de sus sistemas de justicia y su apoyo al estado de derecho. Su libro más reciente, *The Rule of Law in Central America* (Estado de derecho en América Central) analiza cómo los países centroamericanos abandonaron la guerra civil y las dictaduras a favor de la democracia en la década de los años noventa, y si ese paso se ve amenazado por la crisis del crimen actual. La Profesora Malone al momento está trabajando en una segunda monografía, *Confronting Crime without Undermining Democracy: Lessons from Latin America* (Confrontando el crimen sin socavar la democracia: Lecciones de América Latina), que analiza cómo algunos países latinoamericanos han reformado con éxito su policía y sus sistemas judiciales.

La Contribución de la Fuerza Aérea Colombiana en el Surgimiento de Colombia como el Nuevo Catalizador Regional

CAPITÁN RODRIGO MEZÚ MINA, FUERZA AÉREA COLOMBIANA.



COLOMBIA ES conocida en muchos lugares del mundo por su problema social derivado del desbordado crecimiento del narcotráfico a finales de los años ochenta¹. Sin embargo la resiliencia de su pueblo logró que los capos más simbólicos del narcotráfico fueran capturados, extraditados y en algunos casos dados de baja por las fuerzas del orden, aunque no se acabara dicho problema. Es precisamente aquí donde comienza dicha reflexión, donde un país que lo ha tenido todo para ser potencia regional, ha tenido que luchar para salir a flote de las vicisitudes que le han aquejado.

Hablar de narcotráfico es hablar de una Organización Transnacional que genera grandes dividendos alrededor del mundo. Según un reporte de la Organización de Naciones Unidas del año 2003, el tráfico ilegal de las drogas genera ingresos mayores a los 322 billones de dólares anuales, esto viene siendo equivalente al 1% del comercio mundial teniendo en cuenta que el GDP (Gross Domestic Product o PIB) mundial asciende a 36 trillones de dólares.

El consumo, a diferencia de lo que se pueda pensar, está propagado en todo el mundo y la alerta situacional, lastimosamente solo obedece a países productores o consumidores, mientras que los países de tránsito tienen una alerta situacional muy baja.

El Narcotráfico: Del mundo para Colombia

Hablar de los inicios del tráfico de drogas en el mundo es hablar de un tema que no ha podido generar un consenso mundial. Algunos documentos referencian que este comenzó en Asia Oriental cuando a mediados y finales del siglo 19 se libró dos guerras del Opio protagonizadas en ese entonces por La Corona Británica y China, algunos académicos niegan la existencia de tráfico ilícito en este caso, ya que dicho comercio en China fue “legalmente” generado. Sin embargo, lo claro es que como resultado 2 millones de chinos cayeron en la adicción². Otros conocedores del tema referencian los inicios del tráfico de drogas a una región como Sur América referenciando tres países; Perú, Bolivia y posterior Colombia durante años 1970, aquí las prácticas históricas indígenas de mascar coca, esta tradición con el tiempo se ha estigmatizado como la expresión más cotidiana de la gestación de un ilícito. Lo clara es que Colombia se convirtió en el referente del narcotráfico durante las últimas tres décadas. Colombia es un nombre que genera diferentes opiniones. Gracias a Hollywood y la industria cinematográfica, Colombia sigue estando en la cabeza de algunos extranjeros como el Estado Fallido³ lleno de traficantes de droga, insurgencia y ahora tráfico sexual.

Es claro que Colombia ha tenido episodios amargos dentro de su historia, pero que también ha gozado de una gran riqueza histórica y cultural que ha servido de referencia para todo el cono sur. Por ejemplo, Colombia es considerada la nación con la democracia más estable en toda Latino América⁴ y sus Gobiernos han mostrado continuidad en sus políticas, aunque en contadas ocasiones dicho estamento gubernamental falló en contener el avance de flagelos como el narcotráfico, las autodefensas ilegales e insurgencia, que en este caso en particular son todos grupos narcoterroristas. Es poco común hablar del narcotráfico sin mencionar sus capos emblemáticos, como Carlos Lehder, La Familia Ochoa Vásquez, Pablo Escobar, Los Hermanos

Rodríguez Orejuela, Gonzalo Rodríguez Gacha, entre otros. Sin embargo y aunque la historia se puede mostrar de muchas formas, la realidad del narcotráfico Colombiano no proliferó solamente por los capos arriba mencionados sino también por la organización narcoterrorista FARC⁵, quien aumentó su poder bélico gracias a un negocio que las ha mantenido activas a lo largo del territorio Colombiano.

Mientras el Cartel de Cali y el Cartel de Medellín evolucionaban y crecían en rutas de exportación ilegal, en las selvas de Colombia se genera el florecimiento de la droga y el pacto por la cocaína se dio en 1982, cuando las FARC tenían en filas no más de dos mil combatientes distribuidos en tan solo 15 frentes. Es allí como el matrimonio FARC-NARCOTRÁFICO se genera en un afán por los capos de tener acceso a la pasta de coca traída del campo, área dominada por las FARC en aquella época; y las mismas FARC con el animo de ser subvencionadas por el servicio de protección a los cultivos de coca en lugares inhóspitos de la geografía Colombiana. De aquí nace el “impuesto revolucionario⁶” que con el tiempo no solo le dio poder económico a las FARC y un crecimiento exponencial en hombres de 15 mil repartidos en 66 frentes, sino también la posibilidad de plantear la estrategia de toma del poder a largo plazo ratificada en 1993⁷. Este impuesto revolucionario representaba entre 10 y 20 por ciento de los ingresos totales que por narcotráfico recibían los capos del momento. Es así como las FARC mutan a un cartel tan o más poderoso de aquellos ya bien conocidos para esa época en Colombia, autosuficiente económica y cada día más fuerte gracias a su nuevo y prolífico negocio⁸.

Por otro lado Pablo Escobar el capo de capos empieza a generar la zozobra en cada rincón de Colombia en una medida desesperada, a través de actos terroristas, pretendía frenar, amedrentar y silenciar todo aquel que estuviera a favor de la extradición. Este panorama desolador no podía ser peor si observábamos con ojo crítico la capacidad de reacción que tenían las Fuerzas Militares. Tan solo 14 mil hombres tenían la responsabilidad de ofrecer seguridad a un país con una extensión mayor a 1 millón de kilómetros cuadrados y un gasto militar por debajo del 3% del PIB. Para el 2002, y luego de una seguidilla de ataques contra la población civil y bases militares o estaciones de la Policía Nacional, las Fuerzas Militares, empezaron a fortalecerse alcanzando a los 140 mil hombres en sus filas y un presupuesto de 4% del PIB.

En esta radiografía Colombiana falta otro protagonista, Fidel Castaño, hermano mayor de Carlos Castaño quien con el concurso de más de 200 capos del narcotráfico, la Familia Ochoa Vásquez y algunos campesinos adinerados formaron el MAS (Muerte a Secuestradores) agrupación formada a raíz del secuestro de un miembro de la familia Ochoa Vásquez⁹, dicha organización con el tiempo dio origen a los GRUPOS DE AUTODEFENSA ILEGALES que lograron tener en sus filas más de 9 mil hombres en armas. Este período fue muy difícil para todo aquel que portaba un uniforme de las fuerzas militares, pues su desprestigio era alto y su respaldo público fueron los más bajos de toda su historia¹⁰.

El apoyo internacional que tenía Colombia era exiguo y mínimo. A tal punto que cuando el Plan Colombia empezó a germinar, la comunidad Europea en cabeza de Francia durante el mes de Octubre de 2000, rechazó dar apoyo al mismo aduciendo que la problemática que tenía Colombia en su momento era un asunto netamente de los Colombianos. Este podría haber sido un segundo episodio del libro escrito por Alfonso Munera, PhD en Historia de la Universidad de Connecticut, “Fracaso de la Nación”, quien muestra como los intereses personales y centralistas del Colombia entre 1717-1821 dominado por el regionalismo, la clase y raza en el caribe Colombiano evitaron la cohesión de un pueblo en contra de un enemigo común, Los Conquistadores¹¹.

El despertar de Colombia

Colombia entendió que debía organizarse y planificar su defensa y no solo el repliegue sino la derrota de todos estos agentes generadores de violencia. Colombia comprendió que solo podría despertar de esta pesadilla haciendo un acto de contrición. Dichos esfuerzos comenzaron a

dar sus frutos con la captura y/o baja de los capos del narcotráfico. Luego el Plan Colombia siguió dando sus resultados durante el lanzamiento de la operación GATO NEGRO. Esta operación develó el arsenal militar de las FARC con conexión desde las Antillas, así mismo sus nexos con mafias de países vecinos como Brasil develado con la captura de *Luiz Fernando da Costa*, alias Fernandiño y cuya aeronave en la cual pretendía escapar, fue interceptada por aviones de combate de la FAC y obligada a aterrizar en Marandúa, una base aérea en el Corazón de los llanos Orientales que fue planificada por el Presidente de la República, Belisario Betancourt en la década de los 80s. De allí en adelante y hasta la fecha Marandúa se ha convertido en el bastión principal en la lucha contra el narcotráfico y un polo de desarrollo para el país.

El Narcotráfico ha sido el mal que ha asolado a Colombia durante las últimas tres décadas¹². Ha sido el combustible económico de los agentes generadores de violencia y la desgracia de muchas familias que han visto a sus miembros sucumbir ante la tentación de conseguir dinero “fácil” con su tráfico pero en el intento han encontrado la muerte o su captura dentro y/o fuera del país.

Hoy Colombia utilizando los preceptos idealistas que Immanuel Kant plasmó en su libro *Perpetual Peace*¹³ (Paz Perpetua), donde soñaba con un mundo lleno de tranquilidad y sin desavenencias domésticas ni internacionales pretende salir adelante. Kant, es hoy en día aún muy criticado por esta postura tan idealista, pero ha servido de base para que otros autores como Bruce Russet y John Oneal autores del libro *Triangulating Peace*¹⁴ (Triangulando la Paz) sentaran bases menos idealistas y más alcanzables en la búsqueda de la paz. Bruce y Russet declaran en sus escritos que la paz de una nación y entre naciones se logra teniendo como premisas; una democracia férrea y continua, interdependencia económica con otras naciones y la participación de Organizaciones Internacionales. La interconexión de estos tres preceptos, con el tiempo resultará en paz y tranquilidad para los pueblos, ya que cada arista de ese triángulo aportará balance, equidad y estabilidad a una nación. Colombia, está entendiendo los conceptos de Russet y Oneal. Hoy en día, Colombia ha fortalecido su democracia, aunque aún falta, sus instituciones son más fuertes y prósperas, sus líderes son escogidos por voto popular y además ha logrado desarrollar mecanismos de protección de los derechos fundamentales de los colombianos tan fuertes y únicos en el mundo como puede ser la Acción de Tutela¹⁵.

Asimismo, Colombia ha podido revertir esa imagen negativa en la región y hoy en día es un líder regional en la asesoría en temas diversos como el desminado de minas anti persona sembradas en Afganistán, la lucha anti drogas en Méjico, además de asesoría directa a sus vecinos de las Antillas, Centro y Sur América. Magazines académicos como *Foreign Affairs*, *Foreign Policy*, y *The Economist*, entre otros, han venido mencionando el milagro Colombiano en sus últimas ediciones y recomiendan se siga su modelo de cambio extremo. Esto ha generado interdependencia económica con los vecinos, también con muchos más países alrededor del mundo. Es así como Colombia ya suma más de 180 entre convenios y tratados con diferentes países del mundo. Colombia hoy en día es más atractivo para la inversión económica, para la mediación social y el asentamiento de empresas multinacionales de todos los hemisferios del mundo. Colombia es considerada una economía emergente y conforma la primera letra del CIVETS (Colombia, Indonesia, Vietnam, Egipto, Turquía y Sur África) países con un desarrollo económico muy por encima del promedio mundial con terreno abonado para la inversión extranjera¹⁶. La Comunidad Europea, que en otrora le dio la espalda, hoy en día lo ve como uno de sus mejores aliados en el tema comercial, es así como un TLC (Tratado de Libre Comercio) se abre paso entre ambas partes, así como con Corea del Sur y Costa Rica¹⁷, sin dejar de mencionar los ya firmados con Estados Unidos y el aún en proceso con China.

En el Tema de Organizaciones Internacionales, Colombia ha dejado de ser el “patito feo”, antes era invitado a cumbres y reuniones de entendimiento por cumplir un protocolo, y era ubicada en las “sillas traseras”. Hoy en día *Colombia es el catalizador de la región*, el proponente de nuevas estrategias para atacar el flagelo del narcotráfico, el modelo económico a copiar por

parte de países desarrollados y en desarrollo¹⁸. Ningún esfuerzo ha sido en vano, la seguridad que impera en gran parte del país es la base para el desarrollo económico.

Hoy Colombia tiene unas Fuerzas Armadas profesionalizadas, respetuosas de los Derechos Humanos y fieles a la aplicación del Derecho Internacional Humanitario, son instituciones con la más alta aceptación y apoyo público, no solo contribuyen a la seguridad sino al crecimiento tecnológico del país.

Algunos ejemplos de esto son:

- La Armada fabrica y exporta embarcaciones tácticas de primera calidad¹⁹.
- La Fuerza Aérea fabrica aviones de entrenamiento como el T-90 ‘Calima’, Aeronaves Remotamente Tripuladas -ARTs (UAVs), proporciona el mantenimiento a todas las aeronaves de la fuerza pública, proyecta en compañía de Brasil la construcción del KC-390, aeronave de transporte pesado²⁰ y actualmente lidera la Interdicción Aérea de Tráfico Ilícito en Centro América, Antillas y Sur América.
- La Fuerza Aérea Colombiana, es altamente activa y gracias a su despliegue rápido ha sido de gran apoyo en los desastres naturales domésticos e internacionales. Entre sus más recientes destacadas ayudas humanitarias están el apoyo a sus nacionales durante el Tsunami en Japón, y los terremotos de sus hermanas naciones de Haití y Chile.

Y es que Colombia a través de la FAC está preparada para brindar apoyo rápido y de primera calidad a quien lo necesite. Este liderazgo la hace partícipe del Sistema de Cooperación entre las Fuerzas Aéreas Americanas (SICOFAA) el cual no solo promueve lazos de amistad entre las fuerzas aéreas de América, sino que también provee coordinación y entendimiento en caso de desastres naturales como los anteriormente descritos. Es así como el pasado mes de Junio, se realizó en Ottawa, Canadá la quincuagésima segunda Conferencia de Comandantes en Jefe de las Fuerzas Aéreas Americanas - CONJEFAMER, quienes pertenecen al SICOFAA, y contó con la presencia de 18 comandantes de Fuerza Aérea quienes tienen su asiento permanente y la participación especial de Jamaica y Méjico quienes asistieron en calidad de observadores. Para Colombia esta reunión fue de gran orgullo pues como nunca el Comandante de la Fuerza Aérea Colombiana fue requerido por la gran mayoría de los países participantes. Esto demuestra el profesionalismo de una Fuerza Aérea que ha dado en los últimos 10 años los resultados más exitosos en la historia reciente de Colombia en contra de los agentes generadores de violencia. Esta efectividad le ha servido para ser ovacionada por sus pares y solicitada formalmente por varios países para que brinde asesoría en temas como interdicción Aérea, planeamiento y desarrollo de operaciones aéreas y entrenamiento de alto nivel.

La Fuerza Aérea Colombiana también participó este año y por primera vez en su historia en el ejercicio RED FLAG, organizado desde 1975 en la Base Aérea de Nellis, Estados Unidos. El propósito de este ejercicio es proveer entrenamiento refinado y de primer nivel a pilotos de Estados Unidos, OTAN y otros países aliados. El alto nivel de sus pilotos sirvió para invitar a la FAC y demostrar por qué es la fuerza decisiva en el conflicto Colombiano. Este buen nombre que ostenta a nivel internacional la Fuerza Aérea Colombiana, no se ha hecho de la noche a la mañana. Desde comienzos del 2003 la Fuerza Aérea ha venido cambiando su modo de operación debido a los retos que se le han impuesto.

La Fuerza Aérea Colombiana en el marco regional

Primero, durante la década de los noventa la Fuerza Aérea se vio forzada a operar las 24 horas del día, en aras de repeler los ataques indiscriminados en contra de la población civil por parte de los grupos terroristas. Segundo, luego del boom del narcotráfico, Colombia y Estados Unidos firmaron un acuerdo de cooperación entre ambas naciones para suprimir el tráfico aéreo ilegal del narcotráfico sobre cielos Colombianos—ABD (AIR BRIDGE DENIAL por su siglas en in-

gles). Durante el 2003, año de activación de dicho convenio, se detectaron más de 630 vuelos sospechosos territoriales al interior del país. La efectividad de sus procedimientos y el profesionalismo de sus tripulaciones sumado con los radares en tierra, lograron disminuir a 5 vuelos anuales ilegales al interior del país. Hoy en día, el tráfico aéreo es casi inexistente dentro del país, obligando a los narcotraficantes a moverse fuera de la frontera, esto es una reducción del 98,6% del comportamiento aéreo ilegal. La Fuerza Aérea entendió que no es suficiente atacar la problemática al interior del país, sino también era necesario compartir toda la experiencia y capacidad alcanzada en el proceso.

De tal manera que por solicitud de países vecinos, Centro América, Antillas y Sur América, hoy está multiplicando su experiencia a través de ejercicios combinados, que para el 2012 se encuentran ya formalizados en 8 Convenios entre Fuerzas Aéreas para atacar el comportamiento aéreo ilegal, y, 9 Convenios adicionales en proceso de formalización, con lo cual Colombia a través de la Fuerza Aérea está cerrando por completo la utilización ilegal del espacio aéreo regional y en consecuencia reduciendo la oferta de narcóticos que ya presenta una reducción del 42% entre el 2007 y el 2010²¹ en las áreas de cultivo y en consecuencia la producción y comercialización en los mercados de consumo, según el último reporte de la Oficina de las Naciones Unidas sobre las Drogas y el Crimen (UNODC por su sigla en inglés). Estos datos son importantes puesto que Colombia demuestra voluntad para acabar con este flagelo que deja un saldo de 200 mil muertos anuales alrededor del mundo. Siendo Colombia uno de los pocos países que combate este problema con una política de estado clara y definida²².

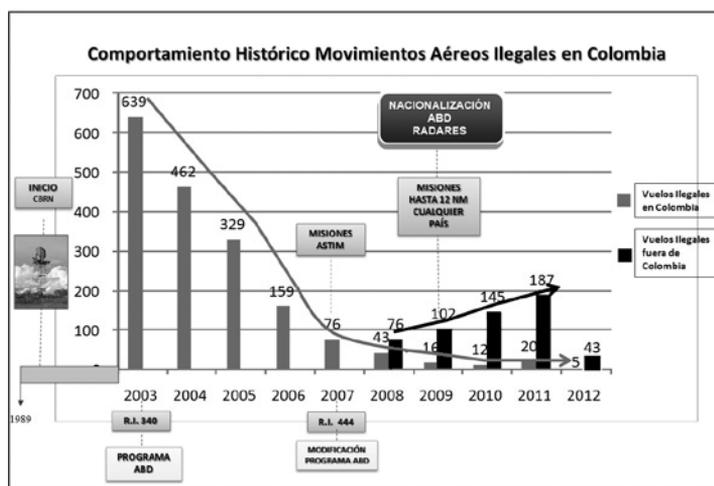
La Fuerza Aérea Colombiana le está dando “cátedra” en operaciones militares a todas las Fuerzas Aéreas del mundo. Las operaciones militares en contra de las FARC como Fénix, donde cae el ideólogo y en su entonces segundo hombre en importancia de las FARC alias Raúl Reyes. Esta operación le permite al país conocer los archivos “X” de las FARC, sus nexos políticos y sus enlaces internacionales, así como la estrategia a largo plazo. La operación Fénix, le abrió la puerta a la FAC a una seguidilla de golpes estratégicos que resultaron en la eliminación de los miembros más sanguinarios de dicha organización como “Mono Jojoy”, jefe militar y Alfonso Cano, su cabecilla²³.

Aunque Las Fuerzas Militares de Colombia unidos a la Policía Nacional han logrado trabajar mancomunadamente con el fin de brindar seguridad y tranquilidad al pueblo Colombiano, la puntería de la FAC ha permitido que la balanza se incline a favor de las fuerzas legales del Estado. La Fuerza Aérea se ha ganado el aprecio y respeto de su pueblo. Su presencia se empieza a sentir en 1932, cuando sus valerosos pilotos defienden su soberanía en la guerra de Perú. Luego se convierte el único bastión de apoyo y protección durante la Segunda Guerra Mundial, cuando sus pilotos valerosamente patrullan sus fronteras luego del hundimiento de una Goleta Colombiana por parte de un submarino Alemán cerca a la Isla de san Andrés en 1942.

Así mismo su presencia en los rincones más inhóspitos de la geografía Colombiana le han merecido su reconocimiento nacional. Durante los desastres naturales de Popayán en 1983, donde mueren más de 300 personas y cerca de 10 mil damnificados, la erupción del volcán Nevado del Ruiz, que dejó un saldo de 20 mil personas muertas en Armero -1985, el terremoto de Armenia, con un saldo superior a 2 mil personas entre los desastres más dolorosos que ha tenido



La FAC transportó 115 Colombianos damnificados del Tsunami en Japón



el pueblo Colombiano, la FAC siempre ha llegado de primera a socorrer a su gente. Hoy, su responsabilidad social llega a los 32 departamentos Colombianos y sus motores ahora se escuchan de manera permanente en Leticia y El Yopal, las bases aéreas más jóvenes de tan próspera institución, las cuales ayudan a multiplicar el esfuerzo de esta fuerza elite que no solo está ayudando a derrotar el narcotráfico, sino también le ha traído progreso social a su pueblo.

La Colombia de hoy

Hoy Colombia sigue cambiando el curso de su historia esperando que quienes aún no se enteran de estos grandes logros, algún día hablen de manera positiva sobre este estratégico país Sur Americano. La sangre derramada por el pueblo Colombiano no ha sido en vano y por eso merece ser tratado con consideración y mucho respeto en el ámbito internacional.

Es así como ya el problema de la droga esta migrando a países vecinos. Por ejemplo, durante la década de lo 90s hasta comienzos del 2000 Colombia era el país de mayor producción en Marihuana, ahora las cifras han cambiado donde Estados Unidos es el productor numero uno de este alucinógeno²⁴. En el tema de producción de hoja de coca, desde inicios del plan Colombia a la fecha dicha producción ha caído en un 65% y ha aumentado en Perú y Bolivia²⁵. Los resultados no se detienen en este campo; en la parte social la criminalidad ha bajado a referencias históricas. Por ejemplo, en el presente año los homicidios han bajo en un 8%. Esto significa que 551 colombianos han dejado de ser asesinados y se ha llegado a la cifra más baja por cada 100 mil habitantes en los últimos 33 años²⁶.

Colombia, gracias a su Fuerza Aérea, hoy se erige ante una comunidad internacional que en el pasado le dio la espalda y hoy lo ve como el mejor modelo a seguir. Los problemas en Colombia no se han terminado, y sin ser triunfalistas, el pueblo Colombiano tiene mucho más por mejorar, pero no podemos ser egoístas con quienes han ayudado a este cambio. Albert Einstein decía *“Si Buscas resultados distintos, no has siempre lo mismo”*, Colombia ha entendido los preceptos del genio más importante de nuestros tiempos. □

Notas:

1. Virginia Marie Bouvier, *Colombia : building peace in a time of war* (Washington, D.C.: United States Institute of Peace, 2009).
2. Edgar Holt, *The opium wars in China* (Chester Springs, Pa.: Dufour Editions, 1964).
3. Barbara Jacobs, “The World’s Banker: A Story of Failed States, Financial Crises, and the Wealth and Poverty of Nations (Book),” *Booklist* 101, no. 4 (2004).
4. Gary Prevost and Harry E. Vanden, *Latin America : an introduction* (New York: Oxford University Press, 2011).
5. Eduardo Mackenzie, *Las FARC : fracaso de un terrorismo*, 1. ed., Colección Actualidad (Buenos Aires: Debate, 2007).

6. Alain Delpirou and Eduardo Mackenzie, *Les cartels criminels : Cocaïne et héroïne : une industrie lourde en Amérique latine*, Collection Criminalité internationale, (Paris: Presses universitaires de France, 2000).
7. Mackenzie, *Las FARC : fracaso de un terrorismo*.
8. Román D. Ortiz, "Guerrilla y narcotráfico en Colombia," *Revista de Seguridad Pública* XXII(2002).
9. La primera incursión directa y pública de los carteles, en materia de violencia, se suscitó a raíz del secuestro de Marta Nieves Ochoa Vásquez, hermana de Jorge Luis, por parte de la organización guerrillera M-19, en 1981.
10. El Espectador, 21 de marzo de 1999, AFP-Bogotá, 8 de diciembre de 2001.
11. Alfonso Múnera, *El fracaso de la nación : región, clase y raza en el Caribe colombiano (1717-1821)*, 1. ed. (Bogotá Colombia: Banco de la República, El Ancora Editores, 1998).
12. Carlos Gustavo Arrieta and Universidad de los Andes (Bogotá Colombia), *Narcotráfico en Colombia : dimensiones políticas, económicas, jurídicas e internacionales*, 1. ed., Sociología y política (Bogotá: Ediciones Uniandes : Tercer Mundo Editores, 1990).
13. Immanuel Kant, *Perpetual peace*, The Library of liberal arts, no 54 (New York,: Liberal Arts Press, 1957).
14. Bruce M. Russett and John R. Oneal, *Triangulating peace : democracy, interdependence, and international organizations* (New York: Norton, 2001).
15. La Acción de Tutela es un mecanismo creado por la Constitución de Colombia de 1991 , inspirado en recursos similares que existen en otros mecanismos de similar finalidad como el Recurso de Amparo que busca proteger los Derechos fundamentales de los individuos al no haber otro recurso para hacerlos cumplir o en el caso de que exista peligro inminente. Es la garantía constitucional del derecho que tiene toda persona a la protección judicial de sus derechos fundamentales a través de un recurso efectivo. Marco legal de la acción de tutela. El marco legal se basa en el Decreto 2591 de 1991 el cual trata del reglamento para el ejercicio de la acción de tutela.
16. William B. Gamble, *Investing in Emerging Markets The Rules of the Game*, (New York: Apress L. P., 2011), <http://www.columbia.edu/cgi-bin/cul/resolve?cli09390956>.
17. Portafolio, "Arranca una semana movida para varios TLC", edición martes 25 de junio de 2012. <http://www.portafolio.co/economia/arranca-una-semana-movida-varios-tlc>.
18. Portafolio, "Modelo económico Colombiano será referencia en G20", edición junio 18 de 2012. <http://www.portafolio.co/internacional/modelo-economico-colombiano-sera-referencia-g20>.
19. El Tiempo, "Cluster fortalecen competencia industrial", edición 31 de agosto de 2011. <http://www.eltiempo.com/archivo/documento/MAM-4791153>.
20. El Tiempo, "Presidente Santos logró avances en materia de seguridad y economía tras firma de acuerdos en Brasil", edición 4 de septiembre de 2010. <http://www.eltiempo.com/archivo/documento/CMS-7892717>.
21. United Nations Office on Drugs and Crime. Policy Analysis and Research Branch., *A century of international drug control* (Vienna, Austria: United Nations Office on Drugs and Crime, 2010).
22. El Tiempo, "Informe dice que mercados de narcóticos tradicionales se estabilizan y crecen los de sintéticas", edición 26 de junio de 2012. http://www.eltiempo.com/vida-de-hoy/salud/drogas-ilicitas-dejan-al-ano-200-mil-muertos-onu_11975166-4.
23. Coronel (R) Luis Alberto Villamarín Pulido, "Fénix, Jaque, Camaleón y Sodoma: Operaciones tácticas con connotaciones político-estratégicas Militar," *Military Review* (2011).
24. United Nations, "World Drug Report 2012" June 2012. http://www.unodc.org/documents/data-and-analysis/WDR2012/WDR_2012_web_small.pdf.
25. United Nations Office on Drugs and Crime. Policy Analysis and Research Branch., *A century of international drug control*.
26. Diario America Economica, "Colombia, Santos destaca el avance en la lucha contra la delincuencia y la guerrilla" edición 16 de junio de 2012.



El Capitán Rodrigo Mezú Mina, Fuerza Aérea Colombiana, se ha desempeñado en cargos tanto operativos como administrativos a lo largo y ancho de la geografía Colombiana. Su especialización es en Defensa Aérea. Los cargos operativos le han permitido aportar al mejoramiento de la seguridad del país y los administrativos la posibilidad de ayudar en la formación militar y académica de los futuros oficiales de la Fuerza Aérea Colombiana. Es un Administrador egresado de la Escuela Militar de Aviación de la FAC con diplomados en Derechos Humanos y de los Conflictos Armados, y un Diplomado en Diversidad y Liderazgo. Es egresado del Old Dominion University, Norfolk , Virginia, donde obtuvo una Maestría en Relaciones Internacionales aplicada a los conflictos Armados. Adicionalmente, el Capitán Mezú es un becario de la Fundación Fulbright y actualmente fue destinado por el alto mando militar de la FAC para aplicar su conocimiento y experiencia en la Dirección de Relaciones Internacionales de la FAC.

Diez Mil Pies y Diez Mil Millas

Reconciliación de la Cultura de Nuestra Fuerza Aérea con los Aviones de Control Remoto y la Nueva Naturaleza del Combate Aéreo

MAYOR DAVE BLAIR, USAF

Acabamos de ganar una guerra donde muchos héroes volaban en aviones. La siguiente guerra puede librarse con aviones sin pilotos. . . . Tiren por la ventana todo lo que han aprendido sobre la aviación en combate y pongámonos a trabajar en la aviación de mañana.

—General Henry “Hap” Arnold, Fuerzas Aérea del Ejército de EE.UU., 1945

Introducción: Una historia, dos aspectos

El fuego nutrido de una ametralladora DShK de calibre 0,50 inmoviliza a un grupo de Mar, Aire y Tierra de la Armada (SEALS por sus siglas en inglés).¹ El grupo, en inferioridad numérica y de armas, tiene una línea de salvamento—el avión en el otro extremo de su radio del controlador de ataque de terminales conjunto. El avión está muy lejos del alcance de cualquiera de las armas de los insurgentes, pero al piloto no le pasa esa idea por la cabeza al concentrarse únicamente en sus camaradas, que no disfrutaban del mismo lujo. De forma muy rápida, una GBU-12 pone al DShK fuera de servicio.² Dos minutos después, unos misiles del atacante acaban con un grupo de insurgentes que trataban de flanquear al grupo. Los SEALs, al no estar ya inmovilizados, responden al fuego, y el adversario se retira. Una vez que se asienta el polvo, los amigos vuelven al sitio de exfiltración.³ Cuando se relata la historia, las acciones de la tripulación marcaron la diferencia entre la vida y la muerte para los valientes miembros de esta fuerza de operaciones especiales.

La parte más importante de esta historia es saber que los buenos regresaron sanos y salvos. Aún así, podríamos contar la misma historia con una tripulación de un avión F-15E Strike Eagle o un MQ-9 Reaper de control remoto (RPA por sus siglas en inglés) como protagonista. En el caso anterior, nuestras instituciones probablemente anunciarían el heroísmo de la tripulación con condecoraciones, pero en el último caso, las mismas instituciones recordarían a la tripulación que sus esfuerzos no reúnen las condiciones de “tiempo de combate”. Las necesidades urgentes del combate tuvieron como consecuencia un crecimiento explosivo de RPA, pero a las personas que satisfacen esas necesidades les dicen que no están en combate. Esta contradicción merece una respuesta.

Como el reconocimiento institucional transmite mensajes eficaces sobre la evaluación relativa, esta distinción merece una exploración adicional. Las fuerzas armadas otorgan medallas de combate por combate, pero en cada nuevo conflicto, la tecnología y las tácticas cambian nuestras definiciones—las líneas del frente se expanden junto con el alcance de las nuevas armas. Este hecho se aplica ciertamente a conflictos actuales, iniciados por enemigos que atacaron por primera vez cuando nos atacaron en nuestra patria por medio de enlaces de transporte y comunicaciones globalizados—conexiones que ahora permiten a nuestros guerreros participar en com-

bate directo desde la patria. De aquí que nuestras definiciones deban reexaminarse a la luz de este frente de batalla globalmente descentralizado.

Respuesta a la sabiduría convencional: Riesgo de combate

Empezamos con el contra-argumento de que los operadores de los RPA no están en combate porque no arriesgan sus vidas. La base de esta idea es el concepto de “riesgo de combate”—las vidas en peligro frente al fuego enemigo clasifican esa actividad particular como combate. Hay dos razones principales que hacen que esta noción sea muy problemática: (1) no diferenciamos entre niveles de riesgo tecnológicamente mitigado en otras plataformas, y (2) en caso de los RPA, simplemente no es cierto.

En primer lugar, ¿cuál es la diferencia de riesgo entre 10.000 pies y 10.000 millas en conflictos normales? Cuando un avión tripulado con dos motores de repuesto roza la parte superior de una zona de combate, muy lejos del alcance de una amenaza realista, ¿por qué consideramos que ese caso es combate pero el disparo de un Hellfire por un Predator como un apoyo de combate? Al profundizar en este asunto, debemos concluir que los avances tecnológicos que reducen el riesgo de combate no deben disminuir la realidad del combate. Los apologistas del statu quo a menudo desapruaban defensas que aprovechan la tecnología como cobardes, pero esas perspectivas normalmente se encuentran desbordadas por individuos capaces de adoptar los cambios que ha traído la tecnología. (Los ejemplos de armas de fuego en Japón, las ballestas medievales y los submarinos de la Primera Guerra Mundial son todos ellos hablan de órdenes arraigadas que invocan el honor para defenderse de los avances tecnológicos).

Al recordar a un piloto de F-22 particularmente vociferante (y ebrio), que afirmaba con énfasis que “luchar una guerra por video teleconferencia no es muy honorable”, podríamos decir lo mismo de disparar un misil más allá de un alcance visual desde un avión caza protegido con tecnología de encubrimiento. Sería difícil imaginarse que el mismo individuo se sintiera forzado a activar su transpondedor de radar al ponerse en contacto con el enemigo, simplemente para restablecer el honor a su víctima mitigando sus defensas tecnológicas. El sistema de control descentralizado del Predator no se adapta menos bien a la categoría de defensas tecnológicas. En otras plataformas, las contramedidas y contratácticas no invalidan la realidad del combate, incluso al mitigar sus riesgos—hacer eso introduce un incentivo profundamente perverso y retrogrado.

En lo que se refiere a lo segundo, no creo que los operadores de RPA corran menos peligro que sus homólogos tripulados. De hecho, afirmo que tal vez sea todo lo contrario. Recuerden que los individuos muertos en el ataque terrorista del 11 de septiembre de 2001 en el Pentágono recibieron el Corazón Púrpura, una medalla de combate. Esta guerra es global, y nuestros enemigos también tienen un alcance global. Si nos encontráramos en la posición de nuestros enemigos, ¿pasaríamos tiempo y llamaríamos la atención tratando de comprar un misil de alto perfil cuando un ataque terrorista a operadores de RPA en Estados Unidos continentales produciría mejores resultados? Esperemos que no se produzca esa situación, pero estoy convencido que la diferencia de riesgo entre ser un operador de RPA en esta guerra es al menos la de un piloto en el teatro de operaciones. ¿En qué se diferencia un ataque terrorista de camino al trabajo del fuego terrestre en un ascenso inicial? En ambos casos, alguien se pone a tiro del enemigo en ruta al área del objetivo.

Además, el acto de emplear cinética conlleva un grado de riesgo personal. Por un lado, los operadores están siempre sujetos a juicios limitados por el tiempo según las instrucciones especiales.⁴ Disparar un arma fuera de esas reglas puede acabar con ellos en la cárcel. Más allá de este caso, un disparo en “peligro inmediato” puede acabar con una baja amiga—el riesgo que aceptamos con el peligro inmediato.⁵ No obstante, la legalidad del disparo no disminuirá su realidad para el operador que hizo el disparo; pero tendrá que vivir con las consecuencias. De la misma

forma, un operador que dispara de acuerdo con las reglas relativas a los daños colaterales tiene que vivir con las imágenes del impacto. Es difícil imaginarse una verdadera salida de apoyo de combate con estas clases de secuelas.

Hacia un mayor entendimiento: Responsabilidad en combate

La responsabilidad en combate ofrece una medida más fiable que el riesgo de combate. La responsabilidad define el combate en términos de dos elementos: (1) responsabilidad ilimitada, incluida la vida y la muerte, e (2) intención del adversario, excluyendo un resultado potencial en el que todos salen ganando (como en un siniestro natural). La medida en la que se invocan estos elementos es la misma en la que una actividad se clasifica como combate. Un individuo tiene responsabilidad de combate si sus opciones pueden resultar directamente en la salvación de vidas amigas o en la terminación de vidas enemigas. En otras palabras, si los individuos inmediatamente señalan, disparan o guían armas o si se les encomienda directamente las vidas de soldados, marineros, aviadores o infantes de marina que se van a poner en peligro, entonces están en combate.⁶

Históricamente, el riesgo y la responsabilidad en combate normalmente se superponen. Antes del advenimiento de los misiles de largo alcance y de los enlaces de datos, el riesgo en combate normalmente era un prerrequisito para emplear armas contra un adversario. No obstante, en tiempos de grandes asimetrías tecnológicas, estas definiciones divergirían. Un samurai con armadura es efectivamente invulnerable a todas las amenazas previsibles, menos a las de otro samurai. Un arquero con un arco largo permanece casi inmune al combate directo debido a sus armas de alcance a menos que sus líneas se rompan. Un submarinista de los primeros años de la Primera Guerra Mundial tiene más que temer del océano que de las armas enemigas. Cuando las asimetrías tecnológicas separan estas definiciones, la responsabilidad en combate capta mejor la totalidad del combate; además, la responsabilidad en combate incluye el riesgo en combate.⁷

¿Cómo sería un modelo de reconocimiento dedicado a la responsabilidad de combate en nuestra guerra aérea actual? Para un avión tripulado, cualquier momento en que los aviadores vuelen en una zona de combate, asumen la responsabilidad de combate ellos mismos y su tripulación o elemento. Cuando los pilotos disparen un arma (incluido un misil de crucero desde fuera de la zona de combate), asumen la responsabilidad de combate por los efectos de esa arma. Esta situación se asemeja mucho a la política actual pero con una justificación más extensiva—medimos a las personas por sus obligaciones con respecto a sus camaradas en peligro así como por el riesgo para ellos mismos.

Los RPA exigen un poco más de interpretación. En contraposición a un avión tripulado, relacionado con combate definido geográficamente en su mayor parte, el RPA requiere una lente causal. Es decir, lo que hacen los individuos en la salida del vuelo define si están en combate o no. Interesantemente, las personas pueden darse cuenta de que van a estar en combate solamente en parte durante la salida. Una salida se considera combate si incluye elementos de responsabilidad en el combate: (1) vidas directamente en juego (2) contra un enemigo en tiempo de guerra. Una salida que no cumpla con esta definición puede satisfacer una definición más relajada para el apoyo de combate: acciones de segundo y tercer orden que activan acciones directas contra el enemigo. Por regla general, alguien en una situación que tome decisiones que afecten directamente el resultado está en combate. Una persona que pone a alguien más en esa situación proporciona apoyo de combate.

Por ejemplo, podemos considerar que los escaneos de sensores en un edificio o el apoyo de combate en una ruta de suministro importante—son acciones contra un enemigo cuando las vidas no estén directamente en juego. Este tipo de misión críticamente importante puede tener a menudo efectos de segundo y tercer orden que salven vidas y ataquen objetivos. Pero en ese

momento, la persona no está en una posición de tomar decisiones que se traduzcan en vida o muerte. Como contraste, considere un escaneo de sensores similar que localice un equipo emplazando dispositivos explosivos improvisados. Cuando los miembros de la tripulación preparan sus misiles con una aprobación de ataque legal, están en combate. Una mirada constante a un edificio se convierte en combate cuando llegue una fuerza de ataque amiga para efectuar una incursión en ese edificio porque la tripulación asume responsabilidad de combate para fuerzas amigas en la pantalla. El desarrollo de objetivos y los escaneos de rutas permanecen típicamente en apoyo de combate. Los ataques cinéticos, el apoyo de acción directa y la escolta armada generalmente se convierten en combate.⁸

Por lo tanto, según la guía actual, una suma de salidas de combate justificaría una Medalla del Aire con el acuerdo de la cadena de mando de combate. De forma similar, una suma de salidas de apoyo de combate justifica una Medalla de Logro Aéreo. Para medallas de una sola misión, la causalidad es la consideración principal. Para tener en cuenta a miembros de una tripulación para que reciban una Medalla del Aire o una Cruz de Vuelo Distinguido de una sola misión, sus acciones deben haber sido el factor decisivo entre la vida y la muerte. Si algunas personas buenas hubieran muerto de no ser por las acciones del Teniente Smith, entonces el teniente es el factor causal de su supervivencia. De forma similar, si el objetivo número cuatro de alto valor está a punto de entrar en un área civil y la destreza superior del aviador Jones permite un disparo de mínimo alcance mientras dicho individuo sigue siendo un objetivo, entonces el aviador es el factor causal en la eliminación del objetivo. Si Smith y Jones cumplen con este requisito, debemos considerar que sus logros son equivalentes a acciones tomadas por la plataforma tripulada.

Conclusión: Efectos de combate que prevalecen por encima del prestigio de la plataforma

En el centro de este debate se basa el carácter sagrado del combate. Los premios y las condecoraciones se encuentran entre las formas más valoradas de reconocimiento formal disponible para las fuerzas armadas. La preferencia relativa de condecoraciones tiene un significado muy claro que hace saber lo que el servicio considera valioso y merecedor de respeto. Existe una tentación peligrosa de usar las condecoraciones para resaltar una plataforma o una capacidad—es imposible exagerar el daño de esta práctica. Al hacer esto, decimos a la gente que lo que son (y pilotan) es más importante que lo que hacen; les decimos que el prestigio es mejor que el valor. En consecuencia, reforzamos la estructura de castas y seguimos generando predicciones sobre el rendimiento relativo que se cumplen por sí solas. Al empezar con el combate y retroceder, enviamos un mensaje mucho más claro, que es que valoramos la contribución de alguien al vuelo. La diferencia que marca la persona es más importante que el avión que pilota.

En primer lugar, este argumento trata de la uniformidad cognitiva, que se hace aún más importante, dado el prodigioso nuevo cuadro de aviadores que son pilotos de RPA. Cuando tenemos un gran número de Tenientes y aviadores completamente nuevos tripulando nuestros RPA actuales, debemos ayudarles a hacer el salto mental desde su estación de control terrestre hasta una zona de combate que nunca han visto, especialmente cuando todas las pistas culturales normales les indican que están en tiempo de paz en Nuevo México. Las consecuencias de no hacer esto son terribles. Cuando cada dos haberes del pabellón y del terreno tienen una mentalidad de combate, la posibilidad de una burbuja de tiempo de paz flotando en el espacio de batalla debe ser aterradora.

En cierta forma, al decir a estos jóvenes guerreros que están volando una misión de apoyo de combate, confirmamos la conclusión natural de que sus cerebros de que están sentados en Estados Unidos en vez de en un área de responsabilidad del Comando Central de EE.UU. (CENTCOM AOR). Si les decimos que no están en combate, ¿quiénes son ellos para no estar de acuerdo? Al

tratar el combate en vez del prestigio como sagrado, eliminamos esta contradicción y ayudamos a estos futuros líderes a reconciliarse con este nuevo tipo de combate. En una tradición naciente de las comunidades Predator y Reaper en desarrollo, hay placas sobre las puertas de entrada de acceso a las salas de combate que proclaman, “Está entrando ahora en el CENTCOM AOR”. Nuestros miembros de la tripulación RPA creen ciertamente en este credo de combate. Solamente pedimos que la institución afirme su veracidad.

Por último, la Fuerza Aérea ha sobrevivido y prosperado siempre como servicio al comportarse de forma pionera e innovadora.⁹ Aunque se basan en verdades eternas de pensamiento militar, nuestro nicho está forjando nuevas formas de guerra, haciendo avanzar la frontera tecnológica para transformar el modo en que nuestra nación libra guerras. Y lo hemos hecho tan bien—pasando del aire al espacio y al ciberespacio, cambiando como respuesta a revisiones de la naturaleza de la guerra que nosotros mismos hemos forjado. Como predijo el General Arnold hace tiempo, ahora luchamos en el aire usando un sistema de pilotaje por mandos electrónicos global cuyos cables de control llegan al espacio y al ciberespacio. Pero la iniciativa y la innovación que expanden continuamente la envolvente no pueden acatar el privilegio establecido. Dicho privilegio está basado en las implicaciones presentes de la distribución de poder del pasado y no puede admitir el cambio, no sea que se reorganice esa distribución. Se convierte en la inercia que nos ancla en el pasado. Para un servicio que se basa en la innovación para sobrevivir, el privilegio es un veneno. Nuestras definiciones y distribuciones de poder deben apoyar la Fuerza Aérea en la lucha actual y siguiente, no en la última. Sobre eso, la *Hoja de ruta integrada de sistemas no tripulados* del Departamento de Defensa predice una fuerza compuesta casi completamente de RPA a mediados de este siglo.¹⁰ En la trayectoria actual, las únicas Medallas del Aire serán las de los libros de historia. □

Notas

1. La *Degtarayova-Shpagina Krupnokaliberniyy* [Degtarayov-Shpagin de calibre pesado] es una ametralladora pesada de la era soviética común en todo el mundo. “Ametralladora pesada de 12,7 mm Degtyarev (DShK-38 y modelo 38/46) (Federación Rusa), Ametralladoras,” Jane’s Information Group, visitada el 23 de febrero 2012, <http://articles.janes.com/articles/Janes-Infantry-Weapons/Degtyarev-DShK-38-and-Model-38-46-12-7-mm-heavy-machine-gun-Russian-Federation.html>.

2. La GBU-12 es una bomba guiada por láser de 500 libras común de los aviones tácticos de EE.UU. “Bombas GBU-10, GBU-12, GBU-16 Paveway II (United States)—Municiones de precisión y guiadas”, Jane’s Information Group, visitada el 23 de febrero de 2012, <http://articles.janes.com/articles/Janes-Air-Launched-Weapons/GBU-10-GBU-12-GBU-16-Paveway-II-United-States.html>.

3. El término *sitio de exfiltración* se refiere a la zona de aterrizaje desde la que se sale una fuerza de operaciones especiales del espacio de batalla después de completar su misión.

4. Las instrucciones especiales son un conjunto de órdenes completas del comandante del componente aéreo de las fuerzas de la coalición que regulan el empleo del poder aéreo en un teatro de operaciones de combate.

5. El término *peligro inmediato* denota disparos empleados en proximidad de fuerzas terrestres amigas cuando la fuerza terrestre opina que el peligro del enemigo es mayor que el de la munición empleada. Formalmente, se refiere al disparo de materiales explosivos dentro del 0,1 por ciento de probabilidad de distancia de incapacitación. Publicación Conjunta 3-09.3, *Close Air Support (Apoyo aéreo inmediato)*, 8 de julio de 2009, V-20, https://jdeis.js.mil/jdeis/new_pubs/jp3_09_3.pdf.

6. Para mantener nuestros términos limpios, usamos *directa e inmediatamente* para referirnos a un participante que está solamente a un paso causal del resultado. Esta distinción útil diferencia entre combate y apoyo de combate. Las acciones de apoyo de combate son críticamente importantes para conformar resultados aunque su impacto no es tan causalmente directo como el de los participantes en el punto de ataque o defensa.

7. Históricamente, a medida que se restablece la simetría, estas definiciones vuelven a converger. Como ejercicio académico, imagine los duelos de flotas de vehículos aéreos de combate chinas y estadounidenses pilotados de forma remota para cada de sus estaciones terrestres. En esta circunstancia, un asiento en un avión tripulado podría ser un lugar mucho más cómodo.

8. Logísticamente, las tripulaciones indicarían si efectuaron o no un apoyo o una cinética de incursión al terminar su salida—información introducida de forma retroactiva en la documentación de vuelo. Este procedimiento se asemeja a un proceso contable para KC-135, donde el estado del combate del avión receptor dicta de forma retroactiva si la misión era de combate o de apoyo de combate.

9. “Nuestra Fuerza Aérea debe su existencia a visionarios que buscaron forma innovadoras de hacer las cosas—en vez de atravesar una línea enemiga, sobrevolémosla. Ahora es el momento de atrevernos a adoptar el espíritu emprendedor que los aviadores han demostrado tener hace mucho al aprovechar las últimas tecnologías y desarrollar nuevas formas de lograr las misiones de la nación”. El General Edward A. Rice Jr., “Building toward the Future” (Formación para el futuro), *Air and Space Power Journal* 26, no. 1 (enero–febrero de 2012): 6, <http://www.airpower.maxwell.af.mil/digital/pdf/issues/jan-feb/Jan-Feb-2012.pdf>.

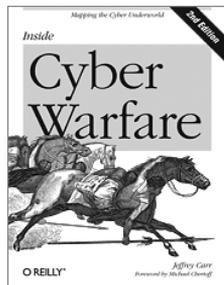
10. Departamento de Defensa, *Unmanned Systems Integrated Roadmap, FY2011–2036* (Hoja de ruta integrada de sistemas no tripulados) (Washington, DC: Departamento de Defensa, Oficina de la Secretaría de Defensa, [2009]), <http://www.fas.org/irp/program/collect/usroadmap2011.pdf>.



El Mayor Dave Blair, USAF (Licenciatura, USAF Academy; Maestría, MPP, Escuela de Gobierno John F. Kennedy, Universidad de Harvard) es un piloto instructor de MQ-1B y un piloto de AC-130U. Ha servido como oficial de operaciones ayudante para combatir y jefe de planes en el tercer Escuadrón de Operaciones Especiales. Como miembro del Comando de Operaciones Especiales de la Fuerza Aérea, ha servido tanto físicamente como mediante telecombate en Irak y Afganistán y en frentes emergentes. Actualmente el Mayor Blair estudia relaciones internacionales como estudiante de doctorado en la Universidad de Georgetown; su disertación trata de aplicar estrategias de perturbación de redes oscuras al problema de tráfico de seres humanos contemporáneos.



Reseña de Libros



Inside Cyber Warfare (Second Edition), by Jeffrey Carr, O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, California, 95472, 294 pages, US\$39.99, ISBN: 978-1-449-31004-2.

Cuando el gusano informático *Stuxnet* dañó el programa nuclear iraní en el 2010, el público recibió un pequeño vistazo de la ciberguerra moderna sin verdaderamente percatarse de la envergadura de este conflicto global. *Inside Cyber Warfare* (Dentro de la ciberguerra) ofrece detalles fascinantes e inquietantes sobre cómo las naciones, los grupos y los individuos en el mundo dependen cada vez más de los ataques en la *Internet* para lograr ventajas militares, políticas y económicas sobre sus adversarios.

Esta segunda edición actualizada se analiza detalladamente el ámbito complejo del ciberespacio y los actores y estrategias involucradas. Usted descubrirá cómo los *hackers* sofisticados trabajando a favor de los estados o el crimen organizado participan pacientemente en un juego arriesgado que puede atacar a cualquiera, indistintamente de su afiliación o nacionalidad.

- Descubra cómo la inversión rusa en las redes sociales beneficia al *Kremlin*
- Aprenda el papel que desempeñan las redes sociales en fomentar revoluciones en el Oriente Medio y en el norte de África.
- Explore el surgimiento de grupos anarquistas tales como *Anonymous* y *LulzSec*.
- Analice las capacidades de ciberguerra de las naciones, inclusive China e Israel.
- Comprenda cómo Estados Unidos puede participar legalmente en operaciones cibernéticas encubiertas.
- Aprenda cómo la guerra de Propiedad Intelectual se ha convertido en el centro de atención principal de las operaciones cibernéticas auspiciadas por los estados.

Jeffrey Carr, fundador y director ejecutivo de *Taia Global, Inc.*, es un experto en inteligencia cibernética y asesor que se especializa en la investigación de ataques cibernéticos por parte de *hackers* estatales y no estatales contra gobiernos e infraestructuras.

O'Reilly Media Staff writer

"Published with permission from O'Reilly Media, Inc."

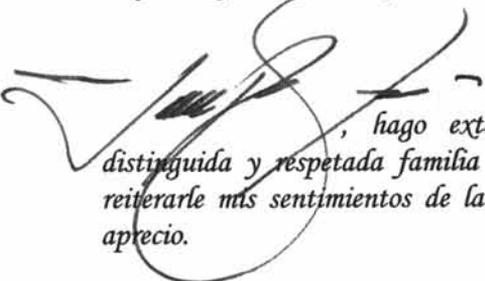


Mayor General
Javier Enrique Rey Navas
Jefe de Planeación del Ejército

Señor Teniente Coronel ®
LUIS F. FUENTES
Fuerza Aérea de EE. UU.

Permítame presentarle un cordial saludo de felicitación, con motivo del otorgamiento de la MEDALLA MILITAR "SAN MIGUEL ARCANGEL" en categoría única otorgada por el consejo de la misma, como justo reconocimiento a sus servicios profesionales y apoyo invaluable al Arma de Aviación del Ejército de Colombia.

Sus publicaciones han sido referencia para nuestros Soldados de Aviación, y nos han ayudado a comprender que los roles con las demás aviaciones y la Fuerza Aérea en nuestro País son preponderantes pero no excluyentes; unidos en operaciones conjuntas y coordinadas para bien de la Patria

 , hago extensiva esta congratulación a su distinguida y respetada familia y aprovecho la oportunidad, para reiterarle mis sentimientos de la más alta consideración, amistad y aprecio.

Bogotá, Septiembre de 2012