

# Para y Desde el Ciberespacio

## Conceptualizando la Inteligencia, Vigilancia y Reconocimiento Cibernético

CORONEL MATTHEW M. HURLEY, USAF

**H**ACE TREINTA años, al inicio de la era digital, la noción de un ámbito sintético y real, donde los seres humanos interactuarían y competirían eran, en gran medida, producto de la ciencia ficción.<sup>1</sup> Nos emocionábamos con películas como *Tron* y *WarGames*; nos estremecíamos al pensar que “*Skynet*” se tornaría consciente de sí mismo, tal como lo presagió la película *Terminator*. Sin embargo, una vez finalizada la película, nos fro-tábamos la pesadilla de nuestros ojos y regresábamos a la luz del mundo “real”.

Hoy vemos el espacio cibernético como algo más que una ilusión de ciencia ficción: Lo consideramos un ámbito operacional, tan significativo como los cuatro entornos tradicionales de tierra, mar, aire y espacio.<sup>2</sup> Sin embargo, el ciberespacio difiere obviamente de esos ámbitos naturales, más familiares. ¿Cómo se aplican la inteligencia, vigilancia y reconocimiento (ISR, por sus siglas en inglés) a este entorno nuevo, dinámico y creado artificialmente? ¿Qué retos enfrenta la iniciativa ISR de la Fuerza Aérea a medida que busca comprender este ámbito operacional innovador? En este artículo se tratan cada una de estas preguntas fundamentales, una por una.<sup>3</sup>

### Definiendo la Inteligencia, Vigilancia y Reconocimiento Cibernético

A diferencia de las operaciones ISR en los ámbitos naturales, aquellas en el ciberespacio aún tienen que definirse oficialmente en la doctrina conjunta o del servicio. A pesar de amplias referencias a “CYBINT” (inteligencia cibernética), su relación con la inteligencia de señales e inteligencia de fuentes abiertas, e inclusive llamamientos a establecer disciplinas más granulares tales como “*SkypeINT*” o “*VoIPINT*,” el razonamiento actual sobre el tema permanece insensato.<sup>4</sup> Tal como el Teniente General Larry D. James, subjefe de Estado Mayor para ISR, declaró en el 2011, “Estamos apenas comenzado a pensar sobre estas cosas desde un punto de vista de Fuerza Aérea”.<sup>5</sup> Por lo tanto, aunque el término *ISR cibernético* ha adquirido cada vez más tracción dentro de los círculos ISR de la Fuerza Aérea, simultáneamente ha provocado indagaciones de otros lugares dentro del Departamento de Defensa (DOD) y el Estado Mayor de la Fuerza Aérea en cuanto a su significado.<sup>6</sup> Este artículo comienza ofreciendo un punto de partida conceptual como un trampolín a la claridad y el perfeccionamiento doctrinal del futuro.

Quizás podamos comprender mejor el ISR cibernético a través de dos actividades que lo componen: ISR *desde* el ciberespacio e ISR *para* el ciberespacio. ISR desde el ciberespacio se remonta a los primeros intentos de extraer datos de las redes de los adversarios durante la década de los años ochenta, y los analistas hoy en día continúan escudriñando el ciberespacio en busca de “cualquier información con valor de inteligencia que podamos recopilar de ese ámbito”, según el Teniente General James.<sup>7</sup> Esto incluye, por ejemplo, noticias de los medios de comunicación extranjeros, salas de *chat* frecuentadas por agentes de amenazas, *blogs* y vídeos de zonas en crisis o imágenes comerciales, tan solo para nombrar unas cuantas aplicaciones. Además incorpora el concepto más familiar de explotación de redes de computadoras (CNE, por sus siglas en inglés). Después de recopilar esta información en el ciberespacio, podemos emplearla para apoyar operaciones en cualquier ámbito.

Por su parte, ISR para el ciberespacio es quizás mejor definido por la *Air Force Policy Directive 10-17* (Directriz de Política de la Fuerza Aérea 10-17), *Cyberspace Operations* (Operaciones Cibernéticas), que le encomienda a la ISR de la Fuerza Aérea que “garantice la capacidad de ofrecer análisis colaborativo, inteligencia fusionada y capacidades ISR PCPAD (planificar y recopilar, recopilación, procesamiento y explotación, análisis y producción, diseminación) que permitan las operaciones ciberespaciales”.<sup>8</sup> Esta definición sugiere la criticalidad de la inteligencia de todas las fuentes durante la planificación y ejecución de las operaciones ciberespaciales. Las operaciones en el ciberespacio exigen más que tan solo ISR desde el ciberespacio, cualquier disciplina de inteligencia puede ofrecer información de valor de inteligencia crucial a las operaciones ciberespaciales.<sup>9</sup> Según fue destacado por el General de División Robert P. Otto, comandante de la Agencia ISR de la Fuerza Aérea, “Cuando decimos ‘ISR para el ciberespacio’, nos referimos a la ISR llevada a cabo para apoyar la superioridad ciberespacial”—indistintamente de la fuente, método o medio.<sup>10</sup>

La CNE, la cual algunos individuos la igualan al ISR cibernético, encaja perfectamente dentro de la primera área de la misión—ISR desde el ciberespacio. En la doctrina de la Fuerza Aérea se define la CNE como “operaciones habilitadoras y capacidades de recopilación de inteligencia llevadas a cabo mediante el uso de redes de computadoras para recopilar datos de los sistemas o redes de información automatizadas del blanco o del adversario”.<sup>11</sup> Más explícitamente, la CNE es “por lo regular llevada a cabo mediante herramientas en la red que penetran los sistemas del adversario. . . . Las herramientas empleadas para la CNE son similares a las que se emplean para el ataque de computadoras, pero configuradas para la recopilación de inteligencia en lugar de interrupción del sistema”.<sup>12</sup> Ambas descripciones implican la intrusión deliberada al *hardware*, *software* del blanco, o redes afines.<sup>13</sup> Sin embargo, no incorpora la recopilación pasiva de información de fuente abierta de posible valor de inteligencia, otra forma importante de la ISR desde el ciberespacio. Esta última podría incluir descargar videos difundidos públicamente de la última contienda del adversario, leer doctrina o publicaciones militares, monitorear salas *chat*, y un sinnúmero de otras actividades que no le hacen nada—ni dejan nada en—a un sistema o red cibernética. No obstante, sí contribuyen a la finalidad esencial de la ISR—hacer llegar la información correcta a los encargados idóneos de tomar decisiones en el momento oportuno.

La concienciación situacional cibernética, otro concepto relacionado con la ISR que aparece de forma destacada en la literatura relevante, tiene que ver con la percepción, discernimiento y entendimiento de quién está presente y qué está sucediendo dentro del ciberespacio, ya sea amigable, hostil o en cualquier lugar en los gradientes.<sup>14</sup> No obstante, la concienciación situacional en general es más que ISR, tornándose en mando y control, elementos no ISR de la concienciación del espacio de batalla e inclusive conocimiento individual.<sup>15</sup> Sin embargo, aunque la ISR es central a la concienciación situacional, ambas no se deben mezclar. Nosotros no consideramos la vigilancia ambiental como una disciplina de recopilación de inteligencia, por ejemplo, aunque es una función de la concienciación del espacio de batalla e incluye procesos analíticos similares. Tampoco consideramos todo el conocimiento humano como “información con valor de inteligencia” aunque el conocimiento presupone la concienciación.

Dado este punto de partida para definir y limitar la ISR cibernética, uno debe explorar el entorno en el cual se lleva a cabo. Tal como lo demuestran los párrafos a continuación, el ciberespacio como ámbito plantea problemas significativos que tenemos que superar si deseamos comprenderlo a cabalidad y operar eficazmente dentro del mismo.

## Los retos del ciberespacio

Martin Libicki, analista de la corporación RAND, ha identificado una tendencia en el razonamiento político y estratégico norteamericano. Específicamente, cuando enfrentamos un nuevo

paradigma (tal como la guerra aérea durante la Primera Guerra Mundial o el uso de aplicaciones militares en el espacio sideral), nuestra primera reacción casi siempre es tratar de aplicar tal innovación basándonos en las reglas del pasado sin tomar en cuenta todo lo demás que también debe cambiar.

Ahora que hemos declarado el ciberespacio un ámbito operacional, Libicki se preocupa que “tomaremos nuestras antiguas normas y las reformaremos”. Sin embargo, él afirma que “eso no se puede hacer en el ciberespacio. Hay que pensar en ello desde el punto de vista de sus propios principios”.<sup>16</sup> Desde luego, hay características compartidas amplias y duraderas en la especialidad ISR y en otras actividades militares a lo largo de todos los ámbitos, pero el punto fundamental de Libicki—que sencillamente no podemos volver a redactar la doctrina existente ni las tácticas, técnicas ni procedimientos incluyendo la *cibernética* dondequiera que encontremos *aire* o *espacio*—amerita que le prestemos atención. La naturaleza singular del ciberespacio trae consigo oportunidades nuevas al igual que retos nuevos, y éstos exigen formas novedosas de pensar en lugar de una solución superficial cortada con el mismo molde.<sup>17</sup>

Los atributos singulares de este entorno operacional más nuevo distinguen la ISR cibernética de actividades complementarias en los “ámbitos naturales”. En el primer lugar, y el más obvio, el ciberespacio fue creado por los seres humanos, quienes continuamente lo modifican; cada *click* en línea o pulsación de una tecla por más de dos mil millones de usuarios se extiende a lo largo del ciberespacio. “Los otros ámbitos son naturales”, destaca el General Michael V. Hayden (USAF, retirado), ex director de la Agencia de Seguridad Nacional y de la Agencia Central de Inteligencia. “Este es la creación del hombre. El hombre puede en realidad cambiar esta geografía, y *cualquier cosa* que suceda ahí, en realidad cambia el espacio *físico* de alguien” (énfasis en el original).<sup>18</sup> El origen del ciberespacio creado por el hombre ha resultado en tres facetas que lo distinguen de los ámbitos naturales relativamente consistentes: complejidad, adaptabilidad y velocidad de cambio. Reconocemos que la naturaleza es compleja, la naturaleza se adapta y la naturaleza cambia—pero no al punto y al ritmo con el que el ciberespacio cambia. Aún podemos reconocer las mismas montañas, mares y estrellas que nuestros antepasados conocieron. Sin embargo, el ciberespacio prácticamente no tiene ninguna similitud a su antecesor de hace tan solo dos décadas—la duración de una carrera militar individual.<sup>19</sup>

Con respecto a la complejidad, el ciberespacio es cautivadoramente complejo y no lineal de modo exasperante. Todo se puede conectar con todo lo demás en el ciberespacio—unos 50 mil millones de dispositivos producidos hasta la fecha—mientras que cambios objetivamente pequeños producen rutinariamente efectos fuera de toda proporción de su escala inicial.<sup>20</sup> Por consiguiente, el razonamiento ciberespacial “debe tomar en cuenta *la relación de las cosas*, o sea, la red, cómo las personas han decidido estructurar y utilizar el ámbito ciberespacial” (énfasis en el original)—una tarea que no es fácil en vista de la cantidad, inestabilidad, imprevisibilidad y complejidad de esas relaciones.<sup>21</sup>

La adaptabilidad intrínseca del ciberespacio contribuye a su complejidad y naturaleza dinámica.<sup>22</sup> Cambia continuamente (a través de las acciones de usuarios diversos) a condiciones tanto dentro como alrededor del ciberespacio, tales como tecnologías nuevas, amenazas o directrices y leyes. Cabe señalar que la *Internet* en sí fue diseñada deliberadamente para facilitar la expansión rápida y la adaptabilidad a la innovación técnica.<sup>23</sup> Los cambios que dan lugar a esas adaptaciones ocurren a un ritmo rápido a medida que tecnologías nuevas, innovadoras y a menudo no anticipadas continúan alterando el paisaje cibernético más rápidamente que los cambios en cualquier otro ámbito técnico.<sup>24</sup> Según un cuarteto de observadores británicos, “El ritmo del cambio puede ser tan abrupto que torna el ciclo de evolución estratégica de acción/reacción convencional en algo obsoleto antes de que comience: es como si un analista de operaciones del gobierno ha sido enviado a observar los efectos en batalla del fusil, solo para descubrir al llegar que se ha inventado la pistola *Maxim*”.<sup>25</sup>

El crecimiento dramático del ciberespacio contribuye a su complejidad y adaptabilidad. A diferencia de los ámbitos físicos, que son relativamente constantes en términos de tamaño, el ciberespacio se está ampliando exponencialmente en cada aspecto significativo.<sup>26</sup> Para mediados del 2011, más de dos trillones de transacciones habían atravesado el ciberespacio, incluyendo 50 trillones de *gigabytes* de datos.<sup>27</sup> Ellos utilizarán 25 millones de aplicaciones para llevar a cabo billones de interacciones diariamente, generando o intercambiando 50 trillones de *gigabytes* de datos *al día*. Las masas en línea tendrán aproximadamente tres mil millones de anfitriones de *Internet* para seleccionar, cada uno de los cuales puede que tengan miles de sitios web individuales.<sup>28</sup> Para aquellas personas que buscan hacer sentido del ciberespacio, su expansión rápida presenta un problema apremiante.

Tradicionalmente, los planificadores y los profesionales militares han equiparado el tamaño y la distancia con escalas de tiempo similares: atravesar grandes distancias o conquistar áreas grandes toma tiempo adicional. Por ejemplo, durante la Segunda Guerra Mundial, tomó más de una semana para que los convoyes navegaran de Estados Unidos a Gran Bretaña, y transcurrieron casi diez meses entre el tiempo en que los Aliados desembarcaron en Normandía y cruzaron el Rin. No obstante, en el ciberespacio, el tiempo como se comprende tradicionalmente en asuntos militares, se ha tornado irrelevante.<sup>29</sup> Teóricamente, podemos lanzar una carga útil cibernética desde la fuente hasta el blanco, desde cualquier punto a cualquier otro en el globo, en menos tiempo de lo que le toma pestañear a una persona común. El ciberespacio nos ha dado operaciones a la “velocidad del *byte*”.<sup>30</sup>

La ubicuidad mundial del ciberespacio, cuando se combina con la velocidad de los efectos cibernéticos, le confiere una dimensión nueva y sobrecogedora a la noción de “alcance global”.<sup>31</sup> Los nódulos cibernéticos físicos habitan en cada uno de los ámbitos naturales—en, alrededor y encima de cada continente y océano. El ciberespacio entrecruza el globo terráqueo, uniendo personas a un grado sin precedentes y brindándoles a nuestros enemigos hasta ahora avenidas de ataque jamás imaginadas.<sup>32</sup> En el pasado, los guerreros siempre han disfrutado de teatros discretos en los cuales operar.<sup>33</sup> Sin embargo, en el ciberespacio, las acciones hostiles puede originar en o ser enviadas literalmente a través de cualquier lugar donde funcione un dispositivo activado por la *Internet*.<sup>34</sup> Además, la naturaleza global del ciberespacio le ha restado sentido a las fronteras tradicionales entre entidades soberanas.<sup>35</sup> En vista de la capacidad de un adversario perspicaz de lanzar instrucciones o ataques a lo largo de múltiples fronteras con casi impunidad, “la geografía es completamente irrelevante”. Po lo tanto no tiene sentido definir la ubicación geográfica de algún servidor donde, digamos del cual surgió un ataque de negación de servicio porque yo podría preparar este servidor que yo uso para lanzar mi ataque en Estados Unidos. Eso no es problema. Yo puedo hacer eso. Puedo utilizar un servidor en China. Inclusive puede utilizar un servidor en Malasia o Brunei”.<sup>36</sup> La difusión mundial y la ambigüedad geográfica del ciberespacio complican la ISR eficaz, ya que no hay espacios físicos estables en los cuales enfocar atención—una partida radical de los conceptos geocéntricos de la ISR.

No tan solo las fronteras de las naciones-estados sino también las naciones-estados en sí se han tornado menos relevantes en el ciberespacio. Ningún gobierno de una nación con facultades cibernéticas puede declarar un monopolio de fuerza en este ámbito, ni tampoco puede afirmar la propiedad total de la infraestructura vital para las operaciones militares.<sup>37</sup> En el primer caso, los costes de entrada bajos al ciberespacio, junto con la disponibilidad difundida de *threatware* (*software* de amenaza) sofisticado, les han presentado a los actores no estatales e inclusive a individuos la oportunidad de llevar a cabo actividades que anteriormente eran de dominio exclusivo del aparato de seguridad del gobierno.<sup>38</sup> Pero ahora, en el ciberespacio, los actores “no necesitan ni estar bien capacitados ni contar con buenos recursos. . . . Sencillamente necesitan contar con la intención y la aptitud de utilizar la tecnología para perpetrar su actividad”.<sup>39</sup> Además, un 90 por ciento de la infraestructura del ciberespacio es propiedad privada a pesar de sus orígenes auspiciados por el gobierno—a pesar del hecho que nuestro gobierno y las fuerzas armadas de-

penden en gran medida en esa infraestructura comercial.<sup>40</sup> Como resultado, en el ciberespacio “las distinciones y divisiones entre los sectores son imprecisas”.<sup>41</sup>

Estas características del ciberespacio contribuyen a “la pregunta más irritante de todas” para los profesionales de ISR: atribución de intromisiones y ataques.<sup>42</sup> Tal como reconoce el Comando Espacial de la Fuerza Aérea, “La capacidad para esconder la verdadera (de origen) fuente de un ataque dificulta identificar al agresor. Además, el diseño de la *Internet* se presta para el anonimato”.<sup>43</sup> Un factor que complica la atribución—el gran número de actores en línea—se refleja por la dificultad de tratar de descubrir una amenaza interna dentro del DOD. Si cada usuario representase un nódulo y cada mensaje electrónico un enlace, uno tendría que analizar 755, 230, 064,000 enlaces entre 237, 387,616 nódulos en un solo año—un cálculo que no incluye búsquedas en la *Internet*, accesos a archivos u otros tipos de actividades cibernéticas teóricamente perceptibles.<sup>44</sup>

Agravando la magnitud del posible conjunto de blancos se encuentran las herramientas cibernéticas que complican la atribución aún más. *Botnets* de hasta millones de máquinas, servidores *proxy* dedicados al anonimato, enrutamiento cebolla (*onion routing*) y técnicas afines todas representan barreras intimidantes a la atribución positiva.<sup>45</sup> Más fundamentalmente, la *Internet* en particular “opera en protocolos intrínsecamente no autenticados”, lo que significa que “la atribución y el no repudio a menudo chocan con el anonimato”.<sup>46</sup> Aunque desalentador, la atribución “no es imposible”, según el Coronel Daniel Simpson, comandante de 659° Grupo ISR; sin embargo, se necesita la labor de un análisis bueno y firme llevado a cabo por profesionales ISR inteligentes”.<sup>47</sup> A pesar de las mejoras con respecto a la atribución, “siempre será más difícil”, según William J. Lynn III, ex secretario adjunto de la defensa. “Los misiles vienen con un remitente, los ataques cibernéticos no”.<sup>48</sup>

Una atribución incompleta o imprecisa también expone a la iniciativa ISR a posibles violaciones de la ley, política y normas constitucionales. La incertidumbre con respecto a la naturaleza de una intrusión (interna o externa; criminal, militar o inteligencia) no tan solo puede demorar la atribución mientras las autoridades del título 10/18 /50 se desenredan, sino que además la atribución imprecisa o prematura puede ocasionar infracciones bajo esas autoridades.<sup>49</sup> Tal como declaró el ex director del FBI, Robert Mueller, “Al principio, uno no sabe si un intruso cibernético puede que sea un actor estatal, un grupo de individuos operando a petición de un actor estatal o un estudiante de secundaria en la acera de enfrente”.<sup>50</sup> Las soluciones propuestas a este reto—tales como compartir datos entre la milicia, la comunidad de inteligencia y la industria; recopilación más enérgica y exhaustiva para dar lugar a la defensa proactiva, o “diseñar nuevamente” la *Internet* para dar lugar a la atribución y ubicación geográfica—han provocado la ira de organizaciones que defienden la privacidad en línea, las libertades civiles y la libertad en la *Internet*.<sup>51</sup> Este artículo no pretende ser una nota o discusión legal.<sup>52</sup> No obstante, cabe destacar que estamos en riesgo de “encontrarnos en aguas desconocidas con respecto a la ley cibernética” en vista de las fronteras inciertas entre la inteligencia y las actividades de cumplimiento de la ley en el ciberespacio.<sup>53</sup>

## El Camino a seguir y recomendaciones

Tomando en cuenta los obstáculos intrínsecos en el ciberespacio, la iniciativa ISR debe efectuar y sostener inversiones apropiadas en ideas, recursos y personal si desea operar eficazmente en el entorno más nuevo. En el campo de las ideas, la primera tarea tiene que ver con definir cómo la ISR encaja en el alcance más amplio de las operaciones cibernéticas. En la actualidad, la Fuerza Aérea y la comunidad conjunta carecen de consenso en cuanto a este punto. Gran parte de la doctrina militar y nacional y las publicaciones de directrices se concentran en actividades cibernéticas ofensivas y defensivas; por su parte, la ISR por lo general es relegada a desem-

pañar un papel de apoyo. Por ejemplo, en el 2010, el Comando Espacial de la Fuerza Aérea—el integrador principal para las funciones básicas de la iniciativa cibernética de la Fuerza Aérea—describió la ISR como “una “capacidad” “necesaria” para las “misiones” de apoyo del ciberespacio, la defensa ciberespacial y la aplicación de fuerza ciberespacial.<sup>54</sup>

Esas nociones no reconocen que a menudo la ISR *es* la misión. En todos los demás momentos en el transcurso de las operaciones cibernéticas, continúa siendo tanto central como esencial. De hecho, las operaciones en el ciberespacio están “saturadas de inteligencia” y sin la ISR, las operaciones cibernéticas “no serían mejor que el conocido bastonazo de ciego”.<sup>55</sup> El Teniente General James afirma que “no separamos la ISR de las operaciones en los ámbitos aéreo y espacial. En el ciberespacio, están aún más entrelazadas”.<sup>56</sup> Por lo tanto, necesitamos conceptos doctrinales, educacionales y organizacionales que recalquen enfáticamente la naturaleza central y operacional de la ISR cibernética—no por su propio bien sino en reconocimiento del hecho de que sin ella estamos sordos y ciegos, funcionalmente, para perjuicio de todas las operaciones.

Sin embargo, para ser eficaz, la ISR cibernética necesita mucho más que énfasis institucional, dinero o personas. La iniciativa debe adaptar su arte del análisis para igualar el entorno operacional. En el caso del ciberespacio, la ISR debe estar globalmente consciente y constantemente vigilante, predecir en lugar de reaccionar, dinámica y ágil y capaz de manejar volúmenes de datos cada vez más exponenciales. Además esta visión requiere cambios en la manera que reclutamos y capacitamos a los profesionales de ISR, cómo los empleamos para proteger las libertades civiles y la privacidad y, de hecho, cómo integramos la ISR cibernética en la iniciativa de inteligencia unificada.

### *La ISR predictiva y la alerta temprana*

Según observadores como Mike McConnell, ex director de inteligencia nacional, la “tecnología vanguardista” actual en la ISR ciberespacial y en la defensa dependen de las “técnicas forenses después de los hechos” para evaluar daños e identificar los delincuentes de ataques individuales.<sup>57</sup> En el pasado, también hemos dependido en la defensa del perímetro y *firewalls* (barreras de control de acceso), pero enemigos capaces a la larga encontrarán la manera de circunvalar o violar cualquier “Línea Maginot Cibernética”, indistintamente de cuán sofisticada sea.<sup>58</sup> En cambio, necesitamos una Línea Cibernética de Alerta Temprana Distante, con atribución y capacidades de defensa, preparada para responder a amenazas antes de que puedan ocasionar daños.<sup>59</sup>

Para facilitar literalmente en un santiamén la alerta más temprana posible de la actividad que está ocurriendo exige un método más predictivo con base en la concienciación global en tiempo real de las actividades cibernéticas y el contexto en las que ocurren.<sup>60</sup> La ISR cibernética predictiva se aprovecha de experiencias anteriores y tendencias emergentes para identificar indicios de delitos digitales latentes, tales como agravios preexistentes contra Estados Unidos, una comunidad activa de “piratas informáticos patrióticos”, charlas banales en línea, tecnologías nuevas o doctrina enemiga.<sup>61</sup> Debemos vigilar éstos y otros posibles datos como parte de “un proceso continuo, aprovechando los indicadores para descubrir actividades nuevas con aún más indicadores a los cuales sacarle provecho”.<sup>62</sup>

### *Ágil y dinámica*

Por supuesto, la alerta “temprana” es relativa. Durante la Guerra Fría, dimos por sentado que los misiles balísticos intercontinentales viajarían unos 30 minutos entre el lanzamiento y el impacto, pero hoy en día un ataque cibernético puede viajar de Pekín a la ciudad de New York en 30 milisegundos.<sup>63</sup> Esa velocidad requiere grados de agilidad y dinamismo que parecen fantásticos, inclusive extravagantes en el contexto de guerra “física”. Según el Dr. Kamal Jabbour, del Laboratorio de Investigaciones de la Fuerza Aérea, la “agilidad cibernética” incluye no tan solo el

análisis rápido sino también “anticipación de comportamientos y efectos futuros y proporcionar eficazmente en tiempo real medidas defensivas.”<sup>64</sup> No obstante, esto exige que la iniciativa ISR al menos empate en todos los aspectos cibernéticos: velocidad, furtividad, flexibilidad, adaptabilidad y otros factores que han hecho que el ciberespacio sean tan desafiante en primer lugar.<sup>65</sup> Las iniciativas científicas y tecnológicas en curso, tales como “*Cyber Vision 2025*” (Visión Cibernética 2025), ofrecen un punto de partida valioso para comprender estos problemas y elaborar soluciones. El Secretario de la Fuerza Aérea, Michael Donley, les ha encomendado a los líderes del servicio que tracen un camino para hacer realidad esa visión.

### *Automatización y visualización*

La enorme cantidad de datos recopilados en el ciberespacio trae a la mente un proverbio chino: “La luz absoluta y la oscuridad absoluta tienen el mismo efecto—no podemos ver nada”.<sup>66</sup> En la actualidad, los sensores cibernéticos recopilan *petabytes* de datos, y la recopilación de *yottabytes* no está muy lejos.<sup>67</sup> Sin embargo, la recopilación ya supera nuestra capacidad de identificar los “*nuggets*”, analizarlos y amoldarlos en inteligencia procesable. Por lo tanto, la ISR cibernética, “requiere la elaboración de algoritmos y capacidades de visualización para hacer que las actividades en el ámbito cibernético sean comprensibles”.<sup>68</sup> Las tecnologías que permiten el análisis automatizado de la ISR, imágenes de operaciones y *software* de predicción caen en un lado de la ecuación y exigen correctamente más atención intelectual y fiscal. Sin embargo, no menos importante—y podría decirse de importancia vital—es el elemento en el otro lado del signo igual de la ecuación: la variable humana.

### *Reclutamiento y entrenamiento*

Muchos de nosotros somos presuntos inmigrantes digitales. Nuestra primera experiencia directa con circuitos integrados tuvo que ver con una calculadora antigua de la década de los años setenta, un reloj digital o quizás los primeros juegos de vídeo. El ciberespacio y la velocidad a la cual evoluciona continúan frustrando y a veces atemorizando a aquellos que se alejaron—por voluntad propia o de lo contrario—del bote análogo hacia el Nuevo Mundo digital. No obstante, nuestros antecesores son una raza diferente. Puede que el nacimiento de los reclutas de hoy haya sido anunciado en un correo electrónico; puede que no recuerden un solo momento en que una computadora no estuviese a la vista. Estos no son los hombres del aire de su padre. Aún siguen siendo los mejores en el mundo, pero puede que el lema “Volar, Luchar y Ganar” tenga una connotación diferente para alguien cuya idea de la guerra se deriva principalmente de nueve años jugando “*Call of Duty*”. Sin embargo, posiblemente esos nativos digitales representan nuestros mayores recursos en el ámbito del ciberespacio. El General Keith B. Alexander, director de la Agencia de Seguridad Nacional y Comandante del Comando Ciberespacial de Estados Unidos, aparentemente reconoce esto, habiendo pronunciado recientemente una propuesta de reclutamiento en una convención de personas que se declaran a sí mismos piratas cibernéticos.<sup>69</sup> El requisito de talento humano está ahí—y es abundante. Una vez a bordo, solo necesita entrenamiento en las normas de primer nivel de las operaciones cibernéticas. Pero eso requiere “pericia técnica y analítica profunda y poderosa”—una pericia que debe progresar continuamente para estar a la par de la evolución explosiva del ámbito.<sup>70</sup> Aunque el Teniente General James afirma que el entrenamiento en la ISR cibernética está mejorando, la tarea aún no está completa.<sup>71</sup> En vista de la evolución continua del ciberespacio, un mayor perfeccionamiento del plan de estudio del código de especialidad de la Fuerza Aérea; cursos superiores y entrenamiento en el trabajo hecho a la medida y que se pueda adaptar debe continuar para calificar entre las prioridades más importantes para la ISR cibernética.

### *“Normalización” de la ISR cibernética*

Personal y entrenamiento, al igual que materiales y tecnologías, recientemente han captado la atención de múltiples iniciativas de alto nivel dentro del DOD y la Fuerza Aérea, incluyendo el estudio del científico en jefe de la Fuerza Aérea titulado “*Cyber Vision 2025*”; la Cumbre Cibernética 2012 de la Fuerza Aérea y la Revisión de la Cartera Estratégica Cibernética del DOD. Resultados concretos—y, por consiguiente, la capacidad futura de la ISR cibernética—dependerá de estos resultados y otras deliberaciones, el entorno fiscal y la evolución continua de amenazas y oportunidades cibernéticas. Sin embargo, conceptualmente, la labor puede y debe comenzar hoy en cuanto a la “normalización” de la ISR cibernética. Tal como el Teniente General James y otros líderes de la ISR de la Fuerza Aérea han mantenido contundentemente, la ISR eficaz debe ser ininterrumpida y neutral en cuanto al ámbito. La ISR pretende ofrecer inteligencia oportuna, relevante y factible a los encargados de tomar decisiones adecuadas. El lugar y los medios para recopilar información de inteligencia son relativamente de poco significado para ese objetivo final. En este contexto, la normalización incluye el desmantelamiento de sistemas compartimentados que hemos construido en torno a *All Things Cyber* y reconocer que, en el análisis final, la información resultante en sí es importante para la misión—no la manera o el ámbito en el cual la adquirimos. No obstante, en virtud de la singularidad del ámbito cibernético, el carácter relativamente novedoso de nuestras operaciones dentro del mismo y las funcionalidades pragmáticas, aún tenemos múltiples obstáculos mentales e institucionales que aclarar antes que la ISR para y desde el ciberespacio sea comprendida, reconocida y abastecida de inmediato como ISR para y desde el aire o el espacio. En un final, esta es una pregunta de educación y liderazgo, pero antes que podamos enseñar y mandar, primero debemos comprender que el ciberespacio se ha convertido en un dominio que presenta demandas y oportunidades ISR básicamente de la misma manera que los demás ámbitos. La inteligencia hacia y desde el espacio también era nueva y compartimentada conceptualmente en un pasado no muy lejano, pero su contribución a la eficacia operacional ha crecido dramáticamente con su novedad que está en disminución.

### *Protección de los derechos civiles y la privacidad*

Sin embargo, cualquiera y todas las inversiones ISR deben acatar la obligación del gobierno de proteger los derechos civiles y constitucionales.<sup>72</sup> El Coronel Simpson reconoce que “la infancia actual del derecho y la política cibernética crea dificultades para la ISR en definir y administrar autoridades y fronteras”.<sup>73</sup> El equilibrio entre la concienciación, la seguridad y las libertades civiles está en evolución y exigen atención constante y conlleva implicaciones considerables para la confianza del pueblo.<sup>74</sup> Esto es más que una inquietud secundaria para la iniciativa ISR; en calidad de profesionales militares sirviendo a nuestros ciudadanos y Constitución estos temas ameritan vigilancia continua y acatamiento estricto. A pesar de las ambigüedades legales que opacan el ciberespacio e indistintamente de cualesquiera decisiones de los tribunales que aparezcan en el futuro, la comunidad de inteligencia en su totalidad debe permanecer firmemente comprometida con la Constitución y el derecho de cada ciudadano a la privacidad.

## Conclusión

Durante el siglo pasado, la Fuerza Aérea y sus antecesores han demostrado su conocimiento de los nuevos ámbitos operacionales—primero en el aire y luego en el espacio. En ambos casos, la ISR resultó ser crítica para abrir y asegurar entornos nuevos. El ciberespacio, con todos sus atributos singulares, compara esa característica fundamental: la ausencia de ISR oportuna, relevante y procesable disminuye el éxito de todas las demás actividades militares a una posibilidad.

A medida que las probabilidades se amontonan contra el defensor en este ámbito nuevo, depender de la probabilidad no es una opción.<sup>75</sup> Las dificultades que la ISR cibernética enfrenta a veces parecen imposibles de resolver, pero solamente aparentan serlo. No hay duda que la velocidad sin precedentes del poderío aéreo ocasionó bastante desorientación mental durante su maduración, al igual que sucedió con la inmensidad del espacio en las siguientes décadas. No cabe duda que, a medida que entramos a un entorno operacional nuevo, nos encontraremos con muchas de las mismas dificultades intelectuales iniciales. No obstante, debemos permanecer confiados en nuestra capacidad para superarlas mediante un entendimiento cada vez más persistente y generalizado del ciberespacio proporcionado por—y contribuyendo a—la ISR cibernética. Para continuar esa tendencia positiva, debemos invertir; para invertir, debemos comprometernos; pero para comprometernos, primero debemos comprender a cabalidad la naturaleza y alcance de los retos y oportunidades que enfrentamos como Fuerza Aérea y como nación. La ISR es la clave para ese entendimiento—en el ciberespacio al igual que en cualquier ámbito de la iniciativa humana. □

#### Notas

1. En *Neuromancer*, William Gibson acuñó proféticamente el término *ciberespacio* para proponer una hipótesis de una ilusión de ciencia ficción, “una alucinación consensual experimentada a diario por billones. . . . Datos extraídos de los bancos de toda computadora en el sistema humano. Complejidad inconcebible”. William Gibson, *Neuromancer* (New York: Ace Books, 1984), 69.

2. La doctrina conjunta define el ciberespacio como “un ámbito global dentro del entorno de informática que consta de la red interdependiente de infraestructuras de tecnología de informática, incluyendo la *Internet*, redes de telecomunicaciones, sistemas de computadoras y procesadores y controladores integrados”. *Joint Publication (JP) 1-02* (Publicación Conjunta 1-02), *Department of Defense Dictionary of Military and Associated Terms* (Diccionario Militar y Términos Afines del Departamento de Defensa), 8 de noviembre de 2010 (según enmendado hasta el 15 de agosto de 2012), 77, [http://www.dtic.mil/doctrine/new\\_pubs/jp1\\_02.pdf](http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf). Sin embargo, el autor se ve obligado a aceptar que “‘Cibernético’ en sí es un concepto tan nebuloso que definir los conceptos básicos de lo que es y cómo afecta el ámbito militar ha tomado años de práctica de planificar horas hombre”. Daniel Wasserbly, “*Charting the Course through Virtual Enemy Territory*” (Trazando el rumbo a través de territorio enemigo virtual), *Jane’s International Defence Review* 44, no. 5 (mayo de 2011): 60. O, tal como el General (USAF, retirado) Michael V. Hayden destacó, “Rara vez algo ha sido tan importante o se ha hablado de ello con menos claridad y menos entendimiento que este fenómeno”. Michael V. Hayden, “*The Future of Things ‘Cyber’*”, (El future de cosas “Cibernéticas”), *Strategic Studies Quarterly* 5, no. 1 (Primavera 2011): 3, <http://www.au.af.mil/au/ssq/2011/spring/hayden.pdf>.

3. En este artículo no se tratan las amenazas—la literatura con respecto a este tema es tan amplia y variada como las amenazas en sí. Sin embargo, en todas las operaciones militares, una respuesta eficaz a la amenaza comienza con ISR sensata, bien planificada y bien ejecutada conceptualmente.

4. Para CYBINT consultar al Dr. Kamal T. Jabbour, *50 Cyber Questions Every Airman Can Answer* (Cincuenta preguntas cibernéticas que cualquier hombre del aire puede responder), (Wright-Patterson AFB (Base Aérea Wright-Patterson), OH: *Air Force Research Laboratory* (Laboratorio de Investigaciones de la Fuerza Aérea), 7 de mayo de 2008), 20, [http://www.au.af.mil/au/awc/awcgate/afri/50\\_cyber\\_questions.pdf](http://www.au.af.mil/au/awc/awcgate/afri/50_cyber_questions.pdf); para la relación de CYBINT con las señales de inteligencia, consultar, por ejemplo, *Air Force Doctrine Document (AFDD) 2-0* (Documento de Doctrina de la Fuerza Aérea 2-0), *Global Integrated Intelligence, Surveillance, & Reconnaissance Operations* (Operaciones globales de inteligencia integrada, vigilancia y reconocimiento), 6 de enero de 2012, 40, <http://www.e-publishing.af.mil/shared/media/epubs/afdd2-0.pdf>; y para inteligencia de fuente abierta según la describe Frederick J. Wattering, consultar “*The Internet and the Spy Business*” (La *Internet* y el negocio de espías), *International Journal of Intelligence and Counterintelligence* 14, no. 3 (otoño 2001): 344. Consultar también el borrador “*Cyber Vision 2025: United States Air Force Cyberspace Science and Technology Vision 2012–2025*” (Visión cibernética 2025: Visión de ciencia ciberespacial y de tecnología de la Fuerza Aérea de EE.UU. para 2012-2025), AF/ST TR 12-01, 1º de septiembre de 2012, 42. Las siglas en inglés “VoIP” significan *Voice over Internet Protocol applications* (Voz sobre protocolo de *Internet*).

5. Sen Iannotta, “Voice for Balance” (Voz para el equilibrio) *DefenseNews*, 1º de noviembre de 2011, <http://www.defense.com/news/article/20111101/C4ISR01/111010318/Voice-balance>.

6. Ya que el autor ha experimentado personalmente múltiples de veces durante los últimos meses, al momento de escribir este artículo.

7. Teniente. General Larry D. James, entrevista por el autor, 30 de julio de 2012.

8. *Air Force Policy Directive 10-17* (Directriz de política de la Fuerza Aérea 10-17), *Cyberspace Operations* (Operaciones ciberespaciales), 31 de julio de 2012, 3, <http://www.e-publishing.af.mil/shared/media/epubs/AFP10-17.pdf>.

9. *Intelligence and National Security Alliance* (Inteligencia y la Alianza para la Seguridad Nacional), *Cyber Intelligence: Setting the Landscape for an Emerging Discipline* (Inteligencia cibernética: Preparando el terreno para una disciplina emergente), (Arlington, VA: Intelligence and National Security Alliance, septiembre de 2011), 14, [https://www.vita.virginia.gov/uploadedFiles/VITA\\_Main\\_Public/Security/Meetings/ISOAG/2012/Sept\\_ISOAG\\_CyberIntel.pdf](https://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Security/Meetings/ISOAG/2012/Sept_ISOAG_CyberIntel.pdf). Consultar también el AFDD 3-12, *Cyberspace Operations* (Operaciones ciberespaciales), 15 de julio de 2010, 24, <http://www.e-publishing.af.mil/shared/media/epubs/afdd3-12.pdf>, en el que se destaca que “emplear efectos cibernéticos de espectro total requiere un método de análisis de inteligencia múltiple” e “ISR de toda fuente enfocada cibernéticamente”.

10. General de División Robert P. Otto, respuestas escritas a entrevista, 14 de agosto de 2012.

11. AFDD 3-12, *Cyberspace Operations*, 49.

12. Clay Wilson, *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues* (Operaciones de información, guerra electrónica y ciberguerra: Capacidades y problemas relacionados con la política), *CRS Report for Congress* (Informe CRS para el Congreso) (Washington, DC: Congressional Research Service, 20 de marzo de 2007), 5, <http://www.au.af.mil/au/awc/awcgate/crs/r131787.pdf>.

13. Bryan Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation* (Capacidad de la República Popular China de llevar a cabo una guerra cibernética y aprovecharse de las redes de computadoras) (McLean, VA: Northrop Grumman Corporation, 9 de octubre de 2009), 8–9, [http://www.uscc.gov/research/papers/2009/NorthropGrumman\\_PRC\\_Cyber\\_Paper\\_FINAL\\_Approved%20Report\\_16Oct2009.pdf](http://www.uscc.gov/research/papers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf).

14. Dr. Kamal Jabbour, “*The Science and Technology of Cyber Operations*” (La ciencia y tecnología de las operaciones cibernéticas) *High Frontier* 5, no. 3 (mayo de 2009): 11, <http://www.afspc.af.mil/shared/media/document/AFD-090519-102.pdf>; “Cyber Vision 2025,” 20; Air Force Space Command (Comando Espacial de la Fuerza Aérea), *Functional Concept for Cyberspace Operations* (Concepto funcional para las operaciones ciberespaciales) (Peterson AFB, CO: Air Force Space Command, 14 de junio de 2010), 7; y Teniente General Michael J. Basla, “*Cyberspace from a Service Component Perspective*” (El ciberespacio desde el punto de vista de un componente del servicio) (discurso, *Cyberspace Symposium* (Simposio Ciberespacial), *US Strategic Command* (Comando Estratégico de EE.UU.), 15 de noviembre de 2011), <http://www.afspc.af.mil/library/speeches/speech.asp?id=686>. En su discurso, el Teniente General Basla, vicecomandante del Comando Espacial de la Fuerza Aérea, describió la concienciación situacional cibernética como “un panorama del espacio de batalla operacionalmente relevante que incluye el estatus de las redes conjuntas, de las redes de la Fuerza Aérea y la disposición de nuestras fuerzas, aliadas o no”.

15. En el *Manual for the Operation of the Joint Capabilities Integration and Development System* (Manual para la operación de la integración de capacidades conjuntas y desarrollo del sistema) (Washington, DC: Joint Staff J8 / Joint Capabilities Division, Pentagon, 19 de enero de 2012), [https://www.intelink.gov/inteldocs/action.php?kt\\_path\\_info=ktcore.actions.document.view&fDocumentId=1517681](https://www.intelink.gov/inteldocs/action.php?kt_path_info=ktcore.actions.document.view&fDocumentId=1517681), se define la zona de capacidad conjunta “concienciación del espacio de batalla” como “la capacidad de comprender disposiciones e intenciones al igual que las características y condiciones del entorno operacional que están relacionadas con la toma de decisiones nacional y militar sacándole provecho a todos los recursos de información, inclusive inteligencia, vigilancia, reconocimiento, meteorológico y oceanográfico” (B-B-2). El mejor ejemplo de los aspectos cognoscitivos individuales de la concienciación situacional es quizás el origen del piloto de combate de una aeronave de un solo asiento del ciclo (OODA) de observar, orientar, decidir y actuar de John Boyd. Ver, por ejemplo, Coronel Phillip S. Meilinger, editor, *The Paths of Heaven: The Evolution of Airpower Theory* (Los caminos del cielo: La evolución de la teoría del poderío aéreo) (Maxwell AFB, AL: Air University Press, 1997), xxiii; y Mayor David S. Fadok, “*John Boyd and John Warden: Air Power's Quest for Strategic Paralysis*” (John Boyd y John Warden: La búsqueda del poderío aéreo de una parálisis estratégica) (Maxwell AFB, AL: School of Advanced Airpower Studies, 1995), 13.

16. Martin Libicki, “*Cyberpower and Strategy*” (Poder cibernético y estrategia) comentarios durante la 8ª Revisión Estratégica Global del Instituto Internacional para Estudios Estratégicos, “*Global Security Governance and the Emerging Distribution of Power*” (Gobernando la seguridad global y la distribución de poder emergente”) *Sixth Plenary Session* (Sexta Sesión Plenaria), 12 de septiembre de 2010, [3], <http://www.iiss.org/EasySiteWeb/getresource.axd?AssetID=46892&type=full&servicetype=Attachment>.

17. Teniente Coronel (USAF) Steven E. Cahanin, “*Principles of War for Cyberspace*” (Principios de guerra para el ciberespacio) informe de investigación (Maxwell AFB, AL: Air War College, Air University, 15 de enero de 2011), 1, <http://www.airpower.au.af.mil/digital/pdf/articles/Jan-Feb-2012/Research-Cahanin.pdf>.

18. Hayden, “*Future of Things 'Cyber,'*” 4.

19. Por ejemplo, comparar el ciberespacio de hoy con su encarnación anterior de inicios de la década de los años noventa, uno vería semejanzas en patrones tales como correo electrónico, tableros de mensajes y conectividad en línea con las bases de datos informativas. Cambios radicales tales como la ubicuidad de los medios de comunicación sociales, videos en vivo, voz en línea y comunicaciones por video, conectividad móvil y, sí, la complejidad y convencimiento de la amenaza cibernética de la actualidad han, en retrospectiva, han dejado muy atrás inclusive los pronósticos más emprendedores de hace 20 años.

20. Cahanin, “*Principles of War for Cyberspace,*” 2; Brookings Institution, *Deterrence in Cyberspace: Debating the Right Strategy with Ralph Langner and Dmitri Alperovitch* (Disuasión en el ciberespacio: Discutiendo la estrategia correcta con Ralph Langner y Dmitri Alperovitch) (Washington, DC: Brookings Institution, 20 de septiembre de 2011), 2, [http://www.brookings.edu/~media/events/2011/9/20%20cyberspace%20deterrence/20110920\\_cyber\\_defense.pdf](http://www.brookings.edu/~media/events/2011/9/20%20cyberspace%20deterrence/20110920_cyber_defense.pdf); y Paul W. Phister Jr.,

"Cyberspace: The Ultimate Complex Adaptive System" (Ciberespacio: El último sistema complejo adaptivo), *International C2 Journal* 4, no. 2 (2010–11): 13–14.

21. Cahanin, "Principles of War for Cyberspace," 2.

22. "Comentarios del Honorable Michael B. Donley, Secretario de la Fuerza Aérea, Conferencia *Cyberfutures* de la Asociación de la Fuerza Aérea, Gaylord National Resort, viernes, 23 de marzo de 2012," 3, <http://www.af.mil/shared/media/document/AFD-120326-056.pdf>.

23. *Department of Defense* (Departamento de Defensa), *Department of Defense Strategy for Operating in Cyberspace* (Estrategia del Departamento de Defensa para las Operaciones en el Ciberespacio) (Washington, DC: Department of Defense, julio de 2011), 2, <http://www.defense.gov/news/d20110714cyber.pdf>.

24. Cahanin, "Principles of War for Cyberspace," 3–4.

25. Paul Cornish et al., *On Cyber Warfare* (Sobre la guerra cibernética) Chatham House Report (London: Chatham House [Royal Institute of International Affairs], noviembre de 2010), 29, [http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110\\_cyberwarfare.pdf](http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf).

26. Aunque puede que el espacio sea infinito, o limitado pero en expansión, o limitado y contrayéndose (las teorías varían), la dimensión humana del espacio—es decir, donde los seres humanos han establecido una presencia permanente más o menos, inclusive remotamente—es casi exclusivamente confinada a nuestro sistema solar. Salvo los aterrizajes en la luna de Apolo y las sondas interplanetarias, lunares o solares, esta dimensión humana radica entre 30 y 22.000 millas sobre el nivel de la superficie de la Tierra.

27. Brookings Institution, *Deterrence in Cyberspace*, 2. Para mediados del 2012, cada minuto de cada día presenció lo siguiente cargándose a o atravesando a través del ciberespacio: 48 horas de videos *YouTube*; 204, 166,667 mensajes de correos electrónicos; 2,000,000 de consultas de búsqueda en *Google*; 684,478 publicaciones en *Facebook*; 571 sitios de *Internet* nuevos; 27,778 publicaciones en el *blog Tumblr* y más de 100,000 *tweets* en *Twitter*. Oliur Rahman, "How Much Data Is Created on the Internet Every Minute?" (¿Cuántos datos se crean en la *Internet* cada minuto?) *Ultralinx*, 24 de junio de 2012, <http://theultralinx.com/2012/06/data-created-internet-minute.html>.

28. "Cyber Vision 2025," 9.

29. Richard M. Crowell, *War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare* (La guerra en la era de la informática: Un manual para las operaciones ciberespaciales en la guerra del siglo XXI), (Newport, RI: Naval War College, 2010), 21, <http://www.carlisle.army.mil/DIME/documents/War%20in%20the%20Information%20Age%20-%20A%20Primer%20for%20Cyberspace%20Operations%20in%2021st%20Century%20Warfare%20-%20R%20M%20Crowell.pdf>.

30. Contrario a la creencia popular, las actividades en el ciberespacio no ocurren a la velocidad de la luz; más bien, el ciberespacio opera a la velocidad de los electrones. La luz viaja a aproximadamente 186,000 millas por segundo, mientras que los electrones—a causa de que tienen masa—viajan "solamente" a dos tercios de esa velocidad—unas 125,000 millas por segundo. Jabbar, *50 Cyber Questions*, 11.

31. Según sugiere Mike McConnell, "Cyber Insecurities: The 21st Century Threatscape" (Inseguridades cibernéticas: Panorama de las amenazas en el siglo XXI), en *America's Cyber Future: Security and Prosperity in the Information Age* (El futuro cibernético de Estados Unidos: Seguridad y prosperidad en la era de la informática), vol. 2, editores Kristin M. Lord y Travis Sharp (Washington, DC: Center for a New American Security, junio de 2011), 25–39, [http://www.cnas.org/files/documents/publications/CNAS\\_Cyber\\_Volume%20II\\_2.pdf](http://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20II_2.pdf).

32. Robin Geiß, "The Conduct of Hostilities in and via Cyberspace" (La conducción de las hostilidades en y a través del ciberespacio), *Proceedings of the Annual Meeting* (Actas de la reunión anual) (American Society of International Law) 104 (24–27 de marzo de 2010): 371; y Crowell, *War in the Information Age* (La guerra en la era de la informática), 21.

33. Inclusive las guerras mundiales no lo fueron, estrictamente hablando, ya que los comandantes Aliados no tuvieron que preocuparse acerca de ese posible empuje del Eje de Suiza a Suazilandia.

34. Geiß, "Conduct of Hostilities," 371; y Cahanin, "Principles of War for Cyberspace," 5.

35. Susan Freiwald, "Electronic Surveillance at the Virtual Border" (Vigilancia electrónica en la frontera virtual), *Mississippi Law Journal* 78, no. 2 (Invierno 2008): 329, <http://www.olemiss.edu/depts/ncjrl/pdf/ljournal09Freiwald.pdf>; Geiß, "Conduct of Hostilities," 371; y Cahanin, "Principles of War for Cyberspace," 5.

36. Brookings Institution, *Deterrence in Cyberspace*, 15; y Crowell, *War in the Information Age*, 21.

37. Por ejemplo "bases" cibernéticas, "espacio aéreo cibernético o "estructura de la fuerza" cibernética.

38. McConnell, "Cyber Insecurities" (Inseguridades cibernéticas) 61; Gregory C. Radabaugh, "The Evolving Cyberspace Threat" (La amenaza ciberespacial en evolución) (documento de trabajo, Agencia de Inteligencia, Vigilancia y Reconocimiento de la Fuerza Aérea, agosto de 2012), 8; Cornish et al., *On Cyber Warfare*, 30; y Crowell, *War in the Information Age*, 21.

39. Intelligence and National Security Alliance (Inteligencia y la Alianza para la Seguridad Nacional), *Cyber Intelligence*, 7. Para evaluaciones similares, consultar Kevin Coleman y John Reed, "Cyber Intelligence" (Inteligencia cibernética), *DefenseTech.org*, 3 de enero de 2011, <http://defensetech.org/2011/01/03/cyber-intelligence/>.

40. Cahanin, "Principles of War for Cyberspace," 5.

41. Cámara de Representantes, Subcomité de los Servicios Armados de la Cámara de Representantes, Testimonio sobre las operaciones ciberespaciales, General Keith Alexander, Washington, D.C., 23 de septiembre de 2010, [1], 111th Cong., 2nd sess., [http://www.defense.gov/home/features/2011/0411\\_cyberstrategy/docs/House%20Armed%20Services%20Subcommittee%20Cyberspace%20Operations%20Testimony%2020100923.pdf](http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/House%20Armed%20Services%20Subcommittee%20Cyberspace%20Operations%20Testimony%2020100923.pdf). En ese entonces, el Representante

tante Ike Skelton (D-Missouri), presidente del Comité de Servicios Armados de la Cámara de Representantes, hizo esta declaración en sus observaciones preliminares.

42. Kenneth Geers, *Sun Tzu and Cyber War* (Sun Tzu y la guerra cibernética) (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 9 de febrero de 2011), [4], [http://www.ccdcoe.org/articles/2011/Geers\\_SunTzuandCyberWar.pdf](http://www.ccdcoe.org/articles/2011/Geers_SunTzuandCyberWar.pdf). Para un análisis más profundo del reto de atribución, consultar a Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Disuasión cibernética y guerra cibernética) (Santa Monica, CA: RAND Corporation, 2009), [http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND\\_MG877.pdf](http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf).

43. Comando Espacial de la Fuerza Aérea, *Functional Concept for Cyberspace Operations* (Concepto funcional para las operaciones ciberespaciales), 10.

44. Rand Waltzman, “Anomaly Detection at Multiple Scales” (Detección de anomalía en escalas múltiples) (presentación, DARPA Cyber Colloquium, Arlington, VA, 7 de noviembre de 2011), diapositivas 3–4.

45. “Onion routing” se refiere a una técnica, originalmente diseñada por la Armada, para esconder el origen y contenido de paquetes a medida que atraviesan una red. Los paquetes son enviados a través de una red de servidores *proxy* seleccionados al azar, con niveles consecutivos de codificación y luego descodificación, antes de entregarlos a su destino final como texto sencillo. W. Earl Boebert, “A Survey of Challenges in Attribution” (Encuesta de los retos en la atribución) en *National Research Council of the National Academies, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Actas de un taller sobre disuasión de ataques cibernéticos: Informando estrategias y creando opciones para la política estadounidense) (Washington, DC: National Academies Press, 2010), 43–46.

46. Jabbour, *50 Cyber Questions*, 9.

47. Entrevista del autor el 8 de agosto de 2012, al Coronel Daniel Simpson, comandante, 659° Grupo ISR. El 659° es la principal unidad ISR de la Fuerza Aérea, y se enfoca en el “análisis de aprovechamiento de la red digital e inteligencia digital en la red”. Consultar Captain Karoline Scott, “New ISR Group Supports Cyber Operations” (Nuevo Grupo ISR apoya operaciones cibernéticas), *Air Force News Service*, 10 de septiembre de 2010, <http://www.af.mil/news/story.asp?id=123221324>; and AFDD 3-12, *Cyberspace Operations*, 24.

48. Kristin Quinn, Vago Muradian y Marcus Weisgerber, “The Pentagon’s New Cyber Strategy” (La nueva estrategia cibernética del Pentágono) *DefenseNews*, 18 de agosto de 2011, <http://www.defensenews.com/apps/pbcs.dll/article?AID=201108180316>.

49. Libicki, *Cyberdeterrence and Cyberwar*, 96.

50. Wasserbly, “Charting the Course,” 60.

51. Decian McCullagh, “House Passes CISPA Internet Surveillance Bill” (Cámara aprueba proyecto de ley para vigilancia de Internet CISPA), ZDNet, 27 de abril de 2012, <http://www.zdnet.com/news/house-passes-cispa-internet-surveillance-bill/6360341>. Un representante que se opuso, Jared Polis (D-Colorado), alegó que la *Computer Intelligence Sharing and Protection Act* (CISPA) (Ley de Intercambio y Protección de Información de Inteligencia Cibernética) “dispensaría toda ley de privacidad puesta en vigor en nombre de la seguridad cibernética. . . Permitiéndole a la milicia y a la NSA a espiar estadounidenses en suelo estadounidense va en contra de todo principio sobre el cual se fundó este país”. Consultar también Sanjay Goel, “Cyberwarfare: Connecting the Dots in Cyber Intelligence” (Guerra cibernética: Conectando los puntos en la inteligencia cibernética) *Communications of the ACM* 54, no. 8 (agosto de 2011): 137; y Mike McConnell, “Mike McConnell on How to Win the Cyber-War We’re Losing” (Mike McConnell explica cómo ganar la guerra cibernética que estamos perdiendo), *Washington Post*, 28 de febrero de 2010, B01, <http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html>. Además de las organizaciones orientadas hacia los derechos en general, tal como el Sindicato Americano para las Libertades Civiles, los grupos defensores incluyen la *Electronic Frontier Foundation* (Fundación de Fronteras Electrónicas) (que ofrece un seminario en “Surveillance Self-Defense” (Autodefensa contra la vigilancia), en <https://ssd/eff/org>), [savetheinternet.com](http://savetheinternet.com) (que cuenta con la “Declaration of Internet Freedom” [Declaración de libertad en la Internet]), the *Electronic Privacy Information Center* (Centro Electrónico para Información de Privacidad), el *Center for Democracy and Technology* (Centro para la Democracia y la Tecnología), el *Technology Liberation Front* (Frente de Liberación Tecnológica), y la *OpenNet Initiative* (Iniciativa de Red Abierta) (“Nuestra meta es investigar, sacar a la luz y analizar prácticas de vigilancia y filtración en la Internet”), <http://opennet.net/about-oni>. Según la opinión y experiencia del autor, ninguna categoría de actividad por parte de la comunidad de inteligencia ha llamado tanto la atención y el rechazo del público en Estados Unidos desde las informes del Comité de la Iglesia en 1976.

52. Para un entendimiento de los debates legales recientes con respecto a la privacidad en el ciberespacio, leyes de búsqueda e incautaciones y otros estándares constitucionales, consultar a Susan Brenner, “Fourth Amendment Future: Remote Computer Searches and the Use of Virtual Force” (El futuro de la Cuarta Enmienda: Búsquedas en computadoras a distancia y el uso de la fuerza virtual), *Mississippi Law Journal* 81, no. 5 (2012): 1229–62; Timothy Casey, “Electronic Surveillance and the Right to Be Secure” (Vigilancia electrónica y el derecho a estar seguro) *University of California–Davis Law Review* 41, no. 3 (febrero de 2008): 977–1033; Elizabeth Gillingham Daly, “Beyond ‘Persons, Houses, Papers, and Effects’: Rewriting the Fourth Amendment for National Security Surveillance” (Más allá de las ‘personas, casas, papeles y efectos’: Reescribiendo la Cuarta Enmienda para la vigilancia de seguridad nacional), *Lewis & Clark Law Review* 10, no. 3 (Fall 2006): 641–71; Dan Fenske, “All Enemies, Foreign and Domestic: Erasing the Distinction between Foreign and Domestic Intelligence Gathering under the Fourth Amendment” (Todos los enemigos, externos e internos: Eliminando la distinción entre la recopilación de inteligencia externa e interna bajo la Cuarta Enmienda), *Northwestern University Law Review* 102, no. 1 (2005): 343–81; Freiwald, “Electronic Surveillance” (Vigilancia electrónica), 329–62; John N. Greer, “Square Legal Pegs in Round Cyber Holes: The NSA,

*Lawfulness, and Protection of Privacy Rights and Civil Liberties in Cyberspace*" (El enfoque no se ajusta a la situación: La NSA, la legalidad y la protección de los derechos a la privacidad y las libertades civiles en el ciberespacio), *Journal of National Security Law and Policy* 4, no. 1 (2010): 139–54; Orin S. Kerr, "Applying the Fourth Amendment to the Internet: A General Approach" (Aplicando la Cuarta Enmienda a la Internet: Un enfoque general), *Stanford Law Review* 62, no. 4 (abril de 2010): 1005–49; Mike McNeerney, "Warshak: A Test Case for the Intersection of Law Enforcement and Cyber Security" (Warshak: Un ejemplo práctico para la intersección del cumplimiento de la ley y la seguridad cibernética), *University of Illinois Journal of Law, Technology and Policy* 2010, no. 2 (Fall 2010): 345–57; Amanda Yellon, "The Fourth Amendment's New Frontier: Judicial Reasoning Applying the Fourth Amendment to Electronic Communications" (La nueva frontera de la Cuarta Enmienda: Razonamiento jurídico para aplicar la Cuarta Enmienda a las comunicaciones electrónicas), *Journal of Business & Technology Law* 4, no. 2 (2009): 411–37; y Mark D. Young, "Electronic Surveillance in an Era of Modern Technology and Evolving Threats to National Security" (Vigilancia electrónica en una era de tecnología moderna y amenazas en desarrollo a la seguridad nacional), *Stanford Law & Policy Review* 22, no. 1 (2011): 11–39. Preguntas representativas planteadas por estas notas y estudios de casos incluyen las siguientes:

- ¿Son las computadoras análogas a "contenedores" protegidos de la "búsqueda e incautación inaceptables" bajo la Cuarta Enmienda?
- ¿Se debe tratar la comunicación en línea igual que la correspondencia sellada bajo los derechos constitucionales y de privacidad (contenido versus no contenido)?
- ¿Está sujeta la vigilancia de las comunicaciones cibernéticas (particularmente correos electrónicos y textos para los cuales hay una expectativa de privacidad) de un individuo específico sujeta a las mismas limitaciones y restricciones que la intervención de las líneas telefónicas?
- ¿Cómo se cercioran los profesionales de inteligencia cibernética que se cumplen las órdenes de la Orden Ejecutiva 12333, Actividades de Inteligencia de los Estados Unidos, para limitar la recopilación contra amenazas extranjeras (por ejemplo, cómo puede uno definir si el sujeto bajo vigilancia o recopilación es o no "un estadounidense" sujeto a protecciones constitucionales y ejecutivas)?
- Por encima de todo, ¿cómo se van a equilibrar los derechos del individuo en comparación con la responsabilidad del gobierno de garantizar la seguridad colectiva contra amenazas extranjeras e internas?

53. McNeerney, "Warshak," 346.

54. Air Force Space Command, *Functional Concept for Cyberspace Operations* (Concepto funcional para las operaciones ciberespaciales), 15.

55. Libicki, *Cyberdeterrence and Cyberwar*, 155, 156.

56. James, entrevista.

57. RADM J. Michael McConnell, entrevista telefónica por el autor, 23 de agosto de 2012.

58. Consultar, por ejemplo, William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy" (Defendiendo un ámbito nuevo: La estrategia cibernética del Pentágono), *Foreign Affairs* 89, no. 5 (septiembre-octubre de 2010): 99.

59. Ned Moran, "A Cyber Early Warning Model" (Un modelo cibernético de alerta temprana) en Jeffrey Carr, *Inside Cyber Warfare* (Dentro de la guerra cibernética) (Sebastopol, CA: O'Reilly Media, 2010), 200; y Geers, *Sun Tzu and Cyber War*, 10.

60. Gregory C. Radabaugh, "The Evolving Cyberspace Threat" (La amenaza cambiante del ciberespacio) (documento de trabajo, Agencia de Inteligencia, Vigilancia y Reconocimiento de la Fuerza Aérea, agosto de 2012), 9.

61. Eric M. Hutchins, Michael J. Cloppert, y Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains" (Defensa de la red de computadoras centrada en la inteligencia informada por análisis de campañas del adversario y cadenas de aniquilamiento de intrusión), (artículo presentado en la Sexta Conferencia Internacional sobre Guerra de Información y la Seguridad, George Washington University, Washington, DC, 17–18 de marzo de 2011), 3, <http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf>; Moran, "Cyber Early Warning Model," 208; y Radabaugh, "Evolving Cyberspace Threat," 9.

62. Hutchins, Cloppert y Amin, "Intelligence-Driven Computer Network Defense," 3.

63. McConnell, entrevista telefónica.

64. Dr. Kamal Jabbour, "Cyber Vision and Cyber Force Development" (Desarrollo de la visión cibernética y la fuerza cibernética), *Strategic Studies Quarterly* 4, no. 1 (Primavera 2010): 65, <http://www.au.af.mil/au/ssq/2010/spring/spring10.pdf>.

65. No es nada extraño que algunos de los guerreros cibernéticos de nuestra Fuerza Aérea se autodenominan "ninjas".

66. Richard Stiennon, *Surviving Cyberwar* (Sobreviviendo la guerra cibernética), (Lanham, MD: Government Institutes, 2010), 121.

67. Un *petabyte* son mil millones de *gigabytes*; un *yottabyte* son mil millones de *petabytes*.

68. "Cyber Vision 2025," 40.

69. Damon Poeter, "DefCon: NSA Boss Asks Hackers to Join the Dark Side" (DefCon: Jefe de NSA le pide a piratas cibernéticos que se unan al lado oscuro), *PC Magazine*, 29 de julio de 2012, <http://www.pcmag.com/article2/0,2817,2407783,00.asp>.

70. *Intelligence and National Security Alliance, Cyber Intelligence*, 14. Consultar también Wayne Michael Hall y Gary Cirenbaum, *Intelligence Collection: How to Plan and Execute Intelligence Collection in Complex Environments* (Recopilación de in-

teligencia: Cómo planificar y ejecutar la recopilación de inteligencia en entornos complejos), (Santa Barbara, CA: Praeger, 2012).

71. James, entrevista. Tal como destaca el Coronel Simpson, “El entrenamiento es otro reto que hay que superar”, en vista de “la falta en la actualidad de aptitud técnica para llevar a cabo un análisis cibernético detallado”. Simpson, entrevista.

72. Lynn, “*Defending a New Domain*,” 103.

73. Simpson, entrevista.

74. Por ejemplo, una encuesta del 2010 reveló que el 88 por ciento de los estadounidenses opinan que deben disfrutar de las mismas protecciones legales de privacidad en línea al igual que en la esfera física. Solamente un 4 por ciento estuvo en desacuerdo. Departamento de Comercio de EE.UU., *Comments of Digital Due Process, in the Matter of Information Privacy and Innovation in the Internet Economy* (Comentarios sobre el derecho procesal digital, en cuanto a la privacidad de información e innovación en la economía de la *Internet*), expediente núm. 1004020174-0175-01 (Washington, DC: US Department of Commerce, National Telecommunications and Information Administration, 14 June 2010), 4, [http://www.digitaldueprocess.org/files/NTIA\\_NOI\\_061410.pdf](http://www.digitaldueprocess.org/files/NTIA_NOI_061410.pdf).

75. Lynn, “*Defending a New Domain*,” 99.



**El Coronel Matthew M. Hurley**, USAF (USAFA; MA, University of Washington; MAAS, Air University; PhD, Ohio State University) es director de doctrina e integración de política para la Oficina del Subjefe de Estado Mayor para Inteligencia, Vigilancia y Reconocimiento, Cuartel General de la Fuerza Aérea de EE.UU., Pentágono, Washington, D.C. Como tal, garantiza que las equidades y mejores prácticas se codifiquen correctamente en los documentos de doctrina y política aliadas, conjuntas y de la Fuerza Aérea. Un oficial de carrera en el campo de la inteligencia, el Coronel Hurley se ha desempeñado en puestos en apoyo al Comando de Movilidad de la Fuerza Aérea, Fuerzas de EE.UU. en Corea, Fuerzas Aéreas de EE.UU. en Europa y Fuerzas Aéreas Aliadas/ Norte de Europa, inclusive despliegues de contingencia al Suroeste de Asia y el Cono de África. Fue acreedor del premio Ira C. Eaker Award y en 1989 recibió el premio de la Fundación Histórica de la Fuerza Aérea por investigación y significado histórico a la Fuerza Aérea. Su obra más reciente, *On the Fly: Israeli Airpower against the Al-Aqsa Intifada, 2000–2005*, fue publicada por el Instituto de Investigaciones de la Fuerza Aérea (AFRI), Base Aérea Maxwell, Alabama, en el 2010.