

AIR & SPACE POWER

JOURNAL
en ESPAÑOL

Volumen 26, N° 3

TERCER TRIMESTRE 2014



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

Editorial	2
La Modernización Militar y las Ciberactividades de China Dr. Larry M. Wortzel, PhD	4
Liderazgo Tóxico, el Clima de la Unidad y la Eficacia de la Organización Dr. George Reed, PhD	20
La Guerra a la Vuelta de la Esquina Dr. James P. Farwell, PhD Sra. Darby Arakelian	29
Requisitos de las Organizaciones Terroristas con Capacidad Internacional Mayor Michael Haack (USAF)	41
La Confianza Agotada en el Espacio Cibernético Común Dr. Roger Hurwitz, PhD	51
Búsqueda y Rescate en el Alto Norte: ¿Una Misión de la Fuerza Aérea? Coronel John L. Conway III, USAF-Retirado	70
La Mini-Guerra en el Siglo XXI Comodoro José C. D'Odorico, Fuerza Aérea Argentina (1927-2014)	83
Estudiantes del AWC-ACSC Promoción 2013-2014	96



Editorial

La modernización y el acelerado desarrollo militar de China se ha convertido en un elemento clave de la política de seguridad de EE.UU., así como la de casi todos los países de la región Asia-Pacífico quienes perciben dichas actividades como un reto a su libertad de acción en el océano Pacífico y como una agresión y amenaza a su seguridad nacional. En el reporte Anual ante el Congreso sobre las actividades militares de China del 2013, el Dr. Woetzel en “*La modernización militar y las ciberactividades de China*” hace una síntesis muy puntual sobre los móviles de la nueva estrategia militar china, la estructura del gasto militar, los nuevos armamentos desarrollados por las fuerzas militares y el reto presentado por sus actividades cibernéticas.

Al centrarnos en el tema del liderazgo del cual nos hemos referido en algunas de nuestras ediciones anteriores, haciendo énfasis en su importancia, es de anotar que mucho se ha acentuado sobre las características de un buen líder, pero poco se ha analizado el daño causado a la organización y a sus empleados por la conducta de líderes abusivos que se exceden en el ejercicio de sus atribuciones, humillan y denigran a sus subalternos, tal como lo describe el Dr. Reed en su aporte sobre “*Liderazgo tóxico, el clima de la unidad y la eficacia de la Organización*”. Consecuente con su análisis, el autor sostiene que las organizaciones militares deben desarrollar y establecer evaluaciones basadas en las percepciones de los supervisores y los subordinados que les permitan identificar y remover a los líderes que él califica como tóxicos.

Al detenernos en un tema de gran actualidad como lo es la introducción y el tráfico ilícito de drogas proveniente de México, encontramos que la falta de una estrategia coherente entre Estados Unidos y México para combatir a los cárteles, constituye una barrera en el logro de los objetivos, de acuerdo a los planteamientos de Farwell, y Arakelian en su ensayo “*La guerra a la vuelta de la esquina. No es un mero problema delictivo.*” Los autores indican que el problema se acentúa debido a las diferentes prioridades y enfoques de la política antidroga de México y los Estados Unidos, teniendo en cuenta que mientras México se concentra en eliminar la violencia y los secuestros, los Estados Unidos intentan eliminar narcotraficantes y detener el flujo de drogas. Como nota concluyente, ambos autores acentúan la tesis de que la guerra contra las drogas no se puede ganar sino manejar y, para ello ofrecen varias acciones a considerar para la resolución de este complejo problema.

Frente al tema del terrorismo, encontramos que mientras la lucha contra el terrorismo, la incidencia y las nuevas modalidades de hacer terrorismo se aumentan cada día más, el esfuerzo por identificar sus causas resulta infructuoso y casi imposible de definir. En su artículo sobre “*Requisitos de las organizaciones terroristas con capacidad internacional*”, el Mayor Haack analiza algunos de los actos de terrorismo ejecutados en el pasado y, en la búsqueda de un denominador común, centra su análisis en los cuatro prerrequisitos ideológicos de las organizaciones terroristas internacionales que han alcanzado un final feliz y sugiere estrategias antiterroristas que puedan ser utilizadas exitosamente para combatir el flagelo del terrorismo.

El Dr. Hurwitz en su artículo “*La confianza agotada en el espacio cibernético común*”, examina el estado del uso común del ciberespacio a nivel global y la necesidad

de establecer acuerdos internacionales para regular su uso, reducir el riesgo colectivo, y proteger la seguridad nacional e internacional para beneficio de todos.

Finalmente, al publicar póstumamente el artículo “*La Mini-Guerra en el Siglo XXI*”, escrito por el brillante analista argentino Don José C. D’Odorico, Comodoro Retirado de la Fuerza Aérea Argentina, recibido a escasos días antes de su muerte el pasado 18 de junio de 2014, evoco con inmenso dolor y sentido de agradecimiento la memoria de quien fue por más de tres décadas un valioso contribuidor de nuestra revista —dejando un legado y fuente de conocimientos que nunca podremos remplazar y que permanecerá durante mucho tiempo entre nosotros.

A handwritten signature in black ink, appearing to read "Luis Fuentes", written over a horizontal line.

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

La Modernización Militar y las Ciberactividades de China*

DR. LARRY M. WORTZEL, PhD

Testimonio del Dr. Larry M. Wortzel ante la Comisión de Servicios Armados de la Cámara de Representantes



Como miembro de la Comisión de Revisión Económica y de Seguridad de EE.UU.-China, presentaré algunos de los hallazgos de la comisión sobre la modernización militar de China, las relaciones de seguridad EE.UU.-China, y las Ciberactividades de China detalladas en el *Informe Anual de 2013 al Congreso*.¹ Debo indicar que las opiniones que presento hoy, son mías. Quiero reconocer el excelente trabajo de nuestro personal en la preparación del informe anual, y especialmente la excelente investigación del equipo de política exterior y seguridad colaborando en la preparación de este testimonio.

La modernización militar de China

El Ejército Popular de Liberación (EPL), la institución militar de China, está en medio de un amplio programa de modernización que presenta retos importantes para los intereses de seguridad estadounidenses en Asia. Esta modernización incluye la creación de una arquitectura de vigilancia y ataque que apoye operaciones a mayores distancias de la costa de China. Convierte al EPL en una fuerza más formidable en todas las dimensiones de la guerra: aire, espacio, tierra,

* Reimpreso de nuestra AU revista *Strategic Studies Quarterly*, Vol 8, No. 1, Spring 2014.

mar y en el espectro electromagnético. El EPL tiene nuevos buques de combate multimisión, aviones, submarinos y una nueva generación de misiles.

En primer lugar, los elementos principales de este programa—como el misil balístico antibuque DF-21D y el creciente número de submarinos avanzados armados con misiles crucero antibuque—están diseñados para limitar la libertad de acción estadounidense en el Pacífico Occidental. El EPL está ampliando y diversificando rápidamente su capacidad para realizar ataques convencionales contra bases, barcos y aviones estadounidenses y aliados en toda la región, incluyendo aquellas que anteriormente no podía alcanzar con armas convencionales, como las instalaciones militares estadounidenses en Guam. A medida que madura la capacidad anti-acceso y negación de área del EPL, aumentarán los costos y riesgos para Estados Unidos en caso de intervención en un potencial conflicto regional que involucre a China.² Los militares chinos, por cierto, conscientes de la historia de los siglos diecinueve y veinte, consideran a estas acciones como estrategias contra la intervención diseñadas para impedir la intervención de militares extranjeros en asuntos de soberanía o territoriales de China.

Es más, el rápido avance de la capacidad de proyección de poderío regional del EPL aumenta la capacidad de Beijing para usar la fuerza contra Taiwán, Japón y reclamantes rivales en el Mar del Sur de China. Lo que es más grave, como la doctrina militar china enfatiza los ataques preventivos, esto aumenta el riesgo en cualquier crisis. Muchos escenarios potenciales de seguridad podrían exigir que Estados Unidos defiendan a sus aliados y socios regionales y mantenga el acceso abierto y seguro a las vías aéreas y marítimas comunes en el Pacífico Occidental.

Al mismo tiempo, el aumento del malestar sobre las capacidades de expansión de China y su mayor firmeza están haciendo que los aliados y socios estadounidenses en Asia aumenten sus propias fuerzas militares y fortalezcan las relaciones de seguridad entre sí. Estas tendencias podrían apoyar los intereses estadounidenses en Asia aligerando la responsabilidad operativa de Washington en la región. Por otro lado, si los vecinos de China buscan capacidad militar que se podría usar ofensiva o preventivamente debido a la percepción de que Estados Unidos sería incapaz de cumplir su compromiso al reajuste del equilibrio en Asia, esto podría socavar los intereses estadounidenses en la región.

En el informe anual de 2013 de la comisión, tratamos sobre los siguientes acontecimientos en la modernización militar de China:

Marina

Portaaviones. Desde la puesta en servicio de su primer portaaviones, el *Liaoning*, en septiembre de 2012, China continúa desarrollando una capacidad de aviación de ala fija necesaria para que el portaaviones lleve a cabo misiones de defensa aérea y ataque ofensivo. El *Liaoning* es un antiguo portaaviones ruso comprado de Ucrania. Fue reacondicionado y modernizado en China. La Marina del EPL realizó su primer despegue y aterrizaje exitoso en portaaviones con el Jian 15 (J-15) en noviembre de 2012, certificó a su primer grupo de pilotos de portaaviones y oficiales de señales de aterrizaje en el primer despliegue operativo del portaaviones entre junio y julio de 2013, y verificó el proceso de operaciones de la cubierta de vuelo en septiembre de 2013.³ El *Liaoning* continuará realizando despliegues cortos y adiestramiento de aviación a bordo del barco hasta 2015 ó 2016, cuando el primer regimiento de J-15 de China debe estar listo para operación. El J-15 es una copia china del Su-33 ruso. Es probable que China siga al *Liaoning* con al menos dos cascos producidos en el país. El primero de estos parece estar en construcción y podría estar operativo antes de 2020.

Misiles balísticos de lanzamiento desde submarino. Se espera que el misil balístico de lanzamiento desde submarinos Julang-2 (JL-2) de China logre capacidad operativa muy pronto.⁴ El misil está en desarrollo desde hace varios años, lo que indica que las industrias militares chinas aún tienen problemas para desarrollar y poner en operación sistemas nuevos. El JL-2, cuando se

combine con el submarino nuclear con misiles balísticos clase Jin (SSBN) de la Marina del EPL, dará a China su primer disuasivo nuclear basado en el mar creíble. El sistema de armamentos Jin SSBN/JL-2 tendrá una autonomía de aproximadamente 4.000 millas náuticas, permitiendo que la Marina del EPL apunte al territorio continental de los Estados Unidos desde las aguas del litoral de China.⁵ Se han desplegado tres Jin SSBN y probablemente se pongan en operación otras dos unidades en 2020.⁶

Capacidad de ataque a tierra desde el mar. Actualmente China no tiene la capacidad de atacar objetivos en tierra con misiles crucero desde el mar. Sin embargo, la Marina del EPL está desarrollando una capacidad de ataque a tierra, probablemente para su submarino de ataque con misiles guiados Tipo-095 y el destructor con misiles guiados Luyang III. Los submarinos modernos y las unidades de superficie armadas con misiles crucero de ataque a tierra (MCAT) complementarán el creciente inventario del EPL de MCAT basados en aire y tierra y misiles balísticos, mejorando la flexibilidad de Beijing para atacar objetivos terrestres a través del Pacífico Occidental, incluyendo las bases estadounidenses en Guam.⁷

Construcción naval. La Marina del EPL continúa aumentando constantemente su inventario de submarinos modernos y unidades de superficie. Se sabe que China está construyendo simultáneamente siete clases de barcos pero es posible que esté construyendo clases adicionales.⁸ Las tendencias en el gasto en defensa, investigación y desarrollo, y construcción naval de China sugieren que la Marina del EPL continuará modernizándose. Para 2020, China tendrá unos 60 submarinos capaces de emplear misiles balísticos intercontinentales, torpedos, minas o misiles crucero de lanzamiento desde submarinos. La fuerza de combate de superficie de China también se ha modernizado y ampliado con unas 75 unidades de superficie capaces de realizar múltiples misiones o que han sido modernizadas significativamente desde 1992.⁹ Las flotas de combate se apoyan en una fuerza de logística de combate que puede realizar reabastecimiento y reparaciones limitadas en marcha. Todas estas naves estarán equipadas para aprovechar un sistema interconectado redundante de comando, control, comunicaciones, computadoras, e inteligencia, vigilancia y reconocimiento (C4ISR) desplegado por el EPL.

Submarinos de ataque. China dispone de una fuerza formidable de 63 submarinos de ataque diésel-eléctricos y nucleares.¹⁰ Estos submarinos están equipados con torpedos nucleares y convencionales, minas, y misiles crucero antibuque.¹¹ En 2012, China inició la construcción de cuatro “variantes mejoradas” de su submarino nuclear de ataque clase *Shang*. También continúa la producción del submarino diésel-eléctrico clase *Yuan*—algunos de los cuales incluirán un sistema de propulsión independiente del aire que hace posible operaciones de duración prolongada— y el SSBN clase *Jin*. Además, China está desarrollando dos nuevas clases de submarinos nucleares y podría diseñar y construir conjuntamente cuatro submarinos de ataque diésel-eléctricos avanzados con Rusia.¹² El creciente número de submarinos de China mejorará significativamente su capacidad para atacar barcos de superficie enemigos a través del Pacífico Occidental y proteger futuras patrullas disuasivas nucleares y grupos de combate con portaaviones.¹³

Fuerza Aérea

Aviones de caza. China también está desarrollando dos cazas de próxima generación, el J-20 y el J-31, que podrían ser de baja observabilidad y disponer de radar de matriz activo de escaneo electrónico.¹⁴ La Fuerza Aérea del EPL realizó los primeros vuelos de prueba del J-20 y J-31 en enero de 2011 y octubre de 2012 respectivamente.¹⁵ Estas aeronaves reforzarán la capacidad de China para proyectar poderío y obtener y mantener superioridad aérea en un conflicto regional.

Aviones de transporte de carga. En enero de 2013, China realizó el primer vuelo de prueba de su avión de transporte de carga desarrollado en el país, el Yun-20 (Y-20). Anteriormente China no tenía la capacidad de construir aviones de transporte pesado, por lo que se apoyaba en un pequeño número de aviones Ilyushin-76 (IL-76) rusos para puentes aéreos estratégicos desde

la década de 1990. Las especificaciones de los aviones, proporcionadas por medios chinos, indican que el Y-20 puede llevar aproximadamente el doble de carga útil que el IL-76 y unas tres veces la carga útil del C-130 de EE.UU.¹⁶ El Y-20 mejorará la capacidad del EPL para responder a eventos de crisis de seguridad interna y contingencias fronterizas, apoyar operaciones militares internacionales de pacificación y asistencia humanitaria, y proyectar poderío en un conflicto regional.¹⁷ Estas aeronaves más grandes y la flota ampliada aumentarán la capacidad del EPL para emplear el Décimo Quinto Ejército Aerotransportado, parte de la Fuerza Aérea del EPL.

Aviones bombarderos capaces de MCAT. En junio de 2013, la Fuerza Aérea del EPL comenzó a recibir nuevos aviones bombarderos Hongzha-6K (H-6K). El H-6K, una variante mejorada del H-6 (adaptado originalmente de un diseño soviético de fines de la década de 1950), ha ampliado su alcance desde unas 2.400 millas hasta 3.100 millas, y puede portar el CJ-10, el nuevo MCAT de larga distancia de China. El CJ-10 tiene un alcance de 900 a 1.200 millas.¹⁸ El sistema de armas bombardero y MCAT ofrece a la Fuerza Aérea del EPL la capacidad de realizar ataques convencionales contra blancos regionales a través del Pacífico Occidental, incluyendo las bases estadounidenses en Guam.¹⁹ Aunque se podría modificar el fuselaje del H-6K para portar un MCAT con carga nuclear de lanzamiento desde el aire, y los MCAT de china probablemente tienen la capacidad de portar una ojiva nuclear, no hay evidencia que confirme que China esté desplegando cabezas nucleares en ninguno de sus MCAT de lanzamiento desde el aire.²⁰ El H-6K podría también portar misiles crucero supersónicos antibuque.²¹

Espacio y contrarresto espacial

En mayo de 2013, China lanzó un cohete a una órbita terrestre casi geosincrónica, marcando el lanzamiento suborbital más elevado desde el Gravity Probe A de los Estados Unidos en 1976, y el lanzamiento suborbital más elevado de China que se conoce hasta la fecha. Aunque Beijing afirma que el lanzamiento fue parte de un experimento científico a gran altitud, los datos disponibles sugieren que estaba probando el vehículo de lanzamiento de una nueva capacidad antisatélite (ASAT) de gran altitud.²² Si es cierto, tal prueba indicaría su intención de desarrollar una capacidad ASAT para atacar satélites en un rango de altitud que incluye el sistema de posicionamiento global (GPS) estadounidense y muchos de sus satélites militares y de inteligencia. En un potencial conflicto, esta capacidad podría permitir que China amenace la capacidad militar estadounidense de detectar misiles extranjeros y proporcionar comunicaciones, navegación y guía de misiles de precisión seguras.

Es más, en septiembre de 2013, China lanzó un satélite al espacio desde el Centro de Lanzamiento de Satélites de Jiuquan, en el oeste de China. Nuestro informe anual cita comentarios de Gregory Kulacki, de la Unión de Científicos Interesados, quien cree que este lanzamiento podría representar una capacidad de lanzar nuevos satélites en el caso de que China tuviera pérdidas en el espacio en combate espacial.²³

China ha mejorado también su capacidad de defensa contra misiles balísticos desplegando el sistema de misiles superficie-aire (SAM) SA-20B fabricado en Rusia. En algunos casos, el sistema SAM CSA-9 producido en China también debe ser capaz de interceptar misiles balísticos.²⁴

El 27 de diciembre de 2012, China anunció que su sistema regional de navegación por satélite Beidou estaba plenamente operativo y disponible para uso comercial. Con 16 satélites y una red de estaciones terrestres, Beidou ofrece a los suscriptores en Asia servicios de navegación de precisión y coordinación de tiempo de 24 horas.²⁵ China planea ampliar el sistema Beidou a un sistema global de navegación por satélite hacia 2020.²⁶ Beidou es una parte crítica de la meta declarada de China de prepararse para luchar guerras en “condiciones basadas en información”, que incluye un fuerte énfasis en el desarrollo de las capacidades de C4ISR y guerra electrónica del EPL. El EPL está integrando Beidou en sus sistemas para mejorar su capacidad de comando

y control y ataques de precisión de larga distancia, y reducir la dependencia del EPL en los servicios de navegación de precisión y coordinación de tiempo extranjeros, como el GPS.²⁷

Misiles balísticos intercontinentales estratégicos

China está aumentando su capacidad de disuasión nuclear mediante la modernización de su fuerza nuclear. Está adoptando medidas como desarrollar un nuevo misil balístico intercontinental (ICBM) transportado por carretera. Este misil podría ser equipado con un vehículo de reingreso múltiple programable independientemente (MIRV), permitiéndole portar hasta 10 ojivas nucleares.²⁸ Además de los MIRV, China podría también equipar sus misiles balísticos con ayudas de penetración y podría estar desarrollando la capacidad de transportar los ICBM por tren.²⁹ Además, de acuerdo con el informe del DoD al Congreso en 2011 sobre las fuerzas armadas de China, el EPL “ha desarrollado y utilizado [instalaciones subterráneas] desde que desplegó sus sistemas de misiles con combustible líquido más antiguos y continúa utilizándolos para proteger y ocultar sus misiles móviles con combustible sólido más nuevos y modernos”.³⁰

Gastos de defensa

Para apoyar su modernización militar, China continuó aumentando sus gastos de defensa en 2013. En marzo, China anunció que su presupuesto oficial de defensa para 2012 se incrementó en 10,7 por ciento en términos nominales a 117,39 miles de millones de dólares, indicando el apoyo del nuevo liderazgo a los actuales esfuerzos de modernización del EPL. Esta cifra representa un 5,3 por ciento del total del gasto de gobierno y aproximadamente 1,3 por ciento del producto interno bruto (PIB) estimado.³¹ El presupuesto anual oficial de defensa de China se ha incrementado por 22 años consecutivos y se ha más que duplicado desde 2006. La mayoría de analistas occidentales concuerdan en que posiblemente Beijing retendrá la capacidad —incluso con menores tasas de crecimiento de su PIB y de los ingresos del gobierno— para financiar la modernización en marcha de sus fuerzas militares.³²

Es difícil estimar el actual gasto de defensa de China debido a la incertidumbre para determinar cómo afecta la paridad del poder de compra de China al costo de las compras militares en el extranjero y de las mercancías y servicios internos de China, así como la omisión de importantes gastos relacionados con la defensa por parte de Beijing. Algunas compras de armas avanzadas, programas de investigación y desarrollo, gastos en seguridad nacional, y apoyo de los gobiernos locales al EPL no se incluyen en las cifras oficiales del gasto de defensa de China. El Instituto de Estudios Estratégicos Internacionales estima que el gasto de defensa real de China es entre 40 y 50 por ciento mayor que la cifra oficial.³³ El Departamento de Defensa de los Estados Unidos estimó que el gasto de defensa real de China en 2012 se situaba entre 135 y 215 mil millones de dólares, o aproximadamente 20 a 90 por ciento mayor que el presupuesto de defensa anunciado.³⁴

Relaciones de seguridad entre EE.UU. y China

Las relaciones entre militares estadounidenses y chinos se profundizaron y ampliaron en 2013 después de varios años de contratiempos. Entre 2012 y 2013, el número de contactos entre militares de EE.UU. y China ha subido a más del doble, desde aproximadamente 20 hasta 40.³⁵ En particular, el contacto entre la Marina estadounidense y la Marina del EPL ha aumentado de manera significativa durante este período. Los contactos claves entre militares en 2013 incluyeron la primera visita a puerto de un barco de la Marina estadounidense a China desde 2009, la primera visita a puerto de un barco chino a Estados Unidos desde 2006, y el segundo ejercicio

contra la piratería entre Estados Unidos y China de todos los tiempos. Adicionalmente, en marzo de 2013 China aceptó la invitación, extendida primero por el ex Secretario de Defensa Leon Panetta en septiembre de 2012, para participar en el Ejercicio Multilateral de la Cuenca del Pacífico liderada por Estados Unidos cerca de Hawaii en 2014.³⁶

El DoD sostiene que una fuerte relación entre militares desarrolla familiaridad en el nivel operativo. El DoD afirma que esto reduce el riesgo de conflicto debido a accidentes y cálculos erróneos, crea líneas de comunicación en el nivel estratégico que podrían ser importantes durante una crisis, contribuye a mejorar las relaciones bilaterales generales, y crea oportunidades para obtener mayores contribuciones de China para la seguridad internacional. El comandante del Comando del Pacífico de EE.UU., Almirante Samuel Locklear, dijo en julio de 2013, “El avance que estamos realizando entre nuestras dos fuerzas armadas es bastante admirable. . . porque podemos sostener un buen diálogo en áreas donde estamos de acuerdo, y hay muchos lugares donde estamos de acuerdo como dos naciones, y podemos también abordar directamente temas de una manera real en donde discrepamos”.³⁷

Han habido ocho rondas de diálogo estratégico entre China y Estados Unidos, gestionadas actualmente por el Foro del Pacífico–CSIS. Éste es un diálogo Track 1.5 que incluye la asistencia de algunos representantes del gobierno estadounidense, pero virtualmente todos los participantes chinos son de alguna parte de su gobierno. Las últimas rondas de diálogo han tratado sobre algunos de los temas estratégicos más importantes que enfrentan China y Estados Unidos, incluyendo la estabilidad estratégica nuclear; la relación entre ciberataques, guerra en el espacio y estabilidad nuclear; la defensa contra misiles balísticos; y la alerta estratégica temprana. En el diálogo han participado oficiales de las fuerzas de misiles estratégicos de China. Veo esto como uno de los diálogos más productivos que han tenido lugar con China. El EPL es un participante activo. Idealmente tales discusiones deberían ser conversaciones directas, gobierno a gobierno, pero es alentador que el EPL y el Ministro de Relaciones Exteriores de China participen en estos asuntos.

En otro acontecimiento positivo, a mediados de noviembre, el Ejército Estadounidense y las fuerzas de tierra del EPL realizaron su primer ejercicio conjunto de todos los tiempos. El ejercicio se centraba en la asistencia humanitaria en desastres y se realizó en Hawaii.³⁸

Mi propia experiencia en contactos directos entre militares con China me lleva a aconsejar cautela en lo que hacemos con el EPL y lo que les mostramos. En mi opinión, no se deben abolir las sensatas limitaciones que el Congreso impone a los intercambios militares con China en la Ley de Autorización de Defensa Nacional (NDAA) de 2000. El informe anual de la comisión también refleja este sentimiento. Los contactos entre militares con China requieren supervisión cuidadosa para garantizar que Estados Unidos no aumente la capacidad de China contra nuestras propias fuerzas, Taiwán, o nuestros amigos y aliados en la región Asia-Pacífico.

En 2013 se realizaron contactos más amplios entre militares de China y Estados Unidos en el contexto de los esfuerzos de China para proyectar las relaciones bilaterales como un “nuevo tipo de relación entre países principales”. Este concepto, promovido fuertemente en 2013 por el Presidente de China Xi Jinping y otros oficiales chinos de alto nivel, plantea que Estados Unidos y China deben, como potencias principales, buscar la cooperación en una gama de temas bilaterales y globales tratando de evitar la clase de competencia dañina que a menudo caracteriza a las relaciones entre las potencias dominantes y las emergentes.³⁹ La cooperación es algo bueno, pero los líderes militares estadounidenses no pueden perder de vista el récord del EPL en cuanto a derechos humanos. Esto dicta limitaciones prácticas sobre lo que hacemos con las fuerzas armadas de China. La misión principal de los militares chinos es mantener al Partido Comunista Chino (PCC) en el poder, tal como lo vimos en la forma en que se usó al EPL durante la Masacre de Tiananmen del 4 de junio de 1989 y en Tíbet.

Ciberactividades de China

Mientras China continúa desarrollando su fuerza naval, fuerza aérea, fuerzas de misiles, y capacidades espaciales y anti espaciales, en los artículos militares chinos, el ciberespacio es un componente cada vez más importante del poderío nacional amplio de China y un elemento crítico de su competencia estratégica con Estados Unidos.⁴⁰ Beijing parece reconocer que las ventajas actuales de Estados Unidos en el ciberespacio permiten que Washington recopile inteligencia, ejerza comando y control de fuerzas militares, y apoye operaciones militares. Al mismo tiempo, los líderes de China temen que Estados Unidos pueda usar la Internet abierta y las ciberoperaciones para amenazar la legitimidad del Partido Comunista Chino.

Desde el *Informe Anual al Congreso de 2012* de la comisión, ha surgido fuerte evidencia de que el gobierno chino está ordenando y ejecutando una campaña de ciberespionaje en gran escala contra Estados Unidos. Hasta la fecha, China ha comprometido una variedad de redes estadounidenses, incluyendo las del DoD y de empresas privadas. Estas actividades están diseñadas para lograr varios objetivos amplios de seguridad, políticos y económicos.

No hay indicaciones de que la revelación pública del ciberespionaje chino en detalle técnico durante 2013 haya hecho que China cambie su actitud respecto al uso del ciberespionaje para hacerse de propiedad intelectual e información patentada. El informe de Mandiant, una empresa privada estadounidense de ciberseguridad, sobre las actividades de ciberespionaje de la Unidad 61398 del EPL dio lugar a que la unidad modificara sus “herramientas e infraestructura” informáticas para hacer que las futuras intrusiones sean más difíciles de detectar y atribuir.⁴¹ Hay unas 16 unidades y agencias de reconocimiento técnico (inteligencia de señales) en el EPL, y al menos siete unidades de guerra electrónica y medidas de contrarresto electrónico.⁴² Cada una de las siete regiones militares de China es apoyada por un regimiento de medidas de contrarresto electrónico, y parece que la Segunda Fuerza de Artillería del EPL tiene su propia unidad de apoyo.⁴³ Estas organizaciones se centran en penetraciones de sistemas informáticos, ciberespionaje y guerra electrónica.

Cuando se le confronta con acusaciones públicas de Estados Unidos sobre ciberespionaje, Beijing usualmente trata de refutar la evidencia indicando la anonimidad del ciberespacio y la falta de información forense técnica verificable. También cambia el foco de los medios presentándose como la víctima de las ciberactividades de Washington y pidiendo una mayor cooperación internacional en ciberseguridad.⁴⁴ En una conferencia de prensa un día después que Mandiant publicó su informe en febrero de 2013, un vocero del Ministerio de Relaciones Exteriores de China dijo, “La especulaciones y acusaciones sin fundamento sobre ataques de piratas informáticos, con varios fines, son poco profesionales e irresponsables y no ayudan a resolver el problema”. También enfatizó que los ciberataques son un serio problema para China.⁴⁵

Sin embargo, varios informes públicos del gobierno estadounidense, reconocimientos de empresas privadas que han sido blanco de ciberespionaje, investigaciones por empresas de ciberseguridad, y los informes de la prensa estadounidense contradicen las perennes negaciones de Beijing. Aunque la atribución es difícil y demanda grandes habilidades, el análisis de tendencia está permitiendo que los profesionales de ciberseguridad desarrollen un entendimiento más amplio de los ciberactores, herramientas, tácticas, técnicas y procedimientos de China.

Amenazas a la seguridad nacional de Estados Unidos

El ciberespionaje chino contra el gobierno estadounidense y la base industrial de defensa presenta una amenaza importante para las operaciones de las fuerzas militares estadounidenses, la seguridad y el bienestar del personal militar, la efectividad del equipo, y el estado de disponibilidad. Aparentemente, China utiliza estas intrusiones para tapar brechas en sus propios programas de investigación, asignar blancos futuros, recopilar inteligencia sobre estrategias y planes

estadounidenses, habilitar futuras operaciones militares, acortar los cronogramas de investigación y desarrollo (I+D) para las tecnologías militares, e identificar vulnerabilidades en los sistemas estadounidenses y desarrollar medidas de contrarresto.⁴⁶

La doctrina militar en China también exige ataques sobre la estructura crítica del territorio nacional del oponente en caso de conflicto. En julio de 2013, un investigador de amenazas en Trend Micro, una empresa privada de ciberseguridad japonesa, anunció que había detectado una intrusión informática china, desde diciembre de 2012, de una trampa “honeypot”.⁴⁷ Había creado la trampa honeypot para simular el sistema de control industrial de una planta de agua en Estados Unidos. El investigador atribuyó la intrusión a la Unidad 61398, según los análisis forenses.⁴⁸ Si resulta cierto, esto sugiere que la Unidad 61398 está recopilando inteligencia de infraestructura crítica además de otros objetivos. Tales actividades son consistentes con la doctrina del EPL, que explica que una función de las operaciones de redes de computadora en tiempo de guerra es “perturbar y dañar las redes de las instalaciones de infraestructura del [adversario], como sistemas de generación de energía eléctrica, sistemas de telecomunicaciones, y sistemas educativos”.⁴⁹

En años recientes se han identificado varios casos de ciberespionaje chino orientados a programas de seguridad nacional de Estados Unidos. En mayo de 2013, el *Washington Post* describió un informe clasificado de la Junta de Ciencia de Defensa, que lista más de 24 diseños de sistemas de armamentos estadounidenses que según junta habían sido accedidos por intrusos informáticos. Según el *Washington Post*, “Oficiales superiores militares e industriales con conocimiento de las intrusiones dijeron que la gran mayoría eran parte de una campaña amplia de espionaje chino contra los contratistas de defensa y las agencias de gobierno de los Estados Unidos”. La lista incluye el sistema de misiles Patriot, el sistema de defensa con misiles balísticos Aegis, el avión caza F/A-18, el avión de combate multifunción V-22 Osprey, y el Buque de combate para litoral.⁵⁰

La información obtenida de las intrusiones en las redes de contratistas militares estadounidenses probablemente mejora el conocimiento de China sobre los sistemas de armamentos estadounidenses, habilita el desarrollo de medidas de contrarresto, y acorta los tiempos de investigación y desarrollo para tecnologías militares de China.⁵¹ Además, las mismas intrusiones que los ciberactores chinos emplean para espionaje también se podrían emplear para preparar ciberoperaciones ofensivas. Los ciberactores chinos podrían insertar funciones latentes en el código del software o los componentes del equipo estadounidense que podrían emplearse en un conflicto potencial entre Estados Unidos y China.

En años recientes ha habido inquietudes sobre los riesgos de seguridad en la cadena de suministro del DoD. En una reunión en mayo de 2013, los comisionados y oficiales del DoD discutieron la interpretación de la ley estadounidense en relación a las fuentes de adquisiciones. Los funcionarios del DoD indicaron que un estándar de evaluación de adquisiciones más estricto que tenga en cuenta las inquietudes de adquisiciones solo se aplicaría a los artículos de la Lista de Municiones de Estados Unidos. Los artículos que no estén en la lista se juzgan por un estándar diferente, que algunos oficiales creen que podría excluir las inquietudes sobre el origen de los productos. Por ejemplo, los artículos adquiridos por las instalaciones de mantenimiento de C4ISR no están sujetos a un control más estricto. Los comisionados plantearon su preocupación de que esta interpretación de la ley estaba limitando la capacidad del departamento para abordar riesgos potenciales provenientes de ciertas fuentes de adquisición. Los comisionados exhortaron al DoD a ampliar el alcance del estándar más estricto a artículos que no están en la lista de municiones.

Actualmente el DoD está yendo en esa dirección. La Sección 806 de la NDAA del Año Fiscal 2011 (Ley Pública 111-383), tiene por objeto abordar el problema, pero aún no se ha implementado plenamente. La Sección 806 autoriza al Secretario de Defensa y a los Secretarios del Ejército, la Marina y la Fuerza Aérea a rechazar fuentes de adquisiciones de tecnología de informa-

ción alegando protección de la seguridad de la cadena de suministro si el DoD recomienda hacerlo.⁵² El Departamento está en el proceso de implementar la Sección 806, habiendo realizado ejercicios de simulación y redactado la Regla Suplementaria del Reglamento de Adquisiciones Federales de Defensa que implementa la Sección 806. En mayo, la regla estaba siendo sometida a coordinación entre agencias.⁵³ Estos cambios en el sistema de adquisiciones del DoD podrían darle a los oficiales la flexibilidad necesaria para proteger todos los sistemas del DoD. Sin embargo, el avance ha sido lento y el problema que resaltaron los comisionados persistirá hasta que se implemente la nueva política, planteando potencialmente una amenaza a la seguridad nacional. Por lo tanto, en el *Informe Anual al Congreso de 2013*, la comisión recomienda al Congreso que exhorte a la administración para que acelere el avance de la implementación de la Sección 806 de la NDAA del Año Fiscal 2011.

Los desarrollos en la computación en nube en China pueden presentar riesgos de ciberseguridad para los usuarios y proveedores estadounidenses de servicios de computación y pueden también tener consecuencias para la seguridad nacional de Estados Unidos. En base a los hallazgos de un informe de Defense Group, Inc. para la comisión, la relación entre el Ministerio de Seguridad del Estado (MSS) y la Zona Especial de Computación en Nube de Chongqing representa una amenaza de espionaje potencial para las empresas extranjeras que usen servicios de computación en nube proporcionados desde la zona o que basen sus operaciones allí.⁵⁴ Además, el plan de enlazar los centros de datos de 21Vianet en China y los centros de datos de Microsoft en otros países sugiere que el gobierno chino podrá algún día ganar acceso a los centros de datos fuera de China a través de centros de datos chinos.⁵⁵ Teniendo en cuenta los temas sobre espionaje, en el *Informe Anual de 2013*, la comisión recomienda que el Congreso ordene a la administración que prepare un inventario del uso existente de plataformas de computación y servicios en nube del gobierno federal y determine dónde se encuentran localizados geográficamente los servicios de almacenamiento de datos y computación. Tal inventario debería prepararse anualmente y reportarse a los comités de jurisdicción adecuados.

La computación en nube también puede mejorar la capacidad de C4ISR del EPL. DGI indica que la computación en nube “podría habilitar el desarrollo y despliegue más efectivo y flexible de los equipos militares, mientras que al mismo tiempo mejora la capacidad de supervivencia de los sistemas de información del EPL al dotarlos de mayor redundancia (permitiendo que las capacidades de un sistema sobrevivan la inhabilitación o destrucción de cualquier nodo individual)”.⁵⁶

Amenaza para la industria estadounidense

El ciberespionaje de China contra las empresas comerciales estadounidenses presenta una amenaza importante para los intereses y la competitividad de las empresas estadounidenses en industrias importantes. Este ciberespionaje complementa al espionaje humano tradicional. Mediante estos esfuerzos, el EPL y las industrias de defensa de China pueden dar saltos en tecnologías y sistemas y llenar las brechas en sus propias capacidades de investigación y desarrollo, ahorrando tiempo y dinero. El General Keith Alexander, Comandante del Cibercomando Estadounidense, estimó que el costo para las empresas estadounidenses del hurto de propiedad intelectual es de unos 250 mil millones de dólares al año, aunque no todas las pérdidas se pueden atribuir a la actividad china.⁵⁷ Las entidades chinas empeñadas en el ciberespionaje y otras formas de espionaje económico probablemente consideran que robar propiedad intelectual e información patentada es más económico que invertir en los lentos programas de investigación y desarrollo.⁵⁸ Estos robos apoyan a los planes nacionales de desarrollo de ciencia y tecnología que el gobierno de la RPC administra y dirige centralmente.

El gobierno chino, principalmente a través del EPL y el Ministerio de Seguridad del Estado, apoya estas actividades proporcionando a las empresas de propiedad del estado información y

datos extraídos a través de ciberespionaje para mejorar su ventaja competitiva, acortar los tiempos de investigación y desarrollo, y reducir los costos. La fuerte correlación entre empresas estadounidenses expuestas y las industrias designadas por Beijing como industrias “estratégicas” indica además un grado de auspicio estatal y posiblemente hasta apoyo, dirección y ejecución del espionaje económico chino.⁵⁹ Tal apoyo del gobierno permite que las empresas chinas superen en la competencia a las empresas estadounidenses, que no tienen la ventaja de usar los datos de inteligencia del gobierno para beneficio económico.⁶⁰

Es difícil cuantificar los beneficios que las empresas chinas obtienen del ciberespionaje. No sabemos todo acerca de las clases de información que se busca y obtiene, ni tampoco sabemos siempre qué actor chino robó la información. Algunos robos pueden producirse pero nunca se detectan. En términos de inteligencia empresarial, algunos robos blancos del robo informático incluyen información relacionada a negociaciones, inversiones, y estrategias corporativas incluyendo correos electrónicos de ejecutivos, planes empresariales de largo plazo, y contratos. Además del robo informático, las empresas chinas casi con certeza adquieren información mediante actividades de espionaje tradicional, lo que limita nuestra capacidad de identificar el impacto del ciberespionaje en particular. No obstante, es claro que China no es solo el líder global en el uso de métodos informáticos para robo de propiedad intelectual, también representa la mayoría de los casos de robo de propiedad intelectual a nivel global.⁶¹ En varias ocasiones en años recientes, los actores chinos han utilizado las ciberactividades para obtener información sensible o patentada de empresas estadounidenses:

- En el informe de Mandiant mencionado anteriormente, hay evidencia que desde 2006 la Unidad 61398 del EPL ha penetrado las redes de por lo menos 141 organizaciones, incluyendo empresas, organizaciones internacionales, y gobiernos de otros países. Estas organizaciones se encuentran localizadas o tienen oficinas matrices en 15 países y representan 20 sectores principales, desde tecnología de la información hasta servicios financieros. Entre las organizaciones afectadas, el 81 por ciento estaban localizadas en Estados Unidos o tenían oficinas matrices en Estados Unidos. Según Mandiant, la Unidad 61398 obtuvo acceso a una amplia variedad de información intelectual e información confidencial mediante estas intrusiones.⁶² La Unidad 61398 es la Segunda Oficina del departamento de reconocimiento técnico del EPL, y tiene base en Shanghai.⁶³
- En otro ejemplo destacado de una empresa china que supuestamente buscaba acceder a propiedad intelectual de una empresa estadounidense mediante ciberespionaje, el Departamento de Justicia (DoJ) en junio de 2013, presentó cargos contra Sinovel Wind Group, una firma del sector energía de China, alegando que Sinovel robó propiedad intelectual de la empresa American Superconductor (AMSC) basada en Massachusetts.⁶⁴ Una vez que Sinovel pudo reproducir tecnología de AMSC después de robar código fuente confidencial, la firma china rompió la asociación, canceló las órdenes existentes, y devastó los ingresos de AMSC. Esta empresa ha enjuiciado en China a Sinovel buscando compensación, un esfuerzo que todavía continúa y le ha ocasionado gastos legales de más de 6 millones de dólares.⁶⁵ Mientras estos juicios se mueven lentamente por el sistema legal chino, y añade más costos legales a ASMC, Sinovel aprovecha las ganancias de la tecnología robada.⁶⁶

Disuasión del robo informático chino

Es claro que revelar el nombre de los perpetradores en China en un intento de avergonzar al gobierno chino no es suficiente para desanimar a las entidades chinas del ciberespionaje contra las empresas estadounidenses. La mitigación del problema requerirá un enfoque bien coordinado entre el gobierno estadounidense y la industria. El Congreso, la administración Obama y

los expertos externos discuten muchas acciones potenciales. Estas acciones incluyen vincular el ciberespionaje económico a las restricciones comerciales, prohibiendo que las empresas chinas que utilizan propiedad intelectual de Estados Unidos tengan acceso a los bancos estadounidenses y prohibiendo el viaje a Estados Unidos de organizaciones chinas que participan en el ciberespionaje. La Comisión de Revisión Económica y de Seguridad de EE.UU. - China recomienda que el Congreso tome las siguientes medidas:

- Adopte una legislación que aclare las acciones que pueden tomar las empresas para realizar el seguimiento de propiedad intelectual robada mediante ciberintrusiones.
- Enmiende la Ley de Espionaje Económico (18 U.S.C. § 1831-1839) para permitir un derecho privado de acción cuando ocurra robo de secretos comerciales.
- Apoye los esfuerzos de la administración para lograr un alto estándar de protección de los derechos de propiedad intelectual en la Asociación Transpacífico y la Asociación Transatlántica de Comercio e Inversiones.
- Aliente a la administración a asociarse con otros países para establecer una lista internacional de individuos, grupos y organizaciones que participan en el ciberespionaje comercial. La administración y los gobiernos socios deben desarrollar un proceso para la validación, la adjudicación y el acceso compartido de la lista.
- Inste a la administración para que continúe mejorando su intercambio de información sobre amenazas informáticas con el sector privado, particularmente con las empresas pequeñas y medianas.

Es mi opinión personal que el Presidente ya tiene la autoridad para imponer sanciones sobre personas, industrias de gobierno y empresas de China a través de la Ley de Facultades para Emergencia Económica Internacional.⁶⁷ Si la magnitud del daño a la economía estadounidense es tan grande como el que cita el General Alexander, el Presidente debería ejercitar esa autoridad.

Mantener el “reajuste del equilibrio” militar estadounidense en Asia

En enero de 2012, la *Guía Estratégica de Defensa* del DoD declaró que los militares estadounidenses “reajustarán necesariamente el equilibrio hacia Asia” enfatizando las alianzas existentes, ampliando las redes de cooperación con los socios “emergentes”, e invirtiendo en capacidades militares para garantizar el acceso y la libertad de maniobra en la región.⁶⁸ El Jefe de Operaciones Navales Estadounidenses, Almirante Jonathan Greenert, explicó la función de la Marina de los Estados Unidos en el reajuste del equilibrio: “Siguiendo las órdenes de la *Guía Estratégica de Defensa* de 2012 . . . la Marina de los [Estados Unidos] ha formulado e implementado un plan para reajustar el equilibrio de nuestras fuerzas, sus puertos de base, y nuestro capital intelectual y asociaciones hacia la región Asia-Pacífico”.⁶⁹ Concretamente, la Marina de los Estados Unidos busca aumentar su presencia en la región Asia Pacífico de unos 50 barcos en 2013 hasta 60 barcos en 2020 y “reajustar el equilibrio de los puertos de base a 60 por ciento” en la región para 2020.⁷⁰

Sin embargo, el informe anual de la comisión señala que el Secretario de Defensa Chuck Hagel, en julio de 2013, dijo que Washington tendría que escoger entre una fuerza militar moderna y más pequeña y una más antigua y más grande si continúa la provisión de fondos con recortes automáticos.⁷¹ El Almirante Greenert ha advertido que las restricciones en el entorno del presupuesto actual podrían retrasar o impedir que la marina estadounidense logre sus objetivos de reajuste del equilibrio.⁷² Hay una creciente preocupación en Estados Unidos y entre sus aliados y socios de que el DoD no pueda cumplir su compromiso de reajustar el equilibrio debido a los presupuestos de defensa decrecientes y las crisis emergentes en otros lugares del mundo. Esto podría dar lugar a que algunos países de la región se adapten cada vez más a China

o busquen capacidades militares que podrían ser usadas ofensivamente o de manera preventiva. Cualquiera de los dos escenarios podría socavar los intereses estadounidenses en la región.

Los exhorto a tener en cuenta que hacia 2020, China podría tener una fuerza naval y fuerza aérea en Asia que supere en número y casi iguale la capacidad técnica de nuestras propias fuerzas. Si nuestra fuerza militar se reduce a causa de nuestros problemas de presupuesto, podremos tener el 60 por ciento de nuestras fuerzas en la región Asia-Pacífico, pero 60 por ciento de 200 barcos es mucho menos que 60 por ciento de una fuerza naval de 300 barcos. Puede que eso no sea suficiente para disuadir a China o tranquilizar a nuestros amigos y aliados en la región. □

Notas

1. El informe completo se puede ver en http://www.uscc.gov/Annual_Reports/2013-annual-report-congress.
2. Acciones “Anti-acceso” (A2) son aquellas que tienen por objeto retardar el despliegue de las fuerzas del adversario en el teatro de operaciones o hacer que las fuerzas operen desde distancias más alejadas del conflicto de las que éstas podrían preferir. Las acciones A2 afectan el movimiento hacia el teatro. Acciones de “Negación de área” (NA) son aquellas que tienen por objeto impedir las operaciones del adversario dentro de áreas donde las fuerzas amigas no pueden o no intentarán impedir el acceso. Las acciones NA afectan el movimiento dentro del teatro. *Air Sea Battle: Service Collaboration to Address Anti-Access & Area Denial Challenges (Batalla Aire Mar: Colaboración del servicio para enfrentar los desafíos Anti-acceso y Negación de área)* (Arlington, VA: Oficina de Combate Aire-Mar de EE.UU., mayo de 2013), 2–4.
3. “Chinese Aircraft Carrier Returns to Home Port (Portaaviones chino vuelve a puerto de origen)”, *Renmin Ribao (People’s Daily)*, 22 de septiembre de 2013, <http://english.peopledaily.com.cn/90786/8407244.html>; “China’s Carrier-Borne Jet Pilots Receive Certification (Pilotos de aviones a reacción de portaaviones de China reciben certificación)”, Xinhua, 4 de julio de 2013, <http://english.peopledaily.com.cn/90786/8310416.html>; “China’s First Aircraft Carrier Leaves Homeport for Sea Trials (Primer portaaviones de China deja puerto de origen para pruebas en el mar)”, Xinhua, 11 de junio de 2013, http://news.xinhuanet.com/english/china/2013-06/11/c_132447284.htm; “China’s Aircraft Carrier Anchors in Military Port (Portaaviones de China ancla en puerto militar)”, Xinhua, 7 de febrero de 2013, http://www.china.org.cn/china/NPC_CPPCC_2013/2013-02/27/content_28071340.htm; y “China Now Capable to Deploy Jets on Aircraft Carrier: Navy (China ahora puede desplegar aviones a reacción en portaaviones: Marina)”, Xinhua, 25 de noviembre de 2013, OSC ID: CPP20121125968098, <http://www.opensource.gov>.
4. *Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China 2013 (Informe Anual al Congreso: Acontecimientos militares y de seguridad que involucran a la República Popular China 2013)* (Washington: DoD, 2013), 31.
5. *The People’s Liberation Army Navy: A Modern Navy with Chinese Characteristics (La Marina del Ejército de Liberación Popular: Una armada moderna con características chinas)* (Suitland, MD: Oficina de Inteligencia Naval [ONI], 2009), 23.
6. *PLA Navy Orders of Battle 2000–2020 (Órdenes de Combate de la Marina del EPL 2000-2020)*, respuesta escrita a la solicitud de información proporcionada a la Comisión de Revisión Económica y de Seguridad de EE.UU.-China (Suitland: ONI, 24 de junio de 2013); y *Annual Report to Congress (Informa Anual al Congreso)*, 10, 31.
7. *Informe Anual al Congreso*, 6–7; y J. Michael Cole, “China’s Growing Long-Range Strike Capability (Crece la capacidad de ataque de larga distancia de China)”, *Diplomat*, 13 de agosto de 2012, <http://thediplomat.com/flashpoints-blog/2012/08/13/chinas-growing-long-range-strike-capability/>.
8. Andrew Erickson y Gabe Collins, “China Carrier Demo Module Highlights Surging Navy (Módulo de demostración de portaaviones de China resalta una marina emergente)”, *National Interest*, 6 de agosto de 2013, <http://nationalinterest.org/commentary/china-carrier-demo-module-highlights-surging-navy-8842>; *PLA Navy Orders of Battle 2000–2020 (Órdenes de combate de la Marina del EPL 2000-2020)*; e *Informe anual al Congreso*, 5–7.
9. *PLA Navy Orders of Battle 2000–2020 (Órdenes de Combate de la Marina del EPL 2000-2020)*.
10. *Ibid.*
11. Sobre Sobre armas nucleares, incluyendo torpedos, minas, misiles crucero antibuque, y ADMs/minas, véase Robert S. Norris, Andrew S. Burrows, y Richard W. Fieldhouse, *British, French, and Chinese Nuclear Weapons (Armas nucleares británicas, francesas y chinas)*, *Nuclear Weapons Databook, vol. 5* (Boulder, CO: Westview Press, 1994), 359; Gregory B. Owens, “Chinese Tactical Nuclear Weapons (Armas nucleares tácticas chinas)” (tesis de maestría, Naval Postgraduate School, junio de 1996), 4; “Global Nuclear Stockpiles, 1945–1997 (Reservas nucleares globales 1945-1997)”, *Bulletin of the Atomic Scientists*, noviembre/diciembre de 1997, 67; “Estimated Nuclear Stockpiles 1945–1993 (Reservas nucleares estimadas 1945-1993)”, *Bulletin of the Atomic Scientists*, diciembre de 1993, 57; y Robert S. Norris, “Nuclear Arsenals of the United States, Russia, Great Britain, France and China: A Status Report (Arsenales nucleares de Estados Unidos, Rusia, Gran Bretaña, Francia y China: Un informe de situación)”, presentación en el Quinto Seminario ISODARCO en Beijing Sobre Control de Armas, Chengdu, China, noviembre de 1996. Sobre torpedos, véase “Archive of Nuclear Data (Archivo de información nuclear)”, <http://www.nrdc.org/nuclear/nudb/datab17.asp>; y Ronald O’Rourke, *China Naval Modernization (Modernización naval de China)* (Washington: Servicio de Investigación del Congreso [CRS], 5 de septiembre de

2013), <http://www.fas.org/sgp/crs/row/RL33153.pdf>. Según sinodefense.com, en diciembre de 2005 China compró torpedos Tipo 53-65 de Rusia y 40 torpedos Shkval en 1998.

12. "China 'Buys Fighter Jets and Submarines from Russia' (China 'Compra aviones de caza y submarinos de Rusia'", *BBC News*, 25 de marzo de 2013, <http://www.bbc.co.uk/news/world-asia-21930280>; y Robert Foster, "Russia to Sell, Co-Produce Lada-class Submarines to China (Rusia venderá o coproducirá submarinos clase Lada con China)", *Jane's Defence Weekly*, 20 de diciembre de 2012, <http://www.janes.com/article/19682/russia-to-sell-co-produce-lada-class-submarines-to-china>.

13. *PLA Navy Orders of Battle 2000–2020 (Órdenes de Combate de la Marina del EPL 2000-2020)*; y *el Informe Anual al Congreso*, 5–7.

14. Roger Cliff, "Chinese Military Aviation Capabilities, Doctrine, and Missions (Capacidad, doctrina y misiones de la aviación militar china)", en *Chinese Aerospace Power: Evolving Maritime Roles (Poderío aeroespacial chino: Funciones marítimas cambiantes)*, editores Andrew S. Erickson y Lyle J. Goldstein (Annapolis, MD: Naval Institute Press, 2011), 252; y Richard Fisher, "Deterring China's Fighter Buildup (Disuadir el aumento de aviones de caza de China)", *Defense News*, 19 de noviembre de 2012, <http://www.defensenews.com/article/20121119/DEFBEAT05/311190005/>.

15. *Informe Anual al Congreso*, 8; y Fisher, "Deterring China's Fighter Buildup (Disuadir el aumento de aviones de caza de China)".

16. "Resumen: PRC Expert Says Yun-20 Transport Makes Strategic Air Force Possible (Resumen: Experto de la RPC dice que el avión de transporte Yun-20 hace posible la Fuerza Aérea Estratégica)", OSC ID: CPP20130128787028, Open Source Center, 27 de enero de 2013, <http://www.opensource.gov>.

17. "Summary: Guangdong Journal Views Strategic Card of 'Yun-20' Jumbo Air Freighter (Resumen: Diario de Guangdong ve carta estratégica en el transporte aéreo Jumbo 'Yun-20')", OSC ID: CPP20130214695013, 31 de enero de 2013; y Andrew Erikson y Gabe Collins, "The Y-20: China Aviation Milestone Means New Power Projection (El Y-20: Hito de la aviación china indica nueva proyección de poderío)", *Wall Street Journal: China Real Time Blog*, 28 de enero de 2013, <http://blogs.wsj.com/chinarealtime/2013/01/28/the-y-20-china-aviation-milestone-means-new-power-projection/>.

18. Zachary Keck, "Can China's New Strategic Bomber Reach Hawaii? (¿Puede el nuevo bombardero estratégico chino llegar a Hawaii?)" *Diplomat*, 13 de agosto de 2013, http://thediplomat.com/flashpoints-blog/2013/08/13/can-chinas-new-strategic-bomber-reach-hawaii/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3Athe-diplomat+%28The+Diplomat+RSS%29; Noam Eshel, "Chinese Air Force Gets More H-6K Strategic Bombers (Fuerza Aérea China recibe más bombarderos estratégicos H-6K)", *Defense Update*, 25 de junio de 2013, http://defense-update.com/20130625_h-6k-bombers-delivered-to-pla-air-force.html; y Chen Boyuan, "H-6K Bombers Delivered to PLA Air Force (Se han entregado bombarderos H-6K a la Fuerza Aérea del EPL)", *China.org*, 22 de junio de 2013, http://www.china.org.cn/china/2013-06/22/content_29197824.htm.

19. *Informe Anual al Congreso*, 33, 42, 81.

20. Ian Easton, *The Assassin under the Radar: China's DH-10 Cruise Missile Program (El asesino bajo el radar: El programa de misiles crucero DH-10 de China)* (Arlington, VA: Project 2049 Institute, octubre de 2009), 1–6, http://project2049.net/documents/assassin_under_radar_china_cruise_missile.pdf.

21. Keck, "Can China's New Strategic Bomber Reach Hawaii? (¿Puede el nuevo bombardero estratégico chino llegar a Hawaii?)"

22. Andrea Shalal-Esa, "RPT-China's Space Activities Raising U.S. Satellite Security Concerns (Informe: Actividades espaciales de China suscita inquietud sobre seguridad de satélites estadounidenses)", Reuters, 14 de enero de 2013, <http://www.reuters.com/article/2013/01/14/china-usa-satellites-idUSL2N0AJ10620130114>; "Beijing to Trigger Arms Race by Testing Anti-Satellite Missiles (Beijing provocará carrera armamentista con prueba de misiles antisatélite)", Central News Agency (Taipei), 13 de enero de 2013, OSC ID: CPP20130115968204; Gregory Kulacki, "Is January Chinese ASAT Testing Month? (¿Es enero el mes de prueba de los ASAT chinos?)" *All Things Nuclear, Insights on Science and Security*, 4 de enero de 2013. <http://allthingsnuclear.org/is-january-chinese-asat-testing-month/>; *China: Informe de actividades del EPL 16–31 de octubre de 2012* (Washington: DoD, 31 de octubre de 2012), OSC ID: CPP20121120440020; "China Dismisses Report on Planned Test Launch of Anti-Satellite Missile (China desestima informe sobre lanzamiento de prueba de misiles antisatélite planeado)", Xinhua, 25 de octubre de 2012, OSC ID: CPP20121025968325; y Bill Gertz, "China to Shoot at High Frontier (China disparará a la frontera elevada)", *Washington Free Beacon*, 16 de octubre de 2012, <http://freebeacon.com/china-to-shoot-at-high-frontier/>.

23. Gregory Kulacki, " 'Kuaizhou' Challenges U.S. Perceptions of Chinese Military Space Strategy (El 'Kuaizhou' reta las percepciones de EE.UU. sobre la estrategia espacial militar china)", *All Things Nuclear, Insights on Science and Security*, 27 de septiembre de 2013, <http://allthingsnuclear.org/kuaizhou-challenges-us-perceptions-of-chinese-military-space-strategy/>.

24. *Informe Anual al Congreso*, 35-36.

25. "'Beidou,' China's Pride (El 'Beidou', orgullo de China)", *Bingqi Zhishi (Ordnance Knowledge)*, 1 de agosto de 2012, OSC ID: CPP20121016680010.

26. "China Targeting Navigation System's Global Coverage by 2020 (China busca cobertura mundial del sistema de navegación para 2020)", Xinhua, 3 de marzo de 2012, http://news.xinhuanet.com/english/sci/2013-03/03/c_132204892.htm.

27. “Navy North Sea Fleet’s New Smart Target Ship Emits Electromagnetic Jamming against Missiles (Nuevo barco de adquisición inteligente de objetivos de la Flota del Mar del Norte de la Marina emite interferencias electromagnéticas contra misiles)”, *PLA Daily*, 4 de agosto de 2013, OSC ID: CHO2013080530196614; Yu Hu, “PLA Jinan MR Extends Military Use of the Beidou Satellite Navigation System (Región Militar Jinan del EPL amplía el uso militar del sistema de navegación por satélite Beidou)”, *Jinan Qianwei Bao (Jinan Front News)*, 17 de enero de 2012, OSC ID: CPP20130222667020; y Sun Chao, Zhang Jun, y Wang Jun, “PLA Chengdu MR Sichuan Div Uses Satellite Navigation to Standardize Time (División Sichuan de la Región Militar Chengdu del EPL utiliza navegación por satélite para normalizar la hora)”, *Chengdu Zhanqi Bao (Chengdu Battle Standard News)*, 3 de noviembre de 2011, OSC ID: CPP20130223667002.
28. Bill Gertz, “China Conducts another Mobile ICBM Test (China realiza otra prueba de ICBM móvil)”, *Washington Free Beacon*, 14 de agosto de 2013, <http://freebeacon.com/china-conducts-another-mobile-icbm-test/>.
29. *Informe Anual al Congreso*, 30; y Bill Gertz, “Riding the Nuclear Rails (En el tren nuclear)”, *Washington Free Beacon*, 25 de enero de 2013, <http://freebeacon.com/riding-the-nuclear-rails/>.
30. *Informe Anual al Congreso*, 36.
31. “Facts Figures: China’s 2013 Draft Budget Report (Cifras reales: Informe de presupuesto preliminar de 2013 de China)”, Xinhua, 5 de marzo de 2013, OSC ID: CPP20130305968101; “China Boosts Defense Spending as Military Modernizes Arsenal (China aumenta el gasto de defensa mientras los militares modernizan su arsenal)”, Bloomberg, 5 de marzo de 2013, <http://www.bloomberg.com/news/2013-03-05/china-boosts-defense-spending-as-military-modernizes-its-arsenal.html>; Luo Zheng, “Investment in Our National Defense Expenditure Mutually Conforms with National Security and Development Interests—Interview with Sun Huangtian, Deputy Director of PLA General Logistics Department, on 2013 National Defense Budget (La inversión en nuestros gastos en defensa nacional se ajusta mutuamente a los intereses de seguridad y desarrollo nacional —Entrevista con Sun Huangtian Subdirector del Departamento de Logística General del EPL, sobre el Presupuesto de Defensa Nacional de 2013)”, *PLA Daily*, 6 de marzo de 2013, OSC ID: CPP20130307088001; “China Boosts Defense Spending as Military Modernizes Arsenal (China aumenta el gasto de defensa mientras los militares modernizan su arsenal)”, Bloomberg, 5 de marzo de 2013, <http://www.bloomberg.com/news/2013-03-05/china-boosts-defense-spending-as-military-modernizes-its-arsenal.html>.
32. Adam Liff y Andrew Erickson, “Demystifying China’s Defence Spending: Less Mysterious in the Aggregate (Desmitificando el gasto de defensa de China: Menos misterioso colectivamente)”, *China Quarterly*, 2013, <http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=8874207>.
33. Instituto de Estudios Estratégicos Internacionales, “China’s Defence Spending: New Questions (Gasto en defensa de China: Nuevas interrogantes)”, *Strategic Comments*, 2 de agosto de 2013, <http://www.iiss.org/en/publications/strategic%20comments/sections/2013-a8b5/china-39-s-defence-spending-new-questions-e625>.
34. *Informe Anual al Congreso*, 45.
35. *Ibid.*, 69-71. Estos contactos incluyen visitas de alto nivel, intercambios recurrentes, intercambios académicos, intercambios funcionales, y ejercicios conjuntos.
36. Shirley Kan, U.S.—*China Military Contacts: Issues for Congress (Contactos entre militares de Estados Unidos y China: Asuntos para el Congreso)* (Washington: CRS, 25 de julio de 2013).
37. Karen Parrish, “U.S.—China Military Ties Growing, Pacom Commander Says (Crecen las relaciones militares entre EE.UU. y China, dice el Comandante del Pacom)”, US Armed Forces Press Service, 11 de julio de 2013, <http://www.defense.gov/news/newsarticle.aspx?id=120440>.
38. Michelle Tan, “Army Hosts China in First Joint Field Exercise (El Ejército comparte con China el primer ejercicio de campo conjunto)”, *Army Times*, 12 de noviembre de 2013, <http://www.armytimes.com/article/20131112/NEWS/311120006/Army-hosts-China-first-joint-field-exercise>.
39. Caitlin Campbell y Craig Murray, *China Seeks a “New Type of Major-Country Relationship” with the United States* (China busca un “Nuevo tipo de relación entre países principales” con Estados Unidos) (Washington: Comisión de Revisión Económica y de Seguridad de EE.UU.—China, 25 de junio de 2013), http://origin.www.uscc.gov/sites/default/files/Research/China%20Seeks%20New%20Type%20of%20Major-Country%20Relationship%20with%20United%20States_Staff%20Research%20Backgrounder.pdf; Michael S. Chase, “China’s Search for a ‘New Type of Great Power Relationship’ (Búsqueda de China de un ‘Nuevo tipo de relación entre grandes potencias’”, *Jamestown Foundation China Brief* 12, no. 27 (7 de septiembre de 2012): 14, http://www.jamestown.org/uploads/media/cb_09_04.pdf.
40. Larry M. Wortzel, *The Dragon Extends its Reach: Chinese Military Power Goes Global* (El dragón amplía su alcance: Poderío militar chino adquiere nivel global) (Washington: Potomac Books, 2013) 17, 40–41, 134, 145–48.
41. Dan Mcwhorter, “APT1 Three Months Later—Significantly Impacted, Though Active & Rebuilding (APT1 tres meses después — Afectada de manera importante, aunque activa y en reconstrucción)”, *M-union*, 21 de mayo de 2013, <https://www.mandiant.com/blog/apt1-months-significantly-impacted-active-rebuilding/>; y Richard Bejtlich (oficial jefe de seguridad en Mandiant), entrevista telefónica con personal de la comisión, 21 de agosto de 2013.
42. *Directorio de Personalidades Militares de la RPC* (Washington: Agencia de Inteligencia de Defensa, marzo de 2013).
43. *Ibid.*
44. William C. Hannas, James Mulvenon, y Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization (Espionaje industrial chino: Adquisición de tecnología y modernización militar)*, (London and New York: Routledge, 2013), 226.

45. “2013 Nian 2 Yue 19 Ri Wajiaobu Fayaren Honglei Zhuchi Lixing Jizhehui (El vocero del Ministerio de Relaciones Exteriores Hong Lei Preside en conferencias de prensa regulares, 19 de febrero de 2013),” Ministerio de Relaciones Exteriores, Beijing, http://www.fmprc.gov.cn/mfa_chn/fyrbt_602243/t1014798.shtml.

46. Comisión de Revisión Económica y de Seguridad EE.UU.–China, *Informe Anual al Congreso de 2012* (Washington: Government Printing Office, noviembre de 2012), 166.

47. Una honeypot es parte de una honeynet, que es una red de computadoras falsa o de despiste, diseñada para atraer a un adversario para identificarlo o darle información falsa. Las honeynet pueden proporcionar inteligencia relativa a “herramientas, tácticas y motivos” del adversario. Proyecto Honeynet, “Short Video Explaining Honeypots (Vídeo corto que explica las honeypot)”, <http://old.honeynet.org/misc/files/HoneynetWeb.mov>.

48. Tom Simonite, “Chinese Hacking Team Caught Taking over Decoy Water Plant (Equipo de piratería informática chino pillado apoderándose de planta de agua señuelo)”, *MIT Technology Review*, 2 de agosto de 2013, <http://www.technologyreview.com/news/517786/chinese-hacking-team-caught-taking-over-decoy-water-plant/>.

49. Wortzel, *Dragon Extends its Reach (El dragón amplía su alcance)*, 142.

50. Ellen Nakashima, “Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies (Informe confidencial lista diseños de sistemas de armas de Estados Unidos puestos en peligro por ciberespías chinos)”, *Washington Post*, 27 de mayo de 2013, http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html.

51. *Ibíd.*

52. Ley de Autorización de Defensa Nacional para el Año Fiscal 2011 (L.P. 111-383), Congreso No. 111, segunda sesión, 7 de enero de 2011, <http://www.gpo.gov/fdsys/pkg/PLAW-111publ383/pdf/PLAW-111publ383.pdf>.

53. Asistente especial al oficial de información jefe del DoD, Oficina del Secretario Asistente de Defensa para Asuntos Legislativos, entrevista por correo electrónico con personal de la comisión, 28 de mayo de 2013.

54. Leigh Ann Ragland y otros, *Red Cloud Rising: Cloud Computing in China (Surge la nube roja: Computación en nube en China)* (Vienna, VA: Defense Group Inc. para la Comisión de Revisión Económica y de Seguridad de EE.UU.–China, septiembre de 2013), 32–34, <http://origin.www.uscc.gov/sites/default/files/Research/Red%20Cloud%20Rising%20Computing%20in%20China.pdf>.

55. *Ibíd.*, 39.

56. *Ibíd.*, 38.

57. Josh Rogin, “NSA Chief: Cybercrime Constitutes the ‘Greatest Transfer of Wealth in History’ (Jefe de NSA: El cibercrimen constituye la ‘Mayor transferencia de riqueza en la historia’”, *Foreign Policy*, 9 de julio de 2012, http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history.

58. Mike McConnell, Michael Chertoff, y William Lynn, “China’s Cyber Thievery is a National Policy—And Must Be Challenged (El robo cibernético de China es una política nacional, y debe ser confrontado)”, *Wall Street Journal*, 27 de enero de 2012, <http://online.wsj.com/article/SB10001424052970203718504577178832338032176.html>.

59. Comisión sobre el Robo de Propiedad Intelectual, *The IP Commission Report* (Washington: National Bureau of Asian Research, mayo de 2013), 12, http://ipcommission.org/report/IP_Commission_Report_052213.pdf; y Comisión de Revisión Económica y de Seguridad de EE.UU.–China, *Informe Anual al Congreso de 2012*, 156.

60. A fines de la década de 1980 y comienzos de la de 1990 se realizó un debate en el Congreso sobre si la comunidad de inteligencia (IC) de Estados Unidos debía compartir información y/o activos de inteligencia con las empresas estadounidenses para proporcionarles una ventaja contra los competidores extranjeros. En 1991, el Director de la Agencia Central de Inteligencia Robert Gates, en un discurso a la IC, estableció claramente que la CIA se limitaría a ayudar a las empresas estadounidenses a salvaguardarse de las operaciones de inteligencia extranjeras. Robert Gates, “The Future of American Intelligence (El futuro de la inteligencia estadounidense)”, discurso a la Comunidad de Inteligencia, Washington, DC, 4 de diciembre de 1991.

61. Comisión sobre el Robo de Propiedad Intelectual Estadounidenses, *IP Commission Report*, 3, 18.

62. *APT1: Exposing One of China’s Cyber Espionage Units (APT1: Revelando una de las unidades de ciberespionaje de China)* (Alexandria, VA: Mandiant, febrero de 2013), 2, 3, 4, 9, 21–23, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

63. APT1, 9.

64. “Sinovel Corporation and Three Individuals Charged in Wisconsin with Theft of AMSC Trade Secrets (Sinovel Corporation y tres individuos son acusados en Wisconsin de robar secretos comerciales de AMSC)”, comunicado de prensa del Departamento de Justicia, 27 de junio de 2013, <http://www.justice.gov/opa/pr/2013/June/13-crm-730.html>.

65. Melanie Hart, “Criminal Charges Mark New Phase in Bellwether U.S.–China Intellectual Property Dispute (Acusaciones criminales marcan nueva fase en disputa clave sobre propiedad intelectual entre Estados Unidos y China)”, Center for American Progress, Washington, DC, 27 de junio de 2013, <http://www.americanprogress.org/issues/china/news/2013/06/27/68339/criminal-charges-mark-new-phase-in-bellwether-u-s-china-intellectual-property-dispute/>.

66. *Ibíd.*

67. 50 U.S.C. § 1701, <http://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter35&edition=prelim>.

68. *Sustaining U.S. Global Leadership: Priorities for 21st Century Leadership (Mantenimiento del liderazgo global de Estados Unidos: Prioridades para el liderazgo del siglo 21)* (Washington: DoD, enero de 2012), http://www.defense.gov/news/Defense_Strategic_Guidance.pdf.

69. Jonathan Greenert, "Foreword (Prólogo)", en *U.S. Navy Program Guide 2013 (Guía del Programa de la Marina de Estados Unidos para 2013)* (Washington: DoD, 2013), <http://www.navy.mil/navydata/policy/seapower/npg13/top-npg13.pdf>.

70. *U.S. Navy Program Guide 2013 (Guía del Programa de la Marina de Estados Unidos para 2013)*.

71. "Statement on Strategic Choices and Management Review, Pentagon press briefing remarks by Secretary of Defense Chuck Hagel (Declaración sobre opciones estratégicas y revisión administrativa, comentarios de prensa del Pentágono por el Secretario de Defensa Chuck Hagel)," Washington, DC, 31 de julio de 2013, <http://www.defense.gov/speeches/speech.aspx?speechid=1978>.

72. Comité de la Cámara de Representantes sobre los Servicios Armados, *Audiencia sobre la Planificación de los Recortes Automáticos en el año Fiscal 2014 y Perspectivas de los Servicios Militares sobre las Opciones Estratégicas y Revisión Administrativa*, Congreso N°. 113, primera sesión, 18 de septiembre de 2013.



El Dr. Larry M. Wortzel, PhD, fue nombrado miembro de la Comisión de Revisión Económica y de Seguridad de EE.UU.-China en 2001 y sirvió dos períodos como presidente de la Comisión. Es un coronel retirado del Ejército de los Estados Unidos que pasó gran parte de su carrera militar de 32 años en la región Asia-Pacífico. El Coronel Wortzel fue agregado asistente del Ejército en China desde 1988 hasta 1990 y agregado del Ejército en China entre 1995 y 1997. Es autor de *The Dragon Extends its Reach: Chinese Military Power Goes Global (El dragón amplía su alcance: Poderío militar chino adquiere nivel global)* (Potomac Books, Inc., 2013). Un graduado del Armed Forces Staff College y del U.S. Army War College, Wortzel obtuvo su maestría y Ph.D. en ciencias políticas en la Universidad de Hawaii.

Liderazgo Tóxico, el Clima de la Unidad y la Eficacia de la Organización

DR. GEORGE REED, PhD

La práctica del liderazgo puede considerarse como sentarse en un espectro con influencia inspiradora, motivadora y ejemplar en un extremo y comportamiento degradante, destructivo y reprehensible en el otro. El buen liderazgo está relacionado con resultados positivos para la organización mientras que el liderazgo deficiente está relacionado con estrés elevado, poca satisfacción, poco compromiso con la organización y poca inclinación para permanecer en el servicio.¹ Lamentablemente, tanto el liderazgo positivo como el negativo se detectan fácilmente en la milicia estadounidense y algunos líderes destructivos llegan a ocupar puestos de poder y autoridad significativas. En este artículo se analiza el fenómeno del liderazgo tóxico y su relación con el clima de la unidad y la eficacia en la organización. A pesar de la importancia del liderazgo en las organizaciones militares, un énfasis solamente en los aspectos positivos del liderazgo no trata ocasiones en que aquellos en puestos de autoridad intentan dirigir de formas que son inconsistentes con los valores subyacentes de la organización. Después de examinar el fenómeno del liderazgo tóxico, en este artículo se sugieren algunos puntos de partida para minimizar su impacto negativo.

Organizaciones militares enfatizan con mucha razón el liderazgo. En la milicia estadounidense, un sin fin de publicaciones doctrinales están dedicadas al tema. El liderazgo es un enfoque del sistema de educación profesional militar desde antes del reclutamiento al cuerpo de oficiales a través de los colegios conjuntos y del servicio superior, y las publicaciones militares comúnmente publican artículos sobre tópicos relacionados con el tema. El liderazgo es visto casi universalmente como un concepto positivo. Los buenos líderes le prestan valor a sus organizaciones, y buscamos líderes responsables de carácter de nuestras academias militares y fuentes de reclutamiento al cuerpo de oficiales. Culturalmente, hay básicamente dos soluciones a virtualmente cualquier problema en las organizaciones militares: el liderazgo y el entrenamiento. Cuando se enfrentan a una catástrofe, sobre todo de índole pública, los líderes son probablemente reemplazados, y un régimen de adiestramiento enfocado en el error sigue rápidamente. Como ejemplo, considere las reacciones al reciente descubrimiento que miembros de un ala de misiles responsables de misiles nucleares balísticos intercontinentales estaban haciendo trampas en los exámenes de capacitación. Los líderes, algunos, que ni hicieron trampa ni encubrieron a los que la hicieron, fueron despedidos, y se implementó entrenamiento adicional.² A pesar de la dependencia en el liderazgo como la base de las organizaciones militares, las nociones aspiracionales del liderazgo propuestas en la doctrina puede que sean muy diferentes a lo que se ve en la práctica. Algunas personas en puestos de autoridad se comportan de manera que tienen efectos perjudiciales en sus subordinados.

En su libro *Bad Leadership (Liderazgo Deficiente)*, la profesora Barbara Kellerman de Harvard propone que estudiar el liderazgo sin tomar en cuenta la posibilidad del liderazgo deficiente es análogo a estudiar la medicina sin considerar las enfermedades.³ Cuando los investigadores llevaron a cabo estudios con grupos en la Escuela Superior de Guerra del Ejército Estadounidense con el fin de adquirir información sobre la naturaleza del liderazgo destructivo, escucharon relatos desalentadores de mal trato a manos de supervisores—trato que es incompatible con los valores militares.⁴ Cuando los resultados de esa investigación fueron publicados en la revista “*Military Review*”, el autor recibió cientos de correos electrónicos de personas que querían contar sus relatos de lo que ellos percibían como abuso por parte de sus líderes, un fenómeno que con-

tinúa hasta el presente.⁵ Nuestra fascinación con el liderazgo y su potencial—lo que James Meindl, Sanford Ehrlich y Janet Dukerich describen como el “romance del liderazgo”—no nos debe impedir examinar el impacto negativo de los comportamientos que influyen que a menudo se manifiestan por aquellos que intentan ser líderes pero lo hacen de manera deficiente.⁶

Cuando se explora el liderazgo tóxico, debemos notar que los individuos que investigan y publican sobre el tema utilizan diferentes palabras claves y etiquetas. La supervisión abusiva, el liderazgo destructivo, la intimidación, la descortesía, los empresarios brutales, la tiranía mezquina, y el liderazgo tóxico son temas relacionados. Ya que en la literatura no hay un consenso sobre la definición, las personas interesadas en aprender más deberían ver más allá de un solo término. Para algunos expertos como Jean Lipman-Blumen, el liderazgo tóxico es sencillamente liderazgo deficiente.⁷ El liderazgo tóxico se identifica por su efecto negativo en la organización, y la fuente puede ser desde la incompetencia, o falta de atención a malevolencia. Otros buscan una definición más explícita. En el 2004, este autor ofreció una definición en tres partes del liderazgo tóxico:

1. Una aparente falta de preocupación por el bienestar de los subordinados.
2. Una personalidad o técnica interpersonal que afecta negativamente al ambiente de la organización.
3. La convicción de los subordinados que el líder está motivado principalmente por intereses propios.⁸

Los primeros dos elementos de la definición mencionada anteriormente son prerequisites, y la tercera es un variable interviniente. En otras palabras, si un supervisor es percibido como despreocupado por el bienestar de los subordinados y tiene un estilo de liderazgo que deprime el ambiente de la organización, hay un problema de liderazgo tóxico. Por un lado, la percepción por los subordinados que el jefe está avanzando a sus expensas empeora el impacto negativo. Si por otra parte, los subordinados perciben que el supervisor con deficiencias interpersonales está motivado por los intereses de la organización y no están intentando avanzar a sus expensas, la situación es menos problemática. Los subordinados tal vez perdonen un estilo de liderazgo brusco si piensan que los motivos son para un bien mayor.

El Ejército de EE.UU. publicó recientemente una definición descriptiva del liderazgo tóxico en la Publicación Doctrinal del Ejército 6-22, *Liderazgo del Ejército*, que es la primera vez que el concepto ha recibido atención como conocimiento institucional en una organización militar:

El liderazgo tóxico es una combinación de actitudes, motivaciones y comportamientos egocéntricos que tienen efectos adversos en los subordinados, la organización y el desempeño laboral. Este líder carece de preocupación por los demás y el clima de la organización, que conduce a efectos negativos a corto y largo plazo. El líder tóxico se comporta con sentido exagerado de autoestima y por intereses propios agudos. Los líderes tóxicos utilizan comportamientos disfuncionales para engañar, intimidar, obligar o castigar injustamente a otros para sus propios fines. El líder negativo cumple con requisitos a corto plazo procediendo al fondo del continuo de compromiso, donde los seguidores responden a la autoridad del líder para cumplir con sus solicitudes. Esto tal vez logre resultados a corto plazo, pero pasa por alto las demás categorías de aptitudes del líder de liderar y desarrollar. El uso prolongado del liderazgo negativo para influir a los subordinados socava la voluntad, iniciativa y potencial de los subordinados y destruye el estado de ánimo de la unidad.⁹ (énfasis en el original).¹⁰

Independientemente de cómo se define el liderazgo tóxico, su impacto es negativo. Numerosas investigaciones han demostrado que el personal militar que trabaja para líderes tóxicos expresa niveles más bajos de satisfacción con sus trabajos, sueldos y prestaciones, supervisores, colegas, e inclusive sus propios subordinados.¹¹ Oficiales subalternos y de mandos medios que

experimentan liderazgo tóxico son menos propensos a permanecer en el servicio militar.¹² Un estudio de 373 miembros de la Guardia Nacional Aérea y sus supervisores indicó una relación entre la supervisión abusiva y una disminución en comportamiento cívico de la organización.¹³ Cuando trabajan para un líder tóxico, los subordinados típicamente cumplen para evitar la ira del supervisor, pero no se esfuerzan más allá—un comportamiento que se equipara con el civismo de la organización. El cumplimiento tal vez sea preferible al incumplimiento, pero no es un sustituto para el compromiso que conduce a tomar riesgos prudentes, creatividad e innovación. Una investigación llevada a cabo en el 2013 de 2,572 militares del Ejército en Irak vinculó la supervisión abusiva con un descenso en la valentía moral de los subordinados y una disminución en la identificación con los valores intrínsecos de la organización.¹⁴ Una tesis reciente enfocada en cadetes de la Academia de la Fuerza Aérea Estadounidense sugirió una relación entre el liderazgo tóxico y un incremento en los niveles de cinismo.¹⁵ El cinismo se equipara a una actitud negativa acompañada por sentimientos de desesperanza, desilusión, e inclusive desprecio de individuos o toda una organización. Una transmisión reciente en la Radio Pública Nacional (NPR por sus siglas en inglés) sostuvo la posibilidad de un vínculo entre el liderazgo tóxico y el suicidio.¹⁶ Podríamos postular que el consumo del alcohol e incidentes de violencia doméstica sería más elevado entre los que trabajan para jefes tóxicos. Las investigaciones sobre el liderazgo tóxico aún comienza, pero las investigaciones en contextos civiles aluden a efectos negativos adicionales.

En una investigación del 2009 sobre la falta de urbanidad en el ámbito laboral realizó una encuesta entre miles de gerentes y empleados de una gama amplia de empresas estadounidenses. Las víctimas de intercambios tóxicos expresaron ira, frustración, y a veces, sentimientos de venganza. El estudio indicó que 48 por ciento disminuyeron su esfuerzos laborales, 38 por ciento disminuyeron la calidad de su trabajo, 66 por ciento dijeron que su rendimiento disminuyó, 80 por ciento perdió tiempo preocupándose por el incidente, 63 por ciento perdieron tiempo evitando al agresor, y 78 por ciento dijero que su compromiso hacia la organizacion disminuyó.¹⁷ Estas cifras representan una pérdida significativa que amerita la atención de ejecutivos, y si se aplican a poblaciones militares, deberán llamarle la atención a líderes de todo nivel. Una encuesta reciente de la organización Gallup encontró que los gerentes representan el 70 por ciento de la varianza en los resultados de compromiso con la empresa de los empleados. También aseveró que solamente el 13 por ciento de los empleados mundialmente se sienten comprometidos.¹⁸ Empleados desvinculados activamente le cuestan a los EE.UU. entre \$450 mil millones y \$550 mil millones de dólares anualmente en la productividad perdida.¹⁹ El veredicto se ha dictaminado. El liderazgo tóxico es contraproducente, ¿entonces por qué no se dedica más atención al fenómeno?

El hecho de que la identificación y eliminación de los líderes tóxicos no son una prioridad más alta está relacionado con la naturaleza de arriba abajo de las organizaciones militares. Las evaluaciones del desempeño laboral y los informes de la capacidad típicamente se basan en las observaciones solamente de los supervisores y excluyen las percepciones de los subordinados. Ya que los líderes tóxicos tienden a ser muy receptivos y aún serviles con sus superiores, no se ven tan mal de arriba hacia abajo. Son vistos como receptivos y capaces de obtener altos niveles de rendimiento de sus subordinados. Un refrán característico sería, “Yo sé que José es un poco brusco, pero cuando él dice que salten, su equipo salta. Obtiene resultados sin duda.” Los líderes tóxicos a menudo son muy dedicados a la organización y tal vez tengan las mejores intenciones. Lamentablemente, manifiestan un estilo interpersonal inapropiado que es dañino a largo plazo. Las medidas de eficacia típicamente son a corto plazo, enfocándose en la misión cumplida más reciente, mientras que la salud y bienestar a largo plazo de los que comprenden la unidad son ignoradas. Algunos expertos sugieren que los líderes tóxicos son astutos operadores que manejan con destreza las fuentes del poder. Se congracean con personas poderosas y manejan cuida-

dosamente sus reputaciones con sus superiores, a la vez que hacen las vidas imposibles para aquellos que tienen que trabajar para ellos.²⁰

El apoyo de los líderes superiores es necesario si el liderazgo tóxico se tratase a nivel de empresa. Las políticas de personal, incluyendo el medio por el cual identificamos y seleccionamos individuos para puestos claves, tal vez sea un punto de influencia vital para lidiar con el problema. Aquellos en la cima de la pirámide de la organización no perciben que la dificultad es tan aguda como en el pasado. Recordarán experiencias tóxicas del pasado pero a menudo las consideran como un reto iniciativo que ellos mismos pasaron exitosamente. A menudo escuchamos el refrán, “La supervisión abusiva realmente era un problema hace años, pero está mejor ahora”. Sus percepciones probablemente sean influenciadas por su puesto. Un amigo una vez comparó la situación al “síndrome de los monos en los árboles”. Él explicó que en los bosques tropicales, la fruta madura más rápidamente en las ramas más altas de los árboles. Los primates de alto rango tienden a congregarse en las ramas altas donde la fruta es más dulce y abundante. Los primates de menos rango están relegados a las ramas bajas. Cuando los primates de alto rango miran hacia abajo, ven las caras sonrientes de los monos. Cuando los monos de menos rango miran hacia arriba, tienen una muy diferente y menos atractiva vista. Lo que vemos depende de dónde estamos ubicados. Una encuesta anual llevada a cabo por el Centro de Liderazgo del Ejército evaluó la calidad de liderazgo a través de cuestionarios completados por más de 16,800 militares y 2,900 personas de la fuerza laboral civil. Esa encuesta a gran escala representativa encontró que los subordinados percibían que el 16 por ciento de los líderes del Ejército eran ineficientes. Esos líderes recibieron alto puntaje en cuanto a la obtención de resultados (una calificación de 78 por ciento de eficacia), pero niveles menores de eficacia en la creación de un ambiente positivo (70 por ciento) y el desarrollo de personal (59 por ciento).²¹ Independientemente de si la calidad del liderazgo es mejor ahora que en el pasado, más trabajo claramente se debe realizar.

La cultura militar también puede ser un impedimento. Soldados, marineros, aviadores e infantes de marina están socializados a respetar al rango sino al individuo. Es una cultura que premia la lealtad, así es que los que se quejan de su jefe no son recibidos favorablemente en los altos niveles de la cadena de mando. Un líder tóxico que se entera de una queja emergente puede a menudo pintar los subordinados desfavorablemente mucho antes que el que se queja pueda sacarle ventaja a una política de puertas abiertas. Por consiguiente, ¿qué puede hacer una persona que está sufriendo bajo un líder tóxico?

La forma más segura de actuar para el individuo desafortunado que se ve vinculado a un jefe tóxico es construir un sistema de apoyo personal para ayudarse a lidiar con la situación y buscar una salida a través de reasignación de trabajo, traslado temporal, renunciar a su empleo cuando sea posible. Muchas veces, las organizaciones militares con altos índices de rotación ofrecen una solución debido al traslado inminente del líder tóxico o los subordinados afectados. Lamentablemente, algunos malos consejos en la literatura popular abogan por tratar a los líderes tóxicos como si fuesen agresores en un parque infantil. Eso tal vez sea buen consejo en un ambiente corporativo donde renunciar al puesto es una alternativa, pero los militares están sujetos a términos de servicio. Aunque conversaciones francas y honestas raramente son malas opciones, un seguidor deberá esperar una reacción negativa cuando enfrenta directamente a un líder tóxico. En la estructura estratificada y regimentada de la milicia, la desigualdad de poder no es ventajosa para el subordinado que está sufriendo. A aquellos que son blancos de un líder tóxico se les aconseja mantener apuntes detallados de intercambios incivilizados y comportamiento inapropiado, incluyendo fechas, horas, y testigos. Parecerá indecoroso llevar un libro sobre un superior, pero si llega al punto donde una queja oficial es indicada, a pesar de los riesgos asociados con el desagradar al jefe, esos detalles ayudarán a apoyar una investigación por el inspector general u otro oficial investigador. Uno debe tener cuidado cuando le pide apoyo a los demás. Alegaciones con múltiples denunciantes tienden a ser tomados más seriamente, pero el motín

aún es un delito sancionado. En algunas circunstancias, una organización se beneficia más cuando un individuo valiente se despreocupa de sus propios intereses y acude a todas las alternativas para rectificar una situación insostenible. Las pruebas indican que las quejas de liderazgo tóxico son tomadas más seriamente. Algunos individuos, incluyendo oficiales de alto rango, están siendo retirados de puestos de mando debido al ambiente que han creado en la organización.

En el 2010, el comandante de un crucero de misiles dirigidos fue retirado de su cargo luego que el informe de un inspector general concluyera que ella creó un ambiente de temor y hostilidad a través de la humillación y denigración de sus subordinados.²² Un general de división de la Fuerza Aérea se jubiló luego que una investigación concluyó que él era “cruel y oprimente” y maltrataba a sus subordinados. Fue caracterizado como una persona que gritaba profanidades, que en un año tuvo seis oficiales ejecutivos y edecanes.²³ El General Martin Dempsey, Jefe del Estado Mayor Conjunto, ha expresado su apoyo por evaluaciones de 360 grados que toman en cuenta la retroalimentación de los superiores, colegas y subordinados como manera de identificar líderes tóxicos. Un artículo en el Air Force Times planteó la interrogante de que si estas evaluaciones serían algún día parte de las evaluaciones oficiales y proporcionó unas ideas de cómo cada rama de las fuerzas armadas está considerando la implementación:

- El Ejército está utilizando las evaluaciones de manera agresiva, con oficiales superiores, subalternos y suboficiales pasando por “la evaluación de múltiples fuentes y retroalimentación” durante los últimos años.
- La Armada está a la vanguardia de las otras ramas de las fuerzas armadas ya que ha experimentado con estas evaluaciones por una década. Todo almirante lo recibe como parte de su capacitación y futuros comandantes y oficiales ejecutivos completan las evaluaciones en la Escuela de Liderazgo de Mando. Además, los alférez de guerra de superficie y jefes de departamento reciben evaluaciones similares durante la Escuela de Oficiales de Guerra de Superficie.
- La Fuerza Aérea tenía poca experiencia previa con evaluaciones de 360 grados, pero durante los últimos 6 meses ha creado un prototipo de evaluación y ha exhortado a algunos generales a que la comiencen a tomar.
- Al momento de cierre de este número, oficiales de la Infantería de Marina no habían respondido a una solicitud para sus comentarios.²⁴

Los líderes tóxicos son mayormente inmunes de la influencia de sus subordinados. Tienden a racionalizar su propio comportamiento, descartan las quejas de sus subordinados, y evitan las encuestas del clima de sus unidades o ignoran los resultados.²⁵ Aunque sean los que más necesitan de consejos y retroalimentación, también son los menos propensos a ser receptivos cuando esos recursos son disponibles. La buena noticia es que son alcanzables por sus superiores.²⁶ Porque responden a sus superiores y se preocupan por su progreso profesional, una conversación clara y enfocada con su jefe puede modificar una conducta problemática. Las personalidades rara vez cambian, pero el comportamiento sí se puede modificar. Por lo tanto, aquellos en puestos de responsabilidad deberán estar alertos a las tendencias tóxicas en sus subordinados y prepararse a tener discusiones difíciles. Deberán utilizar palabras concisas y ser directos. En vez de decir, “Haces un buen trabajo y me impresionan todos tus logros; sin embargo, debes trabajar en tus habilidades interpersonales”, deberán decir, “Tu equipo detesta trabajar para ti; eres percibido como mezquino, abusivo, y que te autopromueves”. Deberán ser específicos en cuanto a conducta observada o reportada que es inconsistente con los valores fundamentales de la organización y demandar cambio mientras ofrece apoyo. Tales conversaciones son incómodas, y hay algo humano en evitar los enfrentamientos, sobre todo con alguien que de lo contrario está cumpliendo con su misión. Invertimos mucho tiempo y esfuerzo para preparar a los líderes, y se les exige mucho. Merecen una oportunidad para desarrollarse, pero si su conducta interperso-

nal no mejora, entonces esos líderes deberán ser retirados de puestos donde pueden dañar a otros. Tales decisiones sobre personal difícil no se deben percibir como un fracaso de liderazgo sino como una práctica necesaria. Hay un momento cuando los esfuerzos de capacitación y desarrollo deberán cesar y retiros, traslados o despidos deberán comenzar. Debemos recordar que las personas que trabajan para un líder tóxico culpan no solamente al individuo sino que tienden a percibir que toda la cadena de mando es culpable por tolerar esa conducta. “Mi jefe es terrible” a veces se interpreta como “La Fuerza Aerea es terrible”.

Trabajar para un supervisor tóxico puede tener un aspecto positivo. Si el subordinado permanece, puede ser una experiencia de desarrollo personal y forjar su carácter. Probablemente sea poco consuelo para aquellos que actualmente trabajan para un líder tóxico, pero puede ser que aprendamos más de un mal líder que de un buen líder. Como mínimo, pueden amasar una lista larga de “cosas que nunca haré cuando yo ocupe este cargo”. Tales experiencias contribuyen a una forma de callos interpersonales. Aquellos que han trabajado para un líder tóxico probablemente no serán afectados por un jefe que tiene un mal día de vez en cuando. Amasar unas habilidades en lidiar con líderes difíciles y colegas problemáticos puede ser bastante favorable. Un supervisor sagáz una vez ofreció un muy buen consejo a su servidor: “Allá afuera siempre habrá un patán con el que te encontrarás. Cómo lidies con la situación determinará si tendrás una carrera larga o corta.”

El Presidente Dwight David Eisenhower, quien además sirvió como el comandante supremo aliado en Europa durante la Segunda Guerra Mundial, bromeó, “No puedes mandar a la gente pegándoles en la cabeza—eso es un asalto, no liderazgo”.²⁷ Debemos reconocer que es importante no solamente lograr la misión sino también mandar de tal forma que engendre el respeto y compromiso de los subordinados. En el 1879, el General de División John Schofield sabiamente observó que

es posible impartir instrucciones y dar órdenes de tal forma en tal tono de voz que inspira en el soldado ningún sentimiento más que un deseo intenso de obedecer, mientras que la conducta opuesta y tono de voz no fallarán en provocar fuerte resentimiento y un deseo de desobedecer. Una forma u otra de lidiar con subordinados, emana de un espíritu correspondiente en el pecho del comandante. Aquel que siente el respeto que merecen los demás no podrá dejar de inspirar en otros gran estima por él; mientras que aquel que siente, y por lo tanto, manifiesta, falta de respeto hacia los demás, sobretodo a sus subordinados, no fallará en inspirar odio hacia él mismo.²⁸

Schofield sabía lo que seguimos redescubriendo. No es solamente lo que les decimos a los subordinados que hagan lo que importa. Cómo se les dice también es de suma importancia. La manera en que se dice es un reflejo de su estilo de liderazgo.

Sería erróneo sugerir que llamados para eliminar el liderazgo tóxico es alguna forma de doblegarse de forma políticamente correcta a los subordinados – un enfoque de “portémonos bien y cantemos ‘Kumbaya’”. El enfoque correcto del liderazgo cumple con las necesidades de los subordinados y las demandas de una situación dada, que pueden variar significativamente. La conducta que es apropiada y aún agradecida en una situación podría ser sumamente inapropiada y destructiva en otra situación. Es parecido al humor: algo considerado divertido en el vestuario podría parecer de mal gusto u ofensivo en otro ámbito. Esa observación supone un alto nivel de conciencia propia y auto—regulación como habilidades importantes para los líderes. Hay tiempo para ser ruidoso y nada es tan eficaz como un berrinche de ira bien actuado del jefe. Los líderes a veces tienen que mandar a sus subordinados a hacer cosas difíciles y peligrosas y se tienen que dirigir a rendimiento de baja calidad; no se pueden dar el lujo de complacer a todos todo el tiempo. Intentar complacer a todos y necesitar ser queridos son antiéticos al buen liderazgo. En las palabras de Robert Sutton, autor de *La regla del no del pendejo (The No Asshole Rule)*, en un

puesto de liderazgo a veces lo considerarán un pendejo.²⁹ Los buenos líderes, sin embargo, no hacen de esa conducta su comportamiento estándar. El hecho de que un supervisor tenga un mal día no indica necesariamente que él, o ella, es tóxico. El patrón de comportamiento percibido por los subordinados a través del tiempo y el impacto acumulado en el ambiente de la organización será el testimonio.

Vemos ejemplos de líderes de grandes personalidades quienes, sin duda, son eficaces, pero también tienen problemas interpersonales. Es difícil discutir con el record de victorias del entrenador de baloncesto Bob Knight, cuyo apodo era “El General”. Ganó muchos campeonatos y amasó un record de victorias envidiable a pesar de berrinches de tirar sillas y públicamente regañar a sus jugadores. Otros dan ejemplos de generales militares famosos como Patton o MacArthur, que mostraban una tendencia de un arquetipo de liderazgo identificable—líderes seguros de sí mismos, su enfoque sensato, autocráticos, autoritarios, sin tomar prisioneros que le prestan poca atención a las opiniones ajenas pero son muy eficaces. Una mitología parece ser asociada con tales formas de liderazgo. De la cultura popular, podemos identificar el socialmente inadaptado y narcisista Dr. Gregory House que interpreta el actor Hugh Laurie en la serie televisiva *House, M.D.* ¿Qué es lo que apreciamos de ese personaje? House es antisocial, y su vida privada es un desastre. Pero es aún brillante y sin igual en sus diagnósticos. Hay algo atractivo de las personas que son libres de las convenciones sociales y logran desempeñar sus labores contra todas las probabilidades. El problema con tales ejemplos, por muy atractivos que sean es, que para cada líder eficaz que actúa como megalómano o narcisista, es posible identificar otro que son tan eficaces, pero humilde y socialmente adepto. Para cada Patton y MacArthur podemos encontrar un Bradley o un Eisenhower. Para cada entrenador Knight, hay un entrenador Mike Krzyzewski, quien, por cierto, tuvo más victorias en su carrera que Knight. Para ser justos, tal vez no sea correcto caracterizar a Patton o MacArthur como tóxicos ya que muchos que trabajaron para ellos apreciaban sus talentos. Sin embargo, a menudo son caracterizados con aspectos oscuros en sus personalidades. Recuerden que Patton fue marginado por pegarle a un soldado hospitalizado y castigado en más de una ocasión por hacer declaraciones públicas imprudentes. El Presidente Truman despidió al extravagante de su cargo como comandante de las fuerzas estadounidenses en Corea cuando parecía que él favorecía una política que el presidente oponía—una expansión del conflicto coreano. Nos quedamos preguntándonos cuán más eficaces hubiesen sido si hubieran modificado algunas aspectos de su conducta problemática.

Ya que hemos planteado el caso que el liderazgo tóxico es un problema merecedor de intervención a todo nivel, debemos reconocer que tal vez no sea razonable esperar que sea eliminado del todo. Simplemente despidiendo los líderes tóxicos conforme son identificados, aunque fuese factible, no es probable. En cuanto a las estadísticas, con respecto al desempeño eficaz, siempre habrá un tercio inferior. Michelle Kusy y Elizabeth Holloway sugieren que los líderes tóxicos florecen en culturas tóxicas.³⁰ Parece ser una condena fuerte que ignora la noción de algunas personas problemáticas, pero merece evaluación. Si tienen razón, las organizaciones militares podrán estar muy atareadas con identificar y remover los líderes tóxicos sin dirigirse a la causa fundamental de la conducta tóxica. Cabe preguntar si creamos líderes tóxicos, los alentamos o premiamos involuntariamente, y los toleramos en nuestros entornos. Estas preguntas merecen evaluación adicional. Mientras tanto, podemos continuar determinando el alcance del problema haciendo las preguntas adecuadas. El liderazgo tóxico se puede medir, así como el ambiente de la organización. La falta de experiencia de los subordinados y el conocimiento de las responsabilidades de sus superiores tal vez impida que los evalúen. Sin embargo, pueden contar si son abusados, humillados y denigrados por sus superiores. Pueden indicar si confían en su liderazgo y si se sienten que sus líderes están actuando según los valores explícitos de la organización. En vez de buscar la eliminación completa de los líderes tóxicos, tal vez sea más razonable esperar que se identifiquen y abordarlos cuanto antes. Ese enfoque implicaría la ejecución de normas para identificar rápidamente los líderes tóxicos e intervenir para contrarrestar su impacto nega-

tivo. Algo es cierto: si no buscamos a los líderes destructivos, no es probable que se hallen hasta que hayan hecho estragos en sus unidades.

Las organizaciones militares se beneficiarían con una estrecha tolerancia de los estilos de liderazgo para reflejar las necesidades de una fuerza totalmente profesional y únicamente reclutada. La vida militar es intrínsecamente exigente y estresante. No es aconsejable hacerla más difícil de lo que tiene que ser con líderes que están infligiendo rumores y menospreciando a sus subordinados. El liderazgo militar es una profesión con alto rendimiento de cuentas. Aquellos que ocupan cargos de gran responsabilidad con razón son sujetos a estándares altos de rendimiento. Es completamente apropiado cuando a tales personas les confiamos los recursos más preciados de la nación—nuestros hijos e hijas. □

Notas

1. George E. Reed, "Toxic Leadership," (Liderazgo tóxico), *Military Review* 84, no. 4 (July–August 2004): 67–71.
2. David S. Cloud, "Air Force Officers in Nuclear Force Suspected of Cheating. Los Angeles Times. January 15, 2014. <http://articles.latimes.com/2014/jan/15/nation/la-na-nuclear-drugs-20140116>.
3. Barbara Kellerman, *Bad Leadership: What It Is, How It Happens, Why It Matters* (Mal liderazgo: Qué es, cómo sucede y por qué es importante), (Boston: Harvard Business School Press, 2004).
4. Richard C. Bullis y George E. Reed, *Assessing Leaders to Establish and Maintain Positive Command Climate: A Report to the Secretary of the Army* (Evaluando a los líderes para establecer y mantener un clima positivo: Informe para el Secretario del Ejército) (Carlisle, PA: US Army War College, 2003).
5. Reed, "Toxic Leadership,".
6. James R. Meindl, Sanford B. Ehrlich y Janet M. Dukerich, "The Romance of Leadership," (El romance del liderazgo), *Administrative Science Quarterly* 30, no. 1 (March 1985): 78–102.
7. Jean Lipman-Blumen, *The Allure of Toxic Leaders: Why We Follow Destructive Bosses and Corrupt Politicians—and How We Can Survive Them* (La fascinación de los líderes tóxicos: Por qué seguimos jefes destructivos y políticos corruptos—y cómo podemos sobrevivirlos), (Oxford, UK: Oxford University Press, 2005).
8. Reed, "Toxic Leadership," 67.
9. Army Doctrinal Publication 6-22 (Publicación doctrinal del Ejército), *Army Leadership*, (Liderazgo en el Ejército), agosto 2012, 3.
10. Army Doctrinal Publication 6-22, agosto 2012,3.
11. George E. Reed y Richard A. Olsen, "Toxic Leadership: Part Deux," (Liderazgo tóxico: Segunda Parte), *Military Review* 90, no. 6 (Noviembre–diciembre 2010): 58–64; y George E. Reed y R. Craig Bullis, "The Impact of Destructive Leadership on Senior Military Officers and Civilian Employees," (El impacto del liderazgo destructivo en los oficiales militares superiores y los empleados civiles), *Armed Forces and Society* 36, no. 1 (October 2009): 5–18.
12. Reed y Bullis, "Impact of Destructive Leadership," (Impacto del liderazgo destructivo), 61–62.
13. Kelly L. Zellars, Bennett J. Tepper, y Michelle K. Duffy, "Abusive Supervision and Subordinates' Organizational Citizenship Behavior," (Supervisión abusiva y el comportamiento cívico de la organización de los subordinados), *Journal of Applied Psychology* 87, no. 6 (2002): 1068–76.
14. Sean T. Hannah et al., "Joint Influences of Individual and Work Unit Abusive Supervision on Ethical Intentions and Behaviors: A Moderated Mediation Model," (Influencias conjuntas de supervisión abusiva del individuo y la unidad de trabajo en intenciones y comportamientos éticos: Un modelo de mediación moderado), al of *Applied Psychology* 98, no. 4 (Julio 2013): 579–92.
15. James M. Dobbs, "The Relationship between Perceived Toxic Leadership Styles, Leader Effectiveness, and Organizational Cynicism" (PhD diss., University of San Diego, August 2003).
16. Daniel Swerdling, "Army Takes on Its Own Toxic Leaders," (El Ejército lidia con su propios líderes tóxicos), *All Things Considered*, National Public Radio, 6 January 2014, <http://www.npr.org/2014/01/06/259422776/army-takes-on-its-own-toxic-leaders>.
17. Christine Porath y Christine Pearson, "How Toxic Colleagues Corrode Performance," (Cómo los colegas tóxicos corroen el rendimiento), *Harvard Business Review*, Abril 2009, <http://kaplanmarketing.com/wp-content/uploads/2010/10/toxic-colleagues1.pdf>.
18. Randall Beck and Jim Harter, "Why Great Managers Are So Rare," (¿Por qué los buenos líderes son tan raros?), *Gallup Business Journal*, 25 de marzo de 2014, http://businessjournal.gallup.com/content/167975/why-great-managers-rare.aspx?utm_source=alert&utm_medium=Monthly&utm_content=morelink&utm_campaign=syndication&inf_contact_key=c5720702f2f2db01711013ff89ca3506f17f89db58f9895d7c3ddd6db8da4412.
19. Gallup Corporation, *State of the American Workplace: Employee Engagement Insights for U.S. Business Leaders* (El estado del lugar de trabajo estadounidense: Recomendaciones de participación para los empleados), (Washington, DC: Gallup

Corporation, 2013), <http://www.gallup.com/file/strategicconsulting/163007/State%20of%20the%20American%20Workplace%20Report%202013.pdf>.

20. Mitchell E. Kusy y Elizabeth L. Holloway, *Toxic Workplace: Managing Toxic Personalities and Their Systems of Power* (El lugar de trabajo tóxico: Administrando las personalidades tóxicas y sus sistemas de poder), (San Francisco: Jossey-Bass, 2009).

21. Ryan Riley et al., 2011 *Center for Army Leadership Annual Survey of Army Leadership (CASAL): Main Findings*, Technical Report 2012-1 (Encuesta anual del 2011 del Centro de Liderazgo del Ejército (CASAL): Hallazgos importantes, Informe Técnico 2012-1), (Fort Leavenworth, KS: Center for Army Leadership, May 2012), http://usacac.army.mil/CAC2/Repository/CASAL_TechReport2012-1_MainFindings.pdf.

22. Mark Thompson, "The Rise and Fall of a Female Captain Bligh," (El surgimiento y la caída de una capitana Bligh), *Time*, 3 de marzo de 2010, <http://content.time.com/time/nation/article/0,8599,1969602,00.html>.

23. Craig Whitlock, "Pentagon Investigations Point to Military System That Promotes Abusive Leaders," (Investigaciones del Pentágono señalan sistema militar que promueve líderes abusivos), *Washington Post*, 28 de enero de 2014, http://www.washingtonpost.com/world/national-security/pentagon-investigations-point-to-military-system-that-promotes-abusive-leaders/2014/01/28/3e1be1f0-8799-11e3-916e-e01534b1e132_story.html.

24. Andrew Tilghman, "360-Degree Reviews May Never Be Part of Formal Evals," (Revisiones de 360 grados pueden que nunca sean parte de evaluaciones oficiales), *Air Force Times*, 30 de octubre de 2013, <http://www.airforcetimes.com/article/20131030/NEWS05/310300010/360-degree-reviews-may-never-part-formal-evals>.

25. Reed, "Toxic Leadership,".

26. Robert I. Sutton, *The No Asshole Rule: Building a Civilized Workplace and Surviving One that Isn't* (New York: Business Plus, 2007)

27. Goodreads, "Quotes by Dwight D. Eisenhower. https://www.goodreads.com/author/quotes/23920.Dwight_D_Eisenhower.

28. Maj Gen John Schofield (discurso al Cuerpo de Cadetes, Academia Militar del Ejército, West Point, NY, 11 de agosto de 1879).

29. Sutton, *The No Asshole Rule: Building a Civilized Workplace and Surviving One That Isn't (La regla del no del pendejo: Creando un lugar de trabajo civilizado y sobreviviendo uno que no lo es)*.

30. Kusy y Holloway, *Toxic Workplace*.



El Dr. George Reed, PhD, es decano adjunto y miembro del cuerpo docente en la Escuela de Liderazgo y Ciencias Educativas en la Universidad de San Diego. El Señor Reed tiene un doctorado en análisis de política pública y administración de la Saint Louis University, una Maestría en Ciencias Forenses de George Washington University, y una licenciatura en administración de justicia criminal de la University of Central Missouri. Antes de pasar a formar parte del cuerpo docente en el 2007, sirvió 27 años en el Ejército como oficial de la policía y se retiró con el rango de coronel. Durante los últimos seis años de su Carrera en el servicio activo, se desempeñó en calidad de director de Estudios de Comando y Liderazgo en la Escuela Superior de Guerra del Ejército de Estados Unidos.

La Guerra a la Vuelta de la Esquina*

No es un mero Problema Delictivo

DR. JAMES P. FARWELL, PhD

SRA. DARBY ARAKELIAN

El programa de televisión *Miami Vice* trataba de historias de agentes encubiertos que luchaban para que los colombianos y sus cohortes de Miami no introdujeran de contrabando cocaína y otras drogas ilícitas en este país. En la vida real, las autoridades de EE.UU. lo hicieron incluso mejor. Demostraron ser tan efectivos que los cárteles de Colombia decidieron desplazar sus operaciones al oeste y encargaron el tráfico de drogas a bandas mexicanas. En vez de dinero en efectivo, pagaban a los traficantes en especie, ofreciendo del 30 % al 50 % de las drogas para que las vendieran por su cuenta, y las bandas pasaron de transportar a distribuir. El tráfico de drogas por México había sido un problema desde hacía mucho tiempo, pero este cambio hizo que aumentara considerablemente.¹

Mientras que los medios de comunicación occidentales se concentraban en gran medida en las muertes de civiles en Siria, a menudo omitían lo que estaba pasando en nuestro patio trasero, donde la violencia mexicana de las drogas había acabado con 110.000 vidas.² El ex-presidente Felipe Calderón declaró que “la guerra más letal es la de las bandas criminales entre sí”.³ Esa declaración refleja solamente una parte de la historia, porque la violencia del cártel afecta en gran medida a Estados Unidos.⁴ A medida que los cárteles luchan entre sí para obtener territorios, la amenaza trasciende fronteras y aumenta el nivel de los problemas de *seguridad hemisférica* que abarcan a Estados Unidos, Canadá, México, y sus vecinos centro- y sudamericanos. Las fuerzas de seguridad mexicanas han hecho incursiones en este país, cientos de agentes de la Oficina de Aduanas y Protección Fronteriza (CBP) de EE.UU. han sido atacados,⁵ e incluso se ha sobornado a soldados de EE.UU. para trabajar como mercenarios al sur de la frontera.⁶ Los cárteles también son cada vez más activos en las ciudades de EE.UU.

Aunque el equipo de Calderón se alardea de haber capturado 25 de sus 37 criminales más buscados,⁷ nadie sugiere que se haya detenido el flujo de drogas. En esta lucha donde hay mucho en juego, aunque México no sea un estado fallido, la guerra está erosionando su credibilidad y capacidad para gobernar. También afecta a la seguridad de la región. En Guatemala, se informa que los cárteles controlan del 40 % al 60 % de todo el país.⁸ El cártel mexicano de Sinaloa ha establecido relaciones con la Mara Salvatrucha (MS-13), una banda fundada en Los Ángeles por inmigrantes salvadoreños.⁹ Los cárteles mexicanos también están relacionados con asesinatos en Argentina y Perú.¹⁰

Aunque Estados Unidos desea detener el tráfico y eliminar a los traficantes de drogas, los mexicanos quieren detener los secuestros y la violencia. Esto ha dejado a México y Estados Unidos sin una estrategia cohesiva para combatir a los cárteles—una situación completamente inaceptable. La mayoría de los observadores, incluido el gobierno mexicano, cree que es un problema hacer cumplir la ley. Cuestionamos si ese método es más efectivo e indicamos que las definiciones convencionales para caracterizar esta lucha no se aplican a este conflicto emergente sin precedentes. El debate requerido sobre cómo proteger los intereses de seguridad vitales de EE.UU. apenas ha comenzado. ¿Qué autoridades legales gobiernan la acción de EE.UU.? ¿Qué

* Reimpreso de nuestra AU Revista Strategic Studies Quarterly, Vol 8, No 1, Spring 2014.

funciones deben desempeñar nuestras fuerzas armadas o policías? ¿Nos basamos en definiciones convencionales de crímenes, terrorismo o insurgencia de alta intensidad para dictaminar soluciones? ¿Cuáles son las ventajas y desventajas de usar las fuerzas armadas o la policía para combatir a los cárteles? La amenaza a los intereses de seguridad nacional de EE.UU. requiere un método diferente. Una combinación de cumplimiento de la ley, reforma social, inteligencia encubierta, operaciones militares especiales, y, según sea apropiado, una acción militar selectiva por parte de México con asistencia indirecta de las misiones por parte de los militares de EE.UU. ofrece una ruta plausible hacia el éxito.

Caracterización del conflicto para determinar una estrategia

Cómo se caracteriza la guerra es importante en lo que respecta a la legislación que la gobierna—¿la ley que regula el cumplimiento de la ley o la ley de un conflicto armado?¹¹ La respuesta afecta las tácticas y la naturaleza de las fuerzas empleadas. Por ejemplo, mientras que la policía puede usar una fuerza letal contra sospechosos que amenazan seriamente la integridad física, el principio de la necesidad militar autoriza a las fuerzas armadas a tomar todas las medidas necesarias que no estén prohibidas por la ley internacional para derrotar a un enemigo.¹² Las fuerzas armadas de EE.UU. y México tienen una función que desempeñar en un conflicto de baja intensidad, luchando contra una insurgencia, o combatiendo el terrorismo, especialmente si esos grupos terroristas apoyan a al-Qaeda.¹³ Hay académicos como Paul Rexton Kan que dicen que aunque los cárteles de drogas comparten ciertas características organizativas y operacionales con las organizaciones terroristas,¹⁴ la guerra de las drogas mexicana no es una insurgencia porque los cárteles carecen de un programa político. El argumento clave de Kan se basa en la opinión común—y equivocada—de que los terroristas buscan objetivos políticos mientras que los criminales están motivados por la avaricia.¹⁵ Al escribir en *Small Wars Journal*, Brad Freden reconoce que los elementos de las operaciones de contrainsurgencia (COIN) son útiles para combatir los cárteles pero dice que “la violencia, el tráfico de drogas y la ilegalidad que observamos en el norte de México no constituye una insurgencia. Los cárteles de drogas no tienen ninguna ideología más que el beneficio, sus aspiraciones es que les dejen tranquilos y no tienen ningún apoyo popular más allá del que puedan comprar con dinero o intimidación” (énfasis en el original).¹⁶ El académico de la Universidad de Maryland Shibley Telhami también considera a los terroristas como relacionados con objetivos políticos y los define como aquellos que escogen a civiles como objetivos de forma deliberada para dichos fines.¹⁷

Aquellos que se oponen a caracterizar las guerras de drogas mexicanas como una insurgencia dicen que los cárteles no han “capturado” al estado para implementar un programa social o político y no están tratando de derrocar al gobierno y reemplazarlo por el suyo propio, sino que se concentran en apartar al estado en su búsqueda de beneficios. Este pensamiento, comunicado hábilmente por Kan, es que “ningún grupo insurgente o terrorista . . . se ha desmantelado neutralizando sus redes financieras”, una declaración que suena a algo nuevo al Tesoro de EE.UU. y otras agencias comprometidas en la financiación del contraterrorismo.¹⁸ La clave del argumento es que los cárteles no buscan “sustituir la ideología existente por la suya ni lograr otros objetivos políticos que se relacionen rutinariamente con grupos armados que instiguen una levantamiento social”.¹⁹

Así pues, ¿debe la lucha contra los cárteles de la droga limitarse a medidas para hacer cumplir la ley y políticas que afecten a un programa de reforma social o se trata de una forma de contrainsurgencia para la que las fuerzas armadas debidamente adiestradas y preparadas para misiones especiales deberían desempeñar una función clave? La mayoría de la gente se opone fuertemente a usar las fuerzas armadas para combatir el tráfico de drogas. Básicamente, su argumento se basa principalmente en tres proposiciones confluentes.

- La guerra de drogas mexicana no es insurgencia, terrorismo o un conflicto de baja intensidad, sino que como mucho es una “guerra de un mosaico de cárteles” que requiere reforma social y hacer cumplir la ley.²⁰
- Las fuerzas armadas no están bien preparadas para luchar en esta guerra. El académico Tony Payan de la Universidad Rice asevera que la estrategia militar de México ha producido hasta 100.000 muertes y “ha dejado a las fuerzas armadas y, cada vez más, a una policía federal militarizada sueltas entre la población civil”.²¹
- Las reformas institucionales para limpiar el sistema de justicia penal de México podría proporcionar una reforma social significativa más una mejor colaboración cohesiva con Estados Unidos.

La guerra de las drogas de México es una clase diferente de guerra, con diferentes actores y dinámicas políticas, para la que el éxito requiere lograr objetivos políticos y de seguridad paralelos. La caracterización de la guerra se basa en si los cárteles de drogas—llamadas a veces organizaciones de tráfico de drogas (DTO) u organizaciones criminales transnacionales (TCO)—tienen una ideología política y buscan el poder político. Ambos factores se aplican a los cárteles. Adoptan una ideología basada en historias, narrativas, temas y mensajes sorprendentemente específicos que van mucho más allá de lo que adoptan otros grupos que son aceptados como políticos, como al-Qaeda, las Brigadas Rojas de Italia, el Sendero Luminoso en Perú, las FARC (Fuerzas Armadas Revolucionarias de Colombia) y el ELN (Ejército de Liberación Nacional) de Colombia o el Ejército del Pueblo Paraguayo (EPP) de Paraguay. Esos grupos aceptan la retórica de una ideología, pero ofrecen poco contenido para definir una. Buscan el poder político, ya sea para derrocar el régimen existente o, como en México, para paralizar y eliminar el gobierno como una amenaza para sus operaciones. Y todas son criminales.

Incluso entonces, el argumento de que los cárteles no presentan una insurgencia porque lo que les motiva es la avaricia o los beneficios, no un programa “político”, no es cierto. No existe una definición aceptada de lo que constituye una agenda política. El científico político Harold Lasswell de Yale probablemente llegó a definir qué opinión les merece la política a los políticos: “La política es quien obtiene qué, cuándo y cómo”.²² El hecho de que un partido busque dinero de forma legal o ilegal puede afectar su estado como delincuentes o ciudadanos respetuosos con las leyes, pero los partidos reúnen fácilmente las condiciones para ser delincuentes y actores políticos. La mayoría de los políticos se burlan de la idea de que los partidos cuyo programa es un proceso político es buscar dinero no son políticos. El delito y la política no son mutuamente exclusivos.

Ideología de los cárteles

La noción de lo que constituye una ideología se presta a distintas expresiones. En política, casi cualquier método constituye un sistema de creencias, aunque no todos los sistemas de creencias son ideologías.²³ En términos amplios, la ideología consiste en un grupo de ideas que definen objetivos, expectativas y acciones y expresan una base cohesiva de pensamiento y comportamiento. Las ideologías ejercen influencia sobre las creencias y los valores que comparten las personas, cómo se ven ellos mismos, y cómo perciben el mundo y su posición en él. La ideología guía la acción e influye en las formas en que las personas se relacionan entre sí. Define las esperanzas, los sueños y las aspiraciones.

Una cualidad destacada de las organizaciones llamadas “terroristas” es su sustantiva falta de ideología. El académico Louise Richardson de Harvard señaló que los movimientos terroristas no describen significativamente el nuevo mundo que tratar de crear.²⁴ Todos los movimientos terroristas, observa, “tienen dos clases de objetivos: objetivos organizativos a corto plazo y objeti-

vos políticos a largo plazo que requieren cambios políticos significativos”.²⁵ Señala que sus causas políticas son sobre el cambio de statu quo, no de ofrecer una visión alternativa del futuro.

El líder colombiano de las FARC, Paul Reyes, admitió que no podía definir un programa de gobierno. La descripción del futuro según el líder de los Tigres tameses, Velupillai Prabhakaran, era la de un simplista estado socialista. El checheno Shamil Basayev dijo que apoyaba el “poder para el pueblo”, sea lo que sea lo que ello significara. Abimael Guzmán del Sendero Luminoso desdeñó las preguntas sobre su visión del futuro, admitiendo que “no hemos estudiado esta pregunta suficientemente”.²⁶ Las FARC y el ELN de Colombia y el Sendero Luminoso de Perú se convirtieron en entidades criminales que se financian con el tráfico de drogas, pero todos declaran luchar por una ideología política. Excepto en el asunto de un cambio de régimen, es difícil distinguir mucho contenido en sus opiniones. No tratan de la forma exacta de gobierno, atención médica, trabajos de educación o artículos que definen lo que los partidos o actores políticos reales ofrecen.²⁷ Al-Qaeda no es diferente. Richardson observa que al definir su visión, Osama bin Laden fue “muy vago”.²⁸ El académico francés Olivier Roy convirtió a bin Laden en algo insignificante por su retórica vacía.²⁹

Por el contrario, los cárteles de drogas mexicanos son muy concretos al urdir una historia, una narrativa, un tema y un mensaje que tiene un significado particular para las audiencias a las que van destinados. La avaricia puede motivar a los cárteles, pero lo que les ha hecho efectivos es su capacidad de reclutar y movilizar a jóvenes mexicanos alienados mediante mensajes sobre lo que ofrecen los cárteles y no el estado: movilidad social, esperanza, oportunidad y prosperidad. Los cárteles de drogas mexicanos obtienen un 6.000 por ciento de beneficios del traficante al usuario; contando desde el precio de compra pagado a los cultivadores, el negocio produce un extraordinario rendimiento de beneficios del 150.000 %.³⁰ En dicho mercado lucrativo, los cárteles encuentran fácilmente muchos reclutas entre los empobrecidos mexicanos, particularmente en las plantas en ensamblaje de Juárez establecidas a raíz de NAFTA, que pagan de \$200 a \$300 al mes. Los cárteles, según se informó, pueden pagar hasta \$5.000 a los jóvenes por un solo acto de violencia.³¹

Los cárteles relatan una historia por la que se definen como enraizados en una imagen romántica del siglo XIX de un bandido robando al rico y una historia nacional en la que los mexicanos ricos y los inversores extranjeros han controlado gran parte de la economía, dejado a la mayoría de los mexicanos empobrecidos.³² Las baladas y los videos musicales de los cárteles descienden directamente de la tradición popular mexicana de idealizar a héroes y leyendas revolucionarias, excepto que las canciones de hoy glorifican a los capos de la droga.³³

Las canciones (*narco-corridos*), videos, medios sociales, letreros y pancartas (*narcomantas*) confieren un aspecto populista que celebra los orígenes humildes de los líderes de los cárteles y sus hazañas. Ricardo Ainslie señala que esta comunicación estratégica ha desplazado el terreno “de una izquierda política acostumbrada durante largo tiempo a un adversario definido como las élites de la nación y acostumbrada desde hace largo tiempo a considerarse a sí misma un movimiento que defendía a los oprimidos”.³⁴

Las narrativas ayudan a definir una cultura específica que atrae a los jóvenes que los cárteles reclutan de forma enérgica. Se manifiesta en la vestimenta: sombreros vaqueros chillones, botas de piel de avestruz, calzado deportivo pretencioso, gorras de béisbol de colores brillantes, ropa ajustada, artículos de joyería vulgares, casas ostentosas, automóviles rápidos, alcohol y una vida glamorosa que ofrece las mejores comidas, hermosas mujeres y acción. Los cárteles proporcionan una forma de vida que ofrece una identidad macho y orgullo a los que los reclutas no tienen otro medio de acceso.³⁵

El escritor Heriberto Yépez de Tijuana, al escribir en *Milenio*, observó acertadamente que los cárteles han evolucionado pasando de ser una economía a ser una ideología que satura la sociedad. El término narco se combina en “traficante de drogas” (*el narco*) y “vida de drogas” (*lo narco*). Yépez indica que narco era un adjetivo que describía un aspecto de la cultura mexicana.

Ahora es cultura: “narco y cultura son sinónimos”.³⁶ Los cárteles dan significado y ofrecen oportunidades concretas que influyen directamente en las normas, los valores, las creencias, las actitudes, la opinión y el comportamiento.

Los mensajes van dirigidos también a las fuerzas armadas. Los Zetas reclutan aprovechándose del hecho de que el salario mínimo en México es de cinco dólares al día, desplegando pancartas —*narcomantas*— preguntando, “¿Por qué ser pobre? Ven a trabajar con nosotros”.³⁷ Una pancarta de los Zetas que colgaba de una avenida importante indicaba: “El Grupo Operativo ‘los Zetas’ te quieren a ti soldado o ex-soldado. Ofrecemos un buen salario, alimentos y prestaciones para su familia. No sufran más malos tratos y no pasen hambre”. Los miembros de al menos un cartel, La Familia Michoacana, sucedidos ahora por los Caballeros Templarios, se consideran luchadores resistentes al crimen. Desarrollaron conocimientos expertos en poder blando para ganarse una credibilidad popular.³⁸ Adoptan una forma extraña de cristianismo y están a cargo de clínicas de rehabilitación de drogadictos. El cartel ofrece trabajos y organiza protestas populares contra el gobierno.³⁹ Por supuesto, hay un lado más oscuro. Los cárteles emplean la violencia dirigida para asegurar lealtad, vengarse, enviar mensajes, reclamar territorios y llenar vacíos de poder.⁴⁰ En otras palabras, los cárteles tienen una forma de pensar política que satisface esperanzas y aspiraciones, además de jugar con los temores, de sus audiencias elegidas.

Captura del poder político

Los cárteles también buscan el poder político de forma agresiva. Lo han logrado tan bien que Calderón reconoció, “Este comportamiento criminal [por parte de los cárteles] . . . se ha convertido en un reto para el estado, un intento de reemplazar el estado”.⁴¹ Han creado una atmósfera de temor e intimidación que deteriora la capacidad del gobierno de operar de manera normal para proporcionar seguridad o asegurar el bienestar de las personas. Las tácticas de intimidación han ahogado la libertad de prensa.⁴² Han “reemplazado o debilitado seriamente” al gobierno en un número creciente de estados mexicanos, incluso en algunos lugares se han convertido en un “gobierno paralelo”.⁴³ Según se informó, los cárteles se gastan *mil millones anualmente* en sobornar a la policía.⁴⁴ Han asesinado a candidatos políticos y militares y oficiales de policía de alto rango. Participan en campañas para subvertir el gobierno mexicano a todos los niveles.⁴⁵ Su extorsión ha obstruido el comercio.⁴⁶

Los Zetas son un ejemplo destacado de la razón por la que la policía normal no derrotará a los cárteles. Otros cárteles han aprendido la lección y han aumentado sus propias capacidades. Los Zetas, al reclutar entre las fuerzas de operaciones especiales de México y armarse con AK-47, dispositivos explosivos improvisados (IEDs), granadas propulsadas por cohete (RPGs) y ametralladoras de calibre 50, se han adiestrado en tácticas de infantería de pequeñas escuadras, usan bien los medios sociales, operan con capacidades de inteligencia refinadas y pueden convertirse fácilmente en una insurgencia encubierta. Será difícil para una fuerza de policía normal enfrentarse a este tipo de milicia.⁴⁷ Aunque no estamos de acuerdo con la forma en que Paul Kan caracteriza la guerra contra las drogas, estamos de acuerdo con muchas de sus ideas sobre cómo tratarla. Desde su punto de vista, cualquier estrategia que consista en enfrentarse primero a los Zetas es visionaria. Entre todos los cárteles, este presenta la máxima amenaza de convertirse de forma encubierta en un movimiento de insurgencia contra el gobierno.⁴⁸ Pero nadie debe subestimar la letalidad de los otros.

Christopher Ljungquist, aunque estaba preocupado por el efecto que podría causar el hecho de llamar a la guerra contra las drogas de México una insurgencia, resumió la opinión de que los cárteles son políticos al declarar que “el estado mexicano está combatiendo insurgencias poderosas y atípicas, armadas con un acceso prácticamente ilimitado a armas de fuego, incluidas baterías antiaéreas y financiado por un comercio experto en narcóticos ilegales por un valor de miles de millones de dólares”.⁴⁹ El anterior secretario de estado de los EE.UU. Hillary Clinton

está entre las personas que están de acuerdo en que México se enfrenta a una insurgencia, al haber declarado que los cárteles “están mostrando cada vez más y más indicios de insurgencias”.⁵⁰

Bard O’Neil y David Kilcullen, aunque no se referían a México específicamente, parecían estar de acuerdo en que una confrontación se considera una insurgencia solamente cuando está motivada políticamente y constituye un levantamiento político.⁵¹ La guerra contra las drogas de México cumple con esa definición. Es una guerra adaptada a una *nueva forma* de contrainsurgencia definida como “una lucha armada para el apoyo de la población” que requiere un método integrado y una unidad de esfuerzo para lograr la seguridad, la erradicación de las drogas, una reforma social, una reforma judicial, ofensivas contra la corrupción, asociaciones multinacionales con los vecinos más afectados por directa o indirectamente por los efectos de la guerra contra las drogas, y esfuerzos militares en forma de misiones especiales contra cárteles bien armados y adiestrados. Es un método iterativo único.⁵²

No todas las actividades criminales se consideran una insurgencia.⁵³ No obstante, la guerra contra las drogas mexicana es un conflicto de baja intensidad, y los cárteles pueden considerarse insurgentes, combatientes hostiles y terroristas. El hecho es que las líneas de separación entre crimen, terrorismo e insurgencia se están haciendo cada vez más borrosas. De hecho, la Administración para el Control de Drogas (DEA) de EE.UU. informa que las organizaciones terroristas extranjeras (FTO) designadas participantes en el mercado de drogas global han pasado de 14 grupos en 2003 a 18 en 2008.⁵⁴ Por lo tanto, es fundamental para Estados Unidos, cuyos intereses de seguridad vitales están relacionados con México así como con el resto del hemisferio en lo que se refiere a manejar y vencer en este conflicto, reconocer lo que está pasando en México y tratarlo de forma realista.

Un método diferente

Empezamos por dos realidades. Primero, las prioridades de México son detener la violencia y los secuestros, mientras que Estados Unidos se concentra en eliminar narcotraficantes y detener el flujo de drogas.⁵⁵ Hasta los primeros años del siglo XX, el negocio de las drogas en México era relativamente pacífico. Los ciudadanos de EE.UU. sufrieron, pero la situación dio buenos resultados para los mexicanos.⁵⁶ En segundo lugar, ninguna de las partes tiene una estrategia para manejar o vencer en esta guerra—un problema complicado por la extrema sensibilidad mexicana de que Estados Unidos intervendrá en su soberanía. El éxito requiere resolver estos retos. Aunque no hay soluciones rápidas, estas acciones merecen consideración:

- Hay que tratar la situación como si fuera un conflicto de baja intensidad contra insurgentes que son criminales y terroristas—y tratarlos como terroristas. No se debe negociar con los cárteles. Están en el negocio en el que desean estar. Los cárteles son un mal, y el mal no puede derrotarse. Debe erradicarse.
- Confiscar y restringir el acceso a las finanzas de los cárteles. Esto es importante ya que su riqueza les da un poder excepcional que debe destruirse. Un reto al que se enfrenta Estados Unidos es la negativa del Departamento del Tesoro de enfrentarse a la realidad de la guerra contra las drogas—o contraterrorismo—que requiere una combinación de operaciones policiales y especiales. El *Washington Post* informa que una propuesta de la Casa Blanca de centrarse en el activo de los cárteles fue rechazado por el Tesoro. Se debe rectificar ese error.⁵⁷ México podría agotar las cuentas bancarias y confiscar el activo de los cárteles. Estados Unidos podía proporcionar apoyo de inteligencia y técnicas para ayudar a localizar dicho activo y después dejar a México a que pasara a la acción. Si Estados Unidos confiscara dichos activos, debe compartirlo con México como incentivo para estimu-

lar la cooperación mexicana. Un elemento clave de este método consiste en interrumpir las relaciones que tienen los cárteles con las redes de terror internacionales.

- El trabajo con el gobierno mexicano para desarrollar misiones militares de fuerzas especiales evitará violaciones de los derechos humanos y dará buen resultado con una autoridad civil pero que tengan los conocimientos expertos y la capacidad militar para enfrentarse y derrotar ampliamente a adversarios armados como Los Zetas. El Presidente Nieto está pensando en no respaldar esta recomendación de crear una gendarmería nacional. Se llame como se llame la fuerza, México necesita una fuerza de misiones especiales efectiva bien adiestrada. Los críticos se preocupan de que los cárteles traten de subvertir y corromper dicha fuerza. Es seguro que harán ese esfuerzo. Pero México y Estados Unidos deben cooperar para asegurar una fuerza efectiva, adiestrada y que se retenga. Aunque no es una tarea fácil, no debe disuadirnos.
- Estados Unidos debe persuadir a Nieto del valor de la ayuda de EE.UU., particularmente en inteligencia, vigilancia y reconocimiento. El *Washington Post* informó el pasado abril que el ex-presidente Calderón había garantizado que aviones de espionaje de EE.UU. accedieran al espacio aéreo mexicano para recopilar inteligencia. Los drones de EE.UU. apoyaron a las patrullas de CBP, y se empleó cibertecnología para combatir el tráfico. El *Post* informó que Estados Unidos también estaba ayudando a establecer objetivos y examinar cuidadosamente haberes de inteligencia potencial.⁵⁸ En Irak, el General Stanley McChrystal formó una fuerza de tarea que contabilizó entre 11.000 y 13.000 miembros de al-Qaeda. Sus homólogos británicos contabilizaron otros 3.500.⁵⁹ Eso se logró mediante la combinación de un equipo que identificaba a los líderes terroristas clave y a los de los escalafones medios y los eliminaba. Los centros de fusión de EE.UU. y México se establecieron en Ciudad de México y Monterrey, informó el *Post*, así como en cuarteles regionales. Aparentemente, aunque la fuerza era más limitada que la fuerza de tarea de McChrystal, fue un paso adelante en el buen sentido.⁶⁰ Nieto puede rehusar dicha ayuda, pero debemos persuadirle de cambiar de curso y dejar claro que los intereses de EE.UU. vitales están en juego—y actuaremos de acuerdo a esto.
- Excepto por sus infantes de marina, que han demostrado ser relativamente efectivos, se deben emplear las fuerzas armadas de México con contención. Los que dicen que la mayor parte del personal militar no está adiestrado para tareas policiales tienen una razón válida. La experiencia de México en usar sus fuerzas armadas ha producido luces y sombras, a la vez que ha alienado a muchos mexicanos. Los infantes de marina de EE.UU. deben continuar sus esfuerzos para trabajar con los infantes de marina de México mediante asistencia de misión indirecta en adiestramiento y equipación.
- Los líderes mexicanos deben persuadir a su población, especialmente a sus élites (que posiblemente a menudo han ayudado, no luchado, a los cárteles),⁶¹ clase media, sindicatos y organizaciones de sociedades civiles para apoyar la lucha contra los cárteles—poner a punto final a los secuestros, a la extorsión, a los robos, al tráfico de seres humanos, al contrabando de armas y al tráfico de drogas. Calderón no puso unos cimientos políticos firmes para luchar en la guerra. El éxito requiere persuadir a los mexicanos de que sus propias vidas dependen de derrotar a los cárteles.⁶² El reto es difícil, pero Nieto no debe repetir los errores de Calderón.
- Trabajar con México para desarrollar una estrategia conjunta y apoyarla con los recursos necesarios. La violencia no afecta a todo el país. Un tercio de los estados mexicanos tienen niveles de violencia similares a Estados Unidos. Una estrategia debe concentrarse en las áreas más violentas; la capital, Ciudad de México, y el centro financiero, Monterrey; y

las áreas turísticas que contribuyen en gran medida a la economía de la nación, como Acapulco, León, San Miguel, Cuernavaca, Guadalajara y Toluca.

- Renovar la Iniciativa de Mérida.⁶³ Se dio demasiado dinero a los contratistas de EE.UU. y demasiado poco a los mexicanos que pudieron marcar una diferencia. México carece de los recursos necesarios para implementar debidamente las reformas institucionales y sociales necesarias para ganar esta guerra. Se trata de un reto a largo plazo, pero el éxito requiere lograr la justicia social en México. Podemos hacer más para ayudar y debemos hacerlo.
- Encontrar soluciones de gestión de fronteras con una división realista de responsabilidad entre Estados Unidos y México.
- Rescindir el Acuerdo de Brownsville, que firmó el anterior Procurador General Janet Reno en 1998. Este acuerdo carecía de la visión futura en que se forzaba a Estados Unidos a notificar al gobierno mexicano sobre las operaciones encubiertas en México. Ese acuerdo obstaculizó la labor de nuestras agencias de policía en los frentes sin un compromiso mexicano.
- Se debe revisar un método hemisférico mirando más allá de México a nuestros vecinos regionales. La guerra contra las drogas amenaza también a Canadá así como a Centro- y Sudamérica. Se deben coordinar acciones con las Fuerzas de Operaciones Especiales (SOF) canadienses para adiestrar a fuerzas armadas centro- y sudamericanas contranarcóticas y a las fuerzas armadas de Guatemala, El Salvador, Honduras y otros aliados latinos mediante la asistencia de las SOF para ayudarles a desarrollar unas capacidades de misiones especiales a fin de derrotar a los traficantes de drogas.

Estados Unidos debe abandonar la retórica derrotista sugiriendo que la guerra contra las drogas solo puede manejarse y no ganarse. Puede y debe ganarse. Pero eso requiere considerarla de forma realista y tomando medidas contra los cárteles para ayudar a México a controlar la situación estratégica. Aunque las fuerzas militares de uso general no son adecuadas para ganar este conflicto, las unidades de misiones especiales son esenciales para derrotar a las fuerzas de los cárteles muy armadas y a menudo bien adiestradas cuyas capacidades pueden superar cualquier capacidad policial normal. México está a la vuelta de la esquina, y muchas de las cosas que afectan sus intereses vitales están relacionados con los intereses vitales de EE.UU. Reconocer esa realidad es el principio, y es hora de pasar a la acción. □

Notas

1. Blog del Narco, *Dying for the Truth: Undercover inside the Mexican Drug War* (Morir por la verdad: encubierto en la guerra mexicana contra las drogas) (Sitio desconocido: Blog del Narco, 2012). El blog lo escriben de forma anónima periodistas mexicanos que ocultan su identidad para protegerse contra la violencia de los cárteles de drogas. El libro documenta la violencia en 2010. Nadie está seguro ya que se informa de muy pocos homicidios—solo el 5 por ciento. El resto es suposición. Durante la presidencia de Calderón, se estiman unas 60.000 muertes, pero otras 25.000 personas desaparecieron (no todas debido a crímenes). Clare R. Seelke y Kristin Finklea, U.S.-Mexican Security Cooperation: *The Mérida Initiative and Beyond* (Cooperación de seguridad de EE.UU.-México: más allá de la Iniciativa de Mérida), (Washington: Congressional Research Service [CRS], 12 de junio de 2013), 3, www.fas.org/sgp/crs/row/R41349.pdf; y “Mexican Military Takes Over Drug-Ridden Port” (Las fuerzas armadas mexicanas se apoderan de un puerto lleno de drogas), AFP, 4 de noviembre de 2013, <http://www.news24.com/World/News/Mexican-military-takes-over-drug-ridden-port-20131105-3>.

2. William C. Martin, “Cartels, Corruption, Carnage and Cooperation” (Cárteles, corrupción, matanzas y cooperación), en *A War That Can't Be Won* (Una guerra que no se puede ganar), editores Tony Payan, Kathleen Staudt y Z. A. Kruszewski (Tucson: University of Arizona Press, 2013), Kindle Loc. 1166/7339.

3. Marcos Pablo Molochnik, “President Felipe Calderon's Strategy to Combat Organized Crime” (La estrategia del Presidente Felipe Calderón para combatir el crimen organizado), en *A War That Can't Be Won* (Una guerra que no se puede ganar), Kindle Loc. 1728/7339.

4. David A. Shirk, "The Drug War in Mexico: Confronting a Shared Threat" (La guerra contra las drogas en México: la confrontación contra una amenaza compartida), Informe especial del Consejo de Relaciones Exteriores no. 60, Marzo de 2011, Kindle Loc. 74/933.
5. Paul R. Kan, *Cartels at War (Los cárteles en guerra)* (Washington: Potomac Books, 2012), 74.
6. Michael Kelly, "Mexican Cartels Are Recruiting US Soldiers as Hitmen, And the Pay Is Good" (Los cárteles mexicanos están reclutando a soldados de EE.UU. como mercenarios y la paga es buena), *Business Insider*, 5 de agosto de 2013, <http://www.businessinsider.com/cartels-are-recruiting-us-soldiers-as-hitmen-2013-8>.
7. "Mexico's Drug Lords: Kingpin Bowling" (Los capos de México: boliche para derribar a traficantes de drogas), *Economist*, 20 de octubre 2012.
8. "Drug Traffickers Have Stranglehold on Guatemala Says Top Prosecutor" (Los traficantes de drogas controlan Guatemala dice un fiscal del estado), *El País*, 23 de febrero de 2011; y Hal Brands, *Crime, Violence and the Crisis in Guatemala (Crimen, violencia y la crisis en Guatemala)*, (Carlisle Barracks, PA: Instituto de Estudios Estratégicos, 2010), 2.
9. Adam Elkus, "Gangs, Terrorists and Trade" (Bandas, terroristas y comercio), *Foreign Policy in Focus*, 12 de abril de 2007. Bandas salvadoreñas de Los Ángeles fundaron el MS-13.
10. Strategic Forecasting, Inc. (Stratfor), *Mexico in Crisis: Lost Borders and the Struggle for Regional Status (México en crisis: las fronteras perdidas y la lucha para lograr una categoría regional)* (Austin, TX: Stratfor, 2009), 197.
11. Vea Gregory E. Maggs, "Assessing the Legality of Counterterrorism Measures without Characterizing Them as Law Enforcement or Military Action" (Evaluación de la legalidad de las medidas de contraterrorismo sin caracterizarlas como un acción policial o militar), 80 Temp. L. Rev., 661 (2007), 3 (copia en línea), http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1826&context=faculty_publications.
12. Vea *Tennessee v. Garner*, 471 U.S. 1, 11 (1985); Manual de Campaña del Ejército de EE.UU. (FM) 27-10, *The Law of Land Warfare (La ley de la guerra terrestre)*, 1956, capítulo 2, sección II, párrafo 29, citando el anexo de la Convención de La Haya no. IV, 18 de octubre de 1907, que incorpora los reglamentos con respecto a las leyes y costumbres de la guerra terrestre, artículo 23(c); y Maggs, "Assessing the Legality of Counterterrorism" (Evaluación de la legalidad del contraterrorismo) 4. Vea también Jimmy Gurule y Geoffrey S. Corn, *Principles of Counter-Terrorism Law (Principios de la ley contra el terrorismo)* (St. Paul: West Group, 2010), 65; Manual de Campaña del Ejército 6-20-10, *Tactics, Techniques and Procedures for the Targeting Process (Tácticas, técnicas y procedimientos para el proceso de determinación de objetivos)*, 8 de mayo de 1996, capítulo 2. Vea generalmente "Protocolo adicional de las Convenciones de La Haya del 12 de agosto de 1949 y relacionado con las Protecciones de víctimas de los conflictos armados internacionales (1977), 1125 UNTS 3 (entrada en vigor el 7 de diciembre de 1978)"; y "Protocolo adicional de las Convenciones de Ginebra del 12 de agosto de 1949 y relacionado con la Protección de víctimas de conflictos armados no internacionales (1977), 1125 UNTS 609 (entrada en vigor el 7 de diciembre de 1978)."
13. La Autorización para usar la fuerza militar promulgada por el Congreso el 14 de septiembre de 2001, P. L. 107-40, autoriza "toda la fuerza necesaria y apropiada" contra personas que ayudaron a las organizaciones participantes en los ataques del 11S "para prevenir cualquier acto futuro de terrorismo internacional contra Estados Unidos."
14. Las citas que hace Kan de Michael Roth y Murat Sever, "The Kurdish Workers Party (PKK) as Criminal Syndicate: Funding Terrorism through Organized Crime" (El Partido de los Trabajadores Kurdos (PKK) como sindicato del crimen: financiación de terrorismo mediante el crimen organizado), *Studies in Conflict and Terrorism (Estudios de conflicto y terrorismo)* 30 (octubre de 2007): 903, para declarar que los cárteles están "(1) involucrados en actividades ilegales y frecuentemente necesitan los mismos suministros; (2) hacen uso de violencia excesiva y la amenaza de la violencia; (3) llevan a cabo secuestros, asesinatos y extorsión; (4) actúan en secreto; (5) retan al estado y sus leyes (a menos que estén financiadas por el estado); (6) disponen de líderes de reserva y soldados de a pie; (7) son muy adaptables, abiertos a innovaciones y son flexibles; (9) adoptan consecuencias letales para miembros anteriores que se hayan ido de grupo".
15. Kan, *Cartels at War (Los cárteles en guerra)*, 6-13.
16. Brad Freden, "The COIN Approach to Cartels: Square Peg in a Round Hole" (El método COIN contra los cárteles: como un pez fuera del agua), *Small Wars Journal*, 27 de diciembre de 2011, <http://smallwarsjournal.com/jrnl/art/the-coin-approach-to-mexican-drug-cartels-square-peg-in-a-round-hole>. Freden admite, no obstante, que algunos principios y prácticas de COIN pueden apoyar una estrategia policial para debilitar o destruir cárteles.
17. Shibley Telhami, *The Stakes (Lo que está en juego)* (Boulder, CO: Westview Press, 2002), 35. El enfoque de Telhami es distinguir entre las fuerzas hostiles o enemigas y los terroristas. Por ejemplo, señala que mientras que Estados Unidos considera que Hizbulá es una organización terrorista, otras partes, especialmente en Oriente Próximo, no lo consideran así, sino un movimiento político o religioso. *Ibid.*, 9.
18. Vea Juan Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare (La guerra del Tesoro: el inicio de una nueva era de guerra financiera)* (New York: Public Affairs, 2013).
19. Kan, *Cartels at War (Cárteles en guerra)*, 8.
20. *Ibid.*, 7; Vea también Payan, Staudt y Kruszewski, eds., *A War That Can't Be Won (Una guerra que no se puede ganar)*.
21. Tony Payan, "The Many Labyrinths of Illegal Drug Policy" (Los muchos laberintos de la política de drogas ilegales), en *A War That Can't Be Won (Una guerra que no se puede ganar)*, Kindle Loc. 352/7339.
22. Harold D. Lasswell, *Politics: Who Gets What, When and How (Política: quién obtiene qué, cuándo y cómo)* (Gloucester, MA: Peter Smith Publishing, 1990).

23. Maurice Cranston, "Ideology" (*Ideología*), *Enciclopedia Británica*, <http://www.compilerpress.ca/Competitiveness/Anno/Anno%20Cranston%20Ideology%20EB%202003.htm>. El filósofo francés Destutt de Tracy expuso las características afirmativas. Karl Marx consideró la ideología como un conjunto de creencias con las que la gente se engaña a sí misma—una teoría que expresaba lo que se les hacía creer en vez de lo que era verdad. *Ibid.*
24. Louise Richardson, *What Terrorists Want (Lo que quieren los terroristas)* (New York: Random House, 2006), 85.
25. *Ibid.*, 75. Hablar de diversos motivos que animan a las organizaciones terroristas, incluida venganza, publicidad, concesiones, causar desórdenes, provocar represión, hacer una muestra de fuerza.
26. *Ibid.*, 86–87.
27. W. Alex Sanchez, "The End of Ideologically Motivated Violent Movements in Latin America?" (¿El final de movimientos violentos motivados ideológicamente en Latinoamérica?), *e-International Relations*, 24 de septiembre de 2012, www.e-ir.info/2012/09/24/the-end-of-ideologically-motivated-violent-movements-in-latin-america/. Sánchez cae también en la trampa de las definiciones convencionales al no reconocer que los beneficios de las actividades ilegales pueden considerarse como una agenda criminal y política, aunque una no implica necesariamente la otra.
28. Richardson, *What Terrorists Want (Lo que quieren los terroristas)*, 86.
29. Olivier Roy, trans. Carol Volk, *The Failure of Political Islam (El fracaso del Islam político)* (Cambridge: Harvard University Press, 1994). Roy dice de forma persuasiva que el Islam político no ha definido una visión concreta y, en la medida en que se haya hecho una, se parece más a políticos izquierdistas radicales que a una religión.
30. Ioan Grillo, *El Narco*, (London: Bloomsbury Press, 2011), Kindle Loc. 2747/6409.
31. "Teens Lured into Mexican Drug Cartels" (Jóvenes atraídos a los cárteles de drogas mexicanos), *Big Country* (Nexstar Broadcasting, Inc.), 19 de abril de 2009, www.bigcountryhomepage.com/story/teens-lured-into-mexican-drug-cartels/d/story/cSPztt2XMEW2GeUVZ-XmRQ.
32. Watt y Zepeda, *Drug War in México (La guerra de las drogas en México)*.
33. Sylvia Longmire, *Cartel (Cártel)* (New York: Palgrave MacMillan, 2011), 102.
34. Ricardo C. Ainslie, *The Fight to Save Juárez (La lucha para salvar a Juárez)* (Austin: University of Texas Press, 2013), Kindle Loc. 4206/6219.
35. Grillo, *El Narco*.
36. Citado en Josh Kun, "Death Rattle" (Estertor agónico), *American Prospect*, 5 de enero de 2012, <http://prospect.org/article/death-rattle>.
37. Ashley Fantz, "The Mexico Drug War: Bodies for Billions" (La guerra de drogas mexicana: cuerpos para miles de millones), *CNN.com*, 20 de enero de 2012, <http://www.cnn.com/2012/01/15/world/mexico-drug-war-essay/index.html>.
38. Kan, *Cartels at War* (Los cárteles en guerra, 43–45; y Akbar Khan, "The War on Drugs: Mexican Cartels" (La guerra de las drogas: los cárteles mexicanos), *Generation.net*, 29 de mayo de 2013, <http://the-generation.net/the-war-on-drugs-mexican-cartels/>. Kan cita a un observador que llama a la Familia Michoacana un "movimiento socialista, populista, de derechas y religioso" dirigido por una organización criminal.
39. Tim Padgett y Ioan Grillo, "Mexico's Meth Warriors" (Los guerreros de la metanfetamina de México) *Time*, 28 de junio de 2010, <http://content.time.com/time/magazine/article/0,9171,1997449,00.html>; y William Finnegan, "Silver or Lead" (Plata o plomo), *New Yorker*, 31 de mayo de 2010, www.newyorker.com/reporting/2010/05/31/100531fa_fact_finnegan?currentPage=all.
40. Kan, *Cartels at War (Cárteles en guerra)*, capítulo 2, describe bien el plan comercial que emplean los cárteles.
41. Payan, "Many Labyrinths of Illegal Drug Policy" (Muchos laberintos de política de drogas ilegal).
42. Blog del Narco, *Dying for the Truth (Morir por la verdad)*; Oscar Villalon, ed., *Blood Calls to Blood: Mexican Writers on the Drug War (La sangre llama a la sangre: los escritores mexicanos en la guerra de las drogas)* (San Francisco: By Liner, 2012); Alfredo Corchado, *Midnight in Mexico: A Reporter's Journey Through a Country's Descent into Darkness (Medianoche en México: el viaje de un reportero durante el descenso de un país a la oscuridad)* (New York: Penguin Press, 2013); Ainslie, *Fight to Save Juárez (La lucha para salvar a Juárez)*; y Guadalupe Correa-Cabrera y José Nava, "Drug Wars, Social Networks and the Right to Information" (Las guerras de drogas, las redes sociales y el derecho a la información), en *A War That Can't Be Won (Una guerra que no se puede ganar)*.
43. Payan, "Many Labyrinths of Illegal Drug Policy" (Muchos laberintos de la política de drogas ilegales). Vea también Ed Vulliamy, *Amexica: War along the Borderline (Amexica: la guerra a lo largo de la frontera)*. (Farrar, Strauss y Giroux, 2010), 246. Shawn Teresa Flanigan ha trazado unos paralelos interesantes entre los cárteles de drogas mexicanos y Hamás y Hizbulá. Todos están relacionados con ubicaciones geográficas relativamente definidas. Todos buscan controlar un territorio específico para mantener el acceso a las rutas de comercio de drogas. Todos tienen relaciones refinadas profundas con los estados dentro de los que operan. Vea Flanigan, "Terrorists Next Door? A Comparison of Mexican Drug Cartels and Middle Eastern Terrorist Organizations" (¿Terroristas a la vuelta de la esquina? Una comparación de los cárteles de drogas mexicanos y las organizaciones terroristas de Oriente Próximo), *Terrorism and Political Violence (Terrorismo y violencia política)* 24, no. 2 (2012): 279–94.
44. Payan, "Many Labyrinths of Illegal Drug Policy" (Muchos laberintos de la política de drogas ilegales).
45. *Fight to Save Juárez (La lucha para salvar a Juárez)* de Ainslie ofrece un relato apasionante del baño de sangre en esa ciudad debido a la violencia del cártel. Es un estudio excelente sobre cómo el gobierno de México ha fracasado para hacer frente a esta lucha. Vea también George W. Grayson, *Mexico: Narco-Violence and a Failed State? (México: ¿narcoviolencia*

y un estado fallido) (New Brunswick, NJ: Transaction Publishers, 2009). Existen muchos informes sobre el problema de corrupción.

46. Vea Vulliamy, *Amexica*, 247. Explica con gran detalle la extorsión practicada incluso entre pequeños comerciantes.

47. George W. Grayson y Samuel Logan, *The Executioner's Men (Los hombres del verdugo)* (New Brunswick: Transaction Publishers, 2012); y Longmire, *Cartel (Cártel)*.

48. Kan, *Cartels at War (Los cárteles en guerra)*, 150–51.

49. Christopher S. Ljungquist, “Mexican Cartel War: Profiling an Unorthodox Insurgency” (La guerra de los cárteles mexicanos; análisis de una insurgencia poco ortodoxa) *Geopolitical Monitor*, 4 de febrero de 2013, <http://www.geopoliticalmonitor.com/mexican-cartel-war-profiling-an-unorthodox-insurgency-4777>.

50. “Clinton Says Mexico Drug Crime like an Insurgency” (Clinton dice que los crímenes de drogas de México son como una insurgencia), *BBC News*, 9 de septiembre de 2010, <http://www.bbc.co.uk/news/world-us-canada-11234058>.

51. Bard O’Neil, *Insurgency and Terrorism: From Revolution to Apocalypse (Insurgencia y terrorismo: de la revolución al Apocalipsis)*, 2ª edición (Washington: Potomac Books, 2005); y David J. Kilcullen, “Three Pillars of Counterinsurgency” (Tres pilares de la contrainsurgencia), declaraciones hechas en el Congreso de Contrainsurgencia del Gobierno de EE.UU. en Washington, DC, 28 de septiembre de 2006, citados ambos en Freden, “COIN Approach to Mexican Drug Cartels” (Método de COIN contra los cárteles de drogas mexicanos).

52. Manual de Campaña del Ejército FM 3-24.2, *Tactics in Counterinsurgency (Tácticas de contrainsurgencia)*, abril de 2009, <https://www.fas.org/irp/doddir/army/fm3-24-2.pdf>.

53. Las organizaciones terroristas y los grupos criminales puede tener conexiones periféricas (posiblemente, al Qaeda). Las organizaciones terroristas pueden tener simpatizantes criminales (posiblemente, Hizbulá). Los empresarios criminales pueden actuar como especialistas o facilitadores en la sombra para grupos terroristas (posiblemente, Viktor Bout, Abu Ghadiyah, Monzer al-Kassar). Los grupos terroristas y las organizaciones criminales pueden colaborar (posiblemente, el Talibán y los traficantes de drogas). Vea <http://fpc.state.gov/documents/organization/141615.pdf>.

54. Declaraciones de Stephen W. Casteel (DEA) y Raphael Perl (CRS), “Narco-Terrorism: International Drug Trafficking and Terrorism—A Dangerous Mix” (El narcoterrorismo: tráfico de drogas internacional y terrorismo—una mezcla peligrosa), preparado para una audiencia llevada a cabo por el Comité Judicial del Senado, 20 de mayo de 2003; y Michael Braun, “Drug Trafficking and Middle Eastern Terrorist Groups: A Growing Nexus?” (El tráfico de drogas y los grupos terroristas de Oriente Próximo) discurso en el Instituto Washington para Políticas de Oriente Próximo, 18 de julio de 2008. El CRS observa que el gobierno de EE.UU. carece de una estrategia o una política para tratar de forma completa la confluencia del terrorismo y el crimen transnacional. John Rollins y Liana S. Wyler, *International Terrorism and Transnational Crime: Security Threats, U.S. Policy and Considerations for Congress (El terrorismo internacional y el crimen transnacional: amenazas de seguridad, política de EE.UU. y consideraciones para el Congreso)*, (Washington: CRS, 18 de marzo de 2010), 4:

55. Dana Priest, “U.S. Role at a Crossroads in Mexico’s Intelligence War on the Cartels” (La función de EE.UU. en una encrucijada en la guerra de inteligencia de los cárteles de México), *Washington Post*, 27 de abril de 2013, http://www.washingtonpost.com/investigations/us-role-at-a-crossroads-in-mexicos-intelligence-war-on-the-cartels/2013/04/27/b578b3ba-a3b3-11e2-be47-b44febada3a8_story.html.

56. Vea Pamela F. Izaguirre, “Narco-Politics: How Mexico Got There and How It Can Get Out” (Narcopolítica: cómo ha llegado México hasta allí y cómo puede salir de allí), Council on *Hemispheric Affairs (Consejo sobre asuntos hemisféricos)*, 22 de agosto de 2013, www.coha.org/narco-politics-how-mexico-got-there-and-how-it-can-get-out/.

57. Priest, “U.S. Role at a Crossroads” (La función de EE.UU. en una encrucijada).

58. *Ibid.*

59. Mark Urban, *Task Force Black (Fuerza de tarea Negra)* (Little, Brown, & Co., 2011).

60. Priest, “U.S. Role at a Crossroads” (La función de EE.UU. en una encrucijada).

61. Watt y Zepeda, *Drug War in México (La guerra de las drogas en México)*.

62. Vea James P. Farwell, *Persuasion and Power: The Art of Strategic Communication (Persuasión y poder: el arte de las comunicaciones estratégicas)* (Washington: Georgetown University Press, 2012); y Longmire, *Cartel*. Longmire presenta una descripción excelente de esos retos y cómo Calderón los percibió y los trató.

63. Seelke and Finklea, *U.S.-Mexican Security Cooperation*, 3. See also Craig A. Deare, “U.S.-Mexico Defense Relations: An Incompatible Interface,” Strategic Forum, Institute for National Strategic Studies, National Defense University, July 2009; and Statement of Assistant Secretary of State for International Narcotics and Law Enforcement Affairs William Brownfield, US House Committee on Foreign Affairs, Subcommittee on the Western Hemisphere, “U.S.-Mexico Security Cooperation: An Overview of the Merida Initiative 2008–Present,” 113th Cong., 1st sess., *CQ Congressional Transcripts*, 23 May 2013.



El Dr. James P. Farwell, PhD, es un experto de seguridad nacional que ha sido consejero del Mando de Operaciones Especiales de EE.UU. Tiene un título de Doctor en Jurisprudencia de la Universidad Tulane y un DCLS en ley comparativa de la Universidad de Cambridge. Es el autor de *Persuasion and Power: The Art of Strategic Communication* (Persuasión y poder: el arte de las comunicaciones estratégicas) (Georgetown University Press, 2012).



La Sra. Darby Arakelian es una experta de seguridad nacional y ex-oficial de la CIA. Tiene un BA en ciencias políticas, ruso y economía de la Universidad de Denver y un MA de estudios de políticas de seguridad de la Universidad George Washington. La Sra. Arakelian se especializa en estrategia y análisis de comunicaciones de terrorismo y contraterrorismo, ciberguerra y monitoreo y análisis de medios automatizados.

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, por sus siglas en inglés), el Ejército Rojo Japonés (JRA, por sus siglas en inglés), 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 en 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 el 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, buscara 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 liberara 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 una 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 chiitas, 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 a 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 ampliara 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, solo 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 en 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 capturaran. 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 de América del Sur (TBA), 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 solo 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).

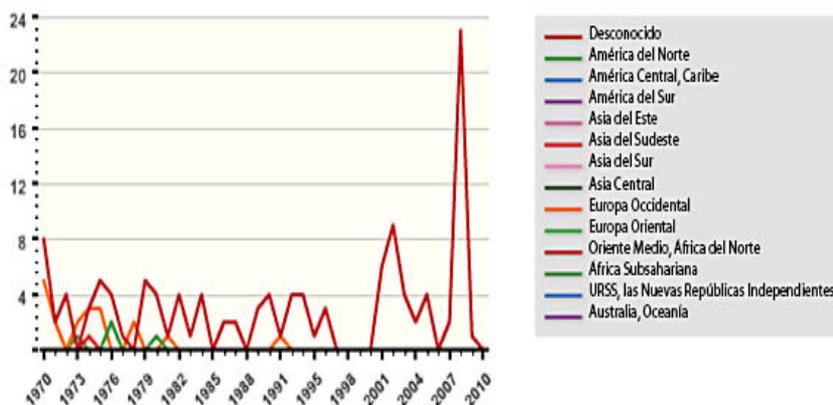


Figura 1. Ataques del FPLP por región

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-

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.

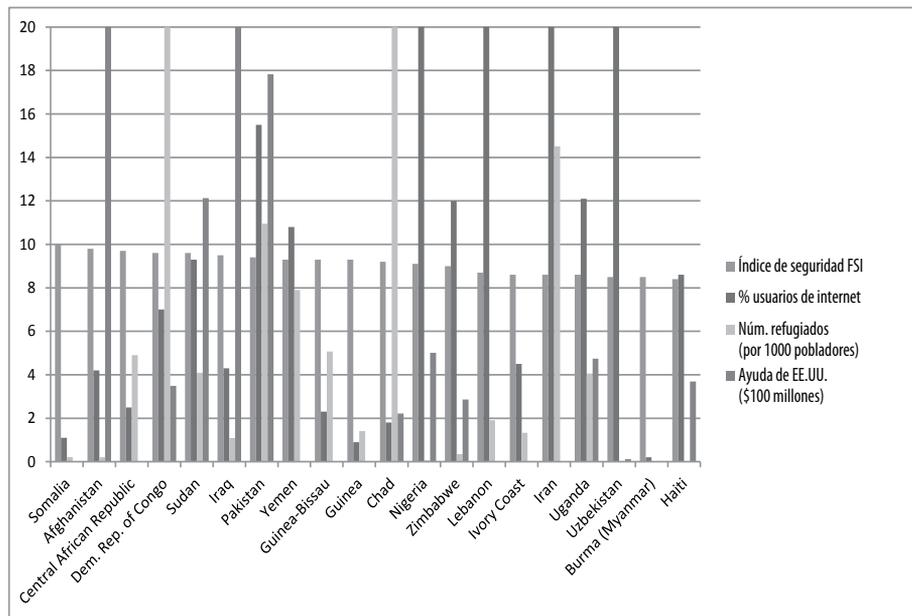


Figura 2

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 solo 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/NSQJ28210E.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://abc-news.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/professional-writing/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/africa.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 2011: 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.

La Confianza Agotada en el Espacio Cibernético Común*

DR. ROGER HURWITZ, PHD

Las autoridades responsables de formular una política reconocen cada vez más la necesidad de contar con acuerdos para regular los comportamientos cibernéticos a nivel internacional. En el 2010, el Grupo de Expertos Gubernamentales sobre Desarrollos en los Campos de Información y Telecomunicaciones en el Contexto de la Seguridad Internacional de las Naciones Unidas recomendaron “el diálogo entre los estados para discutir normas relacionadas con el uso del estado de la tecnología de información y comunicaciones (ICT, por sus siglas en inglés), para reducir el riesgo colectivo y proteger la infraestructura crítica nacional e internacional”.¹ Desde entonces, Estados Unidos, Rusia, China y otras potencias cibernéticas han propuesto normas para discusión y, en noviembre de 2011, el Reino Unido convocó una conferencia intergubernamental para discutir sobre las “reglas del juego” cibernéticas.² Estas actividades son un cambio positivo de la primera década de este siglo, cuando Estados Unidos y Rusia no podían llegar a un acuerdo sobre lo que se debía discutir y el acuerdo internacional existente para el ciberespacio—la Convención de Budapest sobre Delitos Informáticos—no cobró mucha fuerza. La Secretaria del Departamento de Seguridad Interna, Janet Napolitano, destacó en el verano de 2011 que los intentos de contar con “un marco internacional exhaustivo” para gobernar comportamientos cibernéticos aún estaba en una “etapa inicial”.³ Puede que esa búsqueda sea desconcertante. Adam Segal y Matthew Waxman, miembros del Consejo sobre Relaciones Exteriores, advierte que “la idea de negociar en un final un tratado de seguridad cibernética mundial y exhaustivo es un sueño imposible”. Según su opinión, las diferencias en ideologías y prioridades estratégicas evitarán que Estados Unidos, Rusia y China lleguen a acuerdos significativos: “Con Estados Unidos y las democracias europeas en un extremo y China y Rusia en otro, los estados discrepan marcadamente en cuanto a temas tales como si las leyes de guerra internacionales y la autodefensa deben aplicar a los ataques cibernéticos, el derecho a bloquear información de los ciudadanos y los papeles que actores privados o cuasi privados deben desempeñar al gobernar la *Internet*”.⁴

Este ensayo se une a ese pesimismo con base en un modelo más extenso de la crisis emergente en el ciberespacio. El argumento esencial es que mantener un ciberespacio seguro significa sostener un espacio común que beneficie a todos los usuarios, pero su sobreexplotación por parte de usuarios individuales resulta en la muy conocida tragedia del espacio común”.⁵ Aquí el recurso común que se puede agotar es la confianza, mientras que los usuarios son naciones, organizaciones e individuos cuyos comportamientos en el ciberespacio no están sujetos a una autoridad central. Sus acciones, que dañan el bienestar de otros usuarios, disminuyen la confianza y la cantidad de sobreexplotación de un recurso común. La tragedia del espacio común se emplea repetidamente como un argumento para la privatización y en retrospectiva para justificar el cercamiento de tierras de los capitalistas agrícolas ingleses en los siglos XVII y XVIII. No obstante, tal tragedia no es inevitable, inclusive cuando los usuarios de un espacio común se suponen sean sensatos en el sentido de maximizar el interés propio. La finada politóloga Elinor Ostrom recibió el Premio Nobel en economía por determinar casos y condiciones en las que, en ausencia del control del gobierno, los usuarios exitosamente se auto organizan para el uso sostenible de un espacio común.⁶ Lamentablemente, tal como se discute a continuación, el estado

* Reimpreso de nuestra AU Revista Strategic Studies Quarterly, Vol 6, Nº 3, Fall 2012.

actual del ciberespacio y sus usuarios no cumple con la mayoría de las condiciones que exhortan esa autoorganización. Ambas posibilidades de las tecnologías cibernéticas—es decir, la manera como las tecnologías hacen posible su uso—y las mentalidades de los usuarios contribuyen al resultado desfavorable.

Incorporar los obstáculos a los acuerdos internacionales dentro de esta perspectiva más amplia hará resaltar los procesos de varios niveles, complejos y transformativos que el ciberespacio les presenta a los estados y a otras entidades que lo administrarían. No es un ámbito pasivo en el que los estados pueden ir en busca de sus intereses preexistentes competitivos o en conflicto, sino uno cuyas tecnologías y aplicaciones que cambian rápidamente crea oportunidades para el conflicto. Además, motiva la cooperación. Por consiguiente, la siguiente sección crea el modelo del ciberespacio como un sistema social basado en un espacio común—un “sistema socio-ecológico” (SES, por sus siglas en inglés) y un “recurso de uso común” (CPR, por sus siglas en inglés) para emplear la terminología de Ostrom—que se puede sostener pero también agotar. La identificación de la confianza como este “recurso” y las implicaciones de su agotamiento recibirán atención particular. En la tercera sección se revisan las variantes que Ostrom y sus colegas han descubierto que fomentan la autoorganización y las evalúa con respecto al ciberespacio. En la última sección se analiza cuáles de las variantes del modelo actualmente desalientan que la autoorganización se puede cambiar en una dirección más alentadora mediante acciones factibles por parte de agentes, eliminando así algunos obstáculos para lograr acuerdos internacionales. También se analiza cómo los estados, a falta de estos cambios, pueden responder unilateralmente a las crisis de la seguridad cibernética.

Los retos del espacio común cibernético

Gobernar un recurso de uso común accesible, o CPR, es un problema de acción colectiva, ya sea que la meta es la explotación sostenible de la industria pesquera o el uso seguro y beneficioso del ciberespacio. Para los CPR naturales, donde ocurre la regeneración de existencias, se necesitan algunos límites en el uso por parte de individuos por cantidad o clase, a menos que el uso final sobrepase la “capacidad de carga”. Esto agota el recurso por debajo del nivel al cual los procesos naturales pueden sostenerlo para una explotación provechosa. Tal como se discute a continuación, esta necesidad de limitar la explotación también puede aplicarse a recursos hechos por el hombre, o artificiales, como el ciberespacio. Limitar o regular el uso por lo regular requiere un estado preexistente u otra autoridad con poder coercitivo, en cuyo territorio se encuentra el CPR—por buenos motivos. Aunque los usuarios podrían aceptar la necesidad de contar con límites, los usuarios individuales están tentados a excederlos creyendo que una presión accidental en el recurso es insignificante con respecto a su sostenibilidad. Además, individuos que se dan cuenta de las infracciones de sus vecinos no estarían dispuestos a sancionarles por temor a represalias. No obstante, Ostrom encontró muchos casos en que las personas administraron exitosamente un CPR sin la necesidad de intervención o privatización por parte del estado. Al analizar esos casos, ella conceptualiza el CPR como que existe dentro de un contexto de las prácticas socioeconómicas y culturales de sus usuarios. Estas prácticas inciden tanto en las opciones de los usuarios individuales acerca de explotar el CPR y en la posibilidad de su regulación colectiva de sostenerlo. Juntos, el CPR y el contexto social, constituyen el sistema socioecológico (SES, por sus siglas en inglés).

Uno se preguntaría cómo un ámbito puede ser un espacio común cuando cada porción de su sustrato físico le pertenece a alguna organización o estado a diferencia de, por ejemplo, los océanos, el espacio aéreo internacional y el espacio exterior. Varias respuestas son útiles para perfeccionar nuestra noción de un espacio común cibernético y cualesquier acuerdos internacionales que lo protegerían. Lawrence Lessig aludió a un modelo de transporte de comunicación por *Internet* que incluye capas para el sustrato físico, los paquetes o sobres electrónicos para

la información y el contenido en sí de la información. Él identificó el espacio común con la capa de paquete, a la cual todos tienen derecho al acceso y a la cual todos pueden contribuir, de manera que cualquier flujo de paquetes cierra el espacio común.⁷ Desde este punto de vista, el espacio común cibernético es similar a los océanos o el espacio aéreo internacional, con el derecho de paso siendo la inquietud principal de los usuarios.⁸ En un final Lessig y otros basaron esta idea del espacio común cibernético en el derecho humano de acceso a la información y libertad de expresión. También resonó con nociones de libertad de movimiento, innovación global para la *Internet* y una esfera evolutiva de información mundial en la que todos pudiesen participar—con la resonancia captada en una palabra: “abierta”. Esfuerzos como *Wikipedia*, *Creative Commons*, cursos gratis de MIT y la blogósfera emergente podrían crear un segundo espacio común—uno de contenido. Con el cambio de milenio, Lessig se percató que esos esfuerzos eran amenazados por empresas de contenido de medios de comunicación, con sus interpretaciones amplias de derecho de autor a expensas del uso justo y su reclutamiento de autoridades estatales para el trato draconiano de presuntas infracciones a los derechos de autor. Él pasó por alto el argumento de una necesidad de proteger el agotamiento de los recursos intelectuales al invocar la imagen de Thomas Jefferson de una vela cuya luz no es disminuida al prender otra vela—un tropo para el Siglo de las Luces que sintetiza la promesa de la *Internet*. El drama en desarrollo fue en el cambio de organizaciones avariciosas utilizando las posibles fechorías de unos cuantos individuos como un pretexto para privatizar la propiedad intelectual común y socavar el acceso necesario para sostener una cultura de *Internet*.⁹

Esta idea de “un espacio común cibernético” apareció hace más de una década, cuando la población en línea era un décimo de su tamaño actual y estaba concentrada en América del Norte y Europa occidental, donde a la *Internet* se le consideraba como otro lugar en una ecología de información y comunicación rica y ligeramente regulada. Sin embargo, pasaba por alto que la *Internet* ya la estaban usando grupos en una lucha violenta contra algunos estados—separatistas chechenos contra Rusia—e inclusive estados liberales ya estaban excluyendo el acceso y la distribución de cierta información, como por ejemplo la pornografía infantil. Desde ese entonces, el uso del ciberespacio, que ahora se extiende mucho más allá de la *Internet*, se ha tornado un problema de seguridad nacional tan omnipresente (“securitización”) o una amenaza a la estabilidad del régimen, que ahora muchos gobiernos filtran o bloquean ciertos flujos de paquetes, por ende reemplazando el espacio común cibernético principal con sus propios recintos “seguros”.¹⁰ No obstante, la visión de un espacio común cibernético notifica partes significativas de las políticas cibernéticas de Estados Unidos y muchos de sus aliados y las posturas que toman con respecto a la regulación internacional del ciberespacio. La adopción más notable es la del Departamento de Estado en cuanto a la libertad en la *Internet*—los derechos de habilitación cibernética del activismo cívico—pero el énfasis en la interoperabilidad global, la no interferencia por parte de estados con paquetes atravesando sus territorios y las decisiones en cuanto a la tecnología de *Internet* llevadas a cabo por tecnólogos en lugar de autoridades políticas son también significativas.¹¹

Sin embargo, un CPR más fácil de identificar, de acuerdo con el modelo SES de Ostrom, es el ancho de banda, el cual puede ser agotado por un *spam*—una sobreexplotación del recurso—resultando en una entrega degradada de comunicaciones más valiosas. Los *spammers* han sido comparados con los contaminantes industriales del espacio común de los recursos naturales porque ellos también le transmiten al público en general las externalidades negativas de sus acciones, ya sean en la forma del tiempo de espera de los usuarios en una red saturada o costes adicionales para más ancho de banda, filtros *antispam*, etc.¹² El fenómeno del *spam* se puede generalizar a las consecuencias del agotamiento del “sentido de seguridad” del público en general; como un producto secundario de los fraudes y robos de identidad en línea al nivel individual y ataques a la infraestructura, como Stuxnet, a nivel nacional. Estas incitan demandas amplias para medidas de ciberseguridad, que son gastos. El suministro de esas medidas, que por lo regu-

lar dan poco resultado, tiene poco efecto en refrenar las amenazas, disminuye la eficacia económica de las comunicaciones y control basado en la cibernética. En vista de que la capacidad de la *Internet* de disminuir los costes en las transacciones es considerada uno de sus beneficios principales para el desarrollo económico y social, los posibles costes elevados de la seguridad cibernética son retardadores para muchos estados y organizaciones, quizás tan retardadores como las consecuencias de ataques a falta de una seguridad adecuada.¹³

El ciberespacio como sistema social

Relacionado muy de cerca con esa inseguridad está el descenso en la confianza pueblo o social, que podría identificarse como el recurso de uso común fundamental en el SES cibernético. Jacques Bus concuerda con el sociólogo Nicolas Luhmann en explicar la confianza como “un mecanismo que disminuye la complejidad y le permite a las personas lidiar con los niveles elevados de incertidumbre y complejidad de la vida (contemporánea)”. Él agrega lo siguiente,

la confianza amplía la capacidad de las personas de poder relacionarse exitosamente con un mundo real cuya complejidad e imprevisibilidad es mucho mayor de lo que somos capaces de aceptar. En este sentido es un mecanismo necesario para que las personas vivan su vida: para comunicarse, cooperar, llevar a cabo transacciones económicas, etc. Enriquece la vida del individuo al exhortar actividad, audacia, aventura y creatividad y enriqueciendo el alcance de las relaciones del individuo con otras personas.¹⁴

La noción de la confianza de los ciudadanos, como se emplea en este documento, también incluye la confianza de las personas en las instituciones, leyes, gobierno e infraestructuras de sus sociedades. La confianza de los ciudadanos con respecto al ciberespacio exhorta a los individuos y a las organizaciones a tener acceso y poder ser consultados entre sí en línea, y que a su vez permite el efecto de red en el ciberespacio; o sea, las externalidades positivas creadas a medida que más personas participan en la red y ocurren más interacciones. Esto es consistente con los hallazgos de científicos sociólogos de correlaciones positivas fuertes entre la confianza de los ciudadanos y el crecimiento económico.¹⁵

La confianza del pueblo en el ciberespacio incluye la confianza en las personas y en las organizaciones con las que los individuos lidian a través de tecnologías digitales y la honradez de las tecnologías en sí. La confianza en otros en línea es problemática porque esos otros podrían ser anónimos o identificados parcialmente, y el contexto de las interacciones con ellos es opaca o confusa. Puede estar respaldada por suposiciones acerca de las inquietudes de otros sobre la reputación y el compromiso con funciones y mecanismos en línea, como por ejemplo certificados y clasificaciones, que pueden confirmar afirmaciones hechas por otros. Sin embargo, últimamente, la confianza en el ciberespacio puede tornarse tensa por la publicidad de las diferentes amenazas cibernéticas mencionadas anteriormente, el fracaso de organizaciones y gobiernos de disuadirlas y el compromiso de los mecanismos de seguridad en línea, como certificados robados. Además, la confianza de los ciudadanos se ve afectada porque muchos usuarios están conscientes que sus actividades en línea se están vigilando, ya sea para la explotación comercial en occidente o para identificar disidentes políticos en países autoritarios.

Estos abusos podrían mermar la confianza del pueblo—o sea, la voluntad agregada de los usuarios de entrar en línea—muy parecido a la sobreexplotación por parte de algunos de sus usuarios que agota un CPR. Desde este punto de vista, la confianza de los ciudadanos es un buen rival cuyo consumo por un usuario disminuye la cantidad de consumo disponible por otros. Por analogía, los abusos en curso contra una cantidad decreciente de confianza del pueblo podrían dar lugar a una provisión no satisfactoria de beneficios en línea que la confianza de los ciudadanos permite. En términos concretos, los individuos y las organizaciones que le temen al delito cibernético, a las invasiones de la privacidad, etc., disminuirían en gran medida su uso de las

redes digitales para transacciones económicas, intercambio de información e interacciones sociales. Pero a diferencia de los recursos de uso común, como los bosques y la industria pesquera, la confianza del pueblo en el ciberespacio no siempre es un buen rival. Las interacciones en línea mutuamente beneficiosas se sostendrán y aumentarán, y éstas son tan numerosas a los niveles individual e institucional que a menudo los abusos se pasan por alto o se olvidan rápidamente. Por consiguiente, hay pocas pruebas de personas saliendo del ciberespacio o evitando sitios populares con políticas de privacidad controversiales. Aún, en algunos países democráticos, los ciudadanos relevantes han exigido que los proveedores de servicio e investigación refrenen el rastreo; algunos gobiernos ya han respondido con políticas regulatorias que obligarán a los compiladores y analistas de datos a hacer ajustes. Estas acciones se pueden interpretar como situaciones en las que los usuarios defienden un CPR acudiendo a la autoridad actual en busca de liderazgo y establecimiento de normas. Ellas muestran que para sostener la confianza en el ciberespacio requiere, además de tecnologías de seguridad, reglas, prácticas transparentes, normas de responsabilidad y medios de compensación aceptables a los usuarios. Los esfuerzos internacionales de lograr acuerdos para proteger y sostener el ciberespacio tendrán, por lo tanto, que tomar en cuenta esas inquietudes, hasta cierto punto. Puede que ese no sea un reto formidable. En vista de que las “aplicaciones” cibernéticas se han tornado indispensables para muchos usuarios, puede que sean aseguradas, por lo menos momentáneamente, por pasos pequeños y superficiales por parte de los proveedores o reguladores, inclusive avisos sobre la política, botones de “inhabilitar” y nuevos, y quizás incomprensibles, acuerdos de servicio. En otras palabras, el ciberespacio ya no es un ámbito aparte para sus usuarios, un lugar para visitar cuando uno lo decide, como un lugar para turistas, sino que ha penetrado y vuelto a tejer la tela de nuestras vidas.¹⁶

Podría decirse que los *spammers*, hackers, recopiladores de datos, pandillas de delincuentes, activistas cibernéticos y agencias estatales que amenazan la confianza de los ciudadanos no buscan destruir la *Internet* o congelar el ciberespacio—no más que los campesinos quienes supuestamente pastoreaban excesivamente el espacio común querían degradarlo. La obra de Ostrom implica que dos tipos de agentes dañan el CPR: los cazadores furtivos fuera del grupo que mantiene al SES y los miembros del grupo que sobrepasan sus derechos al CPR. En este caso, los delincuentes cibernéticos, los terroristas y ciertos activistas—por ejemplo Lulzsec—serían los cazadores furtivos en el ciberespacio. En la imaginación popular, y a menudo en sus propias imaginaciones, ellos ocupan la imagen de piratas—individuos o grupos fuera de los países y más allá de las leyes de las naciones.¹⁷ De hecho, algunos analistas opinan que la cooperación internacional para contener esos grupos se puede realizar fácilmente y constituye el primer paso hacia acuerdos más exhaustivos sobre el ciberespacio. Por supuesto, en calidad de cazadores furtivos o parásitos, estos grupos no buscan la destrucción del ciberespacio, ya que eso los “dejaría sin trabajo”.

El segundo tipo incluye gobiernos, proveedores de servicio en línea, corporaciones multinacionales y otros—las susodichas partes interesadas—quienes reconocen la necesidad de contar con límites pero que con frecuencia hacen alarde de esos límites en busca de intereses individuales. Inclusive estados que diseñan armamento cibernético para dañar las infraestructuras y gobiernos basados en la cibernética que espían a sus ciudadanos en línea valoran su propio uso del ciberespacio a la vez que planifican restringir su uso por otros. La ambivalencia resultante de muchos gobiernos quizás se capta mejor en un documento blanco chino reciente que celebra la *Internet* por permitir el desarrollo económico y social, destaca su uso haciendo propaganda de los ciudadanos y en campañas contra la corrupción provincial, pero estipula que

ninguna organización o individuo puede producir, duplicar, anunciar o propagar información [en la Internet] que contenga lo siguiente: estar en contra de los principios cardinales establecidos en la Constitución; poner en peligro la seguridad del estado, divulgar secretos de estado, socavar el poder del estado y poner en peligro la unificación nacional; dañar el honor e intereses del estado; instigar el

odio o la discriminación étnica y poner en peligro la unidad étnica; poner en peligro las políticas religiosas del estado, propagar ideas heréticas o supersticiosas; propagar rumores, interrumpir el orden social y la estabilidad; diseminar material obsceno, pornografía, apuestas, violencia, mal trato y terror o participar en actos delictivos; humillar o calumniar a otros, abusar los derechos legales e intereses de otros; y otros contenidos prohibidos por la ley y las regulaciones administrativas.¹⁸

Desde este punto de vista, el problema estratégico con la *Internet* no es su uso doble si no sus muchos usos. Tantos, de hecho, que esfuerzos unilaterales como las inspecciones profundas de paquetes para refrenar los “usos no deseados” en sí amenazan la estabilidad y sostenibilidad del ciberespacio.

Actores sofisticados que amenazan la confianza del pueblo en el ciberespacio podrían prever las consecuencias adversas de sus actos. Además, podrían calcular que cualquier daño que hagan, la disminución de la confianza del pueblo será moderada o las ganancias en usar la *Internet* aún serán tan grandes que la confianza de los ciudadanos y la accesibilidad mutua permanecerán por encima de algún umbral mínimo. Como ya se ha destacado, tendencias recientes apoyan ese cálculo. Sin embargo, hasta el punto en que su conducción no se puede ni generalizar ni continuar indefinidamente—o sea, sin consecuencias devastadoras—a la pregunta, “¿Qué sucedería si todos siempre actuasen como usted?”, ellos tienen que responder, como Yossarian, “Sería un gran tonto si no lo hiciera”. La alternativa es que todos los yossarianos actúen juntos para cambiar la situación. Bajo las condiciones actuales, ¿es eso posible en el ciberespacio? ¿Puede una cantidad significativa de actores relevantes abandonar prácticas que lo amenacen y comprometerse con reglas que lo sostengan?

Variables de la autoorganización

Ostrom y sus socios han identificado 10 variables críticas para la autoorganización en un sistema socioecológico—es decir, reglas de uso eficaces y que se cumplan para un recurso de uso común en ausencia de una autoridad estatal.¹⁹ Cada variable se explica a continuación, algunas veces con citas directas de Ostrom (ya sea en letra cursiva o entre comillas), mientras que la manifestación en el ciberespacio se describe y evalúa con respecto a su efecto en la autoorganización. Los efectos alentadores, desalentadores y neutrales son identificados por +, -, ó 0, respectivamente. Las variables tienen que ver con las propiedades de los recursos que se explotan en el SES y las características de la población de usuarios. De conformidad con la observación que la confianza del pueblo en el ciberespacio depende de la fiabilidad de su *hardware* y *software*, al igual que el comportamiento de sus usuarios, sus propiedades se toman en cuenta al evaluar las variables relevantes.

Como se verá, las explicaciones de Ostrom de los efectos de las variables en cuanto a la posibilidad para la autoorganización son consistentes con un modelo actor racional: la probabilidad de la autoorganización aumenta mientras más su contribución para sostener el recurso de uso común exceda los costes de lograr que agentes firmen acuerdos y hacer cumplir los acuerdos. Por lo tanto, mientras más bajos sean esos costes, habrá mayor probabilidad para la autoorganización. La suposición con respecto a su proceso es que los estados a través de acuerdos multilaterales establecerían reglas y regulaciones para el ciberespacio; ellos harían cumplirlas directamente o le otorgarían el poder a una agencia internacional para hacerlo.

Tamaño del Recurso (-)

Recursos grandes con fronteras poco definidas disuaden la autoorganización a causa de los costes elevados de definir fronteras, vigilar su uso y rastrear las consecuencias de la mala conducta.

El tamaño del ciberespacio, según lo miden varios billones de dispositivos conectados a la *Internet*, disuade definir sus fronteras y vigilar los comportamientos en él. Como experimento de reflexión, supongamos que las “fronteras” para un ciberespacio fiable fueron definidas por una lista gigante mantenida centralmente de varios billones de dispositivos seguros verificados, con “seguros” designándolo libre de *malware* o que no ha participado en espionaje u otras operaciones de penetración. Sería necesario actualizar continuamente esta lista para acomodar los dispositivos que se le agregan a la *Internet* y la verificación recurrente de dispositivos seguros, porque cualquiera estaría vulnerable a un ataque de un anfitrión falsificando un dispositivo seguro. Este método sería muy costoso y tan solo parcialmente eficaz en inspirar la confianza de los usuarios; algunos ataques son tan furtivos que solamente se descubren después que ha ocurrido, si acaso.

Trazar las fronteras y vigilar el comportamiento puede ser más factible, económico y convincente si los gobiernos nacionales asumen la responsabilidad de los dispositivos y los usuarios en sus territorios certificando las máquinas y otorgándoles credenciales a los usuarios. Entonces, medios unilaterales y multilaterales podrían proteger los ciberespacios nacionales definidos. Esos medios incluyen la implementación de “*firewalls* nacionales” y la reducción de portales nacionales, pasaportes cibernéticos para los usuarios y la asignación de direcciones IP consecutivas para territorios específicos. Esas medidas no detendrían todos los ataques externos y explotaciones dentro de un ciberespacio nacional, pero facilitarían definir el origen de los ataques y responsabilizarían a las autoridades en el estado donde originó un ataque.²⁰

El sistema resultante extendería el principio de la soberanía nacional—la piedra angular de las relaciones internacionales contemporáneas—hacia el ciberespacio²¹ y aumentaría el control de los estados sobre las actividades en línea de sus residentes. Algunos estados, inclusive unas cuantas democracias liberales en occidente, ya han adoptado o abogado por algunas de esas medidas para lidiar con las amenazas a la seguridad cibernética. Sin embargo, muchos gobiernos, organizaciones y usuarios individuales se opondrán al pleno desarrollo del sistema por varias razones. Primero, sancionaría la fragmentación de la *Internet* en muchas “*internet* en un país” con una consiguiente restricción de comunicaciones globales. Ese proceso ya presagiado en China, Irán y otros países autoritarios, atrasaría los esfuerzos de crear un espacio común para la discusión de temas tales como el cambio climático, conocimientos científicos e investigaciones médicas en una agenda global. Segundo, las corporaciones multinacionales y otros agentes de la globalización, inclusive administradores económicos en países autoritarios, considerarán que este sistema es un obstáculo para la economía global en la que los negocios en cualquier parte pueden tener abastecedores y usuarios en todas partes. Para ellos, un aspecto particularmente amenazante de la proyección de soberanía nacional hacia el ciberespacio es la posible restricción en el movimiento de recursos de información. Tercero, los defensores de derechos humanos se opondrán a conceder el derecho a definir un ciberataque a gobiernos nacionales, ya que sus definiciones pueden incluir una amplia serie de contenido, tal como se mencionó anteriormente con respecto a China, al igual que códigos maliciosos. Cuarto, los encargados de formular las leyes probablemente dudarán si los gobiernos aceptarán la responsabilidad de los ataques cibernéticos que originan en sus territorios bajo este sistema. Esas dudas se pueden basar en las prácticas actuales de los gobiernos que alegan ignorar de dónde provienen los ataques o que no cuenta con los medios para reprimir todos los ataques.

Por último, las fronteras nacionales en el ciberespacio son una manera de analizar minuciosamente el espacio común y privatizar los pedazos. En vista de que este espacio común es una red, su desmantelamiento involucra una pérdida de valor. O sea, la suma de los valores de las partes será menos que el valor del total original. La pérdida se definirá en diferentes maneras, pero su anticipación motivará una resistencia amplia a la idea de fronteras cibernéticas nacionales. No obstante, la idea pone de relieve preguntas acerca del carácter del espacio común cibernético: si es una capa fina de comunicaciones en, y a la larga reducida a, entidades y jurisdicciones geofísicas diversas, o si provee conjuntos de experiencias—un modo de ser—en la que los usuarios

podiesen adquirir entidades nuevas que trascienden la identidad nacional. Jacques Bus analiza la pregunta, afortunadamente libre de los acostumbrados panegíricos acerca de la *Internet* aplandando el mundo:

La globalización, evidentemente impulsada por ICT nuevos y la red, crea un entendimiento y por ende más confianza mediante la propagación de información sobre la historia y la reputación de las sociedades, las características de las sociedades y las vidas de las personas viviendo en ciertas sociedades, y permitiendo la comunicación mundial fácil. Puede que de hecho esto conlleve a un desgaste adicional del concepto que “el animal humano está mejor en casa”. Puede que posiblemente lleve a la necesidad de contar con una visión completamente nueva de las sociedades y su unión y el papel que la confianza debe desempeñar en esto.²²

Número de Usuarios (-)

Mientras más sea la cantidad de usuarios de un CPR, los costes de transacción de unirlos y que estén de acuerdo con el cambio serán mayores. Por lo tanto, el tamaño del grupo desalienta la autoorganización, pero “su resultado en la misma depende de otras variables SES y los tipos de tareas de gestión previstas”.

Los dos mil millones de personas que ya tienen acceso a la *Internet* constituyen el grupo de usuarios más grande en la historia de la humanidad. Ellos deben tener la oportunidad de expresar sus inquietudes en cualesquier negociaciones internacionales sobre los usos del ciberespacio, ya que en muchos casos estas inquietudes probablemente serán diferentes a las del gobierno y otras partes interesadas poderosas. Por ejemplo, los usuarios en lucha contra sus propios gobiernos de hecho rechazarían que esos gobiernos representaran sus intereses con respecto al anonimato, el rastreo en línea y el contenido permitido. Por otra parte, reuniones mundiales recientes sobre el cambio climatológico y el ciberespacio en sí han demostrado que los procesos que están abiertos a grupos que alegan representar los intereses de los ciudadanos individuales rápidamente se pueden tornar difíciles de controlar, consumen mucho tiempo y son poco productivos. Por ese motivo, una interpretación de la soberanía nacional, por cada estado que represente legítimamente los intereses de sus ciudadanos, es no solo oportuna sino justa.

Lamentablemente, inclusive esta estratagema no disminuirá las partes interesadas relevantes a una cifra razonable. Las negociaciones tendrán que incluir representación de los sectores industriales, especialmente ICT, y organizaciones internacionales representadas, al igual que los estados, ya que ellos pueden ofrecer no solo el conocimiento técnico para informar sobre las propuestas sino también bloquear las implementaciones de cualesquier acuerdos a los que se hayan llegado sin ellos. Tal como sugiere Ostrom, la cifra de las partes involucradas puede que no determine en sí la dificultad de llegar a un acuerdo. En cambio, cuando hay más partes involucradas, especialmente cuando los temas son complejos, habrá una mayor cantidad de reclamos concurrentes que toman tiempo reconciliar, si es que se pueden reconciliar. Todas las negociaciones para la Convención de la ONU sobre el Derecho del Mar (CDM), que regula otro espacio común, duraron una década a pesar de basarse en siglos de derecho marítimo y estar más confinadas a asuntos de soberanía del estado. Hay mucha menos tradición jurídica para la cibernética y, hasta ahora, no ha habido ningún esfuerzo concertado para armonizar leyes cibernéticas a nivel estatal. Por lo tanto, la Convención de Budapest sobre el delito cibernético, que ha sido muy limitada y orientada regionalmente, ha sido lenta en lograr el acatamiento, y muchos de sus signatarios han enumerado varias reservas.²³ Quizás algún alivio de estas posibilidades desalentadoras lo podría proveer el ciberespacio en sí, en que el conjunto de opiniones, consultas y negociaciones ahora se pueden llevar a cabo virtualmente al igual que en persona. Al organizar la

información, reducir los costes de transacción y agilizar las comunicaciones, las herramientas cibernéticas podrían permitir la toma de decisiones acerca de sus propios futuros.

Unidad móvil de recursos (-)

A causa de los costes de observar y administrar un sistema, la autoorganización es menos probable con unidades móviles de recursos... que con unidades fijas, tales como árboles y plantas o agua en un lago.

Hay tres tipos de dispositivos de movilidad que hacen que su vigilancia sea difícil y costosa. Primero, como ya se ha mencionado, la condición de un dispositivo puede cambiar rápidamente de “seguro” a “comprometido”, a menudo descubriendo el cambio más tarde, si se descubre. Segundo, durante su transcurso, los ataques y las explotaciones cibernéticas a gran escala típicamente desplegarán diferentes máquinas ubicadas en direcciones IP diferentes y emplazamientos geofísicos. Por ejemplo, durante un ataque distribuido de denegación de servicio distribuido (DDoS, por sus siglas en inglés) en sitios del gobierno estadounidense, los sitios de mando y control (C2) se afirma emigraron de computadoras en Corea del Sur a algunas en Chicago y Berlín. Por lo tanto, cualquier vigilancia o defensa específica a un ataque, como bloquear posibles sitios C2, probablemente incluirá jurisdicciones múltiples con problemas de coordinación consiguientes. Investigaciones posteriores serán similarmente complicadas y la atribución inevitablemente incierta. Como resultado, las partes en un acuerdo que prohíban esos ataques no pueden depender de la vigilancia para verificar que están cumpliendo con el acuerdo o para identificar infractores. Tercero, el surgimiento de la computación móvil en la forma de *laptops*, *smartphones* (teléfonos inteligentes) y tabletas ha aumentado en gran medida la superficie de ataque del ciberespacio y la tarea de cualquier programa de seguimiento en el futuro. La movilidad física de estos dispositivos también significa que durante su vida útil están expuestos a una variedad de amenazas cibernéticas y entornos de vigilancia y a cambios en su propio estatus de seguridad. Serán más vulnerables que una máquina atada a un solo servidor dentro de una organización que cuenta con una seguridad cibernética competente. Son más propensos a la penetración, el robo de su información y el compromiso. Una vez comprometidos, se pueden convertir en portadores para redes comprometedoras a las cuales se conectan más tarde, algo parecido a las intranets empresariales.²⁴

Importancia de los recursos para los usuarios (+)

En casos exitosos de autoorganización, los usuarios o bien dependen del recurso para gran parte de su sustento o le asignan un valor elevado a la sostenibilidad del recurso.

Un incremento de actividad alrededor del mundo incluye la creación, recopilación, embalaje, uso y distribución de la información. *La Internet* y otras partes del ciberespacio son esenciales para estas actividades. Varias ponencias del gobierno sobre la seguridad cibernética son claras al reconocer la importancia económica, social, cultural y científica del ciberespacio. Al hacer un llamado para la “creación de una cultura de seguridad cibernética global”, la Asamblea General de la ONU reconoció

la contribución cada vez mayor efectuada por las tecnologías de información en la red a muchas funciones de la vida cotidiana, el comercio y el suministro de bienes y servicios, investigación, innovación y el espíritu empresarial, y al flujo libre de información entre los individuos y las organizaciones, gobiernos, negocios y la sociedad civil.²⁵

Inclusive regímenes autoritarios en Irán, Egipto y en otras partes quienes enfrentaron protestas masivas organizadas por medios cibernéticos han titubeado cerrar la *Internet* en sus propios países a causa de la dependencia de sus economías en la misma.

Sin embargo, gobiernos y diplomáticos, han sido menos claros en reconocer cuán fundamental la confianza del pueblo es para el ciberespacio. Al solicitar discusiones sobre normas internacionales para el ciberespacio, el grupo de la ONU de expertos gubernamentales adoptó principalmente una perspectiva de seguridad nacional: El delito cibernético y otros tipos de amenazas cibernéticas son perjudiciales para las funciones gubernamentales, económicas y sociales; la falta de un entendimiento común sobre las intenciones detrás de ciertos comportamientos en el ciberespacio puede crear conflictos que pueden intensificarse y amenazar la seguridad internacional.²⁶

Productividad del Sistema (+)

Si un recurso ya se ha agotado o es muy abundante, los usuarios no verán la necesidad de administrar en el futuro. Los usuarios necesitan observar algo de escasez antes de invertir en la autoorganización.

El crecimiento del delito cibernético, el índice de ataques y explotaciones, la proliferación del *malware* y las amenazas a la infraestructura cibernética crítica han planteado preguntas sobre si los beneficios del ciberespacio se pueden sostener bajo las prácticas de seguridad actuales. Esas preguntas claramente motivan los diferentes llamados para acuerdos internacionales sobre el comportamiento ciberespacial. Jacques Bus destaca que la posibilidad de que los estados estén detrás de muchas de las amenazas cibernéticas “es prueba de la urgencia de llegar a acuerdos internacionales sobre refrenamientos en y la defensa contra ataques cibernéticos y de contar con una cooperación internacional para controlarlas”.²⁷ Después de identificar la confianza del pueblo como un recurso escaso en el ciberespacio, Bus continúa expresando que, “Los sectores público y privado tienen que trabajar juntos a nivel internacional para crear una infraestructura bien balanceada de tecnología y leyes/regulación que les otorgue a los ciudadanos la confianza de usar las oportunidades del nuevo mundo digital”.²⁸ En un discurso pronunciado en la Conferencia sobre Seguridad en Munich en el 2011, el ministro de relaciones exteriores británico, William Hauge, hizo conexiones similares:

*Estamos trabajando con el sector privado para garantizar una infraestructura crítica segura y fuerte y la base de destrezas fuertes necesarias para sacarle provecho a las oportunidades económicas del espacio cibernético, y para crear una concienciación sobre las amenazas en línea entre los miembros del público. Pero al ser globales, las amenazas cibernéticas también requieren una respuesta colectiva. En Gran Bretaña creemos que ha llegado el momento de comenzar a buscar un acuerdo internacional sobre las normas en el ciberespacio.*²⁹

Previsibilidad de la dinámica del sistema (0)

La dinámica del sistema necesita ser lo suficiente predecible de manera que los usuarios puedan calcular qué sucedería si ellos estableciesen leyes particulares o territorios a los que no se puede entrar.

Las consecuencias de no contar continuamente con una regulación internacional son más predecibles que el efecto del acuerdo y vigilar en busca de algunos patrones de comportamiento. Con el deterioro de la confianza del pueblo en el ciberespacio, la expansión del uso—en términos de tiempo invertido, aplicaciones y dependencias—disminuirá y eso estará acompañado por menos crecimiento o disminución en los incentivos para el desarrollo. Algunos usuarios puede que ya hayan reducido su uso de las redes públicas para la transmisión crítica de datos; algunas organizaciones han reducido el número de puntos de acceso o portales para ellos. Estas medidas puede que crezcan hacia la separación y la fragmentación generalizadas—fenómenos que le quitan valor al ciberespacio.

Proyectar la pérdida en valor de un ciberespacio vulnerable en comparación con uno seguro es problemático porque hay diferentes modelos para evaluar el valor socioeconómico de las redes cibernéticas. No obstante, parece razonable suponer que a medida que usuarios nuevos provenientes de estratos económicos inferiores y países menos desarrollados, el valor económico de las redes aumentará a un régimen más bajo que en las etapas iniciales de su crecimiento.³⁰ Esa tendencia cuenta con implicaciones mixtas para la autoorganización. Primero, los proveedores tendrán pocos incentivos para aumentar sus inversiones en la seguridad cibernética—especialmente si los costes de seguridad corresponden a la cantidad de usuarios. Pero la falta de acción por parte de los proveedores pondría más presión en los gobiernos para que busquen acuerdos que disminuyan las amenazas. Por otra parte, la tendencia también sugiere que cualquier retiro de los usuarios no disminuirá inicialmente el valor de la red. Por lo tanto, hasta que la situación se considere intolerable y no solamente mala, los gobiernos, conscientes de los costes de los acuerdos, podrían resistir la presión y demorar la autoorganización, a pesar de que su pueblo exige acción.

Liderazgo (0)

Cuando algunos usuarios de cualquier tipo de sistema de recursos cuentan con destrezas empresariales y son respetados como líderes locales como un resultado de la organización previa para otros fines, la autoorganización es más probable.

Al liderazgo le faltan negociaciones a nivel estatal, potencialmente productivas, pero no por falta de actores que han desempeñado papeles en organizar el ciberespacio. Durante la última década, *Internet Corporation for Assigned Names and Numbers (ICANN)* (Corporación para la Asignación de Nombres y Números en *Internet*) ha provisto la administración competente, aunque criticada frecuentemente, de las asignaciones de ámbitos y supervisión de los registros. Ha acomodado el crecimiento espectacular de la *Internet* y las demandas comerciales que lo acompañan con un rediseño de políticas para dominios de nivel superior. Si bien no ha sido particularmente abierta a la participación popular especificada en su modelo de múltiples grupos interesados, ha retenido la confianza de los proveedores de servicio y el respeto de la mayoría de los estados, tal como lo comprueba la restricción de la ONU de buscar participación en la administración de la *Internet*. Pero la ICANN no es un especialista en normas y carece de las destrezas políticas y la influencia para reconciliar los intereses en competencia entre los estados en cuanto a comportamientos cibernéticos y seguridad. Además, muchos estados la consideran una herramienta de la política estadounidense.

La *Internet Engineering Task Force (IETF)* (Fuerza de Tarea de Ingeniería de *Internet*) ha ejercido liderazgo en los protocolos de *Internet*, en su mayoría como el endosante de normas. Su propia historia es un ejemplo de autoorganización entre las partes interesadas para la gestión de un espacio común, pero su proceso amorfo de toma de decisiones es un modelo difícil para las negociaciones en cuanto a refrenar las actividades de seres humanos. En todo caso, no está calificada para estar al frente de esas negociaciones, su ámbito está limitado al ámbito técnico, su importancia en ese ámbito ha disminuido a medida que las inquietudes ahora se enfocan más en aplicaciones móviles y otras capas más allá de su alcance, y su membresía aún es estadounidense y europea en su mayoría.³¹

El *International Telecommunications Union (ITU)* (Sindicato Internacional de Telecomunicaciones), la agencia de la ONU responsable del ICT, tiene la ambición de estar al frente de la formulación de políticas y la administración del ciberespacio, y estuvo a cargo de la organización de la *World Summits on the Information Society (WSIS)* (Cumbres Mundiales sobre la Sociedad de la Información), que se enfocaba en aspectos menos transcendentales: usos del ciberespacio orientados hacia el desarrollo, gobernanza de la *Internet*, reducción de brechas digitales. Considerada en occidente como una herramienta para los intereses políticos rusos y chinos, carece de credibili-

dad política para asumir el liderazgo en aspectos difíciles tales como espionaje cibernético, derechos de información y así por el estilo. Probablemente también carece de capacidad tecnológica; las normas de seguridad cibernética que creó y promovió en colaboración con la *International Organization for Standardization (ISO)* (Organización Internacional para la Estandarización) resultaron ser costosas y poco viables.

Normas/Capital Social (+)

Si los usuarios comparten normas de reciprocidad y confían entre sí lo suficiente para acatar acuerdos, enfrentarán costes de transacción más bajos al llegar a acuerdos y monitorear. La globalización económica en curso y la ausencia de guerras interestatales importantes pudiesen sugerir que las potencias principales están desarrollando estructuras de reciprocidad adecuadas y mecanismos para evitar conflictos. De hecho, esta evaluación es sustentada por los temores expresados en los llamados para normas cibernéticas que los malos entendidos acerca de los comportamientos ciberespaciales podrían desencadenar conflictos no deseados. No obstante, no llevar a cabo negociaciones sobre regulaciones ambientales suscita dudas que a las negociaciones sobre el ciberespacio les vaya mejor, especialmente en vista de que las grandes potencias tienen diferencias ideológicas sobre el ciberespacio, tan grandes como las diferencias entre los intereses económicos que bloquean las resoluciones de los problemas ambientales.

En términos generales, los políticos rusos y chinos buscan extender el principio de soberanía nacional al ciberespacio estableciendo una norma de que el estado sea el árbitro final en asuntos relacionados con el ciberespacio en su territorio.³² Desde una perspectiva occidental, sus motivos son controlar el espacio ideacional que las redes cibernéticas le permiten a sus pueblos y evitar averiguaciones en cuanto al uso de la cibernética por sus gobiernos o representantes para campañas militares, espionaje político, espionaje industrial y delincuencia. No obstante, recuerden que las tradiciones políticas en Rusia y China, inclusive en los días antes del comunismo, les otorgaba el poder a las autoridades estatales de decidir qué debían pensar sus ciudadanos, y que el principio de soberanía nacional bloquea a extranjeros de interferir con el ejercicio de ese poder. Además, los funcionarios rusos están plenamente conscientes que los insurgentes o terroristas chechenos han empleado tecnologías cibernéticas en sus luchas violentas contra Rusia. Entonces, una *Internet* descontrolada puede ser políticamente amenazante y fácil de explotar por rivales externos, en particular en Estados Unidos. Por ejemplo, cuando protestas alimentadas por la cibernética ocurrieron en Rusia, Vladimir Putin, el premier, candidato presidencial y blanco de las protestas, catalogó esas protestas como la labor de “enemigos extranjeros”.³³ Desde este punto de vista, extranjeros facultando disconformidad dentro de un país no es una contribución al debate público; es “guerra de información” llevada a cabo para debilitar regímenes al punto de mayores adaptaciones con extranjeros o inclusive el derrumbe. En el 2008 Rusia, China y otros integrantes de la *Shanghai Coordination Organization (SCO)* (Organización Coordinadora de Shanghai) ya habían acordado prohibir apoyar o auspiciar la diseminación de información potencialmente perjudicial. En septiembre de 2011, en lo que parecía ser una respuesta al apoyo por parte de gobiernos extranjeros y diásporas al activismo cibernético en el mundo árabe, Rusia propuso que los países anotaran las actividades en línea de sus residentes sospechosos de esas diseminaciones.

En cambio, Estados Unidos y sus aliados de la OTAN tienden en sus declaraciones a considerar el ciberespacio como una institución central para la economía global, un medio para el intercambio mundial científico y cultural, un espacio común para el debate político y el desarrollo y un medio social. En vista de esta variedad de funciones, de ahí también el modelo de múltiples partes interesadas para el control y defensa del ciberespacio, con los estados siendo un tipo de parte interesada, junto con las organizaciones no gubernamentales, proveedores de servicios, compañías ICT, entidades de infraestructura crítica, usuarios empresariales y usuarios individuales. Pero en vista de que el ciberespacio, particularmente la *Internet*, es víctima de ataques y ex-

plotaciones de delincuentes, terroristas e inclusive estados, en virtud de su autoridad y capacidades, los estados tienen la responsabilidad principal de proveer la seguridad necesaria sin dañar los intereses de otras partes interesadas. La diseminación de normas y tratados, tales como la *Budapest Convention on Cybercrime* (Convención de Budapest sobre el Delito Cibernético), son instrumentos para cumplir con esa responsabilidad, al igual que la promoción de una cultura y capacidades de seguridad cibernética alrededor del mundo.³⁴

Este enfoque, combinado con una visión de la *Internet* de hace una década, hace caso omiso de los cambios demográficos y tecnológicos que están rehaciendo el ciberespacio y las expectativas para él: el cambio de cientos de millones de usuarios concentrados en América del Norte y Europa conectados a la *Internet* a través de computadoras a billones de usuarios con la mayor parte en el sur y el este de Asia conectados a través de dispositivos móviles y el surgimiento de una *Internet* de cosas. Como resultado, aquellas prácticas que una vez parecían estar en el interés de todos ahora son controversiales y refutadas.³⁵ India, Brasil y América del Sur—las voces principales en asuntos cibernéticos entre los países “no alineados”—quieren que estos cambios sean reconocidos como partes principales concedidas en cualesquier negociaciones. Por consiguiente, favorecen la transferencia de autoridad lejos de agencias orientadas hacia la tecnología, reflejando el modelo de partes interesadas múltiples, inclusive ICANN e IETF, hacia una agencia más orientada hacia la política, posiblemente bajo la ONU, aunque no necesariamente la ITU, que le concede a cada estado una misma voz.

Conocimiento del SES (+)

Cuando los usuarios comparten un conocimiento común de atributos SES relevantes, cómo sus acciones los afectan entre sí y otras reglas empleadas en SES, ellos percibirán costes de organización más bajos.

Los diversos llamamientos para reglas cibernéticas reflejan el conocimiento de los encargados de formular leyes que ciertos comportamientos trastornan las actividades normales, siembran la desconfianza del pueblo y amenazan la sostenibilidad del ciberespacio. Su disposición para discutir problemas más allá de los delitos cibernéticos reconoce que aquellos que se comportan mal pueden incluir sus propios gobiernos y ciudadanos. Por lo tanto, se necesitan menos tiempo y dinero para despertar la conciencia o convencer a los escépticos que hay un problema y que la cooperación internacional puede ayudar a resolverlo. Elegir qué se va a hacer requiere más conocimiento de las dependencias entre los diversos procesos en el ciberespacio, particularmente cómo las posibilidades tecnológicas afectan los comportamientos sociales (de los agentes). Los esfuerzos de contar con reglamentación ambiental muestran que aquellos que se sienten amenazados por la propuesta de soluciones amplias y exhaustivas se opondrán, inclusive si se les ofrecen pagos adicionales. Entonces el problema de que el espacio tiene que degradarse con la selección de algún blanco cuya solución propuesta podría lograr tracción, ayuda a reducir el nivel general de la inseguridad cibernética y crear confianza entre los diversos agentes, permitiendo así la búsqueda de otros blancos. Una sugerencia frecuente es que los estados cooperan para reprimir las pandillas de delincuentes cibernéticos negándoles sus medios de cobrar en efectivo sus robos. Esta sugerencia comprende que (a) la dependencia de las pandillas en ciertos bancos y (b) el delito cibernético sirven como un laboratorio de desarrollo y prueba para malware que más tarde será utilizado por las agencias de inteligencia en algunos estados. Menos conocido es el hecho de cuán fuerte estas agencias dependen de las pandillas y, por lo tanto, los incentivos que sus estados necesitan para cooperar con la propuesta.

Normas de Opciones Colectivas (0)

Cuando los usuarios cuentan con la autonomía total al nivel de opción colectiva para diseñar y hacer cumplir algunas de sus propias reglas, tienen costes de transacción más bajos al igual que costes más bajos en defender el recurso contra la invasión por otros.

Esta variable implica que mientras más personas puedan considerarse a sí mismas como los autores de las reglas que se esperan ellos acaten, más personas acatarán esas reglas. Esto es importante para la seguridad cibernética y la confianza del pueblo en el ciberespacio, porque una buena “higiene en la computadora” a los niveles institucional e individual puede eliminar una cantidad considerable de delitos y explotaciones, quizás tanto como un ochenta por ciento.³⁶ Lamentablemente, la cantidad de usuarios y la dispersión de su representación pareciera excluir la participación del pueblo en formular leyes, tal como se mencionó anteriormente. Por consiguiente, los usuarios podrán ver su acatamiento a las reglas como parte de un esfuerzo global interdependiente para sostener el ciberespacio y, por lo tanto, para su propio beneficio. Las directrices que reciban de los superiores probablemente justificarán las reglas solamente en términos de proteger al individuo o la organización.

Cambiando las variables y respuesta en caso de una crisis

Los valores de las variables de Ostrom, resumidas en la tabla a continuación, no favorecen la autoorganización en el SES cibernético. Las condiciones no son oportunas para acuerdos productivos, que se puedan poner en vigor bajo los cuales las partes interesadas, especialmente los estados, limiten sus comportamientos cibernéticos que merman la confianza. Tal como lo indican los valores positivos para las variables “importancia del recurso” y “productividad del sistema”, las expresiones generalizadas de temor por el futuro del ciberespacio han suscitado interés en esos acuerdos. Sin embargo, no se debe esperar nada más allá hasta que los valores de algunas variables tecnológicas y otras variables sociales cambien. Podría decirse que la búsqueda ahora de un acuerdo global exhaustivo o una alternativa a los acuerdos entre aquellos que “piensan igual” será contraproducente. Probablemente profundizará la desconfianza entre las potencias cibernéticas principales y desalentará compartir el conocimiento útil del SES cibernético. Ese parece ser el resultado principal de la reciente conferencia en Londres sobre las “reglas del juego” cibernéticas.³⁷

Variable	Valor
Tamaño del recurso	-
Número de usuarios	-
Unidad móvil del recurso	-
Importancia del recurso	+
Productividad del sistema	+
Previsibilidad de la dinámica del sistema	0
Liderazgo	0
Normas/capital social	+
Conocimiento del SES	+
Normas de opciones colectivas	0

Varias medidas factibles podrían mejorar las perspectivas para acuerdos eficaces o sostener la confianza del pueblo en el ciberespacio. Consideren lo siguiente.

Crear Gestión de Identidad Global

Jacques Bus recomienda la creación de un “sistema fidedigno interoperable y global para la identificación y autenticación” como esencial para la confianza entre los usuarios de *Internet*.³⁸ Los estados, inclusive algunas democracias liberales, ya les están exigiendo identificación a los usuarios de *Internet*. La interoperabilidad de las normas locales facilitaría, de ser necesario, la identificación de un usuario de un dispositivo enlazado a la *Internet* en cualquier lugar. Los usuarios retendrían su anonimato o privacidad bajo este régimen, ya que diferentes sitios y transacciones exigirían diferentes grados de divulgación. Los regímenes autoritarios podrían identificar más fácilmente a personas en redes cibernéticas de resistencia, pero encontrarían que están mejor al no identificar a aquellos que muestran una resistencia no violenta, mientras tratan de identificar y reprimir los violentos. Esa estrategia podría canalizar a los opositores hacia redes no violentas y darles a los regímenes más espacio para respirar. Su restricción en este aspecto podría permitirles a los estados que apoyan a sus opositores a cooperar en el sistema de identificación. En términos de las variables de Ostrom, la gestión de la identidad disminuye algunos de los efectos nocivos de la movilidad del recurso.

Aumentar la participación del pueblo en la seguridad cibernética

Las discusiones sobre las políticas de seguridad cibernética en públicos informados y relevantes pueden tener el efecto doble de poner presión en los gobiernos nacionales respectivos e involucrar a esos pueblos en los procesos de formulación de políticas. La resolución de la ONU para la “creación de una cultura global de seguridad cibernética” prevé que la seguridad cibernética nacional tendrá una participación amplia de la sociedad, inclusive la del sector privado, la sociedad civil, el mundo académico e individuos, pero permanece callada con respecto a las funciones de formulación de políticas para los actores no gubernamentales. Las asociaciones públicas-privadas que ya han surgido en Europa y América del Norte parecen estar enfocadas en coordinar esfuerzos a nivel empresarial y compartir información, sin criticar ni cambiar las políticas. Pero a los miembros no gubernamentales, particularmente cualquier corporación transnacional (TNC, por sus siglas en inglés), por ejemplo *Freedom House*, se les debe exhortar que sugieran reglas. Muchos han experimentado ataques cibernéticos en una variedad de entornos legales y tecnológicos y probablemente saben mejor que los observadores o gobiernos cuáles leyes y prácticas cibernéticas deben armonizar con los países como parte de los acuerdos internacionales.

The Internet Governance Forum (IGF) (Foro de la Gobernanza de *Internet*), un órgano consultivo establecido por la ONU y basado en un modelo de partes interesadas múltiples, también podría utilizarse para que el pueblo hiciese aportes en las conversaciones a nivel global sobre las reglas para el ciberespacio. En sus reuniones se han discutido temas sobre la seguridad cibernética pero hasta el momento ha dejado en manos de los gobiernos nacionales y agencias especializadas las propuestas para la política. Pero el IGF podría utilizar herramientas y técnicas cibernéticas, tales como sondeos en línea y colaboración del público para recopilar y agregar opinión pública acerca de reglas y regulaciones necesarias en cualquier acuerdo futuro.

Creando la Confianza mediante la Cooperación Internacional en una Tarea “Fácil”

Aunque puede que acuerdos exhaustivos sobre los comportamientos en el ciberespacio fuesen inalcanzables, la cooperación internacional en algunas amenazas cibernéticas y emergencias puede ser fuerte y eficaz, por ejemplo, la respuesta mundial al gusano *Conficker* y la alianza de trabajo de los CERT de Japón, China y Corea del Sur. En estos casos, la cooperación se basa en “normas invisibles” o compromisos compartidos entre los tecnólogos cibernéticos, pero le puede dar alguna confianza a los formuladores de política que están observando a sus países colaborando juntos sobre los problemas cibernéticos. Por lo tanto, su confianza puede crecer con más

casos donde un reto provoca un compromiso profesional ampliamente compartido y la cooperación resultante logra algo de éxito. Algunos delitos cibernéticos parecen ser candidatos aptos para el reto, notablemente la pornografía infantil, el fraude de bajo nivel, y el robo de identidad. Sin embargo, hay una necesidad que alguna agencia esté al frente de promover la urgencia de reprimir el delito seleccionado.

Este artículo ha empleado el reduccionismo económico para argumentar que no se dan aún las condiciones para llegar a y hacer cumplir acuerdos internacionales sobre los usos del ciberespacio. El argumento sostiene que si las personas que explotan un espacio común saben que la explotación exagerada degradará ese espacio común, ellos pueden acordar a limitar su comportamiento, siempre y cuando los costes de llegar a un acuerdo y hacerlo cumplir sean asequibles. En este argumento, la autolimitación está en servicio del interés personal—sostener sus propios beneficios del espacio común. En lo que respecta al actor, ya sea un individuo, organización o nación, el ciberespacio es tan solo otro ámbito donde busca su propio interés personal. El ciberespacio, por supuesto, es mucho más rico. Se ha convertido en la base y el medio para reorganizar gran parte de la vida contemporánea social, económica, cultural e intelectual en los países desarrollados. Provee un medio principal para una conversación global sobre asuntos compartidos. En la medida en que retenga la confianza del pueblo, el ciberespacio cultiva nuevos lazos sociales e identidades que aumentan los preexistentes, como la nacionalidad. Por todo ello, exige algo de lealtad.

Inclusive sus defensores no piensan que un acuerdo cibernético internacional protegería lo suficiente a estados, organizaciones e individuos de los diferentes ataques que surgen en el ciberespacio. Aunque un tratado sería una restricción en sus signatarios y facilitaría las sanciones de sus infractores, una defensa cibernética adecuada al nivel estatal aún exigiría resistencia (endurecimiento) de las redes digitales, especialmente aquellas que apoyan la infraestructura crítica; resistencia de las organizaciones que probablemente serían atacadas y disuasión razonable con respecto a los no signatarios. A falta de un acuerdo(s) internacional, la dependencia en esos otros componentes aumentaría moderadamente. Además, en vista de que las redes digitales son necesarias para la globalización económica, los estados continuarán cooperando en el plano técnico con respecto a la gobernanza de la *Internet* al menos hasta el punto de garantizar la interoperabilidad al nivel global. Esa cooperación no se extenderá a controlar el espionaje industrial, proteger infraestructuras de información crítica o garantizar la libertad de información, tres temas que han surgido recientemente como los focos de desconfianza entre los estados. Estos y otros problemas cibernéticos al nivel internacional probablemente se discutirán en un futuro a medio plazo en una manera fragmentada y gradual—la estrategia para salir del paso. Estos no son necesariamente malos resultados, y pocos usuarios experimentarán alguna pérdida de los beneficios del ciberespacio. Por otra parte, la inseguridad ahí continuará, y la oportunidad de forjar la confianza del pueblo a un nivel global habrá pasado. □

Notas

1. *Un General Assembly, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security"* (Asamblea General de la ONU, "Informe del Grupo de Expertos Gubernamentales sobre los Desarrollos en el Campo de la Información y las Telecomunicaciones en el Contexto de Seguridad Internacional) A/65/201, 30 de julio de 2010, <http://www.unidir.org/pdf/activites/pdf5-act483.pdf>.

2. Para un repaso de la conferencia en Londres, consultar a Peter Apps, "Disagreements on Cyber Risk East-West 'Cold War'" ("Desacuerdos sobre el Riesgo Cibernético y la 'Guerra Fría' Este-Oeste"), Reuters, 2 de febrero de 2012, <http://www.reuters.com/article/2012/02/03/us-technology-cyber-idUSTRE8121ED20120203>.

3. "Remarks by Secretary Napolitano before the Joint Meeting of the OSCE Permanent Council and OSCE Forum for Security Cooperation" (Declaraciones de la Secretaria Napolitano ante el Comité Conjunto del Consejo Permanente OSCE y el Foro OSCE para la Cooperación de la Seguridad), Comunicado de prensa del Departamento de Seguridad Interna, 1º de julio de 2011, <http://www.dhs.gov/ynews/speeches/2011-napolitano-remarks-osce-council-austria.shtm>.

4. Adam Segal y Matthew Waxman, “Why a Cybersecurity Treaty Is a Pipe Dream” (Por qué un tratado de seguridad cibernética es un sueño imposible), *Council on Foreign Relations (Consejo sobre Relaciones Exteriores)*, 27 de octubre de 2011, <http://www.cfr.org/cybersecurity/why-cybersecurity-treaty-pipe-dream/p26325>.

5. Consultar a G. Hardin, “Tragedy of the Commons” (Tragedia en el espacio común), *Science* 162 (1968): 1243–48, para una formulación clásica del argumento.

6. Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action (Gobernando el espacio común: La evolución de instituciones para la acción colectiva)* (Cambridge, UK: Cambridge University Press, 1990); Ostrom et al., “A General Framework for Analyzing Sustainability of Social-Ecological Systems” (Un marco general para analizar la sostenibilidad de los sistemas socioecológicos), *Science* 325, no. 5939 (24 de julio de 2009): 419–22.

7. Lawrence Lessig, “The Public Domain” (El ámbito público) *Foreign Policy*, 30 de agosto de 2005, http://www.foreignpolicy.com/articles/2005/08/30/the_public_domain.

8. Para esa analogía, consultar Abraham Denmark y James Mulvenon, eds., *Contested Commons: The Future of American Power in a Multipolar World* (El espacio común en pugna: El futuro del poder estadounidense en un mundo multipolar) (Washington: Center for a New American Security, 2010).

9. Al emplear la sociedad de una aldea del espacio común inglesa como su metáfora rectora, los defensores de una Internet donde la información fluye libremente puede que hayan tenido tendencias hacia una visión idílica o prelapsaria. En una revisión desdeñosa de Lewis Hyde, *Common as Air (El espacio común como aire)* (New York: Farrar, Straus, and Giroux, 2010), la labor de uno de esos defensores, David Wallace-Wells, cita la evaluación de E. P. Thompson en su obra clásica *The Making of the English Working Class (La creación de la clase laboral inglesa)* (New York: Vintage Books, 1966) esa cultura agraria inglesa antes del cercamiento era “intelectualmente vacante...y evidentemente pobre”. Hacer caso omiso que el cercamiento obligó a las personas a abandonar sus tierras y no mejoró las vidas de los que quedaron atrás, Wallace-Wells sostiene por analogía que estamos sentenciados a una esterilidad cultural sin los cercamientos de derechos de autor amplios en su “The Pirate’s Prophet: On Lewis Hyde” (El profeta del pirata: Sobre Lewis Hyde) *Nation*, 15 de noviembre de 2010, <http://www.thenation.com/article/155619/pirates-prophet-lewis-hyde?page=0.0>.

10. Para la securitización de la cibernética en Estados Unidos, consultar M. Dunn Cavelti, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (Seguridad cibernética y la política de la amenaza: Esfuerzos de EE.UU. de asegurar la era de información) (New York: Routledge, 2008). Para tipos y extensión de las prácticas de cercamiento, consultar Ronald Deibert et al., eds., *Access Denied: The Practice and Policy of Global Internet Filtering (Acceso denegado: La práctica y política de filtrar la Internet global)* (Cambridge: MIT, 2008); y Deibert et al., editores, *Access Controlled (Acceso controlado)* (Cambridge: MIT, 2010).

11. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (Estrategia internacional para el ciberespacio: Prosperidad, seguridad y transparencia en un mundo interconectado)* (Washington: The White House, May 2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. También consultar Secretaria de Estado Hillary Clinton, “Remarks on Internet Freedom” (Comentarios sobre la libertad de la Internet), 21 de enero de 2010, <http://www.state.gov/secretary/rm/2010/01/135519.htm>. La denuncia prominente del Departamento de Estado del filtrado motivado políticamente por gobiernos extranjeros lo llevó a oponerse a los proyectos de ley del Congreso contra la piratería (SOPA y PIPA) que hubiesen exigido el filtrado motivado comercialmente de sitios web extranjeros.

12. “Jo Twist, Web Guru Fights Info Pollution,” *BBC News*, 13 de octubre de 2003, <http://news.bbc.co.uk/2/hi/technology/3171376.stm>. La intención de otro tipo de consumo exorbitante de ancho de banda, la denegación de servicio distribuido, es infligir directamente otros tipos de costes, tales como reputación, financieros o políticos, en sus blancos al obligar a los servidores de red del blanco a fallar bajo la aglomeración de demandas de servicio. La DDoS puede escalar al nivel de un problema de seguridad nacional, como fue el ejemplo del ataque en el 2007 a los sitios web gobierno estonio e infraestructuras críticas.

13. Discusión de los obstáculos y costes de una seguridad “adecuada” para las tecnologías intrínsecamente vulnerables del ciberespacio están más allá del alcance actual. Además de los costes para personal de seguridad cibernética, se incluyen costes mucho menos estimables para modernizar las culturas empresariales. Muchas empresas, especialmente en el sector financiero, han optado por diferir esos costes y tratar cualquier pérdida al delito o espionaje cibernético como costes de actividades comerciales, a la vez que intentan ocultar esas pérdidas por temor a los costes a sus reputaciones. Cuando este artículo fue a imprenta, supe que L. Jean Camp, “Reconceptualizing the Role of Security User” (Reconceptualizando el papel que desempeña el usuario de seguridad) *Daedalus* 140, no. 4 (2011): 93–107, también aplica el análisis de Ostrom de autoorganización al reto de la seguridad cibernética. Sin embargo, el enfoque de Camp es en las posibilidades de los usuarios finales individuales de formar comunidades a menor escala en las que compartir información sobre amenazas cibernéticas e higiene cibernética se practican eficazmente.

14. Jacques Bus, “Societal Dependencies and Trust” (Dependencias sociales y confianza) en Hamadoun Touré et al., *The Quest for Cyber Peace (La búsqueda del ciberespacio)* (Geneva: International Telecommunications Union, 2011), 18.

15. *Ibid.*, 19, citando a Francis Fukuyama, *Trust: The Social Virtues and the Creation of Prosperity* (Confianza: Las virtudes sociales y la creación de la prosperidad) (New York: Free Press, 1995), y Robert Putnam et al., *Making Democracy Work: Civic Traditions in Modern Italy* (Haciendo que la democracia funcione: Tradiciones cívicas en la Italia moderna) (Princeton, NJ: Princeton University Press, 1993). Para un ejemplo negativo, consultar a Anthony Padgen, “The Destruction of

Trust and Its Economic Consequences in the Case of Eighteenth-Century Naples” (La destrucción de la confianza y sus consecuencias económicas en el caso de Nápoli en el siglo XVIII) en *Trust: Making and Breaking Cooperative Relations (Confianza: Estableciendo y rompiendo relaciones cooperativas)*, editor, Diego Gambetta (London: Basil Blackwell, 1988), 127–41.

16. El uso de los iraníes de las redes anónimas Tor sugiere que algunos usuarios necesitan tanto la cibernética que inclusive una cantidad pequeña de reconfirmación los provocaría regresar a utilizar aplicaciones comprometidas anteriormente, a pesar de los riesgos involucrados. Las gráficas para el uso están adulteradas, mostrando que inmediatamente después que las autoridades iraníes anunciaron un bloqueo o vigilancia de un sitio Tor en particular, la cantidad de usuarios iraníes en la red baja precipitadamente. Luego se vuelve a reponer después que los creadores de Tor anuncian una solución a las medidas iraníes. Consultar <https://metrics.torproject.org/users.html?graph=direct-users&start=2010-11-28&end=2012-02-26&country=ir&dpi=72#direct-users>.

17. Daniel Heller-Roazen, *The Enemy of All: Piracy and the Law of Nations (El enemigo de todos: La piratería y las leyes de las naciones)* (Cambridge: MIT Press, 2008).

18. Oficina de Información del Consejo Estatal de la República Popular China, “*The Internet in China*” (La Internet en China), 8 de junio de 2010, http://www.china.org.cn/government/whitepaper/node_7093508.htm.

19. Elinor Ostrom, “*General Framework for Analyzing Sustainability of Social Ecological Systems*” (Marco general para analizar la sostenibilidad de los Sistemas Socioecológicos), *Science* 325 (24 de julio de 2009): 419–22.

20. Una opinión de “responsabilidad estatal” es elaborada en el borrador ruso para una “*Convention on International Information Security*” (Convención internacional sobre la seguridad de la información), presentada en la *Second International Meeting of High-Level Officials Responsible for Security Matters* (Segunda reunión internacional de funcionarios de alto nivel responsables de los asuntos de seguridad), Ekaterinburg, Russia, 22 de septiembre de 2011, <http://2012.inforum.ru/2012/files/konvencia-mib-en.doc>. Un problema con cualquier plan que les asigna responsabilidad a los estados por los comportamientos cibernéticos de sus vecinos es que muchos estados carecen de la concienciación de la seguridad cibernética, la capacidad y las destrezas de computación forense. Este problema y el papel que desempeñan muchas naciones avanzadas tecnológicamente de ayudar a que los menos avanzados incrementen sus capacidades son reconocidos en *US International Strategy for Cyberspace* (Estrategia Internacional Estadounidense para el Ciberespacio) y la Resolución de la Asamblea General de la ONU, “*Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures*” (Creación de una cultura global de seguridad cibernética y evaluación de los esfuerzos nacionales por proteger las infraestructuras de información crítica) A/Res/64/211, 17 de marzo de 2010, <http://www.citizenlab.org/cybernorms/ares64211.pdf>.

21. Chris Demchak y Peter Dombrowski, “*Rise of a Cybered Westphalian Age*” (Surgimiento de una era westfaliana cibernética) *Strategic Studies Quarterly* 5, no. 1 (Primavera 2011), 32–61.

22. Bus, “*Societal Dependencies and Trust*” (Dependencias sociales y confianza) 21.

23. Stein Schjøllberg, “*Wanted: a United Nations Cyberspace Treaty*” (Se busca: Un tratado ciberespacial de las Naciones Unidas) en Andrew Nagorski, editor, *Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway* (Disuasión cibernética global: Opiniones de China, Estados Unidos, Rusia, India y Noruega) (New York: EastWest Institute, 2010), 11.

24. Ellen Nakashima y William Wan, “*In China, Business Travelers Take Extreme Precautions to Avoid Cyber-Espionage*” (En China, viajeros comerciales toman precauciones extremas para evitar el espionaje cibernético) *Washington Post*, 26 de septiembre de 2011, http://www.washingtonpost.com/world/national-security/in-china-business-travelers-take-extreme-precautions-to-avoid-cyber-espionage/2011/09/20/GIQA6cR0K_story.html. Consultar también a Joel Brenner, *America the Vulnerable* (Estados Unidos, el vulnerable) (New York: Penguin Press, 2011), 61ff.

25. Resolución 64/211 de la Asamblea General de la ONU: “*Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures*” <http://www.citizenlab.org/cybernorms/ares64211.pdf>.

26. UN General Assembly Resolution 65/201: “*Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*” <http://www.unidir.org/pdf/activites/pdf5-act483.pdf>.

27. Touré et al., *Quest for Cyber Peace*, 16.

28. *Ibid.*, 25.

29. Discurso del Secretario de Relaciones Exteriores William Hague, “*Security and Freedom in the Cyber Age—Seeking the Rules of the Road*” (Seguridad y libertad en la era cibernética—buscando las reglas del juego) discurso ante la Conferencia de Seguridad en Munich, 4 de febrero de 2011, <http://www.fco.gov.uk/en/news/latest-news/?view=Speech&id=544853682>.

30. Según la famosa ley de Metcalfe, el valor de una red es en proporción al número de conexiones cruzadas entre sus usuarios N , o sea N^2 . El crecimiento (o descenso) en valor con cada usuario que se une (abandona) la red es en proporción a $2N$. La ley de Leek que es más extrema, iguala el valor de la red con el número de audiencias específicas que se pueden formar del número de usuarios, v.gr., el número de conjuntos secundarios menos el conjunto nulo de N o $2N^2$. Por lo tanto el valor de la red se duplicaría increíblemente (o se dividiría en la mitad) con cada usuario que se une (o abandona) la red. Una solución más razonable, especialmente para redes grandes, asume el uso diferencial por aquellos en la red. Consistente con las leyes de energía (fenómenos a largo plazo), se supone que el uso disminuya de forma exponencial con la demora en unirse a la red. El uso o transacciones sobre los usuarios N describe una hipérbola, con los primeros en unirse son los que más usan la red. El beneficio acumulativo, por ende el valor de la red, es entonces proporcional al área debajo de la curva o el logaritmo natural de N ($\ln N$). El incremento (descenso) en el valor de la red con cada persona que se une (o abandona) es significativamente menos que el calculado por la ley de Metcalfe, y el

cambio es que disminuye en lugar de aumentar. Por lo tanto, si para el proveedor de la red el coste de adquirir un usuario es fijo, se llegará a un punto en la disminución de ganancias del valor.

31. Mi agradecimiento a Phillip Hallam-Baker por la discusión sobre este punto.

32. Borrador Ekaterinburg.

33. Michael Bohm, “*Putin Chasing Imaginary American Ghosts*” (Putin persigue fantasmas estadounidenses imaginario) *Moscow Times*, 9 de febrero de 2012,

<http://www.themoscowtimes.com/opinion/article/putin-chasing-imaginary-american-ghosts/452802.html><http://www.themoscowtimes.com/opinion/article/putin-chasing-imaginary-american-ghosts/452802.html>.

34. Ver Resolución 62/211 de la Asamblea General de la ONU: “Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures,” adoptada el 17 de marzo de 2010.

35. Ronald Deibert y Rafal Rohozinski, “*Contesting Cyberspace and the Coming Crisis of Authority*” (Contienda en el ciberespacio y la crisis venidera de la autoridad) en Deibert et al., *Access Contested* (Acceso impugnado), 21–41.

36. Brenner, *America the Vulnerable*, 239–44; y Brenner, comunicación personal, 2010.

37. Apps, “Disagreements on Cyber Risk East-West ‘Cold War.’”

38. Bus, “Societal Dependencies and Trust,” 24.



El Dr. Roger Hurwitz, PhD, es un científico investigador en el Computer Science and Artificial Intelligence Laboratory (CSAIL) (Laboratorio de Ciencias Computacionales e Inteligencia Artificial [CSAIL] de MIT), profesor emérito en el Canada Centre for Global Security Studies (Centro de Estudios de Seguridad Global de Canadá) en la Universidad de Toronto, y fundador de Explorations in Cyber International Relations (ECIR) (Exploraciones en Relaciones Cibernéticas Internacionales [ECIR]), un programa de Iniciativa de Investigación Minera en Harvard y MIT. Entre sus obras actuales se encuentra la investigación de normas cibernéticas internacionales, el desarrollo de sistemas computacionales para datos de eventos y ontología cibernética, y creación de modelos de las complejidades de incidentes cibernéticos de gran repercusión. La labor del Dr. Hurwitz es sufragada por la Office of Naval Research (Oficina de Investigaciones de la Armada). Cualquier opinión, hallazgo y conclusiones o recomendaciones que se expresan en este artículo son las del autor y no necesariamente reflejan la opinión de la Oficina de Investigaciones de la Armada.

Búsqueda y Rescate en el Alto Norte:

¿Una Misión de la Fuerza Aérea?

CORONEL JOHN L. CONWAY III, USAF, RETIRADO

Los buscadores de oro hacen cosas extrañas en el sol de medianoche.

—Robert W. Service

El “Bardo del Yukon” se sorprendería con las extrañas cosas nuevas en la tierra del sol de medianoche. Lo que no le sorprendería son las cosas que nunca cambian: seis meses de oscuridad, peligro constante, frío entumecedor, y aventureros dispuestos a enfrentar estas tres cosas en búsqueda de fama, fortuna, o simplemente “una buena mirada a su alrededor”. Algunas de sus motivaciones incluyen depósitos inexplorados de petróleo y gas natural, la descongelación sin precedentes (en la historia conocida) del hielo del Ártico, una cruzada por los derechos territoriales, el encanto del legendario Paso del Noroeste, y “el turismo de aventura”. Todo esto ha dado lugar a una mayor actividad humana—y con ello un mayor riesgo de calamidad humana provocada por el insensato, el improvisado, o el desafortunado. La Capitana Melissa Bert, ex capitana de puerto y comandante de la Guardia Costera en el sector Juneau, hace eco de estas preocupaciones: “No me preocupa una guerra en el Ártico. . . . Pero sí me preocupa que no estemos preparados para manejar un desastre grande en el área. Nadie lo está, pero a medida que más gente vaya allí, aumenta más la probabilidad de que suceda”.¹

Un asunto de recursos inexplorados

El estimado del Estudio Geológico Estadounidense de 2008 sobre los recursos del Alto Norte, considerado el estudio más acreditado hasta la fecha, sugiere que el 13 por ciento del petróleo inexplorado del mundo y el 30 por ciento del gas natural no descubierto yacen en el Ártico.² Esto equivale a unos 90 mil millones de barriles de petróleo; 1.669 billones de pies cúbicos de gas natural; y 44 mil millones de barriles de gas natural líquido; un total que supera a todas las demás cantidades conocidas de petróleo y gas natural en el Ártico.³ Como la mayor parte del territorio ártico ha sido reivindicada, en términos prácticos la “carrera” por estos recursos naturales explotables casi ha terminado. Sin embargo, la explotación económica mediante derechos de arriendo y nodos de transporte siguen siendo poderosos incentivos.

Debido a que muchos de estos recursos quedan en aguas costeras relativamente poco profundas (150 metros), “son técnicamente recuperables” pero no necesariamente “económicamente recuperables”—es decir, no existe infraestructura para desarrollar petróleo y gas mar adentro en el Ártico, particularmente en América del Norte. Los estimados indican que pasará por lo menos una década antes de que se disponga del capital y la tecnología para comenzar seriamente el proceso de extracción.⁴ El altamente publicitado y costoso intento de Royal Dutch Shell (más de 4,5 mil millones de dólares) de ser el primero en perforar intensamente en el Mar de Chukchi pone en relieve estos problemas. En 2012 la empresa solo perforó modestos pozos exploratorios, una meta distante de los seis pozos profundos planeados, antes de abandonar sus esfuerzos al acercarse el fin de la corta temporada. Posteriormente, su barco de perforación encalló en una isla deshabitada 300 millas al suroeste de Anchorage, y como consecuencia se incrementaron las exigencias de una regulación ambiental más estricta de la exploración costa afuera. Shell ha cancelado sus planes para la próxima temporada de exploración, causando que otros examinen

con cuidado sus planes propuestos.⁵ No obstante, no se puede impedir el atractivo de esta gran cantidad de petróleo y gas inexplorado por mucho tiempo, a pesar de la inquietante preocupación de que ocurrirán desastres similares en las etapas iniciales de la explotación y extracción.

Los pasos a través de la zona más septentrional del mundo

El Alto Norte también encierra la promesa de una ruta de tránsito más corta entre el Lejano Oriente y Europa: el sueño de siglos del Paso del Noroeste (figura 1) y la apertura de una ruta marítima a través de la parte norte de Rusia. La Ruta del Mar Septentrional, que sigue estrechamente la línea costera a lo largo de la franja septentrional de Rusia, ha visto más tránsito de transporte ártico que su contraparte canadiense. Cuarenta y seis nave transitaron esta ruta en 2012, transportando más de un millón de toneladas de carga—un 53 por ciento de aumento en tonelaje en relación a 2011. Más barcos, asistidos por la considerable flota de rompehielos de Rusia (más de 30), aumentarían ese total en los próximos años, y China ha anunciado su primer viaje comercial por el lugar para este verano.⁶ El tráfico marítimo de apoyo a las operaciones de perforación también continúa creciendo. El retroceso de la cobertura de hielo marino en el Alto Norte durante el verano ha hecho que el muy buscado Paso del Noroeste sea una nueva realidad—por lo menos a fines del verano y comienzos del otoño. Los pronósticos de que esa ruta “competiría con el Canal de Suez” y estaría “libre de hielo” para 2015 han tenido que aceptar a regañadientes una estimación más moderada de ambas; no obstante, la promesa de un paso libre de hielo y una ruta marítima más corta hacia y desde Europa y Asia continúa ganando tracción y atención internacional.⁷

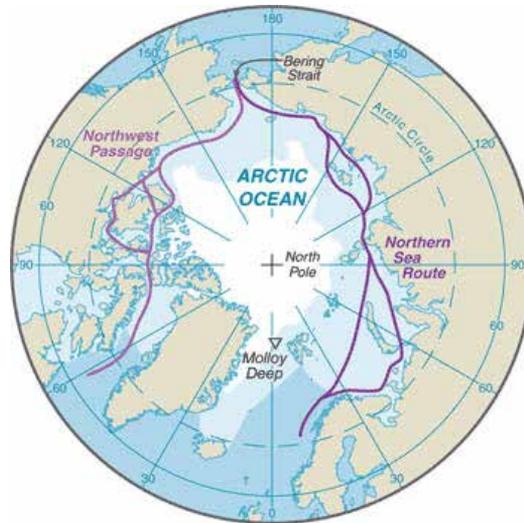


Figura 1. El Paso del Noroeste y la Ruta Marítima Septentrional. (Reimpresión de “Océano Ártico”, en Agencia Central de Inteligencia, *The World Factbook*, consultado el 3 de septiembre de 2013, <https://www.cia.gov/library/publications/the-world-factbook/geos/xq.html>.)

El Paso del Noroeste incluye en realidad más de una ruta a través del Archipiélago Canadiense, una extensión de territorio que consiste de 73 islas principales y 18.114 islas más pequeñas que abarcan un área aproximadamente igual al tamaño de Groenlandia. El paso de más al sur tiene una profundidad sumergida de solo 13 metros mientras que el del norte tiene una profundidad promedio de 200 metros. El canal de más al sur, el Estrecho Unión, encierra la

promesa de menos hielo pero no lo podrían usar las naves de profundidad sumergida grande. Hacia el norte, el recientemente abierto Estrecho de McClure (2007) es más profundo pero tiene más hielo.⁸ Un estudio noruego de 2011 lista no menos de siete rutas diferentes a través del Paso del Noroeste, explicando que el canal de navegación actual ofrece las mejores condiciones de hielo marino en el momento.⁹

Aunque algunos observadores usan el término *libre de hielo* para describir el Paso del Noroeste, se debe tener cuidado porque incluso el “mar abierto” puede contener témpanos de hielo. *Libre de hielo* es un eslogan para los comentaristas de prensa, pero los expertos prefieren el término más preciso de *con menos hielo*.¹⁰ Además, incluso esa descripción indica que aún hay hielo presente. El geógrafo canadiense Frédéric Lasserre señala las formaciones de hielo multitemporada (congeladas, deshieladas y recongeladas) que son particularmente densas y muy difíciles de identificar como riesgos importantes a la navegación a través de cualquier estación “libre de hielo” o “con poco hielo”.¹¹

El profesor Michael Byers de la Universidad de British Columbia concurre, agregando que el adelgazamiento del hielo produce más témpanos en las aguas del Ártico Oriental a medida que los glaciares de Groenlandia se mueven más rápidamente hacia el mar. El hielo glacial es muy duro, explica él, y los “témpanos sumergidos” de hielo glacial son especialmente peligrosos incluso para los barcos “con refuerzo para hielo”, aquellos con casco reforzado pero sin capacidad rompehielo. No obstante el hundimiento del barco de pasajeros con refuerzo para hielo *MS Explorer* en el Antártico en 2007 sobresale como un ejemplo cruel de lo que puede pasar cuando incluso una nave como esa choca con hielo de varios años.¹² La evaluación noruega pinta una imagen aún más desalentadora. Refutando el término *libre de hielo*, sostiene que “la mayoría de expertos del transporte Ártico ven este término como indicando hielo infestado con témpanos, témpanos medianos y témpanos sumergidos”, concluyendo que “desde el punto de vista de un marinero ‘... con menos hielo, se necesitará más capacidad rompehielo’.”¹³

Quizás la discusión más moderada—entre docenas de opiniones contrarias—de un derretimiento inminente de hielo del Ártico viene del Centro para Soluciones de Clima y Energía en su documento *Climate Change & International Security: The Arctic as a Bellwether (Cambio climático y seguridad internacional: El Ártico como barómetro)* (2012).¹⁴ Ese estudio indica tres fechas para un Ártico libre de hielo (es decir, 80 por ciento de pérdida de hielo marino histórico durante el verano) basado en extrapolaciones lineales y no lineales de la extensión mínima de hielo marino en el verano. Como cabe esperar, estas proyecciones varían ampliamente entre 2025 y 2072.¹⁵ El asegurador Lloyds de Londres, más interesado en las ganancias que en la grandilocuencia, está de acuerdo con las predicciones científicas de rango medio pero advierte que el hielo más delgado puede significar más acción de las olas y destrucción más abrupta de la placa de hielo, aumentando la incertidumbre total. En realidad, el Paso del Noroeste es una dinámica compleja de hielo, islas y condiciones climáticas cambiantes que hacen que el tránsito sea un desafío y el desastre dependa solo de una mala decisión.

Los entusiastas exaltan las rutas de transporte más cortas a través del Ártico y predicen un renacimiento del transporte polar, pero éste no es el caso. El transporte hacia el Asia desde puertos del Mediterráneo (por ejemplo, de Marsella a Shanghai) no proporciona ventaja económica basada en distancia mientras que los destinos de alta latitud a alta latitud—digamos, de Marsella a Yokohama—sí ofrecen tal ventaja. Un análisis de 20 pares de ciudades que podrían usar el Paso del Noroeste o la Ruta Marítima Septentrional encontró que solo tres de ellas son más cortas a través del Paso del Noroeste.¹⁶ No obstante, la posibilidad de rutas marítimas más cortas hacia y desde los mercados de Asia y Europa a través del Alto Norte continúa atrayendo más atención y mayor actividad humana.

Actualmente, solo transatlánticos, aventureros privados, y unas cuantas naves comerciales se aventuran por el Paso del Noroeste, pero un aumento importante en el tránsito (69 [1906–2006]; 40 [2010–11]; y más de 30 en 2012) preocupa a los expertos en búsqueda y rescate (SAR)

que ven un desastre potencial en un entorno despiadado.¹⁷ Los expertos destacan también las ayudas de navegación deficientes como un contribuyente importante a las preocupaciones de seguridad a lo largo del Paso del Noroeste. Un artículo del *Wall Street Journal* resalta el problema dominante de la cartografía del fondo marino: “En general, los mapas de Marte son unas 250 veces mejores que los mapas del fondo marino de la Tierra.” Otro informe advierte que a la tasa actual de trabajo, un levantamiento cartográfico completo de las aguas del Ártico Canadiense tardaría tres siglos.¹⁸

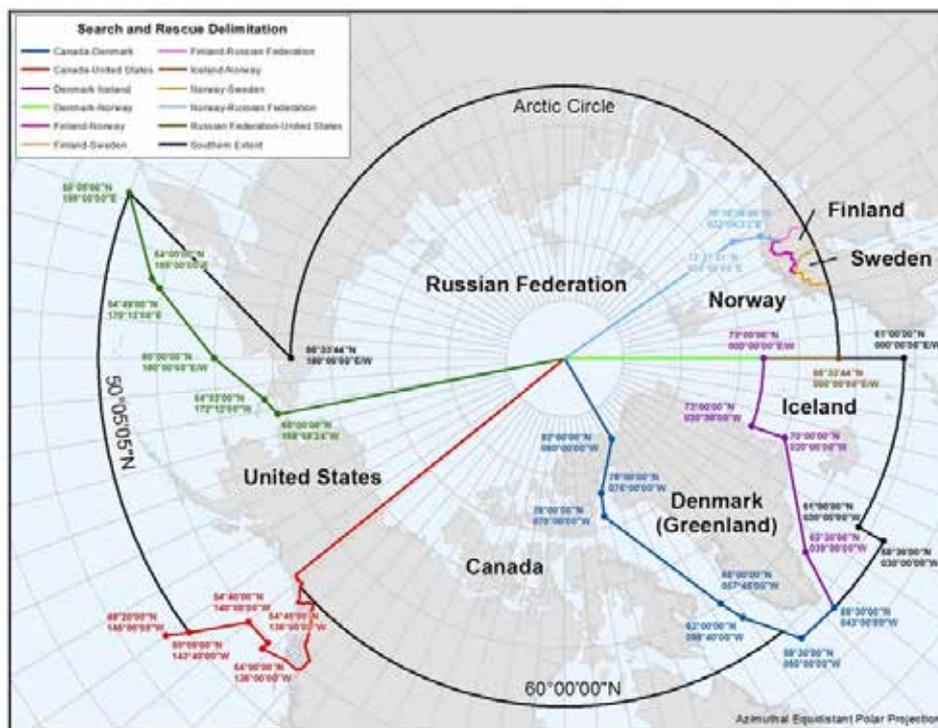


Figura 2. Acuerdo de SAR del Ártico, áreas de aplicación. (Basado en las coordenadas geográficas en el anexo al *Acuerdo sobre Cooperación en Búsqueda y Rescate Aeronáutica y Marítima en el Ártico*, 12 de mayo de 2011, <http://www.ifrc.org/docs/idrl/N813EN.pdf>. Mapa del “Acuerdo de Búsqueda y Rescate en el Ártico”, Portal del Ártico, consultado el 3 de septiembre de 2013, <http://arcticportal.org/features/751-arctic-search-and-rescue-agreement>.)

El Consejo del Ártico y el Acuerdo de Búsqueda y Rescate de Nuuk

En 1996, ocho naciones con territorio o intereses claramente definidos en la región (Estados Unidos, Canadá, Rusia, Finlandia, Noruega, Dinamarca, Islandia y Suecia) formaron el Consejo del Ártico “para proporcionar un medio de fomentar la cooperación e interacción entre los Estados del Ártico, con la participación de las comunidades indígenas del Ártico y otros habitantes del Ártico sobre asuntos comunes del Ártico”.¹⁹ El consejo solo trata asuntos no relacionados con la seguridad que enfrentan los estados del Ártico; las poblaciones indígenas de la región y los observadores lo catalogan como “formado más por científicos y estudiosos que por estadistas”.²⁰

Consciente de su propuesta anterior de 2008 para “fortalecer más las capacidades de búsqueda y rescate en torno al Océano Ártico”, el consejo firmó un tratado de SAR en Nuuk, Groenlandia, en 2011—*El Acuerdo sobre Cooperación en Búsqueda y Rescate Aéreo y Marítimo en el Ártico (el Acuerdo de Nuuk)*, donde se declara que cada parte establecerá y mantendrá una “capacidad de búsqueda y rescate adecuada y efectiva” dentro de su área designada (figura 2).²¹ Además, obliga a las naciones miembro a coordinar los esfuerzos de SAR en caso de accidentes aéreos, hundimientos de barcos crucero, derrames de petróleo, u otros desastres a través del Alto Norte.²²

Estados Unidos es responsable de las operaciones de SAR en Alaska y una franja amplia de los accesos al Estrecho de Bering. Esto también abarca las proximidades occidentales al Paso del Noroeste y las proximidades orientales a la Ruta Marítima septentrional, paralelas a la Península de Kamchatka en Rusia. Estados Unidos tiene también responsabilidad de SAR en los Mares de Beaufort, Chukchi, y del Ártico que se extienden hasta el Polo Norte. Aunque no es el área más grande mencionada en el *Acuerdo de Nuuk*, su tamaño podrá a prueba los recursos estadounidenses. Un punto clave en el acuerdo—que hace reflexionar a los planificadores de SAR—es que cualquiera de las partes puede solicitar asistencia de cualesquier otra parte o partes si es necesario, garantizando que se “proporcione asistencia a cualquier persona en peligro”.²³

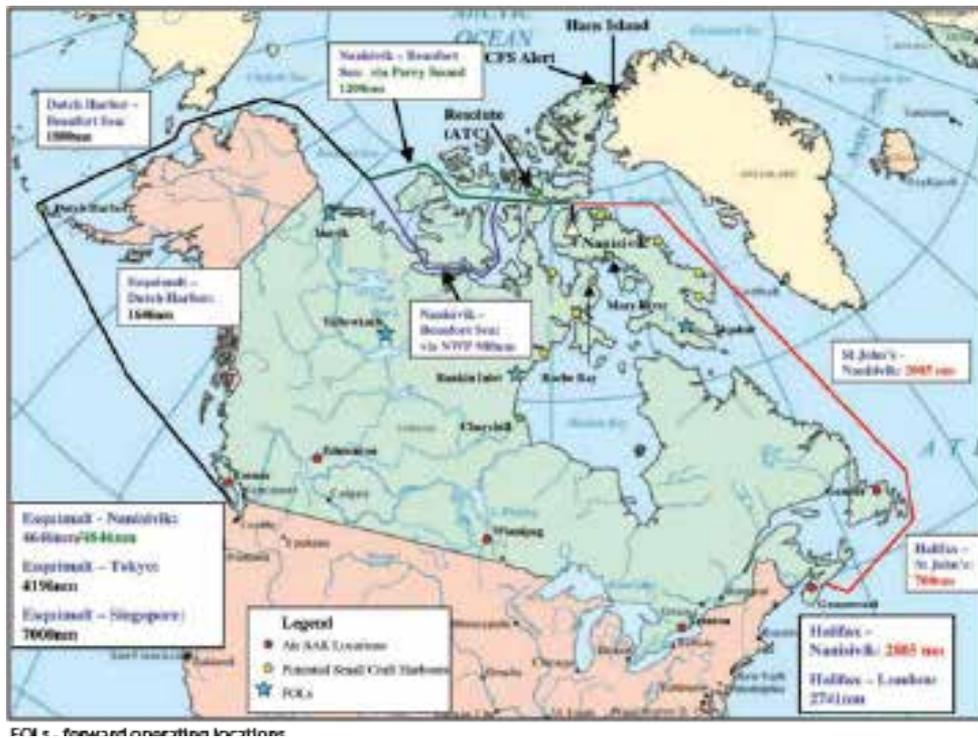


Figura 3. Distancias de patrulla operacional en el Ártico. (Reimpresión de Michael Byers y Stewart Webb, *Titanic Blunder: Arctic/Offshore Patrol Ships on Course for Disaster* (El error del Titanic: Buques patrulla de alta mar en el Ártico en ruta al desastre) [Ottawa: Rideau Institute, Centro Canadiense para Alternativas de Política, abril de 2013], 37, http://www.policyalternatives.ca/sites/default/files/uploads/publications/National%20Office/2013/04/Titanic_Blunder.pdf.)

A pesar del mayor número de tránsitos sin problemas por el Paso del Noroeste, las noticias de otros tres cruceros de pasajeros en 2013 ha suscitado la preocupación de que un desastre importante allí recibiría una respuesta lenta de las fuerzas de rescate —consideradas por algunos como demasiado distantes y de reducido número para ayudar rápidamente (figura 3).²⁴ La colocación de los activos de SAR de Canadá resalta este dilema potencial: que el único centro de coordinación de rescate (CCR) del país en Trenton, Ontario, abarca la mayor parte del Ártico canadiense, pero está situado más cerca de la costa norte de América del Sur, por ejemplo, que de la Estación de Fuerzas Canadienses en Alert, Nunavut.²⁵

El tiempo de vuelo desde Winnipeg hasta Resolute Bay en el corazón del Paso del Noroeste en un C-130H de Canadá dura más de cinco horas; los helicópteros hacia la misma área desde Comox tardarían más de 11 horas.²⁶ Aunque un CC-177 de las Fuerzas Canadienses (la versión canadiense del C-17 de la USAF) demostró que puede aterrizar y despegar desde la pista de aterrizaje de grava de 1.670 metros de largo en la Estación de las Fuerzas Canadienses en Alert, ésta no es la aeronave principal de SAR de Canadá y en ocasiones no estaría disponible para esa misión.²⁷ Los defensores del concepto actual de bases de aeronaves señalan que la mayoría de rescates ocurren en la parte sur de Canadá, no en el Alto Norte. Sin embargo, aumenta la presión para ampliar la presencia de SAR en el Ártico Canadiense hacia el norte. Los activos marítimos principales del Alto Norte de Canadá, dos rompehielos, tienen la enorme tarea de patrullar los 2,222 kilómetros del Paso del Noroeste.²⁸ Hasta el momento, la suerte ha estado del lado de ellos. En 2010 los 120 pasajeros del “crucero de expedición para adultos mayores” reforzado para hielo, *Clipper Adventurer*, fueron evacuados por un rompehielos de la Guardia Costera de Canadá que estaba en las cercanías (dos días de viaje) después que el barco encalló en el Golfo de la Coronación del Mar de Beaufort.²⁹ El tráfico aéreo y marítimo está aumentando rápidamente en el Alto Norte, aumentando la probabilidad de que ocurran contratiempos. Dada la insuficiencia de activos canadienses, en cantidad y colocación, la probabilidad de que se solicite la asistencia de Estados Unidos a los rescatistas canadienses también aumenta.

El papel de Estados Unidos en SAR del Alto Norte: Es la tarea de la Guardia Costera

Según el *Acuerdo de Nuuk*, la Guardia Costera es la “autoridad competente” de los Estados Unidos en los esfuerzos de SAR. Más importante aún, se señala al servicio y al Departamento de Defensa como las “agencias” de SAR de EE.UU. Los CCR estadounidenses en el acuerdo incluyen el Centro de Coordinación de Rescate de Aviación de Elmendorf en la Base Conjunta Elmendorf–Richardson (JBER) y el Centro de Coordinación de Rescate en Juneau, Alaska.³⁰ Aunque la Guardia Costera tiene bases permanentes en Alaska, todas ellas se encuentran situadas por debajo del Círculo Ártico. Las aeronaves de la Guardia Costera tienen base permanente en Kodiak, unos 1.287 km al sur de Point Barrow, requiriendo el tránsito sobre la cordillera Brooks de 2.700 metros de altura hasta la Vertiente del Norte. El puerto importante más cercano a Point Barrow está en las Islas Aleutianas, otros 805 km al sur, y esta primavera la Guardia Costera anunció que no tenía planes de desarrollar ninguna infraestructura costera en la década entrante.³¹ Los draconianos recortes a la solicitud de presupuesto del servicio para el año fiscal 2014 recayeron con fuerza sobre los activos de aviación, limitando sus opciones de respuesta de aviación en el corto plazo.³²

El estudio *Resumen final del análisis de misión en la Región de Gran Latitud de la Guardia Costera de los Estados Unidos* de 2010 también proponía una flota de rompehielos bastante más grande para aumentar la flota de un rompehielos mediano y un rompehielos pesado de la Guardia Costera, pero la solicitud de presupuesto para el año 2014 incluye solo \$2 millones de dólares para estudios de diseño de un proyecto de unos mil millones de dólares durante unos 10 años.³³ Construir

solo uno no será suficiente: se necesitan tres rompehielos pesados y tres medianos solo para cumplir los requisitos reglamentarios mínimos de la Guardia Costera.³⁴ *La Estrategia del Ártico* de 2013 del servicio señala la “ampliación de asociaciones” como uno de sus objetivos estratégicos pero no detalla específicamente quiénes serán esos socios.³⁵

El año 2014 puede ser decisivo en el Alto Norte para los planes del Ártico de la Marina. *El Mapa de ruta del Ártico* posterga toda decisión importante de estructura de fuerzas del Ártico hasta el *Informe de Revisión Cuadrienal de la Defensa* de 2014. Incluso si la Marina propone en ese informe una función mayor en el Ártico, los fondos y el equipo no estarán disponibles por una década o más.³⁶ Un aspecto común en el *Mapa de Ruta* de la Marina, el *Resumen de Regiones de Gran Latitud* de la Guardia Costera, y su nueva *Estrategia del Ártico* es la ausencia de alternativas de respuesta a desastres distintas de rompehielos y activos de aviación orgánicos de la Guardia Costera/Marina—incluyendo la exclusión evidente de la Fuerza Aérea. Esta última es mencionada brevemente en el *Mapa de Ruta* de la Marina en relación a “acuerdos existentes” así como “operaciones de vigilancia y estado del tiempo por satélite”, pero es invisible en el *Resumen de Regiones de Gran Latitud* de la Guardia Costera y su *Estrategia del Ártico*.³⁷

No obstante, existe el requisito general de que Estados Unidos asista a los firmantes del *Acuerdo de Nuuk* si se le solicita. Rusia con sus más de 30 rompehielos, importante población en el Ártico, y la resurgente Flota del Norte, parece capaz de realizar operaciones de SAR sin ayuda externa. Sin embargo, Canadá podría necesitar nuestra asistencia en el Paso del Noroeste para complementar sus limitados recursos. Tanto Canadá como Groenlandia pueden solicitar la ayuda estadounidense para SAR en los accesos orientales al paso del Noroeste.

“¿A quién se va a llamar?”

Los activos de la Fuerza Aérea ya realizan misiones de SAR en Alaska, coordinadas a través del RCC No. 11 en JBER, usando helicópteros y aviones de ala fija del Ala No. 176 de la Guardia Nacional Aérea de Alaska.³⁸ Todas las aeronaves de la Fuerza Aérea en Alaska deben ser parte los esfuerzos de SAR, particularmente a lo largo del Paso del Noroeste, los accesos al Estrecho de Bering, y en los Mares de Beaufort y Chukchi. Además, la Fuerza Aérea tiene los recursos y la capacidad para llegar a cualquier lugar de desastre en el Alto Norte con más rapidez que otras naves de superficie—sean éstas estadounidenses, canadienses, o de otro país—y proporcionar apoyo de comando, control y comunicaciones hasta que se resuelva la crisis. Su enfoque de SAR en el Alto Norte debe centrarse en tres elementos: bases, aeronaves y asociaciones.

Bases

Hay dos bases de la Fuerza más al norte de los 60 grados, bien posicionadas para el lanzamiento y recuperación de cualquier esfuerzo de SAR: Eielson AFB a 64°39'56"N y Thule Air Base (con su pista de aterrizaje de 3.050 metros de largo), 1200 km al norte del Círculo Ártico a 74°31'52"N. Al sur de Eielson se encuentra JBER con otra pista de aterrizaje de 3.050 metros así como el RCC No. 11. En el borde exterior de la cadena de Islas Aleutianas se encuentra la Estación de la Fuerza Aérea de Eareckson (anteriormente Shemya AFB), un campo de aterrizaje alternativo o de emergencia, y planta de reabastecimiento de combustible administrada por contratistas y el sitio de una instalación de radar “Cobra Dane” de la Fuerza Aérea. La pista de aterrizaje de 3.050 metros de Eareckson y varios hangares constituyen una base en el lejano oeste para cualquier operación de SAR.

Aeronaves

El número y la variedad de aeronaves de la Fuerza Aérea disponibles en Eielson y JBER ampliarían enormemente las opciones de respuesta de SAR. Eielson es base del Ala de Cazas No. 354 (F-16s) y el Ala de Reabastecimiento Aéreo de Combustible No. 168 de la Guardia Nacional Aé-

rea de Alaska. JBER sirve de base al Ala No. 176 de la Guardia Nacional Aérea (aviones C-17 y C-130 así como aeronaves HC-130 y HH-60G para SAR). También sirve de base a la Tercera Ala de la Fuerza Aérea, con C-17s y C-12s, los aviones del Sistema de Advertencia y Control Aero-transportado E-3, varios cazas, y dos centros de operaciones aéreas y del espacio. Como Canadá ha demostrado que los C-17 pueden operar desde una pista de grava de 1.670 metros de largo en la parte norte de Canadá, los C-17 de la Fuerza Aérea podrían hacer lo mismo.³⁹

Otro activo de SAR (fuera de Alaska), el Ala Aerotransportada No. 109 de la Guardia Nacional de Nueva York, equipada con esquí, tiene amplia experiencia en el Antártico y ha realizado misiones para la Fundación Nacional de Ciencias en el Ártico. Las rotaciones de aeronaves hacia Alaska, similares a las asignaciones temporales en el Antártico, podrían reforzar a otros activos y ofrecer otra opción de SAR. Las aeronaves a control remoto también pueden desempeñar una función. *El Mapa de Ruta del Ártico de la Marina* proponía que esas plataformas realicen “recopilación de datos, monitoreo e investigación”, pero las misiones de SAR que utilizan Global Hawk podrían añadir una unidad de apoyo persistente para toda la región.⁴⁰ Los Global Hawk podrían cubrir un área hasta el Polo Norte y—si los vientos y el tiempo lo permiten—a través de toda la longitud del Paso del Noroeste y sus proximidades.⁴¹

Debemos enfatizar que SAR en el Alto Norte no es una misión que dure todo el año, a pesar de las declaraciones de rutas “libres de hielo” inminentes. La estación de punta para actividades—entre marzo y principios de octubre—seguirá siendo predecible por algún tiempo más. De conformidad con la política de la Oficina del Secretario de Defensa de que dice que “SAR . . . no es una misión de determinación de tamaño o forma de fuerza para [el Departamento de Defensa]“ pero que el departamento contribuirá “cuando se le necesite y según su disponibilidad”, no se crearían nuevos activos de SAR.⁴²

Asociaciones

La coordinación de los esfuerzos de SAR de la Fuerza Aérea pueden constituir el desafío más grande. Por ejemplo, el *Plan de Comando Unificado* de 2011 realineó áreas de responsabilidad (ADR) en el Alto Norte (figura 4). Anteriormente, el Comando del Pacífico de EE.UU. (PACOM) tenía un área desde el Estrecho de Bering hasta el Polo Norte y hacia el oeste a lo largo de la costa de Siberia hasta el Mar de Kara. El realineamiento de 2011 mantuvo el litoral del Pacífico Ruso en el ADR de PACOM, pero nada hacia el norte. Mientras tanto, las proximidades orientales al Estrecho de Bering, antes una responsabilidad compartida con el Comando del Norte de EE.UU. (NORTHCOM), son ahora responsabilidad única de NORTHCOM. PACOM retiene la responsabilidad de las proximidades occidentales extremas hasta el Estrecho de Bering y los mares adyacentes a Rusia Siberiana, pero nada hacia el norte u oeste. La responsabilidad de Alaska es ahora únicamente de NORTHCOM.

Sin embargo, los activos de la Fuerza Aérea en Alaska pertenecen principalmente a las Fuerzas Aéreas del Pacífico (PACAF) (PACOM). Esta dicotomía quiere decir que NORTHCOM/Fuerza de Tareas Conjunta de Alaska tiene que usar aeronaves de PACAF (PACOM) basadas en Alaska para disuadir la agresión, defender el espacio aéreo, responder a los desastres naturales y causados por el hombre en la región, y llevar a cabo SAR. Simultáneamente, PACAF ha de preparar estos mismos recursos con base en Alaska para realizar las tareas de tiempo de paz y el adiestramiento de tiempo de guerra de PACOM.⁴³ Las proximidades orientales al Paso del Noroeste adyacentes a Groenlandia y la costa este de Canadá quedan en el ADR del Comando Europeo de EE.UU., y NORTHCOM tendría que coordinar con ese comando si llegara al Departamento de Defensa algún pedido de SAR de esa transitada región.⁴⁴ Además, la Fuerza Aérea debe desarrollar una estrecha colaboración con la Guardia Costera para que cada uno pueda entender la misión y las capacidades de conducción de SAR del otro. Esta sinergia debe beneficiar a ambas organizaciones. Igualmente, las Fuerzas Canadienses y la Fuerza Aérea deben forjar una relación

Las fuerzas Norteamericanas actuales y proyectadas de SAR son inadecuadas para la tarea debido a la distancia y los recursos disponibles. El uso de todo lo anterior para realizar rescates no es solo sensato sino también imperativo. En consecuencia, tanto la Guardia Costera como el Departamento de Defensa podrían recibir el pedido de ayuda de nuestro vecino. El *Acuerdo de Nuuk* proporciona el marco estructural de todo esto, y requiere que las naciones firmantes extiendan ayuda de SAR a cualquier nación que la solicite. El silencio actual de los planificadores de la Guardia Costera y de la Marina, así como su dependencia en los rescates de superficie que utilizan recursos escasos, no es congruente con las realidades de tiempo y distancia. La Fuerza Aérea está posicionada para ayudar, pero no es sensato montar un esfuerzo de SAR sin planificación ni coordinación previa. Es tiempo de agregar el peso de la Fuerza Aérea al esfuerzo, comenzar el proceso de coordinación y prepararse para asistir. □

Notas

1. Peter Apps, "Melting Arctic May Redraw Global Geopolitical Map (El derretimiento del Ártico podría redibujar el mapa geopolítico global)," Reuters, 3 de abril de 2013, <http://www.reuters.com/article/2012/04/03/us-arctic-resources-idUSBRE8320DR20120403>. La Capitana Bert se desempeña actualmente como jefe de la División Legal Marítima e Internacional en el Cuartel General de la Guardia Costera de los Estados Unidos, en Washington, DC.
2. Estimación del Servicio Geológico Estadounidense tal como se cita en el informativo estándar, Dirección General para Políticas Exteriores de la Unión, Dirección B, Departamento de Política, Parlamento Europeo, asunto: La Geopolítica de los Recursos Naturales del Ártico, 31 de agosto de 2010, 4, <http://www.tepsa.eu/download/Valor%20Ingenimundarson.pdf>. Véase también Servicio Geológico Estadounidense, "GIS Data: Circum-Arctic Resource Appraisal (North of the Arctic Circle) Assessment Units (Datos GIS: Unidades de estimación de la valoración de recursos del círculo polar ártico (Norte del Círculo Polar Ártico)", 2009, <http://energy.usgs.gov/RegionalStudies/Arctic.aspx#3886226-gis-data>.
3. Siete áreas en el Ártico contienen aproximadamente el 87 por ciento de las reservas conocidas de petróleo y gas. Dos son a horcajadas de Groenlandia, tres más abrazan la costa norte de Rusia y sus aguas adyacentes, y las últimas dos quedan a lo largo de la costa de Alaska y el Territorio del Yukon en Canadá. La mayor parte del gas natural sin desarrollar queda en Rusia Asiática mientras que se estima que la Cuenca de Alaska del Ártico contiene más del 40 por ciento (29.960 millones de barriles) de la totalidad del petróleo del Ártico no descubierto —más del triple de la cantidad del siguiente campo más grande (la Cuenca de América-Asia). Toda esta supuesta abundancia debe ser moderada por la fría realidad: los expertos en petróleo y gas consideran que incluso si se explotaran plenamente, los campos del Ártico no sustituirán a los recursos y la capacidad del Oriente Medio. Hobart King, "Oil and Natural Gas Resources of the Arctic (Recursos de petróleo y gas natural del Ártico)", Geology.com, consultado el 12 de agosto de 2013, <http://geology.com/articles/arctic-oil-and-gas/>.
4. Yue Wang, "Experts: Arctic Drilling for Security (Expertos: Perforación en el Ártico por seguridad)", UPI, 16 de julio de 2012, http://www.energy-daily.com/reports/Experts_arctic_drilling_for_security_999.html.
5. Tom Fowler, "For Shell, Wait 'til Next Year in the Arctic (Para Shell, hay que esperar hasta el próximo año en el Ártico)", *Wall Street Journal*, 31 de octubre de 2012, B10, <http://online.wsj.com/article/SB10001424052970204789304578086770366680196.html>. La empresa petrolera Statoil de Noruega anunció que postergaría sus operaciones como mínimo un año mientras que el gigante petrolero francés Total dijo que los riesgos ambientales eran demasiado grandes para continuar la exploración en el Ártico. Véase también Tom Fowler y Ben Lefebvre, "Shell Puts Off Drilling in Alaska's Arctic (Shell posterga la perforación en el Ártico de Alaska)", *Wall Street Journal*, 27 de febrero de 2013, B7, <http://online.wsj.com/article/SB10001424127887324662404578330423854552576.html>.
6. Trude Pettersen, "China Starts Commercial Use of Northern Sea Route (China inicia el uso comercial de la ruta marítima del norte)", *Barents Observer*, 14 de marzo de 2013, <http://barentsobserver.com/en/arctic/2013/03/china-starts-commercial-use-northern-sea-route-14-03>.
7. Algunos titulares seleccionados refuerzan esta noción del derretimiento prematuro del hielo: "Northwest Passage Channel Appears Free of Ice (El canal del Paso del Noroeste parece libre de hielo)", *Fierce Homeland Security*, 16 de agosto de 2012; "Study Predicts Arctic Shipping Quickly Becoming a Reality (Estudio predice que el transporte por el Ártico se convierte rápidamente en una realidad)", *Calgary Globe and Mail*, 4 de marzo de 2013; "Open Seas: The Arctic Is the Mediterranean of the 21st Century (Mares abiertos: El Ártico es el Mediterráneo del siglo 21)", *ForeignPolicy.com*, 29 de octubre de 2012; y (hasta mayo de 2013) "White House Warned on Imminent Arctic Death Spiral (Casa Blanca advertida sobre inminente espiral de muertes en el Ártico)", *Guardian*, 2 de mayo de 2013.
8. Frédéric Lasserre, "High North Shipping: Myths and Realities (Transporte en el Alto Norte: Mitos y realidades)", *en Security Prospects in the High North: Geostrategic Thaw or Freeze?* (Perspectivas de seguridad en el Alto Norte: ¿Deshielo o congelamiento geoestratégico?), Documento del Foro NDC 7, editores Sven G. Holtmark y Brooke A. Smith-Windsor (Roma: Universidad de Defensa de la OTAN, mayo de 2009), 195, http://www.google.com/url?sa=t&rct=j&q=high%20north%20shipping%3A%20myths%20and%20realities&source=web&cd=1&ved=0CCoQFjAA&url=http%3A%2F%2Fmercury.ethz.ch%2Fserviceengine%2Ffiles%2FISN%2F102391%2Fipublicationdocument_singledocument%2F517b6a62-

3f36-40be-a577-1f3a9337124c%2Fen%2Ffp_07.pdf&ei=nZoDUvq1OcuqyQGuqoCIAw&usg=AFQjCNGyNDWmyKCgLcYMfHVHUA5rk13aHw&bvm=bv.50500085,d.aWc. Canadá afirma que la totalidad del Paso del Noroeste queda dentro de territorio canadiense y debe seguir las pautas canadienses para el paso, incluyendo pedir permiso. Estados Unidos, entre otros en la comunidad internacional, sostiene que la totalidad del paso está en aguas internacionales. Esto no es un tipo de disputa de “Latitud cincuenta y cuatro cuarenta o Vamos a la batalla” entre Estados Unidos y Canadá, pero —en ocasiones— deteriora las relaciones diplomáticas.

9. Karl Magnus Eger, *Marine Traffic in the Arctic: A Report Commissioned by the Norwegian Mapping Authority (Tráfico marítimo en el Ártico: Informe encargado por la Agencia Noruega de Cartografía)*, ARHC2-04C (Oslo: Analyse & Strategi AS, 15 de agosto de 2011), 7–8, http://www.iho.int/mtg_docs/rhc/ArHC/ArHC2/ARHC2-04C_Marine_Traffic_in_the_Arctic_2011.pdf.

10. Ronald O'Rourke, *Changes in the Arctic: Background and Issues for Congress (Cambios en el Ártico: Antecedentes y problemas para el congreso)*, Informe CRS para el Congreso R41153 (Washington, DC: Servicio de Investigación del Congreso, 24 de julio de 2013), 58, <http://www.fas.org/sgp/crs/misc/R41153.pdf>. Los datos del informe de 2012 mostraron más hielo polar deritiéndose a mayor velocidad, intensificándose la discusión científica (ibid., 12).

11. Lasserre, “High North Shipping (Transporte por el Ato Norte)”, 194.

12. Michael Byers, “Canada’s Not Ready to Have the World in the Arctic (Canadá no está preparada para recibir al mundo en el Ártico)”, *Globe and Mail*, 15 de agosto de 2012, <http://www.theglobeandmail.com/commentary/canadas-not-ready-to-have-the-world-in-the-arctic/article4481519/>.

13. Eger, *Marine Traffic in the Arctic (Tráfico marítimo en el Ártico)*, 8.

14. Rob Huebert y otros *Climate Change & International Security: The Arctic as a Bellwether (Cambio climático y seguridad internacional: El Ártico como barómetro)* (Arlington, VA: Centro para Soluciones de clima y energía, mayo de 2012), <http://www.c2es.org/publications/climate-change-international-arctic-security/>.

15. Ibid., 11-12. Otro hecho interesante es que los modelos de clima basados en física demuestran que probablemente la tasa de pérdida de hielo disminuirá antes de que el Ártico avance hacia un estado libre de hielo, lo que podría causar una sobrestimación de la tasa de pérdida de hielo en futuro.

16. Lasserre, “High North Shipping (Transporte por el Ato Norte)”, 192-95. Otras tres rutas son aproximadamente equidistantes a través del Alto Norte o de la Ruta Marítima Septentrional.

17. De todo el tránsito por el Paso del Noroeste en 2012, solo dos fueron naves comerciales —el barco petrolero con refuerzo para hielo *Gotland Carolina* y el barco de pasajeros con refuerzo para hielo *Hanseatic*. “Alluring Northwest Passage—the Transit Tally So Far (La atracción del Paso del Noroeste—Número de viajes hasta el momento)”, *Sail-World.com*, 25 de febrero de 2013, <http://www.sail-world.com/CruisingAus/index.cfm?SEID=2&Nid=106937&SRCID=0&ntid=0&tickeruid=0&tickerCID=0>. Aunque este sitio indicaba 24 recorridos, los oficiales del Servicio de Guardacostas de Canadá registraron 30 cruces del Paso del Noroeste en 2012.

18. “U.S. Draws Map of Rich Arctic Floor ahead of Big Melt (EE.UU. confecciona un mapa del rico suelo del Ártico antes del gran deshielo)”, *Wall Street Journal*, 31 de agosto de 2007, <http://online.wsj.com/article/SB118848493718613526.html#articleTabs%3Darticle>. Un artículo de 2012 indica que solo un 10 por ciento de las aguas del Ártico Canadiense están cartografiadas “según las normas modernas”. Véase K. Joseph Spears y Michael K. P. Dorey, “Arctic Cruise Ships: The Pressing Need for Search and Rescue (Buques crucero del Ártico: La necesidad urgente para la búsqueda y rescate)”. *Canadian Sailings*, 17 de octubre de 2012, <http://www.canadiansailings.ca/?p=4830&print=1>. Véase también Byers, “Canada’s Not Ready (Canadá no está preparada)”.

19. “About the Arctic Council (Acerca del Consejo del Ártico)”, Consejo del Ártico, 7 de abril de 2011, <http://www.arctic-council.org/index.php/en/about-us/arctic-council/about-arctic-council>. Dinamarca también representa a Groenlandia y las Islas Faroe en el consejo.

20. Crocker Snow Jr., “Analysis: The Arctic Council, Lead Sled Dog of the High North (Análisis: El Consejo del Ártico, guía de trineos del Alto Norte)”, *GlobalPost*, 4 de octubre de 2012, <http://www.globalpost.com/dispatch/news/regions/americas/121003/analysis-the-arctic-council-lead-sled-dog-the-high-north>.

21. *La Declaración de Ilulissat*, Conferencia sobre el Océano Ártico, Ilulissat, Groenlandia, 27–29 de mayo de 2008, 2, http://www.oceanlaw.org/downloads/arctic/Ilulissat_Declaration.pdf; y el *Acuerdo de Cooperación en Búsqueda y Rescate Aeronáutico y Marítimo en el Ártico [Acuerdo de Nuuk]*, 12 de mayo de 2011, preámbulo y artículo 3, párrafo 3, <http://www.ifrc.org/docs/idrl/N813EN.pdf>. Al trazar los límites de esas áreas, la *Declaración* tuvo cuidado de no afirmar que esos límites no se utilizarán como precedentes para una disputa limítrofe sin resolver (artículo 3, párrafo 2).

22. Consejo del Ártico, *Nuuk Declaration on the Occasion of the Seventh Ministerial Meeting of the Arctic Council (Declaración de Nuuk sobre la ocasión de la séptima reunión ministerial del Consejo del Ártico)*, 12 de mayo de 2011, *Nuuk, Groenlandia*, <http://www.arctic-council.org/index.php/en/document-archive/category/5-declarations>. Observe que la *Declaración de Nuuk de 2011* anunció el *Acuerdo de Nuuk* de 2011 sobre SAR, entre otras cosas. Éste es el primer tratado internacional del Consejo del Ártico.

23. Ibid., artículo 7, párrafos 3 (d) y (e). El *Acuerdo de Nuuk* también detalla la “Autoridad competente” de cada nación (apéndice 1), agencias de SAR (apéndice 2), y las localizaciones del centro de coordinación de rescate (RCC) (apéndice 3).

24. Esto incluye el paso del yate privado más grande del mundo (un condominio flotante llamado el Mundo) en 2012. Para un ataque frontal a los planes canadienses actuales para buques patrulla de alta mar en el Ártico, véase Michael Byers

y Stewart Webb, *Titanic Blunder: Arctic/Offshore Patrol Ships on Course for Disaster (El error del Titanic: Buques patrulla de alta mar en el Ártico en ruta al desastre)* (Ottawa: Rideau Institute, Centro Canadiense para Alternativas de Política, abril de 2013), http://www.policyalternatives.ca/sites/default/files/uploads/publications/National%20Office/2013/04/Titanic_Blunder.pdf.

25. “The Arctic Is a Long Way from Canada’s Search and Rescue Techs (El Ártico está muy lejos de los técnicos de búsqueda y rescate de Canadá)”, Nunatsiaq Online, 3 de noviembre de 2010, http://www.nunatsiaqonline.ca/stories/article/556011_the_arctic_is_a_long_way_from_canadas_search_and_rescue_techs/. El artículo original señalaba que Trenton, Ontario, estaba más cerca a Quito, Ecuador, que a Nunavut, pero que la distancia se calculaba mediante mapas Mercator de “tierra aplanada”. Los trazados que usan Google Earth extienden la distancia hasta una línea justo debajo de Panamá, bisecando Venezuela y a través de la parte norte de Colombia.

26. Michelle Zilio, “Someday ‘Your Number Is Going to Come Up’: Lagging Arctic SAR Risks Much; Experts (Algún día ‘Tu número va a salir’: Afectando bastante los riesgos de SAR en el Ártico, dicen los expertos)”, iPolitics, 3 de enero de 2013, <http://www.ipolitics.ca/2013/01/03/someday-your-number-is-going-to-come-up-lagging-arctic-sar-risks-much-experts/>.

27. Teniente Jill Strelieff, “Canadian Forces High Arctic Operation Furthest Northern Patrol for Canadian Rangers (Los canadienses obligan a la Operación del Alto Ártico más al norte para los rangers canadienses)” (publicación noticiosa del National Defense and Canadian Forces), Marketwire, 26 de abril de 2010, <http://www.marketwire.com/press-release/canadian-forces-high-arctic-operation-furthest-northern-patrol-for-canadian-rangers-1153921.htm>.

28. Ésta es la distancia desde un punto en el mar de Beaufort desde el Territorio del Yukon de Canadá hasta Nanisivik, cerca de la entrada a la Bahía de Baffin en la costa este de Canadá vía Parry Sound y el Estrecho de McClure. Usando la vía del paso de menos profundidad el Estrecho Unión se reduce la distancia de navegación a aproximadamente 900 millas náuticas. Véase Byers y Webb, *Titanic Blunder (El error del Titanic)*, inserto de mapa. Usando el modelo noruego, se considera que el Paso del Noroeste tiene 2.400 kilómetros.

29. “JHC Navigating Limits Sub-Committee: Recent Incidents, 29.8.2010, Cruise Ship Runs Aground in Canadian Arctic,” Lloyd’s Market Association, consultado el 8 de agosto de 2013, http://www.lmalloyds.com/Web/Market%20Places/_nbsp_nbsp_Marine/Joint_Hull/Navigating_Limits/Web/market_places/marine/JHC_Nav_Limits/Navigating_Limits_Sub-Committee.aspx.

30. *Acuerdo Nuuk*, apéndice 1, 2, y 3, respectivamente. El Centro de Coordinación de Rescate Conjunto en Juneau (USCG D17 RCC), con personal de la Guardia Costera, es responsable de la región de SAR que corresponde a la parte sureste de Alaska, la cadena de Islas Aleutianas, y las aguas del litoral de Alaska. El CCR de Alaska es una misión de la Fuerza Aérea que abarca la masa de tierra del territorio continental de Alaska al norte de 58 grados de latitud norte y al oeste de 141 grados de longitud oeste. Véase “Frequently Asked Questions (Preguntas frecuentes)”, Base Conjunta El-mendorf-Richardson, consultada el 13 de agosto de 2013, <http://www.jber.af.mil/shared/media/document/AFD-120314-029.html>.

31. David Perera, “Papp: Coast Guard Plans No Arctic Shoreside Infrastructure (Papp: La Guardia Costera no planea ninguna infraestructura a lo largo de la costa ártica)”, Fierce Homeland Security, 22 de mayo de 2013, <http://www.fiercephomelandsecurity.com/story/papp-coast-guard-plans-no-arctic-shoreside-infrastructure/2013-05-22>.

32. Los activos de la Guardia Costera fueron recortados en 92,24 por ciento en el debate del Comité de Asignaciones de la Cámara de Representantes para el año fiscal 2014. Al final, la solicitud de presupuesto de la Guardia Costera para el año Fiscal 2014 fue recortada en más de 13 por ciento en relación al año anterior. David Perera, “2014 Budget Request: Coast Guard (Solicitud de presupuesto de 2014: Guardia Costera)”, Fierce Homeland Security, 11 de abril de 2013, <http://www.fiercephomelandsecurity.com/node/89222/print>.

33. Existe un tercer rompehielos de propiedad estadounidense, pero no es parte del Departamento de Defensa y ni siquiera de Seguridad Nacional. La Fundación Nacional de Ciencias tendrá su propio rompehielos liviano, el *Sikuliaq*, en 2014, asignado para misiones científicas en el Golfo de Alaska y el Mar Meridional de Bering. Cámara de Representantes, *Testimonio del Dr. Kelly Falkner, Subdirector, Oficina de Programas Polares, Fundación Nacional de Ciencias, ante el Comité de la Cámara de Representantes sobre Transporte e Infraestructura, Subcomité sobre Guardia Costera y Transporte Marítimo*, 112th Congreso, 1ra sesión, 1 de diciembre de 2011, http://www.nsf.gov/about/congress/112/kf_coastguardarctic_111201.jsp. Véase también ABS Consulting, *United States Coast Guard High Latitude Region Mission Analysis Capstone Summary (Resumen final del análisis de misión en la Región de Gran Latitud de la Guardia Costera de los Estados Unidos)* (Arlington, VA: ABS Consulting, julio de 2010), 15, <http://assets.fiercemarkets.com/public/sites/govit/hlssummarycapstone.pdf>. Véase también Ronald O’Rourke, *Coast Guard Polar Icebreaker Modernization: Background and Issues for Congress (Modernización de los rompehielos polares de la Guardia Costera: Antecedentes y problemas para el Congreso)*, Informe CRS para el Congreso RL 34391 (Washington, DC: Servicio de Investigación del Congreso, 24 de julio de 2013), “Summary (Resumen)”, <http://www.fas.org/sgp/crs/weapons/RL34391.pdf>.

34. O’Rourke, *Polar Icebreaker Modernization (Modernización de los rompehielos polares)*, 9. La Guardia Costera necesita varios rompehielos además del modelo 3 + 3 para lograr una presencia continua en el Ártico y el Antártico.

35. Guardia Costera de los Estados Unidos, *United States Coast Guard Arctic Strategy (Estrategia del Ártico de la Guardia Costera de los Estados Unidos)* (Washington, DC: Headquarters US Coast Guard, mayo de 2013), 31–32, <https://www.hsdl.org/?view&did=736969>. La estrategia propone “multiplicadores de fuerza” en un enfoque para el Ártico que involucre a “todo el gobierno”.

36. Fuerza de Tareas sobre Cambio Climático/Oceanógrafo de la Marina, *U.S. Navy Arctic Roadmap (Mapa de ruta del Ártico de la Marina de los Estados Unidos)* (Washington, DC: Departamento de la Marina, octubre de 2009), 11, 14, 17, http://www.navy.mil/navydata/documents/USN_artic_roadmap.pdf. *El Mapa de Ruta* pide una revisión de los acuerdos existentes con la Fuerza Aérea, entre otros, pero en ninguna parte solicita apoyo adicional de ese servicio. El estudio de la Marina se refiere más al Ejército que a la Fuerza Aérea.

37. Fuerza de Tareas para Cambio Climático/Oceanógrafo de la Marina, *U.S. Navy Arctic Roadmap (Mapa de ruta del Ártico de la Marina de los Estados Unidos)*, 11, 23. *La Estrategia del Ártico* de la Guardia Costera de los Estados Unidos (ver nota 35) menciona las obligaciones de SAR y el requisito de compartir la carga con otras naciones del Ártico pero apenas trata sobre alguna estrategia futura. Podría desplegar activos en avanzada a Barrow, Alaska, en los meses de verano. Aparte de planear más rompehielos para ayudar en SAR, la *Estrategia* guarda silencio en relación a los planes futuros.

38. En el testimonio ante el Congreso, el teniente gobernador de Alaska llamó al Ala No. 176 la “vanguardia de América para búsqueda y rescate en el Océano Ártico”, observando que la “respuesta de la Guardia Costera tiene base muy alejada”. Cámara de Representantes, “*America is Missing the Boat (Estados Unidos está perdiendo la oportunidad)*”, *Declaración para que figure en actas, el Honorable Mead Treadwell, Teniente Gobernador del Estado de Alaska, ante el Comité sobre Transporte e Infraestructura de la Cámara de Representantes de los Estados Unidos, Subcomité sobre Guardia Costera y Transporte Marítimo*, Congreso No. 112, 1ra sesión, 1 de diciembre de 2011, 9, http://housemajority.org/joule/pdfs/27/hjr0034_treadwell_testimony.pdf.

39. Para ponerlo moderadamente, el comando y control de estos activos es confuso, pero la unidad de comando es un asunto separado de una falta de visión relacionada al uso de activos de SAR de la Fuerza Aérea en el Alto Norte. Para ver una discusión completa de asuntos de comando y control y recomendaciones para cambio, véase Peter Ohotnicky, Braden Hisey, y Jessica Todd, “Improving U.S. Posture in the Arctic (Mejora de la postura estadounidense en el Ártico)”, *Joint Force Quarterly*, edición 67 (cuarto trimestre de 2012): 56–62, http://www.ndu.edu/press/lib/pdf/jfq-67/JFQ-67_56-62_Ohotnicky-Hisey-Todd.pdf.

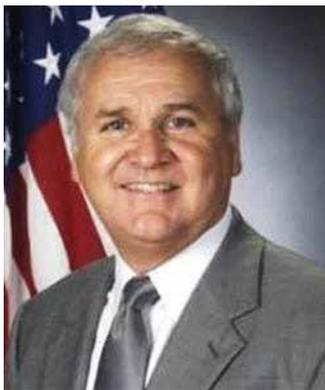
40. Fuerza de Tareas para Cambio Climático/Oceanógrafo de la Marina, *U.S. Navy Arctic Roadmap (Mapa de Ruta del Ártico de la Marina de los Estados Unidos)*, 25, actividad 5,11.

41. “RQ-4 Global Hawk”, hoja de datos, Fuerza Aérea de EE.UU., 16 de octubre de 2008, <http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104516/rq-4-global-hawk.aspx>. Este perfil supone un rango nominal de 2.500 millas náuticas, voladas desde Eielson AFB.

42. Departamento de Defensa, *Report to Congress on Arctic Operations and the Northwest Passage (Informe al Congreso sobre Operaciones en el Ártico y el Paso del Noroeste)*, OUSD (Política) (Washington, DC: Departamento de Defensa, mayo de 2011), 14, http://www.defense.gov/pubs/pdfs/tab_a_arctic_report_public.pdf.

43. Al año siguiente, el comandante de NORTHCOM designó a Alaska como un “área de interés clave” e identificó deficiencias en varias áreas, incluyendo capacidades que habilitan SAR.

44. Para tener una idea del surgimiento del tráfico marítimo comercial entre la costa Oeste de Groenlandia y Canadá adyacente al Paso del Noroeste, véase Jane Kokan, “Greenland: Canada’s Arctic Neighbour (Groenlandia: Vecino Ártico de Canadá)”, *FrontLine Defence* 9, no. 1 (enero/febrero de 2012): 23–27, http://www.frontline-canada.com/downloads/12-1_RAdmKudsk.pdf.



El Coronel John Conway, USAF, Retirado (BA, MA, University of Alabama) es un analista de defensa militar en el Instituto de Investigaciones de la Fuerza Aérea, Base Aérea Maxwell, Alabama. Se desempeñó en calidad de oficial de inteligencia con asignaciones en el Cuartel General de la Agencia de Inteligencia de la Fuerza Aérea, Comando Norteamericano de Defensa Aeroespacial, y en la Agencia de Seguridad Nacional. Fue el oficial superior de inteligencia en el Cuartel General del Comando de la Reserva de la Fuerza Aérea (AFRC), Base Aérea Robins, Georgia, y ocupó varios cargos de inteligencia a nivel de ala y escuadrón, inclusive un periodo de servicio en combate con el II Centro de Apoyo Aéreo Directo en la Provincia Pleiku, República de Vietnam. Su última asignación en el servicio activo fue como jefe, División de Apoyo Antidroga, Cuartel General del AFRC. Después del servicio activo, el Coronel Conway fue ingeniero de sistemas y contratista de ayuda técnica para la Dirección U-2 en la Base Aérea Robins y como asesor civil para el Centro de Operaciones Gordon de Seguridad Regional, Fuerte Gordon, Georgia, después del 11 de septiembre de 2011. El Coronel Conway es un contribuyente frecuente en el *Air and Space Power Journal*.

La Mini-Guerra en el Siglo XXI

COMODORO JOSÉ C. D'ODORICO, FUERZA AÉREA ARGENTINA-RETIRADO

Nota del Editor: *A continuación publicamos un artículo del ilustre y prolífico escritor Don José C. D'Odorico, Comodoro Retirado de la fuerza aérea argentina, fallecido el pasado 18 de junio de 2014. Este artículo—recibido dos semanas antes de su lamentable partida— es solo un ejemplo del legado y tesoro intelectual que hoy nos deja y de su espíritu de colaboración como escritor asiduo. Es por ello, que su extenso aporte académico será el sello que lo identificará para siempre en nuestra revista y que permanecerá durante mucho tiempo entre nosotros.*

Gangs y Murderers

La sociedad de nuestros días transcurre en un clima de ilusión engañosa porque quiere que la paz que anhela con fervor, dure infinitamente. El hombre comienza a divagar sobre la guerra destructiva, al suponer que está dejando de existir como una faceta malévolamente del ser humano. Ahora los pueblos se sumergen en espectaculares proyectos que pugnan para transformarse en realidades tangibles y sumarse a los que ya nos sirven de estímulo. El tiempo, con su ritmo impertérrito, no se inmuta pero no deja espacio para las promesas postergadas.

Los pueblos, que están enfrascados en ese idilio imaginario, giran alocadamente entre sí y con rivales trajinados que piensan vivir el sueño por la sola unción de desearlo. Es posible que olviden cándidamente que la guerra nació con el planeta y la querrela encarnizada que estalló es el ícono remanente de su existencia y su realidad. Así viene sucediendo desde la aparición de las civilizaciones. En este tablado, la guerra luce su espectacularidad y sus métodos atroces de expandirse.

La guerra se reitera esporádicamente con intervalos de relajamiento, pero siempre hay otra porque hay rivales que quieren imponer sus intereses con la urgencia. La visión dantesca que empuja la defensa es el recurso que esperan los Estados para contener a los rivales belicosos. En ese escenario hay dos conceptos que patrocinan el argumento que sigue a continuación. En primer lugar, la verificación de las premisas del líder y de los expertos, ligadas al dilema ancestral de la conducción. En segundo término, el planteo encuentra a los contrarios discurriendo para establecer la primacía de su voluntad. Consecuentemente, la discrepancia de los factores subrayados abre paso a la contienda. En esa arena se desarrolla la interrelación de las naciones, cada una aportando los valores que está deseando cultivar. En suma, esta introducción retórica permite presentar el problema central que tiende a destronar el *crimen organizado* y sus apetencias alejadas de la ley.

El dilema, las premisas que lo identifican y la selección de los operadores, constituyen parte de la combinación de la situación. En ese cuadro de la realidad se instala el conflicto sin averiguar las causas y los detalles que no poseen trascendencia. Por otro lado, continúa la valoración de las premisas que integran el gran dilema estatal y entonces es apropiado hacer el estudio de los caracteres humanos que integran las pandillas del *crimen organizado*. La mayoría de los miembros se agrupan en *gangs*,¹ constituidos por individuos denominados popularmente *murderers*² “soldados” y *racketeers*, que cumplen tareas en los lugares más azarosos y de mayor actividad ilegal. Esos bandoleros ofician de vanguardias armadas rudimentarias del *crimen organizado*, aunque su conducta está muy lejos de parecerse a la de los servidores de los organismos nacionales.

El *gang*, que posee un dominio territorial en el país donde comete los delitos, es conducido históricamente por un jefe que suele ser conocido como en la tradicional nominación mafiosa “*don, capo o caporegime*”, aunque el título no es absoluto. El capo de esa gavilla tiene el control total de la agrupación, que incluye el derecho de vida o muerte de los integrantes. Uno o más

lugartenientes de confianza, que eventualmente sustituye al líder, colaboran con el *caporegime*, cubren las espaldas del jefe y vigilan a los miembros del grupo.³

El *gang* se configura con un grupo heterogéneo de individuos de variada procedencia y con reducida educación, pero saben cómo adiestrarse para delinquir y acumular poder, usando artes que ponen a prueba su astucia con las leyes que regulan la convivencia del Estado. El *gang* repudia a la sociedad culta y pacífica, pero conserva el secreto silenciosamente en beneficio de sus intereses. No obstante, la modernización de las civilizaciones actuales aconseja que el *crimen organizado* reciba a socios universitarios para infiltrar la economía y las finanzas públicas, mientras se fundan nuevos *gangs* y se expanden.

El *crimen organizado* en América apareció antes de los dramáticos años de la recesión mundial (1933-34), aunque durante ese lapso hubo un intenso contrabando de alcoholes. Hoy, el *crimen organizado* demuestra un ingenio que lo convierte en empresas de gran envergadura, aunque su manera de operar denuncia su origen ilegal. Las guerras de pandillas se han reducido sustantivamente pero no se extinguieron. Ahora los *gangs* se caracterizan por sus actos aislados pero salvajes y el ensañamiento de los asesinatos que aún cometen.

Los “soldados” y *sicarios*, provienen ordinariamente del *lumpenproletariado*⁴ metropolitano y de otros países, haciendo intrascendente el problema de la nacionalidad. El *murderer* genuino está al servicio fiel de los dirigentes del *gang* y ejecuta tareas en las que debe unir el ingenio con la resistencia física, como en las operaciones militares especiales (SF).

Los “soldados”, hombres y mujeres del *crimen organizado*, no acostumbran a formular preguntas, simplemente ejecutan la orden recibida. Cualquier error los expone a un riesgo mortal ya que las sanciones son capitales. El número de “soldados” controlado por un *capo* varía, pero no comanda cantidades excesivas que le cause dificultades. Generalmente los *capos* se encargan de las necesidades logísticas fundamentales de sus dependientes y, además, los distribuyen en sitios donde las transacciones financieras poco claras son menos investigadas por las autoridades.

Es ampliamente conocido que las transgresiones ilegales son más productivas cuando los técnicos administran las finanzas y por eso, en los *gangs* no es raro encontrar economistas, abogados y otros profesionales que no abandonan su profesión original. Las operaciones dirigidas por *capos* en áreas metropolitanas aprenden a usar las reglas del MOUT (Military Operations in Urban Terrain) y por lo tanto las autoridades no deben olvidar esas aptitudes de los “soldados” cuando son perseguidos.

Los asesinatos masivos —en este continente los hay— realizados por *gangs* de narco-traficantes, cometidos por *sicarios* y “soldados”, informalmente equivalen a una LIC (Low Intensity Conflict), aunque el Estado niegue el hecho. Las víctimas registradas son el fruto de represalias, sanciones internas, guerras entre bandas y otras represiones de los miembros de las organizaciones, lo cual recomienda la intervención indubitable de las FF.AA. del país porque las policías están siendo claramente superadas por los *gangs*.

El número de caídos por diversas causas es correlativo con las fuerzas del *gang* y los asesinos contratados, que llegan a integrar una entidad belicosa y amenazante, con capacidad para producir daños sustanciales a la población. Pero este no es el problema que nos interesa dilucidar ahora, sino la manera de impedir que el *crimen organizado* pueda llevar a cabo sus viles planes. Es una razón que merece hacer un esfuerzo especial por la consecuencia del beneficio para la sociedad.

El Teatro de Operaciones (TO)

Los comentarios repasados se refieren al conocimiento trascendido de la intimidad de la corporación, que no tiene reparos en conformar una formidable concentración económica y financiera con artificios que desprecian sistémicamente las leyes del Estado nacional. El paso inicial de una incipiente *campana* consiste regularmente en un examen pormenorizado sobre las minu-

cias vinculadas con la presencia y desempeño del *crimen organizado*. Conocer al enemigo es el primer movimiento que Sun Zi⁵ jamás olvidaría antes de un ataque, porque permite reunir ventajas insuperables previas a la batalla.

La *campana* es comandada por el jefe del Estado como indiscutible responsable supremo que debe emitir las órdenes desde un centro unificado, desde donde conservará la visión de las operaciones que combinen todos los objetivos que aún sean secretos, incluyendo la participación voluntaria de la ciudadanía y el apoyo de tecnología discreta. La resolución adoptada por el gobierno encierra una gran responsabilidad política y por lo tanto exige un examen minucioso de la realidad. La *campana* se tiene que caracterizar por la prudencia, la oportunidad de las providencias, la voluntad *clauswitziana* inquebrantable del líder y debe ser tan cautelosa como sea posible. Ya que el bosquejo del plan contra el *crimen organizado* es de gran complejidad, las correcciones que sean imprescindibles solo se deben efectuar después de un estudio pulcro de cada sector del documento.

La *campana*, como despliegue físico de fuerzas, considera al territorio nacional un todo nominado TO donde se puede maniobrar con libertad de acción política, pero la movilidad del *crimen organizado* hace sospechar el cruce de fronteras geográficas con la eventual colaboración de terceros, incluyendo la del país usurpado. La preparación de las operaciones requiere paciencia y continuidad para reunir la Inteligencia criminal y por lo tanto se debe prever el uso de una estrategia sin tiempo durante un período prolongado. La *campana* corre el riesgo de ser infiltrada por espías del *crimen organizado* y por lo tanto demanda una meticulosa selección de personal de todas las categorías. Además es preciso elegir a los expertos más convincentes para el planeamiento y conducción a partir de la premisa operativa en el TO.

Es fundamental contar con una infraestructura civil defensiva utilitaria, apta para contrarrestar el desafío de los grupos de *murderer* que operan subrepticamente. Es curioso, pero ante esta amenaza extendida aún no se conoce una institución totalmente apropiada para tales fines y los pobres efectos que se observan en general hasta la fecha, crean una sensación de desilusión. Arriesgando una respuesta, apreciamos que la falencia reside en no haber usado un método restrictivo más incisivo para encarar esa clase de problemas, cuyo éxito sería la desaparición drástica de la organización criminal.

El territorio donde se realizan los procedimientos es el Estado mismo, pero puede haber sobre pasaje de las fronteras geográficas. Si las autoridades acuerdan con los Estados colindantes, simplificarán el acorralamiento de los criminales. En ese escenario, normalmente amplio, los “soldados” y guerrilleros mantienen un número moderado de efectivos en acción, pero la cantidad les permite proteger la producción y el envío del contrabando despachado a otras regiones. Inclusive, hay un especial sistema de seguridad para los trasportes, a los cuales los criminales le otorgan una particular atención porque las pérdidas son onerosas. Desde los centros de producción, hay rutas conectivas cubiertas y no pocas veces “liberadas”⁶ para efectuar el comercio ilícito, las cuales cuentan con la vigilancia de guerrilleros diestros para bloquear el peligro que generan las fuerzas legales.

En virtud de las elucubraciones antes citadas, el Estado se encuentra en un buen punto de partida para atacar con las mejores chances al *crimen organizado* y sin tener que acudir a recursos más costosos de la defensa general. Entonces se plantea el interrogante clave que brota de la especulación desarrollada, ¿qué impide que el gobierno organice un Comando Operativo exclusivo, permanente, funcionalmente independiente y únicamente subordinado al jefe de Estado, para reunir toda la información nacional vinculada con la actividad del *crimen organizado* y con la misión de demoler la estructura trasgresora que crea tantas dificultades de seguridad y culturales a la sociedad y las autoridades? La respuesta es una obviedad elemental, que coincide con el razonamiento socio-político. En estas circunstancias, la voluntad del Estado es la creadora de los ardides defensivos.

Así como el Estado acepta libremente la cooperación de entidades civiles que quieren ayudarlo, es imaginable que ningún habitante reflexivo desdeñe un centro ejecutivo dedicado a perseguir incansablemente al *crimen organizado*. Solo una gestión profundamente corrompida podría oponerse a una alternativa de esta índole, donde el más alto rango del gobierno ejerce la supervisión. Como el Comando sería controlado únicamente por la jefatura del Estado, toda otra autoridad ajena a la misión quedaría excluida de los asuntos tratados reservadamente en ese órgano.

Además de los comentarios expuestos, hay grupos opositores y reaccionarios que se rehúsan a establecer defensas especiales contra el crimen organizado, entendiendo que hay justificaciones objetivas que no las aconsejan. Seguramente son elementos que miran con particular simpatía a los traficantes de drogas, lavadores de dinero, los que hacen trata de personas y realizan toda clase de negocios turbios. El efecto de tales delitos es suficientemente grave como para que el Estado intervenga con viveza, en principio con sus medios de seguridad civil y de ser preciso, con recursos más rotundos.

Cuando hay una cifra elevada de víctimas con motivo de la intervención de “soldados”, *guerrilleros* y *sicarios*, y la fuerza policial con sus equipos superados por los más modernos de los delincuentes, suele ser escasa, se aconseja el empleo de Fuerzas Especiales (SF) sin demora. En esa coyuntura, los servicios *medevacs* son solicitados redundantemente. Las fuerzas de protección civil más avanzadas, generalmente están radicadas en las metrópolis mayores y las huestes del *crimen organizado*, conciente de ese despliegue, se concentra en áreas geográficas más salvaguardadas, donde puede planear sus correrías con menor inquietud. Las estadísticas mundiales aún son insuficientes y carecen de información confiable sobre los *gangs* internacionales, que son imprescindibles para emprender una *campana* de envergadura.

A pesar de la disponibilidad de instrumentos de variada naturaleza que pueden ser usados oficialmente para descalabrar la infraestructura del *crimen organizado*, en nutridas ocasiones la Administración es obligada a recurrir a elementos imprevistos y probablemente menos preparados para hacerse cargo de un componente defensivo contra las bandas. Ese déficit es un motivo principal para que el gobierno sea compelido a adoptar decisiones más tajantes y lógicas contra el crimen. Tal solución se puede alcanzar convocando unidades militares específicas para explotar la fuerza de choque y el estado de ánimo que despierta en la ciudadanía. La defensa articulada tiene más reciedumbre, especialmente contra el narco-tráfico que es el más pernicioso de los delitos.

Ante la agresión del *crimen organizado*, el gobierno está obligado a aumentar la represión dejando de lado las intrascendencias judiciales documentarias y las demoras que atrasan el sistema actuante, sobre todo cuando traban el efecto positivo contra la delincuencia y anulan las ventajas. No pocas veces la actividad ilegal recibe una réplica más leve que la merecida. Con el fin de hacer más engorrosos los desenlaces, el *gang* reclama a su favor las normas que protegen los derechos humanos, poniendo énfasis en la salvaguarda de los delincuentes y colocando en una situación embarazosa a las instituciones oficiales.

Los *caporegime* que dirigen los *gangs* imponen a sus huestes una de las tradiciones mafiosas más antiguas e inflexibles, la *omerta*, que es respetada temerosamente por todos los componentes. Sin embargo, la arcaica lexicografía siciliana se ha ido diluyendo a medida que la modernidad cambió la vida social de las *famiglias*,¹⁰ que van quedando como legado de lo que fue un período irrepetible.

Aunque el *consigliere*¹¹ de nuestros días no es el único asesor en quien confían los directores de la gavilla, aún sigue siendo alguien en el cual se respalda el jefe facineroso que tiene la voz decisoria en la *famiglia*. De todos modos, el *consigliere* no ha perdido su antiguo prestigio porque es el beneficiario que conoce los secretos del *gang* y con su experiencia contribuye a lograr los objetivos más complicados de la corporación. Como el *consigliere* suele ser abogado, atiende la mayoría de los asuntos legales donde está implicado el *gang*.

A las cosas

Con esta sentencia de Ortega y Gasset, formulamos una invitación que puede derribar la arquitectura del *crimen organizado*. Habiendo adquirido un conocimiento básico sobre el comportamiento y composición de este gremio ilícito, estamos en aptitud de concebir una idea que persigue el quebranto de la organización criminal. Es la proyección de una ofensiva contra el *gang*, poniendo en valor la voluntad y decisión implícita en la vida democrática que abraza el gobierno y es capaz de causar un daño terminal a los criminales.

El plan de *campana* se dedica a la anulación de todos los *gangs* radicados en un área geográfica determinada, a los cuales se los considera como unidad dentro de la realidad circundante que caracteriza al TO. Para que la *campana* planificada sea lucrativa y tenga un efecto trascendente concreto, tiene que ser conducida por la entidad superior del Estado y debe ordenarse a las premisas relacionadas con la justicia. El plan que se emita será confiable en tanto cuente con el apoyo de un sistema judicial recto e intransigente. Las operaciones represivas no se deben detener hasta alcanzar cada objetivo, porque el *crimen organizado* no da tregua a menos que sea forzado.

El Estado requiere un órgano operativo de funcionamiento continuo e independiente de otras instituciones armadas internas (Gendarmería, Policías Federales, órganos políticos, etc.), pero sin ser privado de hacer contacto con esas organizaciones. El instituto nominado por el gobierno como lo juzgue apropiado [ejp. Comando Especial Policial (CEP) o Comando Contra el Crimen Organizado (CCCO)], recibirá la responsabilidad de investigar y resolver la mayoría de los asuntos donde se encuentre inmiscuido el *crimen organizado* y sus satélites.

En esta narrativa, la *mini-guerra* (LIC) se inicia como un acontecimiento policial, aunque con más estrépito debido a la cantidad de *murderers* que participan. El gobierno, cuando interviene para frustrar el disturbio, debe utilizar unidades con adiestramiento MOUT para preservar la infraestructura y el desplazamiento urbano, sin dejar de acosar a los delincuentes.

Una *mini-guerra*, como estrategia político-militar contra la entraña del *crimen organizado*, es un arte que recurre a los recursos más ingeniosos del Estado y por consiguiente se gana el rechazo total de los bandoleros. Por eso, el personal destinado a estos fines tiene que ser adiestrado con intensidad, como habitualmente lo hacen las SF, Delta o SEAL, o como sean llamadas en otros países.

Si alguien entiende que una LIC, por reducida que sea, es comparable con la rutina de las fuerzas policiales y equivalentes, comete una equivocación, porque las fuerzas que persiguen a los proscritos tienen tácticas, técnicas y estilos de conducción distintos. El contraste se aprecia igualmente en las variadas intervenciones de las organizaciones estatales, aunque la *campana* de una LIC se orienta de modo concordante con la contienda. La coacción con fuerzas policiales comunes suele concluir en un juicio formal que no asegura una sanción justa para los implicados en el hecho criminal.

En cambio, la *campana* de la LIC que fue elegida como opción represiva, puede eliminar al *crimen organizado*. Ese período bélico finaliza cuando el último residuo delictuoso grupal desaparece de la comunidad. Es importante que la Administración conserve el secreto de los procedimientos utilizados en la *campana*, por cuanto las filtraciones informativas son frecuentes durante la LIC. Un investigador sagaz siempre tiene una pregunta a flor de labios. ¿Por qué el *crimen organizado* ha registrado una expansión alarmante en muy corto tiempo a pesar que los Estados, utilizando mayormente organizaciones civiles, lo han perseguido con obstinación a lo largo de los años?

La primera respuesta que surge presume que los actores del proceso represivo, actúan con manifiesta condescendencia y no evidencian energía judicial. En ciertos países hay organismos legales que tratan a los *racketeers* de la corporación con una benevolencia que asombra, puesto que regularmente aplican las leyes más favorables para los acusados, aduciendo sentimientos

humanos que tales individuos no demuestran para sus víctimas. En otros casos, la corrupción alcanza niveles escandalosos en algunas esferas de la Administración. La complicidad de los burocratas es comprensible porque se enriquecen sin apocamiento.

Pocos gobiernos cumplen al pie de la letra la totalidad de las resoluciones sancionadas por los Parlamentos y no es raro que al poco tiempo de comenzar una *mini-guerra*, la voluntad y entusiasmo de las autoridades se enfríe, mientras que los *dons y caporegime* aprovechan para descansar en lugares seguros hasta que vuelva la persecución. Cuando el sistema defensivo de la Administración es flácido, hay sectores que piensan que ha llegado la ocasión de remontar el *crimen organizado*. Por eso no es casual que los capos inviertan dinero en conquistar la amistad de funcionarios encumbrados.

Si la organización civil que auxilia a la justicia para cumplir sus disposiciones más severas es insuficiente para neutralizar una gavilla de *murderers* bien armada, disciplinada y diestra en las operaciones furtivas, no cabe duda que ha llegado el momento de introducir modificaciones o sustituir el sistema. Las fuerzas militares/militarizadas que en época de paz no tienen un empleo acorde con su misión de origen, constituyen una excelente fuente de obtención. Desde luego, quedan fuera de consideración las unidades y materiales para la *guerra convencional*.

El empleo de fuerzas militares en cuestiones internas, particularmente en aquellos países donde se nota una hiper sensibilidad a la democracia, despierta reacciones enrevesadas en los ambientes socio-políticos que no simpatizan con el estamento militar. Analíticamente, advertimos que es una interpretación equivocada del concepto de defensa, pues se la divide en interior y exterior sin reparar que son partes de un todo indivisible. La práctica de tal criterio conduce irremediablemente a un debilitamiento de la seguridad nacional.

El empleo de la fuerza militar/militarizada en el interior del país, no inmuta el régimen democrático de un Estado. Los dirigentes políticos opuestos piensan que así protegen las libertades civiles y acusan con ligereza a quienes suponen que violan los fundamentos de la democracia al emplear fuerzas armadas en la defensa interna. Pero olvidan un detalle y es que estas fuerzas constituyen parte sustantiva de la república. Quienes asuman que la intervención de su sistema militar/militarizado en una operación de seguridad interior es un riesgo para la democracia, debieran reflexionar porque dicha asistencia preserva la salvaguarda del régimen criticado.

Si el *crimen organizado* poluciona a las policías con su amoralidad, ha llegado el momento de investigar la intervención de esos cuerpos de seguridad civil, técnicamente destinados a conservar la protección de la comunidad. De producirse ese evento, habrá que convocar a fuerzas militares/militarizadas alistadas para combatir a la delincuencia bajo el estricto control del gobierno. Un problema de defensa interior, también es incumbencia de la defensa nacional y por ende, del interés del sistema que prevalece en el país.

¿Están las fuerzas antes citadas en condiciones de desafiar al *crimen organizado*? No, hasta tanto sean entrenadas para cumplir dicha misión. Entonces la *mini-guerra* dejará de ser un fenómeno inútilmente agresivo, para convertirse en un planteo que acoge los beneficios del orden y la paz. El precio que pagaría el pueblo sería justamente compensado. Consecuentemente, ¿porqué no invertir esos recursos que ofrecen alternativas tan ventajosas para derrotar al *crimen organizado*, sin que la sociedad sea lastimada seriamente?

La *mini-guerra* prevé que el enemigo sea continuamente hostigado por las fuerzas específicas civiles y militares para evitar que los “soldados” del *gang* cometan delitos aberrantes aprovechándose del régimen democrático. Para que estos resultados sean obtenidos, hay que crear un Comando Operativo de alcance nacional, facultado para establecer relaciones internacionales bajo la dirección del gobierno. Ese comando sería exclusivo, de funcionamiento continuo bajo la supervisión y dirección única del jefe de Estado. Un Estado Mayor (EM) ejecutivo tendría a su cargo el planeamiento y desarrollo de las *campañas* aprobadas en la jefatura del Estado.¹² La institución también se ocuparía de investigar las culpabilidades individuales y colectivas, sin que sea compelida a dar explicaciones al resto de la Administración.

Por su lado, el periodismo debe atenerse a reglas restrictivas que no perjudiquen las operaciones de Inteligencia. La prensa protestará por estas imposiciones, pero la seguridad de la comunidad tiene sus costos y por lo tanto hay que aceptar las medidas limitativas. El resguardo nacional está por encima de los intereses de la información popular y esa norma debe ser comprendida por los informantes públicos.

Durante la descripción de la matriz defensiva contra el *crimen organizado*, ratificamos que la propuesta oficial tendría una configuración exclusiva, militar o militarizada pero independiente, cuya finalidad se dedicaría con exclusividad a destruir la organización criminal invasora de los centros neurálgicos del país. Por lo tanto, la composición debe reunir una cantidad de especialistas y auxiliares, así como técnicos calificados en condiciones de participar de la gran variedad de acontecimientos donde se encontrará con el enemigo.

También es el momento de saber cómo recibirá el público en general y los políticos en particular un órgano de esta naturaleza, pero presumimos que al considerar la labor que desempeñará, obtendrá la aprobación y el soporte de toda la sociedad honesta. En cambio reconocemos que será complicado reclutar el personal para el Comando, debido a las aptitudes exigibles a los candidatos. Por este motivo, la selección de personal que deba realizarse, se efectuará preferentemente en el interior del organismo y sus ramificaciones.

No es de extrañar que el funcionamiento del Comando de referencia produzca una tormenta de protestas en algunas asociaciones civiles que ven con una desviada sensibilidad un exagerado tono *militarista* que influye sobre el trabajo de las cortes. Es una reacción ideológica tendenciosa que no ha intuido las ventajas del método de mayor seguridad para los ciudadanos. Pero los dirigentes que perciben la verdad como secuela de la realidad, ignoran las voces fatuas y vacías de lógica.

Nadie puede negar que los *murderers* obran con criterio prehistórico, pues no vacilan en masacrar a sus víctimas. Los millares de caídos en todo el mundo, lo atestiguan con sobrado realismo. Si predomina el sentido común, hay que planear una defensa acorde con la amenaza, sin argumentos retóricos, porque la supervivencia de la sociedad es prioritaria. La actividad de los *sicarios* no se fundamenta en teorías académicas. Solamente son verdugos que piensan en matar a un adversario que apenas conocen, simplemente porque es la misión que le ordenaron los *capos*. Esa realidad no debe ser tergiversada por los eternos voceros de las falsas estipulaciones que vanamente alimentan las protestas.

En nombre de los derechos humanos, las personas ultra sensibles adjudican a los sicarios el sello de delincuentes recuperables, fundándose tal vez en el asesoramiento de sicólogos que no son duchos en el estudio de las mentes atormentadas de las gavillas que integran el *crimen organizado*. Una visión extravagante da lugar a que la conducta de la delincuencia se valore con insólita tolerancia y hasta encuentre justificaciones a las fechorías. En la actualidad, a las sociedades más culturalizadas les repugna la sentencia de muerte y se oponen a las condenas judiciales que imponen penas de reclusión por vida, aduciendo razones con rebuscados fundamentos sobre inequidades entre reos y victimados. No obstante, la pena de muerte sigue siendo aplicada en una cantidad de Estados.

Aun con las dudas que usualmente coronan las premisas del dilema de la conducción, es interesante cavilar sobre el pensamiento sin ambages del prestigioso novelista Mario Puzo,¹³ cuando usaba como en un ajedrez a los *don* y los *caporegime* que animaban sus excitantes novelas sobre el *crimen organizado* como una duplicación de la realidad con nombres ficticios.

Dejando correr su pensamiento en un sencillo razonamiento, sin que le temblara la mano, el escritor expuso su criterio con honesta convicción, “*we don't know if capital punishment is a deterrent, but we know that men that we execute will not murder again*” (no sabemos si la pena capital es una disuasión, pero sí sabemos que los hombres que ejecutamos no volverán a matar nuevamente). Con un estilo franco, dio a conocer un enfoque neto sobre la interminable discusión entre la pena de muerte y el derecho a la vida que se plantea irremisiblemente antes de cada

sentencia capital, donde se discute el derecho de los reos a sobrevivir sin ponderar acabadamente la esencia del delito.

Revisando esta síntesis, llegamos a la conclusión que la guerra menuda (LIC) es elegible por el gobierno después de haber evaluado cuidadosamente la premisa operativa que ilumina el dilema del líder y la transforma en una operación utilitaria del siglo XXI. El procedimiento, con una alta esperanza, habilita el planeamiento para la eliminación del *crimen organizado* y obtiene de esa manera el profundo aprecio de la sociedad que espera quedar libre de las turbas al conseguir la seguridad tan anhelada por el ciudadano común. Por lo tanto, es hora de exponer ideas para discutir las libremente en los centros especializados. En algunos países se ocultan neciamente los conflictos internos y la Administración se resiste a considerarlos por razones que no entiende el sentido común. Usualmente hay algún interés político detrás de esa posición o ambiciones personales, que únicamente enredan la realidad.

Propuesta y respuesta

La habilitación de un organismo cívico-militar permanente y exclusivo contra el *crimen organizado*, equivale a crear la trama de un complejo. Nos referimos a un Comando que recibiría una directiva estratégica sin tiempo del gobierno y cuya misión se daría por terminada con la desaparición del *crimen organizado*, lo cual significa que debería hacerse cargo de la totalidad del problema ilícito que comprende la investigación y la represión. A una institución de este tipo no se la puede conducir recurriendo a códigos desconocidos despectivamente por los *gangs*. Uno de los delitos que produce mayor beneficio a los manipuladores, es el *lavado de dinero*, aunque demanda intervenciones bancarias cómplices. También hay que computar la compra-venta de bienes muebles e inmuebles con el dinero *blanqueado* en el mercado legal.

El Comando imaginado sería muy diferente a otros de las FF.AA. por su estructura interna y el número elevado de expertos que debiera dotarlos para realizar actividades poco corrientes. Además de la investigación de los hechos ilegales, habría que adicionarle una fuerza militar/militarizada muy entrenada y de veloz inserción. La composición orgánica del Comando Operativo constaría de numerosas divisiones relacionadas con el *crimen organizado* e inclusive laboratorios afines, para acordar con las cualidades singulares del rival. Esa misma clase de órgano es repetible en cualquier Estado con *gangs* del mismo tipo. Los reflejos de su acción serán inmediatamente detectados por las bandas en actividad y comenzarían a ser respetados porque acusarían las consecuencias.

Si bien consideramos valioso el empleo de un comando defensivo para perseguir las múltiples derivaciones del *crimen organizado*, es imposible pensar en composiciones estandarizadas debido a las diversidades locales y los factores a tratar. Por eso es saludable convocar frecuentemente a las divisiones domésticas para discutir los errores y el rendimiento del conjunto. El comandante debe ser un militar experimentado en el arte de la *guerra no convencional*, puesto que tendría que conducir en MOUT y para eso precisa amplio conocimiento afín. No hay que nominar a un comandante civil por su falta de calificación para dirigir a fuerzas mixtas, sin embargo, a veces los intereses políticos del gobierno exceden el límite de la sensatez y se hacen nombramientos desafortunados que arruinan los resultados. No es de extrañar que los *caporegime* procuren obtener favores del comandante e inviertan cuantiosas sumas de dinero con ese destino o alisten trampas para ganar la simpatía oficial.

El Comando Operativo debe contar con una dotación civil y militar de élite, escrupulosamente elegida, que antes de ingresar debe recibir entrenamiento con las SF para satisfacer las exigencias sico-físicas. Al entrenamiento MOUT se le dará una particular atención y se puede solicitar la cooperación del Ejército. Los miembros de los equipos deben recibir armas modernas y más eficientes que las empleadas por los delincuentes. La superioridad del Comando Operativo sobre las organizaciones delictivas es un requisito incontestable, pues hay que reducir las

bajas del personal cuanto sea posible. Además, se entregará material de vuelo CSAR (Combat Search & Rescue) y sanitario al Comando para atender pedidos medevac.

Para el desplazamiento de las fuerzas del Comando en la superficie, conviene recurrir al empleo de vehículos rodantes blindados, livianos y rápidos (MRAP, Mine Resistant-Ambush Protected). Asimismo, la institución contará con su propia biblioteca técnica y laboratorios específicos. Una vez completadas las investigaciones, los *dossiers* de los *racketeers* se entregarán a las cortes junto con los delincuentes capturados, donde serían juzgados sumariamente por magistrados duchos en esas fechorías.

Si los acusados son juzgados por tribunales expertos, se conseguirá una decadencia más rápida de la organización, porque habrá menos demora en el trámite documental y una aceleración de los procedimientos. En este sistema represivo es importante la rapidez y la continuidad de la investigación, por lo cual el gobierno debe acostumbrarse a que las luces del edificio asignado al Comando Operativo no se apaguen nunca. Todas las divisiones del Comando debieran permanecer agrupadas en una misma residencia por razones prácticas.

Para que esta institución tan particular acompañe con acierto las metas oficiales, hay que asegurar su independencia. Es recomendable aislarla de los partidos políticos, como también de las entidades dogmáticas que difunden ideologías peregrinas que se contraponen a los criterios establecidos para hacer desaparecer la delincuencia colectiva. Los planes encaminados por los *dons* para pervertir a los funcionarios que ocupan posiciones decisorias, se hacen más incisivos al intuir que existe una perceptible atracción estatal sobre los beneficios ilegales. Por lo tanto, los directores del Comando deben estar alerta para bloquear los ensayos que se realicen. Aquellos funcionarios seducidos por una suma de dinero, deben saber que arriesgan su libertad ambulatoria como cualquier ciudadano y pueden ser enviados a la cárcel por iguales causas que los miembros del *gang*.

La difusión de la honestidad de los integrantes del Comando reafirma el prestigio preventivo y obtiene el reconocimiento del pueblo, lo cual es una verdadera preocupación de los delincuentes. Al retener el jefe de la Administración el control del Comando, evidentemente la institución gana con el éxito y pierde con la frustración. Hay que tener presente que la agresión contra la autoridad política opuesta a los *gangs* es un objetivo permanente de los elementos fuera de la ley y por lo tanto el Comando anti crimen debe ser acicateado desde la cúpula para neutralizar a los sectores reaccionarios.

Es importante que la persecución oficial contra el *crimen organizado* no sea titubeante, por cuanto la situación ambiental sería aprovechada por los hábiles miembros del *gang*. La eventual interrupción parcial del procedimiento produciría el deterioro de un sistema defensivo relativamente caro por los ingredientes humanos y materiales que lo configuran. Para preservar la estabilidad de los escenarios y como refuerzo del contexto, hay que tomar en cuenta el adiestramiento militar continuo del personal de la comandancia, que debe recibir un adoctrinamiento ético-moral complementario.

La organización de un sistema defensivo con aptitud operativa militar/militarizada es el prolegómeno del alistamiento para una *mini-guerra* que se le impondrá al *crimen organizado*. No obstante, aunque se trate de una mini-contienda, se regirá con los patrones y las directivas de una estrategia sin tiempo debido a la imposibilidad de calcular preventivamente la fecha de finalización. En esta *campana*, el éxito del Comando depende del sostén que reciba del gobierno y la comprensión de la comunidad. Las reglas serán consignadas con estilo de leyes y proporcionarán al ejecutivo una fluida libertad para desarrollar las operaciones. Toda restricción que inhiba la dinámica del Comando Operativo, dará una ventaja a los criminales.

En el refugio del *crimen organizado*, se agrupan los *murderers* dirigidos por sus *caporegime* y se configuran disciplinados *gangs* que disponen de ingentes cantidades de dinero y armas. Por eso, sostener el embate de los bandoleros durante un tiempo indeterminado, no es fácilmente soportable para fuerzas sin el abastecimiento apropiado. Esta descripción lacónica brinda una idea de

las exigencias de una mini-contienda. El plan inicial abarca un lapso breve y luego se extiende en función de los resultados de las sucesivas operaciones. La composición del rival, amerita proceder de esa manera porque el efecto no logrado a tiempo, genera graves consecuencias a toda la nación.

Algo más sobre la mini-guerra

El crimen organizado sigue creciendo en medio de un ominoso clima político extendido. Es una miscelánea que involucra capos, la contratación de mercenarios trajinados, la contaminación con las drogas y las relaciones político-sociales que construye con llamativa habilidad el *gang* durante su proceso evolutivo. En algunos países, la impunidad es un icono público que cierra el vínculo con las autoridades. A esa situación se adiciona la descomposición cívica que se agrega a los regímenes democráticos y las consecuencias comienzan a manifestarse en forma de rutina estable. Aunque las policías rectas se esmeran cumpliendo su deber, a menudo sus esfuerzos profesionales son interferidos con los artilugios introducidos diestramente por los bandidos.

La redacción de un plan con esencia ofensiva, pone a prueba la habilidad político-militar del gobierno y su decisión, porque a veces tiene que superar incómodos apremios de instituciones civiles que promocionan ideologías advenedizas y doctrinas opuestas a las oficiales, atentando contra la solución que le interesa al Estado. En estos casos, el gobierno tiene que priorizar la prevalencia de los intereses comunes y postergar los reclamos de los sectores minoritarios.

El planteo previo identifica dos tipos de grupos socio-políticos con actitudes diferenciadas ante el delito. En primer lugar, están quienes quieren resolver la dificultad operativa sin dar cuartel a los proscritos, utilizando recursos y doctrinas rigurosos contra el segmento de los que viven fuera de la ley. En segundo término, están las entidades que evidencian cálidos sentimientos humanitarios y consideran a los maleantes como personas que necesitan comprensión y rearme moral, alejados del ambiente contaminado que los ahoga.

En base a estas reflexiones, es probable que el gobierno que decida poner en funciones un Comando Operativo militarizado con una impronta dispuesta a combatir el crimen de manera continuada y enérgica, deba sobrepasar dificultades debido a las protestas que podrían levantar algunas instituciones ideologizadas y con una comprensión distorsionada de los derechos humanos, a los cuales se les asigna un sentido nítidamente tendencioso.

Aunque el Comando Operativo posea un alto rendimiento, tiene que afrontar la paradoja de la fuerte oposición de entidades que muestran una acentuada inclinación a considerar a los delincuentes como seres en condiciones de ser recuperados con ayuda de la educación y la sicología. La religión y las doctrinas humanitarias son reluctantes a la aplicación de condenas muy severas, pues están convencidas que los internos pueden cambiar sus errores y por consiguiente necesitan otra oportunidad para volver a ser ciudadanos correctos.

Esa clase de instituciones cree en la redención honorable del delincuente pero no hace lo necesario para materializar una fe de débil probanza y que luego buena parte de los criminales no ratifica. En base a las deducciones preliminares realizadas, todo gobierno está en condiciones de orquestar una estructura técnica eficiente que constituya un Comando Operativo militar/militarizado, con aptitud para preparar una *campana* contra un *gang* moderno, acordando con una impronta que se fundamenta en decisiones lógicas y con sentido común. Dicha *campana* se dedicaría a combatir el crimen de modo sostenido, aun escuchando las protestas de los grupos amigos de expresar apreciaciones ambiguas sobre los derechos humanos.

En este conflicto y en cualquier otro de igual tipo, la prensa y sus diversas herramientas originan un cúmulo de dificultades que pueden ser un gran dolor de cabeza para el comandante del organismo operativo. Una *campana* apta para anular la actuación del *crimen organizado* implantado, exige una cuidadosa reserva de la información civil y militar que utiliza, dada la naturaleza de los temas tratados. Por su lado, la supervivencia del *gang* tiene similar exigencia y la *omerta* se

encarga que los delincuentes de la corporación lo ratifiquen bajo amenaza. Ergo, las mutuas filtraciones son objetivos prioritarios para ambos contendientes.

En la LIC bajo tratamiento, la prensa registra y divulga datos que pueden representar infidencias graves para el planeamiento represivo. Por lo tanto, la eficacia de la labor del Comando Operativo es valorada durante la evolución de la *campaña*, en especial si es capaz de conseguir el reconocimiento del pueblo por la seguridad que brindan las unidades en operaciones. A modo de resumen, el Comando Operativo cumple su tarea represiva en el TO contra el *crimen organizado*, actuando centralizadamente con un mando único.

Aunque el Comando proceda con prudencia en todas sus intervenciones sin llegar a ser timorato, encontrará difícil impedir la barbarie que caracteriza las represalias de un *gang* de la actualidad, por lo cual el Estado debe responder con una fuerza apropiada, aunque cueste la vida a los “soldados”. Esos individuos saben de antemano el riesgo que corren al ingresar en las filas del *gang*. Las palabras de Mario Puzo pueden ser consideradas muy crueles, pero no carecen de lógica y sentido común.

El objetivo que fija el Comando Operativo, generalmente reclama un esfuerzo suplementario que no es previsto con anticipación por los planificadores, pero esa discrepancia no es suficiente para modificar los aspectos que el comandante establece en la directiva estratégica sin tiempo inicial. Aunque es poco creíble, la imaginaria derrota del *crimen organizado* en sus múltiples expresiones, tiene origen preferente en fuentes internas de la agrupación, donde se nota las faltas de coincidencias entre el interés de los *capos* y las disidencias más notorias. La discordancia influye en las definiciones tácticas del organismo ejecutivo y puede causarle tanto atrasos como costos más elevados.

El uso de aviones en la represión ha modificado la interdicción al movimiento de ilícitos, porque el Estado puede imponer diversos procedimientos para barrer del cielo a los contrabandistas volantes. Actualmente, los delincuentes emplean cualquier tipo de plataforma en vuelo para trasladar productos valiosos, desde corta a larga distancia. Los radares 3D de aplicación militar detectan a la mayoría de esas aeronaves, pero no siempre están disponibles, porque no hay en el país o deliberadamente los escamotean.

Los contrabandistas aéreos son fácilmente alcanzados por los aviones de la Fuerza Aérea, generalmente más potentes, pero durante el momento de la interdicción se plantea en las autoridades una duda que no ha sido despejada definitivamente. Las aeronaves descubiertas, ¿pueden ser derribadas sin más trámite cuando violan el espacio aéreo? Hay países que autorizan el derribo al cumplirse ciertas condiciones. Otros prohíben esa alternativa aduciendo excusas legales y humanas, aunque hay sospechas de complicidad con la burocracia. Mientras tanto, los contrabandistas continúan sus vuelos, eludiendo a los aviones militares.

Hay Estados donde el contrabando aéreo se realiza con gran facilidad y todo hace suponer que hay de por medio consentimientos muy bien recompensados. Pero el *crimen organizado* no se mueve solo a través del aire. También ha utilizado vehículos mini-sumergibles sub-acua que los contrabandistas llegaron a operar en gran cantidad, porque tenían la gran ventaja de evadir la observación aérea y solo podían ser atrapados por embarcaciones de superficie de alta velocidad.

La *mini-guerra* contra el *crimen organizado* es un concepto defensivo, conjunto e interno, cuyo objetivo es la derrota de la corporación y a ese fin demanda un planeamiento de alta calidad porque está en riesgo la comunidad. El Comando Operativo es el único organismo oficial autorizado para dirigir la *mini-guerra* y debe demostrar a la Administración sus capacidades para esos fines. Si el *crimen organizado* no supera sus problemas de supervivencia, puede ser alentado a retirarse del TO para evitar la desarticulación y buscar nueva geografía donde instalarse con menos peligro.

Otro asunto a comentar es el relacionado con la necesidad de modernizar periódicamente el texto doctrinario-operativo. Si este sistema defensivo logra mejorar la seguridad del país, es difí-

cil entender por qué a las fuerzas militares/militarizadas idóneas eventualmente se les niega la intervención en la obtención del objetivo. Una cuestión escabrosa es la inserción de grupos revolucionarios asociados al *crimen organizado* por ideas afines que aspiran a subsumir las instituciones democráticas. Probablemente sea una de las dificultades más difíciles de solucionar por el Comando ejecutivo, aun aprovechando la habilidad de su personal.

Cuando las autoridades nacionales adoptan actitudes firmes para desarmar la estructura criminal, el *gang* se auto escuda en algún otro TO ocasional y más protegido hasta que se atenúa la *campana* de represión. Podríamos decir que es una reproducción de las *contra-campanas* que solían planear las fuerzas maoístas chinas en las guerras de los años '30. No siempre la delincuencia sabe como emplear el tiempo, pero la tendencia general es a no derrocharlo y hacerlo coincidir con sus previsiones ejecutivas. Cuando se dan esas circunstancias, el gobierno no debe imaginar que el repliegue de su adversario es conclusivo. Si el Comando está cumpliendo un procedimiento ofensivo, no lo debe detener en ningún momento porque la operación quedará frustrada.

Después de hacer estas disquisiciones sobre la *mini-guerra* contra el *crimen organizado*, podemos deducir algunas inferencias a modo de oportuno ejemplo en un evento de esta índole, pero es recomendable no avanzar más allá de la realidad que configura la centuria en curso. El conflicto que lleva a cabo el *crimen organizado* es considerado un problema operacional objetivamente progresivo desde que se constituyó en un proyecto opositor a mediados del siglo pasado. Por lo tanto, son paralelizados en concordancia con las contiendas de esta índole, o sea, deben ser comprendidos con las características implícitas en las corporaciones ilegítimas.

Después de comentar estas generalidades sobre la criminalidad, es pertinente preguntar cuándo se compartirá un acuerdo entre las partes comprometidas sobre el modo de eliminar los *bunkers* del *crimen organizado*. Inicialmente, la arquitectura del Comando Operativo reclamará una abundante labor de funcionarios, autoridades y profesionales en estrecha cooperación, puesto que es preciso combatir a un rival tan complejo con los medios más apropiados que se puedan conseguir. En ese sentido incluimos a la premisa creativa del líder que está al frente de la *campana*.

Es probable que la sociedad se alarme ante la gestación de una *mini-guerra*, pero el temor decrecerá cuando adquiera conciencia de la realidad y aprecie las ventajas que deja el avance del fenómeno. En la medida que la *mini-guerra* transcurre y consigue su finalidad, se registran los resultados positivos de la defensa y aumenta la confianza en el Comando Operativo. Esa sensibilidad tan especial también es percibida por la población, que se mantiene siempre alerta a los hechos que produce corrientemente el *crimen organizado*, especialmente el narco-tráfico y su incidencia sobre la juventud. Es el momento de gozar el beneficio reportado por el conflicto a la salud del pueblo.

Notas

1. Bandas de delincuentes al mando de un *don*, *capo* o *capovegime*, que explotan toda clase de rubros ilícitos (narco-tráfico, contrabando, trata de personas, lavado de dinero, etc.).
2. *Murderer*, asesino profesional; "soldado", individuo al servicio fiel de un *capo*, jefe de una banda; *racketeer*, extorsionador, chantajista y estafador, capaz de cometer cualquier delito.
3. Ver "The Family Corleone", Edward Falco, Hachette Book Group, May 2012, USA.
4. Término marxista que designa la parte más pobre del proletariado, el que por su condición de vida e inteligencia es incapaz de asimilar la teoría y conciencia de los notables pensadores revolucionarios.
5. General chino de relevantes conocimientos tácticos. Habría vivido en el siglo V a.C. y sus conocimientos se concentraron en el libro el Arte de la Guerra, cuya vigencia actual aún es válida.
6. Son las rutas que cuentan con la ceguera ficticia de los funcionarios que han sido cooptados y por lo cual los transportadores de productos ilegales están en condiciones de circular con gran tranquilidad.
7. Traslado de heridos y muertos, a cargo de personal para-médico, recurriendo a trasportes terrestres, aéreos y navales. Durante el transporte se suele realizar las primeras curas con personal y equipo de a bordo. Los trasportes medevac suelen tener un equipamiento sanitario para emergencias.

8. Dirigente de antigua tradición mafiosa, es respetado profundamente en las organizaciones. Normalmente cuenta con su propia dotación de “soldados” que le responden con absoluta devoción y constituyen una cuadrilla con aptitud para desarrollar actos delincuenciales de importante efecto. Los caporegime aplican sus propios criterios de justicia, cuyas características son absolutas.

9. Es el silencio sin concesiones, nadie habla y todo aquel miembro del grupo delictivo que verborrea sobre las realizaciones del gang, sabe de antemano que corre el peligro de ser ejecutado sin piedad. Los sicarios se encargan de las ejecuciones.

10. Una sociedad sanguínea, a la cual se suman eventualmente otros miembros por vía del vínculo matrimonial que es celosamente respetado por el grupo. En su carácter de consejo ampliado, la familia es la entidad que se ocupa de proponer ideas y administrar los negocios espurios del gang.

11. Habitualmente es un profesional de las leyes que pertenece a la banda o es miembro de un estudio prestigioso que atiende el gang. Es el encargado de mantener relaciones con sectores públicos, personajes relevantes e inclusive otros gangs. Además se aboca a la solución de los problemas legales que tienen los miembros de la familia.

12. La independencia del Comando Operativo es vital, porque lo blindo contra la corrupción, una de las artes nocivas más usadas por los criminales para ganar a los agentes del gobierno de mayor fuste, incluyendo el sistema judicial. Los casos de corrupción descubiertos, deben sancionarse con dureza.

13. Mario Puzo, fallecido el 02 de julio de 1999, demostró su experiencia en las relaciones con la mafia siciliana (crimen organizado) y no tuvo reparos en presentar sus ideas en su libro “Fools Die”. Su relato fue objetivo y por consiguiente realista. Fue el autor de la galardonada historia “Il Padrone” (El Padrino).



El Comodoro (FAA-R) José C. D'Odorico, (1927-2014) fue piloto de transporte aéreo con más de 5.000 hrs de vuelo, habiéndose retirado del servicio activo en 1975. Se especializó en el estudio de la guerra revolucionaria marxista-leninista y la guerra subversiva. Fue autor de tres libros y más de 350 artículos profesionales, algunos de los cuales fueron publicados en *Air University Review* y *Air & Space Power Journal*. Se desempeñaba como Asesor de la *Revista de la Escuela Superior de Guerra Aérea* (RESGA) antes de su fallecimiento ocurrido el pasado 18 de junio de 2014.



**OFICIALES DE LAS FUERZAS AERÉAS
IBEROAMERICANAS EGRESADOS DE LA ESCUELA
SUPERIOR DE COMANDO Y ESTADO MAYOR (ACSC),
MAXWELL AFB, ALABAMA, PROMOCIÓN 2013–2014**



De izquierda a derecha: Coronel José E. San Román (México), Teniente Coronel Víctor Samaniego (Paraguay), Teniente Coronel Darío Hernández Vega (El Salvador), Subcomisionado Oliver Martiz (Panamá), Comandante Luis Octavio García Blasco (España), Teniente Coronel Mauricio Tejedor Medina FAC (Colombia), Teniente Coronel Alberto Ureña (República Dominicana).



**OFICIALES DE LAS FUERZAS AÉREAS
IBEROAMERICANAS EGRESADOS DE LA ESCUELA
SUPERIOR DE GUERRA AÉREA (AWC),
MAXWELL AFB, ALABAMA, PROMOCIÓN 2013–2014**

FOTO NO DISPONIBLE

Teniente Coronel Milton Zablah (Chile), Coronel Julio Londoño (Colombia), Coronel Javier Sandoval (México)