

# Lecciones Douhetianas Aplicadas al Combate en el Espacio Cibernético

CAPITÁN LUÍS E. POMBO CELLES, FABRA

ANDRE GONÇALVES

*“A menudo, la formulación de un problema es más esencial que su solución, la cual podría ser tan solo cuestión de destreza matemática o experimental”.*

-Albert Einstein

**L**A HISTORIA de la humanidad está marcada por conflictos de interés que a menudo resultan en conflictos armados. Por consiguiente, los estados deben dicha situación para preservar sus mejores intereses y, en ocasiones, garantizar su supervivencia. Históricamente, los países que se preparan para la posibilidad de un conflicto futuro, especialmente en términos de apresto tecnológico, tienden a tener una ventaja sobre los demás. Actualmente vivimos en una era de información, donde tenemos a la *Internet* como el eje central de las comunicaciones en nuestra sociedad global. De hecho, nuestra dependencia en esa red de computadoras nos lleva a darnos cuenta que ese combate probablemente se llevará a cabo en espacio cibernético. De manera interesante, en términos de prepararnos para un conflicto futuro nos convendría analizar el pasado—específicamente los conceptos de la aviación expresados por el general italiano Giulio Douhet, un pionero de la estrategia de poderío aéreo durante inicios del siglo XX.

Muy a menudo los estados soberanos van a la guerra para resolver sus diferencias, empleando cualquier medio necesario—inclusive tecnologías tanto antiguas como nuevas—para lograr sus metas. Tomemos por ejemplo el aeroplano. Menos de una década después de su invento varias naciones comenzaron a utilizarlo para mejorar sus capacidades de combate. Su entrada al servicio militar ha cambiado completamente la cara de la guerra. Hoy observamos una revolución similar con el advenimiento de la *Internet* y su inclusión en todos los aspectos de nuestra vida. El conflicto en el espacio cibernético se ha convertido en una realidad—una que la milicia ya no se puede dar el lujo de pasar por alto. Pero, ¿cómo definimos un curso de acción sobre algo que nunca existió anteriormente en la historia de la civilización?

Para poder responder esa pregunta, en este artículo analizamos los primeros ocho capítulos del libro *The Command of the Air* (El comando del aire), escrito por el General Giulio Douhet entre 1921 y 1927<sup>1</sup>. En ese libro, Douhet ofrece sus impresiones acerca de esta novedosa embarcación y sugiere cómo se debe utilizar en combate. La analogía a la guerra cibernética es evidente: Una tecnología nueva a inicios de sus capacidades comienza a evolucionar rápidamente tanto en el ámbito civil como militar y se involucra en la defensa nacional. En este artículo se resumen brevemente el contenido de cada capítulo y relaciona la discusión de Douhet con la situación presente en el espacio cibernético. (Cabe destacar que los títulos de los primeros ocho capítulos de la edición brasileña *The Comand of the Air*, empleados aquí, corresponden a las ocho secciones del capítulo 1, “*The New Form of War*” [La nueva forma de guerra]), libro 1, “*The Command of the Air*”, edición norteamericana.)<sup>2</sup>

## Capítulo I, “Los medios técnicos de la guerra”

En el capítulo 1, el General Douhet reflexiona acerca de la entrada de la aeronave como un arma en las operaciones militares. Aquí encontramos sus primeras críticas acerca de la idea persistente de utilizar la aviación como una fuerza auxiliar para la armada y el ejército, especialmente en misiones de exploración y reconocimiento. Douhet destaca la lógica de crear una fuerza independiente que pudiese desarrollar el potencial completo del aeroplano como arma de guerra. Douhet finaliza el capítulo tratando la necesidad de estudiar lo más preciso posible la capacidad de este nuevo tipo de equipo en el campo de batalla en comparación con el armamento en tierra y en el mar. De manera similar, debemos analizar y perfeccionar nuestra capacidad técnica existente para llevar a cabo esa acción (un ataque cibernético), para lograr los objetivos militares en caso de una guerra.

El conflicto en Osetia del Sur en el 2008, entre Rusia y Georgia, probablemente será recordado como el primer altercado entre dos estados soberanos en que un ataque cibernético precedió el comienzo de las hostilidades<sup>3</sup>. Es decir, el conflicto comenzó en el mundo virtual antes que comenzar en el mundo real. Por lo tanto, la proyección del poder militar comenzó en tierra y luego se trasladó al mar, al aire, al espacio exterior y ahora al espacio cibernético—su quinta dimensión de rendimiento. A medida que tratamos de comprender la magnitud de este cambio y prepararnos para una lucha posible en este entorno, debemos cuantificar nuestras capacidades y alcance cibernético.

## Capítulo 2, “Las nuevas posibilidades”

Douhet destaca que antes del advenimiento de la aviación, las guerras estaban restringidas a la superficie de la tierra/agua de la Tierra, algunas más conducentes a la facilidad de movimiento que otras. Naturalmente, las defensas se colocaban a sí mismas para proteger las zonas de acceso codiciadas por el enemigo, quienes podían llegar al territorio deseado con tan solo romper las líneas de defensa y haciéndolas retroceder. En cambio, el defensor puede proteger su territorio solamente manteniendo al agresor fuera de una línea de defensiva.

Sin embargo, esos asaltos se sintieron directamente solamente con relación al alcance del armamento empleado. Aunque participaban completamente en el conflicto, las naciones distinguieron entre los combatientes y los no combatientes, entonces para estos últimos la vida no cambió demasiado en los periodos de paz o guerra. Con la introducción de la aeronave, esas suposiciones dejaron de existir porque esas plataformas no estaban limitadas por las rutas predefinidas en la tierra o en el agua. Los efectos del combate ya no estaban restringidos al frente porque la aeronave podía volar sobre las líneas de defensa para llegar a los blancos dentro del territorio enemigo. Asimismo, toda la defensa que conocemos en la actualidad puede tornarse irrelevante en el entorno cibernético porque se basa en proteger contra un ataque físico en lugar de un ataque virtual. Lo que es peor, dicho ataque podría ser dirigido no solamente a instituciones militares sino a cualquiera de los cinco anillos (liderazgo, producción principal, infraestructura, población y fuerzas en servicio) descritos por John Warden III.<sup>4</sup>

Por ejemplo, los agresores pueden utilizar el espacio cibernético para robar datos de las organizaciones públicas o privadas, utilizar a los ciudadanos como herramientas involuntarias para difundir información falsa, dañar o destruir la infraestructura, interrumpir los abastos básicos (por ejemplo, la electricidad, agua y servicios bancarios) e implicar a figuras políticas en escándalos falsos mediante el robo de datos personales como correos electrónicos o mensajes móviles. En vista de que proteger a cualquiera de este tipo de amenaza es prácticamente imposible, está claro que necesitamos una organización preparada y capacitada para actuar en defensa de las instituciones democráticas a todos los niveles (federal, estatal y local), en los tres poderes del

gobierno (legislativo, ejecutivo y judicial) y en cualquier segmento privado de la sociedad que apoye la seguridad nacional.<sup>5</sup> Esta fuerza organización debe ser capaz de actuar en un entorno virtual contra una amplia variedad de enemigos apoyados por una variedad de fuentes (por ejemplo, otros estados, grupos políticos o religiosos, empresas delictivas, etc.).

### Capítulo 3, “La turbulencia”

En esta parte del libro Douhet explica cómo las capacidades del armamento empleado en la Primera Guerra Mundial favoreció las acciones de defensiva en lugar de las acciones de ofensiva y cómo las naciones que participaron en la guerra prácticamente se fueron a la bancarrota a causa del esfuerzo necesario para luchar en una manera tan estática. O sea, un incremento en la potencia de fuego en las armas utilizadas implica un incremento correspondiente de alcance y régimen de tiro; por lo tanto, aunque el agresor posee una mejor arma, tiene que enfrentar una defensa más fuerte apoyada por ametralladoras y artillería. Por consiguiente, estos tipos de ataques exigen más hombres, armas, abastos y recursos, y por ende saturar los recursos de una nación. Douhet concluye que, después del conflicto, esta experiencia llevó a algunas naciones a darle suma importancia a la construcción de barreras y fortificaciones, aunque el aeroplano podía sobreponerse fácilmente a estos obstáculos e invertir la situación, dándole al agresor la ventaja.

Brasil ha creado estructuras con el propósito de proteger y permitir el uso de las fuerzas armadas en el entorno cibernético. Según la recién Política para la Defensa Cibernética establecida por el Ministerio de Defensa, la protección eficaz contra las operaciones cibernéticas depende no solo del segmento militar sino también de la sociedad brasileña en general, inclusive las instituciones privadas y civiles.<sup>6</sup> Las actividades maliciosas en la *Internet* instigadas por piratas (*hacker*) principiantes ahora están tomando la forma de ataques llevados a cabo por profesionales para promover la causa de varias organizaciones. Por ejemplo, la campaña de espionaje cibernético conocida como Octubre Rojo, que comenzó en el 2007, buscaba obtener información clasificada y acceso a redes seguras en diferentes países en el mundo. Al menos tres ataques fueron dirigidos a instituciones diplomáticas y científicas en Brasil.<sup>7</sup> La incapacidad de identificar al autor de ese ataque dificulta definir el propósito de obtener esa información.

### Capítulo 4, “El arma ofensiva”

Aquí, Douhet destaca la dificultad de adoptar una actitud defensiva hacia el armamento aéreo ya que a diferencia de las fuerzas terrestres y marítimas, las aeronaves pueden atacar desde cualquier dirección, indistintamente de las barreras geográficas o las hechas por el hombre. Esa actitud conduciría a una reducción de las fuerzas de defensa a causa de la necesidad de crear un círculo defensivo en lugar de una línea de defensa empleada hasta el momento. Él explica la inutilidad de esas fuerzas dispersadas protegiendo completamente contra un empleo en masa de aeronaves. La diferencia entre la velocidad de las fuerzas de defensa en tierra y las aeronaves de ataque evitaría que las anteriores asistieran en la zona de ataque. Douhet sugiere que, a diferencia de la práctica en conflictos anteriores, ahora es necesario contar con más efectivos para defender un blanco que atacando, cambiando así el índice de recursos asignados entre defensa y ataque a favor del último. Él concluye este capítulo con uno de sus axiomas más famosos: Que uno puede conquistar el aire solamente evitando las operaciones aéreas del enemigo tomando acción ofensiva contra sus recursos mientras que aún están en tierra—no colocando defensas en nuestro territorio esperando que ellos ataquen.

El espacio cibernético se puede utilizar para estrategias tanto de defensa como de ataque. En la Doctrina Básica de la Fuerza Aérea Brasileña (DCA 1-1) se incluye, entre sus muchas misiones de fuerza aérea, la defensa cibernética, concebida para proteger los sistemas de comunicaciones

amigos y la tecnología de la informática para el mando y control, para ocasionar daño a los sistemas correspondientes del enemigo y recopilar información relevante acerca de la estructuras del opositor.<sup>8</sup> El uso del entorno virtual en un conflicto no está limitado solamente al uso de estrategias de ofensiva para obtener una ventaja inicial; más bien, debemos tener en cuenta que esto funciona de dos maneras y que tendremos dificultades en identificar los blancos del enemigo para represalia. En vista de que el anonimato es la carta de triunfo en este tipo de combate lo debemos utilizar a nuestro favor, especialmente en acciones dirigidas a componer bases de datos de amenazas similares y verificar la extensión de las capacidades de combate del enemigo (ya sea ofensiva o defensiva) en el espacio cibernético de manera que podamos medir sus puntos fuertes y debilidades. Además, en virtud del desarrollo rápido de las amenazas, su amplia gama de posibilidades y la posibilidad de daños extensos, debemos recopilar esa información de manera continua—no solamente durante un estado de conflicto.

## Capítulo 5, “La magnitud de las ofensivas aéreas”

Analizado fuera de su contexto histórico, este capítulo resultó ser una de las secciones más controversiales del libro. Aquí Douhet defiende el uso de armas explosivas, incendiarias y químicas, no solamente sobre blancos militares sino también sobre la población civil para poder afectar el estado de ánimo y por ende reducir el apoyo del pueblo por el conflicto. Además, destaca que una unidad militar se hubiese preparado para soportar un ataque de la artillería del enemigo pero no de uno de aeronaves volando profundo en el territorio y por lo tanto sufriría del impacto directo de municiones aéreas.

Además, Douhet compara la potencia de tiro de los buques de guerra de la poderosa flota británica con un modelo genérico de un aeroplano, alegando que con una carga de bombas de dos toneladas en cada aeronave equivaldría al ataque de un solo lado de tres buques de guerra, pero el precio de un solo buque costaría el equivalente de 1,000 de esas aeronaves. Por último, concluye alegando que en un choque entre las dos plataformas, la aeronave tendría la ventaja total de emplear su armamento con impunidad.

Evaluando en retrospectiva la propuesta de Douhet para atacar civiles, en virtud de nuestra familiaridad con cada conflicto importante durante el último siglo, sabemos que él estaba equivocado al imaginar que solamente el poderío aéreo podría afectar el estado de ánimo de los civiles al punto de exigirles a sus líderes que se rindiesen incondicionalmente. En realidad, una campaña aérea nunca llegó al punto de socavar el estado de ánimo nacional, pero quizás un conflicto virtual podría tener más éxito en este tipo de misión y, aunque no socavase el estado de ánimo, subvertiría de manera significativa la voluntad del pueblo de luchar contra el opositor.

En Brasil en el 2010, un tercio de las transacciones comerciales entre negocios y consumidores se llevaron a cabo en la *Internet*. Una investigación llevada a cabo el año siguiente reveló que el 48% de los brasileños tienen acceso a la *Internet*, pero solamente el 20% de esos usuarios la utilizan para comprar, principalmente por la falta de confianza en esas transacciones.<sup>9</sup> A pesar de su capacidad de representar un volumen de negocios elevado (quizás por su velocidad y conveniencia), la *Internet* aún enfrenta fuertes rechazos por parte de los brasileños cuando se trata de la confianza y credibilidad como una herramienta para hacer negocios. Sin embargo, las declaraciones del impuesto sobre la renta federales (y la mayoría de las declaraciones estatales y municipales) del país dependen exclusivamente del uso de programas existentes en la *Internet* para bajar y enviar formularios. Además, con respecto a las operaciones de operaciones comerciales, contamos con la tercera bolsa de valores más grande del mundo por su valor en el mercado.<sup>10</sup> La cifra actual de cuentas con acceso a la *Internet* ha crecido a un promedio de 18% entre el 2002 y el 2011, y en el 2012, 25% de todas las transacciones bancarias se llevaron a cabo en la *Internet*.<sup>11</sup>

Lo que vemos aquí es un tipo de paradoja: Una nación con gran dependencia en el mercado de la *Internet* pero que no la considera una herramienta confiable para esas transacciones. Ahora, imaginen cuáles serían las repercusiones en este mercado si sus sistemas fuesen sacudidos por el robo en masa de información personal, cancelaciones de órdenes bancarias o en el mercado, o la interrupción del acceso por un par de horas o días. Esta situación probablemente se agravaría por las dificultades legales de castigar a los culpables (aún si fuesen identificados—algo que rara vez ocurre), por ende exponiendo a los usuarios del sistema no tan solo a su fragilidad sino también a la invulnerabilidad de los autores. Aunque medir la pérdida financiera de esos ataques es difícil, e inconclusa, en el mejor de los casos, podemos suponer que el problema es grave—testigo de ello es el hecho que en el 2012 los bancos brasileños invirtieron una cantidad sustancial de dinero en tecnología de informática para contrarrestar el fraude electrónico.<sup>13</sup>

## Capítulo 6, “El comando del aire”

En esta parte el autor recalca la idea central de su libro: En la guerra, dominar el aire significa la victoria y perder ese dominio significa la derrota. Él alega que para vencer las defensas de una nación uno no puede aceptar ni un remedio temporal ni una solución parcial en las iniciativas para prepararse para la guerra ya que la aviación sería esencial para dictar el curso de la batalla. Él deja claro que en el futuro la guerra se llevará a cabo en tres campos de batalla (tierra, mar y aire) y que cada uno requerirá una fuerza especializada para emprender operaciones diferentes para entornos diferentes, aunque todo debe ser coordinado para garantizar la victoria. Por lo tanto, uno no puede emplear la aviación tan solo como un medio auxiliar del ejército y de la armada; en cambio, debe constituir una tercera fuerza empleada para lograr el comando del aire.

No obstante, establecer la supremacía en el espacio cibernético o un dominio en el espacio cibernético presenta dificultades porque es una dimensión virtual esparcida por todo el mundo. Sin embargo, las tecnologías nuevas ofrecen soluciones nuevas para lograr un antiguo objetivo—la victoria. Por ejemplo, en el 2008, una compañía de comunicaciones pudo reorientar, por 18 minutos, alrededor del 15% de todo el tráfico de información en la red mundial a través del mismo país en el que estaba ubicada. *China Telecom*, la compañía responsable, negó su culpabilidad, destacando que la mayoría del tráfico pasa a través de Estados Unidos. Indistintamente de su intención, debemos aceptar la magnitud de esta hazaña, que involucró tremendas cantidades de información que pudo haber sido almacenada para analizarla más a fondo.<sup>14</sup>

Extrapolando de Douhet, podemos decir que los próximos conflictos en el entorno virtual tendrán un frente nuevo—el entorno virtual—y que debemos poder asegurar nuestro uso de la *Internet* a la vez que se lo negamos al enemigo. Para ello es necesario contar con una fuerza con el personal adecuado y capacitado para este fin—uno que actúe por sí solo con objetivos y doctrina independiente en cooperación con otras fuerzas pero no subordinada a ellas. Entonces, de surgir la necesidad, ¿debemos actuar debidamente (como lo hicimos cuando la fuerza aérea se convirtió en una rama independiente) o debemos anticipar el problema?

## Capítulo 7, “Las consecuencias extremas”

Luego, Douhet formula dos corolarios para apoyar su idea que una nación debe conquistar el comando del aire para garantizar la victoria. Primero, él recalca que la seguridad de una nación y, por consiguiente, su defensa, depende de estar en una posición para conquistar el comando del aire durante un conflicto. Segundo, él alega que todos los esfuerzos de defensiva en tiempo de guerra deben tener como objetivo lograr los medios para derrotar el dominio del aire. Douhet reitera que para controlar este ámbito uno debe destruir la capacidad de volar del enemigo y que solamente las aeronaves capaces de atacar blancos tanto dentro del territorio enemigo (en

tierra y en el mar) y en el aire pueden hacerlo. Además, él insiste que solamente una fuerza aérea separada (enfocada en el combate en el aire) puede conquistar el comando del aire de un enemigo—una nación que puede ir en contra del concepto de defensa nacional de su propio país.

Consciente de la controversia de su postura, Douhet reafirma su tesis de que es necesario analizar esta herramienta singular con una mentalidad nueva y tratar de apartarnos de antiguos conceptos y preceptos, aceptando una nueva era en la curva evolutiva del conflicto e incorporar a la aeronave en la planificación militar. Él destaca que la eficacia de nuestras tropas (y por ende la defensa de nuestra nación) exige que anticipemos cambios en el carácter de la guerra en lugar de adaptarnos después que ocurren. Continuando, él alega que este cambio no significa que las fuerzas terrestres y navales deben ser extinguidas; en cambio, él solo pide que la nación reconozca la importancia de emplear una fuerza aérea independientemente en lugar de relegarla al margen a una función auxiliar.

De manera similar, una fuerza que lucha por la ventaja en el espacio cibernético, no debe estar sujeta a ninguno de los comandos militares existentes. Además, debemos tomar en cuenta cuestiones legales ya que caracterizar un ataque cibernético como un delito es diferente a considerarlo un acto de guerra hostil, una distinción que plantea unas cuantas preguntas importantes:

- ¿Debemos tener dos (o más) servicios armados diferentes protegiendo el espacio cibernético?
- De ser así, ¿dónde están las fronteras de sus jurisdicciones?
- ¿Qué sucede si un soldado percibe un delito o un policía descubre un acto de guerra en el espacio cibernético?
- A propósito, ¿cómo debemos diferenciar entre un delito y un acto de guerra en el espacio cibernético?
- En el espacio cibernético, ¿debe un soldado también ser un policía, un policía también debe ser un soldado, o necesitamos un tipo de profesional diferente con aptitudes muy específicas?
- ¿Es mejor contar con varios servicios armados, cada uno con su propia fuerza cibernética, haciendo su propio trabajo y, de ser necesario, intercambiar información? ¿O debemos tener un servicio armado singular que centralice todas las operaciones importantes mientras que las ramas ya establecidas utilicen sus propios recursos para necesidades específicas como fuerzas auxiliares—similar a la manera como la comunidad de inteligencia funciona?

Un ejemplo de esta complejidad ocurrió en el 2010 cuando un virus *Stuxnet* de computadoras atacó las instalaciones nucleares en Irán, afectando no tan solo la red virtual sino también ocasionando daños físicos.<sup>15</sup> Esa acción ¿sería un delito o acto hostil contra esa nación? Si un evento similar sucediese en Brasil, ¿seríamos responsables de identificar al responsable y sugerir una respuesta proporcional? ¿La Policía Federal? ¿El Departamento de Defensa? ¿El Departamento de Justicia? En esa situación, la responsabilidad de evitar, combatir y asesorar debe radicar en una “Fuerza Cibernética” que tenga la libertad de actuar independientemente del acto en sí (como delito, acto de guerra, acto de terrorismo, acción política, etc.) para defender el estado. En la era de la informática, ya no podemos perder tiempo decidiendo quién es el responsable, sino debemos definir cómo lidiar con el problema. Medidas secundarias tales como acciones diplomáticas, declaraciones públicas para audiencias internas y externas, reunir un gabinete para lidiar con la crisis, y así sucesivamente, serán todas insignificantes si no podemos detener una amenaza que podría suceder y desaparecer en cuestión de horas. Tal como Douhet abogó por una fuerza que dominaría el aire, nosotros también debemos establecer una Fuerza Cibernética independiente preparada para combatir y ganar en el espacio cibernético.

Para proteger la nación y sus instituciones, dicha fuerza debe estar conformada por profesionales militares y civiles; debe ser guiada por las políticas de la Policía Nacional, especialmente en manejar las operaciones de defensa e inteligencia; y mantener canales de comunicación abiertos con los servicios cibernéticos auxiliares de las comunidades de seguridad y defensa. En resumen, la fuerza tendría una estructura jerárquica con control centralizado y ejecución descentralizada, gobernada por sus propias regulaciones y guiada por una doctrina específica en línea con las metas del estado. El comandante o director de la Fuerza Cibernética debe tener acceso directo al presidente y, respetando el principio democrático de equilibrio de poderes, debe estar sujeto a los mismos controles que el poder judicial y el legislativo le aplican a las fuerzas militares y a la comunidad de inteligencia.

## Capítulo 8, “Fuerza Aérea independiente y aviación auxiliar”

Por primera vez Douhet emplea el término *fuerza aérea* para designar una rama de las fuerzas armadas cuyo propósito es lograr el dominio del aire. Esta fuerza nueva, independiente de las demás, debe estar preparada para luchar sola en busca de sus propios objetivos, pero siempre buscando un terreno común (o sea, la defensa nacional) con la armada y el ejército. Él está de acuerdo que ambas armas requieren aeronaves específicas para apoyar sus misiones (su concepto de aviación auxiliar). Douhet finaliza este capítulo y la primera parte del libro afirmando que el ejército y la armada deben usar aeronaves para ir en busca de sus propias metas y no mirar a la fuerza aérea para este fin porque esta institución nueva tiene la misión sin precedentes de dominar el aire en tiempo de guerra.

Al igual que el uso del aire no debe ser exclusivo a la Fuerza Aérea, mucho menos a la milicia, el uso de la *Internet* no debe ser delegado exclusivamente a una Fuerza Cibernética independiente. Los adelantos en la *Internet* (tanto en los campos militares como los civiles) en las áreas de servicios, recreo, redes sociales, comunicaciones y así sucesivamente, no se pueden negar ni deben estar sujetos a censura o limitación. Por lo tanto, todos los servicios armados involucrados en la defensa y seguridad deben utilizar el espacio cibernético, pero siempre llevar a cabo sus tareas y alcanzar sus metas más eficientemente. Con ese fin, su personal debe recibir entrenamiento especializado, al igual que los pilotos del ejército y la armada, al igual que personal en otras agencias gubernamentales. Por lo tanto, cada sector poseería recursos especializados, pero la responsabilidad de luchar a los niveles estratégico, operacional y táctico para lograr la supremacía/superioridad cibernética debe permanecer con la fuerza específica creada para este fin. Asignar esta responsabilidad entre todos los servicios armados haría que cada uno atendiese solamente sus propios intereses, y nadie responsable por la red en general. Esa estructura enfrentaría una nueva ventaja contra una fuerza bajo un comando unificado y objetivos precisos (mantener el dominio del espacio cibernético y negárselo al enemigo) capaz de enfocar todo su poder en las vulnerabilidades de un opositor dispersado.

## Conclusión

*“Es más fácil desintegrar un átomo que un prejuicio”*

—Albert Einstein

En este artículo se ha mostrado que el conflicto en el mundo virtual ya es una realidad. Y que debemos prepararnos para ese tipo de eventualidad. Sin embargo, las trayectorias a escoger están oscurecidas por el manto de la ignorancia ya que no hemos presenciado (al menos no apa-

rentemente) un choque en el espacio cibernético con proporciones similares a una guerra convencional que nos permite analizar y crear una doctrina basada en lecciones aprendidas, y aplicarla a nuestra estrategia de defensa. Por ese motivo, en este artículo se extrapolaron los conceptos de un teórico de poderío aéreo quien ha experimentado un problema similar con otra tecnología en otro momento. Al igual que los conceptos de muchos otros teóricos, los de Douhet enfrentaron una resistencia fuerte, pero sus ideas acerca del uso de una herramienta nueva, su función en dictar el curso de la guerra y la importancia de una fuerza independiente con metas específicas parece relevante a nuestra manera de lidiar con el entorno del espacio cibernético.

Al igual que Douhet, estamos experimentando un cambio en la curva de evolución del conflicto. Las estrategias para luchar en el espacio cibernético aún no están bien definidas, pero esta nueva dimensión será parte de todos los conflictos a partir de este momento y cambiará completamente la manera como pensamos, planificamos, nos entrenamos y actuamos en combate. Tratando de anticipar el problema, en el artículo se analizó la guía de alguien quien había atravesado un periodo similar de revolución doctrinal. Quizás la lección más importante que se puede aprender de Douhet es que debemos comenzar a pensar en términos de una fuerza separada para luchar en el espacio cibernético porque emplear solamente porciones de las organizaciones de hoy para esa tarea resultará inadecuado para nuestra defensa nacional, como fue el caso con el poderío aéreo hasta que surgió una fuerza aérea independiente. Al crear una Fuerza Cibernética independiente, verdaderamente estaremos más preparados para los conflictos que se avecinan. Sin embargo, si continuamos tratando al poder cibernético como un medio para asistir a las demás fuerzas a lograr sus metas en lugar de aceptar una Fuerza Cibernética independiente solamente nos estaremos preparando para luchar un conflicto que ya ha sucedido—y la historia nos muestra que aquellos que seleccionen este camino comienzan con una desventaja. ¿Es eso lo que queremos? □

#### Notas

1. Giulio Douhet, *The Command of the Air* (El comando del aire), traductor, Dino Ferrari (1942; nueva edición, Washington, DC: *Office of Air Force History*, 1983).
2. *Ibid*, 3-33.
3. Capitán Paulo Shakarian. "The 2008 Russian Cyber Campaign against Georgia" (La campaña cibernética rusa contra Georgia en el 2008). Disponible en: <[http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview\\_20111231\\_art011POR.pdf](http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20111231_art011POR.pdf)>. Consultado el 1° de mayo de 2013.
4. Consultar John A. Warden III, *The Air Campaign: Planning for Combat* (La campaña aérea: Planificando para el combate) (Washington, DC: *National Defense University Press*, 1988).
5. Fernando Valeika de Barros. "The Cyberwar has Begun" (La guerra cibernética ha comenzado). Consultado el 1° de mayo de 2013, Disponible en: <[http://www.observatoriodaimprensa.com.br/news/view/\\_ed712\\_a\\_ciberguerra\\_ja\\_com\\_ecou](http://www.observatoriodaimprensa.com.br/news/view/_ed712_a_ciberguerra_ja_com_ecou)>.
6. Ministerio de Defensa Brasileño. MD 31-02-P Cyber Defence Policy (MD 31-02 Política de Defensa Cibernética), 2012.
7. "Red October: A Brazilian Perspective on the Attacks (Octubre Rojo: Una perspectiva brasileña sobre los ataques). Consultado el 2 de mayo de 2013, <<http://www.defesanet.com.br/cyberwar/noticia/9450/Outubro-Vermelho—Uma-visao-brasileira-sobre-os-ataques>>.
8. DCA 1-1, Doctrina Básica de la Fuerza Aérea Brasileña, 2012.
9. Leonardo Antonioli. "Statistics, Data and Projections on the Internet in Brazil" (Estadísticas, datos y proyecciones sobre la Internet en Brasil). *To be Guarany*, consultado el 29 de abril de 2013. <[http://tobeguarany.com/internet\\_no\\_brasil.php](http://tobeguarany.com/internet_no_brasil.php)>.
10. "Timeline Bovespa", Portal IG, consultado el 26 de abril de 2013, <[http://extras.ig.com.br/infograficos/ibovespa/internet\\_no\\_brasil.php](http://extras.ig.com.br/infograficos/ibovespa/internet_no_brasil.php)>.
11. Fabio Barros, "Internet Banking is the Preferred Channel of Brazilian Users (La Internet bancaria es el canal preferido de usuarios brasileños), Convergencia Digital, consultado el 27 de abril de 2013, <<http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=30231&sid=5#.UZDNofKBIdV>> Consultado el 27 de abril de 2013.
12. Adenele Garcia Ram, "Virtual Crimes" (Delitos virtuales), *Ámbito Jurídico*, consultado el 29 de abril de 2013, <[http://www.ambito-juridico.com.br/site/?n\\_link=revista\\_artigos\\_leitura&artigo\\_id=11529](http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11529)>. Consultado el 29 de abril de 2013.

13. José Pedro Teixeira Fernandes, "Ciberwar as the New Dimension of XXI Century Conflicts" (La guerra cibernética como la nueva dimensión de los conflictos en el siglo XXI), SciELO Portugal, consultado el 29 de abril de 2013. [http://www.scielo.gpeari.mctes.pt/scielo.php?pid=S1645-91992012000100005&script=sci\\_arttext](http://www.scielo.gpeari.mctes.pt/scielo.php?pid=S1645-91992012000100005&script=sci_arttext); y Toni Sciarretta, "Banks Lose Up to R\$ 3.1 Billion to Fraud and Spend R\$ 4 Billion Safely (Bancos pierden hasta R\$31 billones a causa de fraude y gastan R\$ 4 con seguridad), Fohla de S. Paulo, consultado el 29 de abril de 2013, <<http://www1.folha.uol.com.br/mercado/1247436-bancos-perdem-ate-r-31-bi-com-fraudes-e-gastam-r-4-bi-com-seguranca.shtml>>. Consultado el 29 de abril de 2013.

14. Altieres Rohr, "China 'Hijacked' Internet Traffic for 18 Minutes, Report Shows" (Informe muestra que China "secuestró" el tráfico en la Internet por 18 minutos). Consultado el 29 de abril de 2013. <http://g1.globo.com/tecnologia/noticia/2010/11/china-sequestrou-trafego-da-internet-por-18-minutos-mostra-relatorio.html>.

15. Carlos Alberto Teixeira, "Stuxnet Virus that Attacked Nuclear Plants in Iran Was Created in Partnership by U.S. and Israel" (Virus Stuxnet que atacó plantas nucleares en Irán fue creado por EE.UU. e Israel). Consultado el 3 de mayo de 2013 <<http://oglobo.globo.com/tecnologia/virus-stuxnet-que-atacou-usinas-nucleares-no-ira-foi-criado-em-parceria-por-eua-israel-2836696>>



**CAPITÁN) LUIS EDUARDO POMBO CELLES CORDEIRO, FABRA** (MBA en Administración Pública – Universidad de la Fuerza Aérea – Río de Janeiro, es egresado distinguido de la Clase 13A, Curso para Oficiales de Escuadrón, Base Aérea Maxwell) está a cargo del curso Empleo de la Fuerza Militar en la Escuela para Oficiales de Escuadrón de la Fuerza Aérea Brasileña (EAOAR) – Río de Janeiro. Además está a cargo de preparar el plan de estudio del curso al igual que enseñar la Doctrina Básica de la Fuerza Aérea. Antes de su cargo actual fue Oficial de Administración de Personal en el 5/8 Escuadrón, Base Aérea Santa María. Es un piloto con más de 3.400 horas de vuelo en el T-25, AT-26, AT-27, C-98, U-42, H-50, H-1H y H-60L.



**PROFESOR ANDRÉ DA COSTA GONÇALVES** es egresado en Letras (Portugués-Literatura) de la Universidad de Río Grande (2000) con una maestría en Educación, Cultura y Comunicación en Periferia Urbana por la UERJ (2010). Actualmente es profesor de lengua portuguesa, literatura y producción de textos y metodología de investigación en la Universidad de la Fuerza Aérea. Cuenta con experiencia en el área de las letras en la Lengua Portuguesa y Metodología de Investigación.