

## **ADIOS A LAS ARMAS POR JOHN CARLIN**

### **TRADUCCIÓN Y ADAPTACIÓN LUCIANO SALELLAS**

**Para aquellos afirmados en la única superpotencia líder mundial, los vientos digitales soplan fríos a través del brillo triunfante de la postguerra fría.**

La gente en Washington juega muchos juegos, pero ninguno con intereses tan altos como el del “día después”. Jugaron una versión de éste en las profundidades de la guerra fría, esperando que el ejercicio sacudiera levemente algunas ideas brillantes para una respuesta estadounidense al ataque nuclear. Ellos juegan esto otra vez hoy, pero el escenario ha cambiado - ahora se preparan para la guerra de la información.

El juego toma a 50 personas, en cinco equipos de diez. Para asegurar una competición justa y fructuosa, cada equipo incluye espías de la CIA, agentes del FBI, policías foráneos expertos, miembros del Pentágono, geopolíticos de la NSC, - no miembros que estén unos contra otros.

El “Día después” comienza en una sala de informes del Departamento de Defensa. Los grupos son presentados con una serie de incidentes hipotéticos que habrían ocurrido en las últimas 24 horas. El sistema de telecomunicaciones de Georgia ha sido inutilizado. El sistema de seguimiento ferroviario New York – Washington falló provocando una colisión frente a frente. El sistema de control de tráfico aéreo ha colapsado. Una bomba ha explotado en una base del ejército en Texas. Etc. etc.

Los equipos son separados en salas separadas durante una hora en la cual preparan informes para el Presidente. “No se preocupe. Estos son incidentes aislados, un juego desafortunado de coincidencias” es una posible conclusión. Otra conclusión podría ser “Alguien, estamos tratando de determinar quién, parece tener a Estados Unidos bajo un ataque a gran escala”. O tal vez sólo “Se concluye que son los sospechosos habituales de la milicia”.

El juego continúa un par de días más tarde. Las cosas han ido de mal en peor. La electricidad desaparece en cuatro estados del noreste, el abastecimiento de agua de Denver se ha secado, el embajador estadounidense en Etiopía ha sido secuestrado, y terroristas han secuestrado un avión 747 de American Airlines en ruta hacia Roma. Mientras tanto en Teheran los Mullah intensifican su retórica contra “El Gran Satán”; tanques iraníes se mueven hacia Arabia Saudita. Christiane Amanpour (de CNN) con chaleco antibalas reporta en vivo desde las afueras de la embajada norteamericana en Addis Ababa. El periodista Peter Jennings, de ABC, entrevista a George Stephanopoulos sobre el estado de ánimo del presidente.

Mientras tanto, los satélites sobre Estados Unidos dejan de funcionar.

Dios, dijo Voltaire, se encuentra del lado de los grandes batallones. No más. Ya no. Ya no del lado de los más ricos, y aunque esto a usted lo sorprenda, y parezca muy extravagante. La tecnología de la información es un gran ecualizador, una nueva mano que puede mover las escalas del poder. Y Para aquellos sobre los terraplenes de la única superpotencia líder mundial, los vientos digitales soplan fríos a través del brillo triunfante de la postguerra fría.

Considere esta letanía: Del antiguo director de la NSA John McConnell: “Somos más vulnerables que cualquier otra nación sobre la Tierra”. O del antiguo director adjunto de la CIA, William Studeman: “La interconexión masiva hace a Estados Unidos el objetivo más vulnerable del mundo”. El ex ministro de justicia Jaime Gorelick: “tenemos un equivalente cibernético a Pearl Harbor en determinado punto y no queremos esperar a esa llamada que nos despierte”.

Miembros del Pentágono comisionan a sus antiguos amigos quienes analizando los resultados del “Día después” concluyeron: “el mayor tiempo dedicado a esta situación, cuanto más se observa, éstos problemas requieren soluciones concretas y en algunos casos hay buenas ideas sobre dónde empezar”.

Nada de esto está siendo desarrollado. Al contrario, hubo un pequeño frenesí de actividad, de lo cual la mayor parte no fu notada por Washington.

Una Comisión Presidencial ha sido establecida; el FBI, la CIA y la NSA han formado a sus propios especialistas en guerra de la información, cuerpos de interagencias conocidos con acrónimos como IPTF (Infrastructure Protection Task Force) (cuerpos de tareas de protección a las infraestructuras), y CIWG (Critical Infrastructure Working Group) (Grupos de tareas de infraestructura crítica). Estos equipos ya están operativos. Los comités asesores de defensa han enviado gruesos y ágiles reportes pidiendo mayores presupuestos, bombas inteligentes, mayor vigilancia para poder combatir al peligro cibernético.

Sin embargo, no hay una dirección clara. Por todo lo que se habla sobre nuevas amenazas hay una reflexión que reza “lo que fue bueno para golpear a la Unión Soviética y a Saddam Hussein también lo será para golpear a un puñado de hackers”.

Hardware más inteligente dice el pentágono. Más grandes oídos dice la NSA. Mejores archivos dice el FBI. Y mientras tanto el “Día después” analiza “qué le decimos a la Casa Blanca?”

Un poco de confusión inducida digitalmente puede afectar el curso de las telecomunicaciones y los mercados financieros. La guerra de información es algo más compleja y acompaña a este proceso. Mientras en Washington lentamente analizan y aceptan estos cambios la tecnología de información está socavando la mayor parte del mundo del conocimiento acumulado acerca de los conflictos armados, desde Sun Tzu, de todos modos.

¿Qué es un acto de guerra? ¿Qué es una respuesta adecuada? ¿Quién es la primer línea de defensa? ¿Qué significa la “infraestructura civil” cuando el 90% de las comunicaciones militares de los Estados Unidos viajan a través de redes públicas? ¿Estamos preparados para ceder libertades civiles en nombre de la seguridad nacional? ¿Necesitamos un ejército? ¿La Marina? ¿Una Fuerza Aérea? ¿Importa si los tenemos? ¿Cómo fomentar un libre e informado debate sobre un tema tan importante sin entrar en pánico?

Todas son cuestiones interesantes, a menos que suceda que tú seas uno de los hombres o mujeres a quienes se les paga para mantener a los Estados Unidos o a otros países seguros para dormir dentro de sus fronteras. En cuyo caso estas cuestiones son una pesadilla.

Para alterarnos ya disponemos breves informes de guerra de información, sin mencionar las amenazas de la realidad física. Qué podría ser peor que aparezcan en breve en el periódico del ejército chino, Jiefangjun Bao.

A continuación se resumen los discursos pronunciados en el pasado mes de mayo durante la ceremonia de fundación del Centro de Investigaciones Estratégicas Militares de Beijing:

“Después de la Guerra del Golfo, cuando todos esperaban una paz eterna, una nueva revolución militar emergió. Esta revolución es esencialmente una transformación de la guerra mecanizada de la era industrial a la guerra de la información de la era de la información. La guerra de la información es una guerra de decisiones y de control, una guerra de conocimientos y una guerra de inteligencia. El objetivo de la guerra de la información será cambiado gradualmente a partir de “la preservación de uno mismo y acabando con el enemigo” a “la preservación de uno mismo y el control del oponente”.

La guerra de información incluye: guerra electrónica, engaño táctico, estrategia de la disuasión, propagando de guerra, guerra psicológica, guerra de redes y sabotajes estructurales.

Continúa el informe: “Bajo las condiciones tecnológicas actuales, la conquista de todas las estrategias de Sun Tzu (de más de 2 milenios atrás) ‘vencer al enemigo sin pelear’ y someter al enemigo a través del uso leve de la fuerza y la destrucción estructural, podrá finalmente ser logrado”.

Algunos de los factores que hacen a la guerra de la información tan compleja son que a pesar de disponer la tecnología que la hace posible el campo de “batalla” es inmenso, difícil de visualizar e infinitamente flexible. La guerra de la información puede ser mucho más precisa. Conceptualmente figura el escenario de Pearl Harbor electrónico como le gusta llamarlo a los estrategas de Washington imaginando un escenario de conflicto donde colapsa todo el sistema de energía, donde “bombas informáticas “ destruyen el mercado de valores, una bomba de pulso electromagnético inutiliza todo el sistema telefónico. O podría ser algo completamente diferente, algo desconocido, que te destruya por dentro. Jugando y alterando la mente colectiva: mostrando un videoclip de 30 segundo donde uno de sus hijos (miembro de fuerza

expedicionaria en Somalía) esté atado y siendo arrastrado por un jeep. Mostrado por CNN.

El grupo de analistas de Washington puede ser parte del problema. “La amenaza se distribuye” dice Dorothy Denning, profesora de ciencias de la computación y criptógrafa de la Universidad Georgetown. Pero la primer respuesta del gobierno es: ‘Ok, quien va a estar a cargo?’ Es el antiguo enfoque jerárquico y no estoy seguro de si funcionará esta vez.

Denning es conocida en la escena de la privacidad electrónica como criptoanalista de la línea dura, pero sobre la guerra electrónica ella suena más “flexible”. “El problema es que la tecnología dar saltos por delante de la seguridad, y va a estar con nosotros para siempre. Lo que tenemos que hacer es hacer frente a nuestra vulnerabilidad y hacer lo mejor que podamos”.

La guerra de la información vista a través del prisma militar es apenas más inspiradora. No habrá para almacenar. No se gastarán 50 mil millones de dólares en programas inútiles. No habrá misiles que controlar. La amenaza de la guerra de información por definición es abrumadora e inestructurada. Cualquier respuesta a un ataque cibernético aunque sea exagerada será mejor que la falta de ella.

Tampoco ayudarán demasiado los nuevos y caros “juguetes” como los cripto guerreros del FBI y la NSA han analizado, mucha de la tecnología relacionada es software sencillo (fácil de duplicar, difícil de restringir y lamentablemente de uso dual, civil o militar.) No es agradable que en cualquier lugar se pueda desarrollar software malicioso (e-bombs) en cualquier pc en cualquier lugar del mundo se pueden hacer.

John Arquilla, profesor de la Escuela Naval de Posgrado en Monterrey, California y uno de los principales analistas del Pentágono lo dice sin rodeos: “Hemos gastado miles de millones de dólares en las últimas décadas en los grandes, caros portaaviones, bombarderos estratégicos y tanques. La revolución de la información sugiere nada menos que estos activos se han convertido en mucho más vulnerables y mucho menos necesarios”. (“Netware and Peace in the global village”, página 52.)

La respuesta inmediata del Pentágono no es la más discreta: “Cubra su trasero”. Su flamante grupo de tareas de ciencias de la defensa, dirigido por dos secretarías auxiliares del DOD (Department Of Defense) recomendó ampliar el entrenamiento en I-War (guerra de la información). Hay ya una escuela de Guerra de la Información y estrategia, parte de la Universidad de Defensa Nacional en las afueras de Washington) y el endurecimiento de la seguridad de los sistemas de información militares de los Estados Unidos (una categoría de cada vez mayor crecimiento conocida como C4I “Command, Control, Communications, Computing and Intelligence”. El reporte incluye una convocatoria a la autoridad legal para permitir “al Departamento de Defensa, fuerzas de la ley y agencias de inteligencia a conducir eficientes y coordinados monitoreos de ataques a la infraestructura de información civil”. Y como buena medida, recomienda invertir 240 millones de dólares para establecer un

permanente “Equipo Rojo” (un supuesto enemigo hostil) (una especie de “Día después” en reversa) y para iniciar rutinariamente un sondeo clave de los sistemas de información de los Estados Unidos buscando sus puntos débiles. Precio total: 5 mil millones de dólares en cinco años, lo suficiente como para pagar un par de bombarderos B-1.

Juego número dos: “Pasar la pelota”. Dice John Petersen, presidente de The Arlington Institute y consultor del Pentágono, “en cualquier momento las cosas empiezan a oler distinto a matar gente y romper cosas, la gente en el ejército empieza señalando en otras direcciones”, que en este caso significa inteligencia en comunidad y fortalecimiento de la ley.

Espías y policías pueden ser los más adecuados para la tarea, al menos para mantener la defensa en el final de la I-War. Pero esta opción es sólo relativa. La I-war puede enfrentar tiempos y distinciones honoríficas entre fuerzas de la ley e inteligencia, entre norteamericanos y demás, entre los tipos de vigilancia permitida en cada nación y la que comienza “al borde del agua”.

El FBI ha creado un Centro de Investigación informática y de evaluación de amenazas a infraestructuras (Computer investigation and Infrastructure Threat Assessment Center) expandiendo a 56 escuadrones de crimen electrónico a lo largo de Estados Unidos. Más notable aún fue una orden ejecutiva firmada por el Presidente Clinton el pasado mes de julio creando un grupo de trabajo de protección a infraestructuras. Presidido por el FBI y con representantes del DOD y NSA, el grupo de trabajo está encargado de elaborar un “modelo de amenaza” y “contramedidas”. Para lograr estos objetivos es poderosamente facultado para exigir “la asistencia, información y asesoramiento” de “todos los departamentos ejecutivos y agencias”. Dice John Pike de vigilancia de la Federación de Científicos Americanos: “La IPTF (International Police Task Force) demostraba lo que todos tememos y de lo que estamos cansados: la nebulosa autoridad de control. Hay gente que busca una licencia de caza y que pareciera que la ha obtenido.”

Una propuesta silenciosa ronda en Capitol Hill, permitir a la NSA realizar el monitoreo interno, en parte por la teoría de que la tecnología digital entre “domésticos” y “extranjeros” artificiales. ¿Dónde está el borde del agua en el ciberespacio?

Es sólo un inminente punto de la I-War. Otro es un complemento al que asola el cripto debate: a pesar de la amplia base de las encriptaciones y del mérito de la defensa de la I-War, la NSA y el FBI se oponen a ella y no sin razones porque hacen a sus misiones de escucha enfrentarse a potenciales enemigos más problemáticos. La NSA, en particular, busca tempranas comunicaciones encriptadas a lo largo del mundo, ocultando su punto de vista incluso la amenaza del I-war que aumenta dramáticamente las expectativas. A puertas cerradas se realizan audiencias donde se debaten presupuestos y sus representantes locales llegado el caso, deben ratificar decisiones difíciles entre las cuales deben decidir y analizar cómo leer los correos electrónicos.

Si estás buscando a alguien para hablar sobre las vulnerabilidades de las redes de computadoras, tendría que ser Howard Frank, Director de la Oficina de Tecnologías de la Información de DARPA. Frank estaba en el quipo que hace 25 años creó a Internet. Dr. Frankenstein, si se quiere, ahora en silencio tratando de proteger su creación de nuevas fuerzas hostiles que la rodean.

Frank, un amable y cortés hombre, responde a las preguntas con paciencia y pone las cosas en perspectiva. Internet, dice, nunca fue concebido para sobrevivir a una guerra nuclear. Afirma que es un mito urbano el hecho de que fue diseñada para ser invulnerable, es feliz de decirlo.

Frank es un veterano del “Día después”, también supervisó uno de los períodos de sesiones. Pero en un momento de la entrevista, permite deslizarse una observación tan melodramática que podemos esperar con confianza una I-War de Hollywood. Estamos conversando acerca de los grandes cortes de energía de la costa oeste del último verano cuando de repente él exclama: “cada vez que oigo hablar de una de estas cosas yo me digo a mí mismo “ok, comenzó” y cuando me entero de que realmente no, pienso que hemos comprado un poco más de tiempo. Sin embargo, comenzará.”

Entonces, ¿qué hacemos? Hemos creado una tecnología durante un período de 20 o 30 años. Nos llevará 10 o 20 años crear una alternativa tecnológica que nos permita disponer sistemas de defensas más sofisticados.

¿Ese tiempo? ¿Quién sabe? Es como la guerra contra las drogas o como las inútiles batallas urbanas contra las cucarachas. No es difícil comprender el problema, pero las soluciones siguen siendo evasivas, resbaladizas, incluso fuera de nuestro alcance.

No es que nadie esté buscando. DARPA, por ejemplo, está solicitando propuestas para “la investigación y el desarrollo de nuevas tecnologías relacionadas con la supervivencia de los grandes sistemas de información cuya operación continua es esencial para la defensa y el bienestar de la nación”. Están hablando de serios negocios aquí. Están hablando de supervivencia. Y lo que tienen en mente no es cualquier infraestructura “endurecimiento”, son tecnologías de vanguardia, basadas en las últimas teorías ecológicas de la informática, versiones digitales de variaciones genéticas y de la respuesta inmune. “Hay modelos naturales de supervivencia proporcionados por los organismos biológicos, las poblaciones y las sociedades” ha declarado DARPA respondiendo a propuestas. “Este programa de investigación utiliza estos ejemplos de metáforas y orientación acerca de cómo diseñar sistemas de información con capacidad de supervivencia.”

Bueno, buena suerte para ellos. En el corto plazo ideas prácticas están siendo implementadas. La Junta Científica de Defensa estima que para mejorar la infraestructura mínima esencial de las redes de información se necesitarán 3 mil millones de dólares para un sistema de emergencias dedicado a mantener todos los servicios activos hasta un máximo de 250 mil millones de dólares (aproximadamente el presupuesto anual del Pentágono) para poder asegurar

toda la infraestructura norteamericana acorde al “Libro Naranja” (standard del DOD, Departamento de Defensa de los Estados Unidos).

La última cifra s imprecisa. Desde un punto de vista técnico es esencialmente imposible distinguir entre la red de telecomunicaciones mundial, la red de comunicaciones de Estados Unidos y un solo objetivo militar. Peor aún, casi todos los cables e interruptores no pertenecen al Tío Sam.

Un miembro del staff de la Casa Blanca que ha trabajado en esta cuestión plantea: “Es una cosa decirlo para el sector privado: ustedes tienen la responsabilidad de defenderse a sí mismos de los hackers”. Bien. Todos a favor. Pero si de repente dicen que la amenaza es un gobierno extranjero o un grupo terrorista no habrá salida del infierno, van a querer pagar por eso. Nos miran a nosotros y dicen: ¿No es ese su trabajo?

El mayor esfuerzo concertado para resolver estas cuestiones está siendo realizado por la Comisión para la Protección de la Infraestructura Crítica, creado por orden ejecutiva de Clinton. El ex fiscal general adjunto Gorelick como describió en una audiencia del senado como “el equivalente del proyecto Maniatan” (que dio origen a la bomba atómica). Presidido por Robert “Tom” Marsh, retirado de la Fuerza Aérea de Estados Unidos con vínculos industriales, la Comisión se encarga de actuar como enlace entre el gobierno (y las agencias usuales) y las compañías del sector privado que poseen y explotan infraestructuras críticas (radio, TV, telefonía y líneas de datos). Las audiencias públicas se están celebrando en todo el país; el objetivo final es un informe de evaluación sobre el alcance de la amenaza y recomendar estrategias para contrarrestarlo.

Hay muchas ideas brillantes freelance en el mercado de la I-War. De hecho, hay una toda una industria artesanal. A partir de infowar.com, un extenso sitio web comercial dirigido por mucho tiempo por Win Schwartau (ver “Information warrior”, Wired 4.08, página 136). William Church, editor en Londres del Diario de Guerra de Infraestructuras (iwar.irg) propone que la I-War tenga “escuadrones de operaciones especiales” con un único objetivo “patrullar en las redes del enemigo”.

Más sobre el “pensar fuera de la caja” proviene de Robert Steele, retirado de la marina de Estados Unidos y ex oficial de la CIA quien dirige una empresa consultora llamada Open Source Solutions Inc. Steele aboga por lo que él llama “SmartNation” (Nación lista), una especie de vigilancia vecinal electrónica, en el que cada nodo (cada ciudadano) es responsable, educado, alerta y es capaz de unirse en una cadena de seguridad en red”.

Michael Wilson (consultor y frecuente contribuyente a debates on line sobre I-War sostiene que debe fortalecerse la criptografía universal. “Mientras estamos en ella, quien sabe si no hay algo mejor que la NSA?”, pregunta Wilson. “Abrir la tecnología, comenzar con criptografía fuerte, seguridad, autenticación, etc. Impulsar a los científicos de Fort Meade hacia desarrollos de hardware y software. Piense en ello como invertir los dividendos de la paz de la Guerra Fría para ayudar a fortalecer a la sociedad para afrontar las nuevas guerras”.

La idea de enfrentar la amenaza de la I-War provoca la apertura y cierta “aparición” de la seguridad nacional.

Marc Rotenberg, director de Electronic Privacy Information Center situado de Washington considera que los debates sobre I-War son una posible puerta de entrada a una reexaminación completa de la seguridad nacional y de las instituciones dedicadas a la seguridad de la misma. “Ahora es el momento para poner más de las actividades de la NSA a la luz pública. Si estas amenazas existen, usted no querrá mantener el debate encerrado en el sótano de la Casa Blanca o en las habitaciones traseras del Pentágono”.

Acorde a John Arquilla debemos lidiar con que el problema de la I-War no es simplemente un problema militar, sino tomamos conciencia de esto, “no seremos capaces de lidiar con la I-War en absoluto”.

¿Reducir el Pentágono? ¿Fondos baratos para “guerreros de la información” luchando desde las sombras? Arquilla dice nuevamente: “Es evidente que existe una preocupación institucional sobre cómo hacer los cambios radicales fuera de un cambio militar pesado, Sin embargo, las limitaciones presupuestarias en última instancia nos conducirán en esa dirección.” Sin especificar en detalles las posibilidades son bastante obvias (reducir a la mitad el presupuesto del Pentágono por ejemplo) y orientar los ahorros hacia una actualización masiva de las redes del país, mediante desgravaciones fiscales y otros incentivos. Esto hará posible que obteniendo ahorros pueda realizarse”. “El rediseño institucional está en su momento, políticamente, y esta debe ser una tarea para el próximo ciclo presidencial” dijo Al Gore.

La buena noticia es que ya vamos por esta vía: en el gobierno como en la industria la reducción y la eficiencia van con el territorio. La mala noticia es que la magia del mercado no es muy tranquilizadora, por ejemplo, un grupo de científicos en computación búlgaros se encuentran subempleados trabajando para Saddam Hussein.

Es una apuesta justa que, tarde o temprano, nos encontraremos dando tumbos hacia un verdadero debate nacional con la esperanza de comenzar un verdadero Pearl Harbor electrónico.

Ciertamente, ningún funcionario electo ha desafiado a la credibilidad de las amenazas de la I-War, siempre y cuando exista el riesgo de que los acontecimientos lo puedan contradecir.

Las cuestiones de cómo contrarrestar el peligro y la forma de hacerlo sin salir más de cuestiones tan problemáticas y candentes como el espionaje interno, el derecho a la intimidad, enemigos ocultos, y las regulaciones oficiales de las redes de propiedad privada.

Esto no es sólo un problema táctico: cuando el FBI, la NSA, la CIA y en Pentágono se reúnen para hablar de seguridad nacional mucha gente comienza a levantar sus copias de la Carta de Derechos. Y cuando la amenaza que habla de todo el mundo desde hackers foráneos sin rostro, terroristas,

creadores de bombas, sin olvidar a los productores de pornografía infantil, se trata de una feria donde la demagogia no estará ausente.

Esto ya sucedió antes, miren en los 50's. La mejor voluntad carece de toda convicción, lo peor se llena de apasionada intensidad y el tejido político comienza a entrelazarse.

Todo esto, por supuesto, puede sonar muy parecido a lo que los amigos chinos llaman "destrucción suave". Como dice William Church: "La forma más dañina de I-War es la guerra política o la guerra psicológica". Y casi cualquier cosa puede ser parte de ella: los cortes de energía, redes de averías, inteligentes campañas de desinformación, cualquier cosa "para obtener que la población sienta que el país se va al infierno."

### ***GUERRA DE REDES Y PAZ EN LA ALDEA GLOBAL UNA ENTREVISTA CON JOHN ARQUILLA Por Ashley Craddock***

El futuro de los conflictos armados no será sobre campos de batalla, sus redes y su información será usada para derrotar a las fuerzas uniformadas.

El asesor del Pentágono John Arquilla tiene un nombre para las respuestas baja tecnología a la guerra de alta tecnología: guerra de redes. Y él cree que los futuros conflictos serán dominados no por superpoderes y naciones-estado sino por pequeños, grupos distribuidos (que van desde las bandas criminales a los rebeldes como los de Chechenia y Chiapas) quienes pueden explotar las tecnologías de información.

Conocido en algunos círculos como "el príncipe oscuro" por abogar agilidad radical, menos jerarquías militares en Estados Unidos, Arquilla es profesor de guerra de información y operaciones especiales en la Escuela Naval de Posgrado de Monterrey, California.

*Wired Magazine: ¿Qué formas tomarán los conflictos futuros?*

*Arquilla:* La Guerra del Golfo ha sido anunciada como la primer guerra de la era de la información, pero veo muy pocas nuevas guerras del golfo. Veo muchas guerras de redes, peleadas por redes. Eso no es simplemente batallas armadas entre las fuerzas uniformadas, es el tipo de conflicto librado por terroristas y organizaciones criminales y revolucionarias, incluso de activistas sociales. Es un tipo muy diferente de conflicto, de hecho, es muy difícil llamarlo guerra. Y sin embargo, lo es, porque es una forma de conflicto y, usualmente, tiene elementos militares.

*¿Qué hay de nuevo acerca de eso?*

Todos los canales interconectados distinguen las redes modernas, cada nodo puede conectarse directamente con otro nodo. Lo que es fascinante es que los contrabandistas, piratas, otras formas de criminales, revolucionarios, y

terroristas se han reorganizado alrededor de estas líneas de redes. Ahora se han casado con la revolución de la información, y esto les ha brindado nuevas y vastas capacidades.

También veremos más guerras de redes porque se pueden librar estas clases de conflictos sin grandes ejércitos sobre el terreno y de hecho, sin tecnologías sofisticadas. Desde el inicio de la Guerra del Golfo no tuvo mucho sentido desafiar a los Estados Unidos directa o convencionalmente. Sólo unos pocos ejércitos (bastante avanzados) participarán en las guerras de alta tecnología del futuro. En lugar de ello, habrá una profusión de problemas para los intereses norteamericanos. Y es este tipo de conflicto para el que no estamos preparados.

¿Los militares norteamericanos están dispuestos a abandonar las estrategias tradicionales? Cada pensador serio sobre el futuro del ejército norteamericano está considerando esta posibilidad.

Una unidad básica de maniobras ya no debe ser un gran grupo de combate (divisiones mecanizadas o brigadas aéreas completas) porque otra tendencia en la era de la información es la creciente letalidad de lo muy pequeño, incluso formaciones de hombres y máquinas. Se pueden observar pequeñas unidades (entre 500 y 700 efectivos). Un escuadrón de infantería puede disponer una gran cantidad de poder de fuego el día de hoy, y esto es posible precisamente a causa de la revolución de la información.

Al mismo tiempo, si el campo de batalla va a ser drásticamente disminuido en términos de unidades de maniobra y tamaño, entonces la necesidad de jerarquías también disminuye.

Las jerarquías fueron diseñadas para hacer frente a ejércitos masivos, para controlar a cientos de miles, incluso millones, de tropas. De hecho, la tradicional estructura jerárquica diseñada para controlar un ejército de masas puede, simplemente, limitar la capacidad de estas nuevas fuerzas. Y el ejército es sensible a esto.

*¿El Pentágono aprende de sus lecciones?*

Mi mayor preocupación es que el énfasis es demasiado tecnológico en su naturaleza (tendemos a pensar en la guerra de información como cibernética, como sistemas no tripulados). Y este simplemente no es el caso. Podríamos encontrarnos también contra oponentes que usen otros medios de difusión de la información y otras formas de organización. El militar es esencialmente jerárquico. Alguien tiene que estar al mando, rango que no desaparece. Pero no debemos olvidar que los agentes no estatales no tienen tales limitaciones.

*¿Qué puede hacer el Pentágono para hacer frente a esos tipos de desajustes?*

Los Estados-Nación y sus administraciones jerárquicas no son adecuados para hacer frente a una ágil red de opositores a quienes nos enfrentamos. La era de la información implica generalidades de los muchos, la descentralización de la autoridad. Esto es altamente perjudicial para la estrategia militar tradicional. Como dijo Napoleón, mejor tener un mal general que dos buenos. Sin embargo, en el ejército norteamericano, se están haciendo esfuerzos para crear formas híbridas de organización, en la que el comandante en jefe tiene lo que en el mundo de los negocios se llama la vista superior: él sabe el panorama general, pero permite una gran transferencia de autoridad, con subordinados librando las campañas.

*¿Esto ha funcionado?*

Nuestros primeros esfuerzos no han sido fructíferos. Estamos frente a una gran variedad de oponentes en la red, incluso en estos momentos: las organizaciones criminales transnacionales, (carteles de la droga, por ejemplo) y sus redes han proliferado y están extendiendo armas de destrucción masiva a través del mundo. Estos son sólo algunos ejemplos de los tipos de oponentes a quienes nos enfrentamos y, sin embargo, lo vemos desde el enfoque del gobierno norteamericano, lo vemos de un modo extremadamente jerárquico, centralizando esfuerzos ya sea para combatir una guerra contra la droga o contra la proliferación de armas.

*¿Las cosas se ven mejores para luchar contra las amenazas convencionales?*

No hay demasiada evidencia que nos permita comprender las implicaciones de pequeños ejércitos, de menores líneas de combate, o incluso de la idea de que el contexto de los conflictos es muy diferente. Por ejemplo, el Departamento de Defensa tiene una política de poder para librar dos guerras convencionales casi simultáneamente. Y cada vez que surge una crisis la pregunta es: ¿Cuán pronto podemos tener un ejército en tierra (de entre 300.000 y 400.000 soldados) en alguna locación para luchar en una guerra de las características de Tormenta del desierto? Pero el hecho es que esta ocasión, probablemente no se plantearía.

*¿Pero no fueron las capacidades de información una de las razones por las que Estados Unidos ganó tan rápidamente la Guerra del Golfo?*

La dirección que los militares toman (disponiendo nuevas tecnologías de información dentro del conocimiento existente de la guerra y de las estructuras existentes) es un gran error. Un instructivo ejemplo de esto fue la guerra franco-prusiana. En 1870, Francia tenía una ametralladora, la primera realmente eficaz en el mundo. Sin embargo, estaba montada en un transporte como una pieza de artillería, se mantiene con la artillería de largo alcance, lo que habría sido una ventaja absolutamente ganadora muy rara vez entra en juego. Los efectos fueron catastróficos

Si los militares norteamericanos simplemente injertan nuevas tecnologías de la información en las estructuras existentes, se corre el riesgo de ser derrotados en uno de los principales conflictos del futuro. Mantener las grandes formaciones masivas de fuerzas, por ejemplo, simplemente crea grandes objetivos.

*Entonces, ¿hemos visto las últimas guerras que utilizaron a ejércitos masivos?*

No lo creo. Si ambas partes disfrutan de niveles similares de tecnologías y de lucha con la misma habilidad, lo que veremos es la incapacidad de cualquiera de las partes para hacerse con el control y el retorno al énfasis del desgaste y las maniobras. Mi esperanza es que, con anterioridad al estallido de estos conflictos, crearemos una generación de oficiales que comprenderán que, por encima de todo, la era de la información se refiere al valor del capital humano en la guerra, así como el hecho de que no siempre podemos contar en la lucha contra un oponente con una muy rudimentaria capacidad de información, al igual que los iraquíes. Tenemos que pensar en la posibilidad de que nuestros oponentes en la lucha están tan bien armados e informados como nosotros.

*¿Qué hay en el camino de un cambio serio?*

Los militares que cambian son usualmente militares que han sido derrotados. Y este es un momento muy difícil para los Estados Unidos. Tenemos una fórmula que ha funcionado. Hemos ganado la Guerra Fría. Hemos ganado la Guerra del Golfo. Hacer las cosas de esta manera es costoso, 250 mil millones de dólares gastados en defensa cada año.

¿Queremos tener la oportunidad en una nueva forma de lucha contra el mero hecho de que puede significar que seremos capaces de hacerlo menos costoso? Yo diría que debemos, porque tenemos limitaciones económicas a las cuales debemos responder. Pero también tenemos que descentralizar nuestras fuerzas armadas por las mismas razones que las empresas están descentralizándose.

*¿Cómo afecta esto a la estructura de poder mundial?*

Ha habido largos debates sobre si las tecnologías de la información tienden hacia el bien o el mal. Mi mayor temor es el aumento de la capacidad de los Estados y los agentes no estatales que utilizarían la tecnología de la información para difundir las formas tradicionales de influencia y poder. Un tipo de información apoyada por el imperialismo podría surgir. Y una forma de mercantilismo criminal puede surgir, practicado por diversas organizaciones piratas en todo el mundo.

*Eso no suena particularmente alegre...*

Existe la posibilidad de que Estados, aprovechando el poder de las redes de información se alineen con organizaciones criminales transnacionales, quienes servirían como sus agentes como forma de librar una guerra de baja intensidad.

Pero hay otra hipótesis: porque el libre flujo de la información aumenta el costo de la represión, Estados totalitarios y autoritarios encontrarán una mayor dificultad de mantener el control.

Mi mayor esperanza es que la revolución de la información plantea la posibilidad de difundir a nivel mundial una serie de valores comunes y acuerdos sobre la naturaleza de los derechos humanos. La interconexión (y los problemas sociales, políticos, y, a veces, las capacidades militares que vienen con esta interconexión) puede ayudar a romper las cadenas en todo el mundo que siguen bajo control autoritario. Es posible que las nuevas tecnologías de la información auguren el surgimiento de una sociedad civil mundial que será autónoma mundial.

LUCIANO SALELLAS  
AUDITOR EN SEGURIDAD INFORMATICA  
<http://www.sr-hadden.com.ar>