La Intersección de la Ley y la Ética en la Ciberguerra

Reflexiones

Mayor General Charles J. Dunlap, Jr., USAF–Ret.

POCOS TEMAS de seguridad han acaparado la atención del público como lo ha hecho el espectro de la ciberguerra. En un editorial reciente, el Presidente Obama advierte que la "ciberamenaza a nuestra nación es uno de los desafíos económicos y de seguridad nacional más graves que enfrentamos".[1] Esto, a su vez, ha planteado numerosas interrogantes sobre los parámetros legales de las ciberoperaciones, incluyendo las reglas aplicables a la ciberguerra actual.[2]

Paralelamente al creciente interés en los aspectos legales de la ciberguerra hay un número creciente de interrogantes que se centran en la dimensión ética. Éste es un aspecto importante para cualquier esfuerzo militar que apenas está surgiendo con respecto a las ciberoperaciones.[3] La creciente preocupación acerca de los aspectos éticos de las actividades en el ciberespacio dio lugar a una conferencia dedicada al tema auspiciada por la Academia Naval de los Estados Unidos en la primavera de 2012.[4] Y más recientemente, apareció un artículo en la revista The Atlantic titulado Is it Possible to Wage a Just Cyberwar? (¿Es posible luchar una ciberguerra justa?) que discute varios temas intrigantes.[5]

El objetivo de este corto ensayo es reflexionar sobre algunos temas que ilustran cómo los temas legales y éticos se cruzan en el ámbito del ciberespacio. Tal intersección no debe ser muy

sorprendente, insiste el historiador Geoffrey Best, "Nunca se debe olvidar que la ley de la guerra, dondequiera que haya comenzado, comenzó principalmente como un asunto de religión y ética . . . "Comenzó en ética" dice Best "y desde entonces ha mantenido un pie en la ética."[6] Es vital entender esa relación para entender el alcance global de las responsabilidades de un cibergue-rrero en el siglo 21.

Ley y ética

¿Qué relación hay entre ley y ética? Ciertamente el cumplimiento de la ley es una responsabilidad ética de línea de referencia, pero es solo eso: una línea de referencia. En la edición de marzo de 2012 del Armed Forces Journal[7] el Teniente de la Marina de los Estados Unidos Gabriel Bradley señala que "La ley del conflicto armado establece estándares mínimos" y prosigue afirmando persuasivamente que es esencial inculcar valores morales y éticos individuales e institucionales–un sentido de honor si se quiere–para asegurar el cumplimiento real de la ley.[8] Y ciertamente tiene razón cuando cita la observación de Christopher Coker que "las leyes pueden reafirmar el espíritu del guerrero; pero no la pueden reemplazar".[9]

Por supuesto, incluso determinar la línea de referencia–es decir, la ley–no siempre es fácil en las operaciones del siglo 21, pero en especial en relación a las ciber-actividades. Entre las varias razones para esto está el hecho que gran parte de la ley del conflicto armado fue diseñada para abordar conflictos librados principalmente con armas cinéticas. No obstante, en la opinión de este escritor, la ley existente puede aplicarse fácilmente a las ciberoperaciones. Esto quizás nos lleva al primer tema relacionado a la intersección de ley, ética y ciberoperaciones, es decir, la noción escuchada algunas veces de que el ciberespacio es un dominio tan nuevo que ninguna ley existente podría–o incluso debería–aplicarse a operaciones militares en él.

Simplemente esto no es cierto. La mayor parte de la ley del conflicto armado no es específica de un dominio. En este sentido considérese un proyecto reciente del Programa de Harvard sobre Política Humanitaria e Investigación de Conflictos para escribir un manual específico sobre la ley internacional aplicable a la guerra aérea y con misiles.[10] Produjo un volumen útil, pero relativamente débil ya que se encontró que había una parte de ley comparativamente modesta que podría considerarse única para los dominios del aire o del espacio. Lo mismo puede decirse sobre el dominio del ciberespacio, para incluir consideraciones éticas.[11]

Además, lo que algunas veces se disfraza como un problema legal en ciberoperaciones a menudo es más un tema técnico o una cuestión de política–no un problema legal auténtico. El muy publicitado asunto de lo que constituye el proverbial "acto de guerra" en el dominio del ciberespacio es un buen ejemplo. Aunque la frase "acto de guerra" es un término político, no un axioma legal, hay frases como "uso de fuerza" y "ataque armado" que sí tienen significado legal, y se podrían relacionar con un incidente bélico en términos de una respuesta contundente.[12]

La interpretación de tales expresiones en el ámbito del ciberespacio, de hecho, se puede resolver con arreglo a la ley, sí–y, sólo "sí" - la tecnología puede proporcionar datos adecuados en relación, por ejemplo, al daño actual causado por el supuesto "ataque", y también suficiente información sobre quién lo hizo. Por supuesto, la ausencia de datos de asignación de atribución (autoría)–técnicamente muy difícil de obtener en el ámbito del ciberespacio–puede ser una barrera legal y ética definitiva para una respuesta contundente. Esto puede ser frustrante cuando la gente quiere "hacer algo" en respuesta a un ciber-incidente, aunque no es excesivo que la ley–y la ética–demanden información confiable sobre quién podría ser responsable antes de lanzar un contrataque de alguna clase.

El hecho que, desde el punto de vista tecnológico, determinar la autoría sea una tarea difícil no es un problema para los abogados o los éticos, sino algo que deben resolver los tecnólogos. Es interesante por eso que los autores del artículo de The Atlantic antes referidos afirmen, en rela-

ción al uso supuesto de un arma cibernética (Stuxnet) contra las instalaciones de desarrollo nuclear de Irán, que "la falta de atribución de Stuxnet plantea inquietudes éticas porque negó a Irán la capacidad de contraatacar, fomentando un comportamiento más extremo".[13]

Aparte de la cuestión de si habría necesariamente una base legal o moral para que Irán contraataque como resultado de la supuesta operación Stuxnet,[14] es interesante que los autores del documento de The Atlantic digan que "para que la atribución funcione, necesitemos convenios internacionales".[15] Estos incluirían, alegan, acuerdos que "los ciberataques deberían llevar una firma digital de la organización atacante" y que se podrían usar ciertos protocolos de red para "facilitar la atribución".[16]

Aunque posiblemente la mayoría de expertos dirían que la ley actual no requiere que se facilite la atribución del acto cibernético,[17] los autores del artículo de The Atlantic no obstante abogan por "mejoras en el monitoreo internacional para rastrear el origen de los ataques" y parecen creer que "los incentivos económicos, como la amenaza de sanciones comerciales, pueden hacer que tales acuerdos sean deseables".[18] Hay en estas propuestas mucho para discrepar, pero se debe elogiar a los autores por al menos iniciar el diálogo de cómo se puede abordar una de las cuestiones legales y morales más desconcertantes de la ciberguerra.

Como en el caso de la atribución, los problemas tecnológicos–no la ley, por sí misma–son también el aspecto más difícil de fijar como objetivo las armas cibernéticas. Los principios fundamentales legales y éticos de distinción y proporcionalidad[19] requieren datos técnicos que proporcionen información a los elementos decisorios sobre quién estaría afectado por una técnica particular, y en qué medida. El que esto sea técnicamente difícil de hacer no es un problema legal o ético, es un problema científico. De hecho, se puede decir que una de las capacidades más necesarias en el mundo de las ciberoperaciones es la capacidad de modelar efectos con precisión confiable para proporcionar a los elementos decisorios -para no mencionar abogados o éticos- la clase de información realmente esencial para lograr juicios razonados acerca del empleo de una ciber-metodología.

¿Ponen los valores legales y éticos dificultades indebidas a los ciberguerreros?

Por encima de las dudas sobre la aplicación de regímenes legales y costumbres éticas para un ciber-escenario particular, está la cuestión más amplia de si se debería aplicar restricciones. Más específicamente, algunos creen que los esfuerzos para aplicar la ley dificultarán tanto los ciberesfuerzos estadounidenses que se pondrá en peligro la seguridad nacional. Este asunto más bien sorprendente está al centro de un debate serio en el que Stewart Baker y su redactor se empeñaron bajo los auspicios de la Asociación Americana de Abogados.[20]

Solo como contexto, el Sr. Baker es un reconocido abogado del cabinete legal Steptoe & Johnson de Washington, y ha servido previamente en el gobierno como consejero general de la Agencia de Seguridad Nacional, y también como Secretario Asistente de Política en el Departamento de Seguridad Nacional de los Estados Unidos. Comienza su polémica de esta manera:

> Los abogados no ganan guerras. ¿Pero pueden perder una guerra? Probablemente lo sepamos pronto. Abogados de diferentes ramas del gobierno han planteado tantas cuestiones legales sensacionales acerca de la ciberguerra que han dejado a nuestros militares incapaces de luchar, o incluso planear para una guerra en el ciberespacio.[21]

El Sr. Baker afirma además que los intentos de "imponer límites en la ciberguerra" están, en su opinión, "condenados al fracaso".[22] Entre los aspectos más preocupantes de su argumento se encuentra uno ético de primer orden que señala la devastación causada por la guerra aérea de la Segunda Guerra Mundial y referencia la declaración del ex Primer Ministro Británico Stanley

Baldwin en 1930 que en la guerra aérea "la única defensa es la ofensa, lo que significa que hay que matar más mujeres y niños más rápido que el enemigo si se quiere salvar uno mismo".[23]

El Sr. Baker prosigue su aparente apoyo del concepto de "matar más mujeres y niños más rápido" del Sr. Baldwin afirmando que si "deseamos defendernos contra los horrores de la ciberguerra, primero debemos encararlos, con el candor de un Stanley Baldwin."[24] Solo después de desarrollar una estrategia de ciberguerra tan encasillada consideraría el Sr. Baker apropiado "pedir que los abogados" den sus "ideas".[25]

Queda fuera del alcance de este ensayo repetir totalmente mi respuesta (aunque el título -¿Ciberguerra ilegal? No si desea ganar"–puede ser indicativo de su contenido), pero bastará decir que es muy importante en la ciberguerra (como en cualquier operación militar) anclar los "límites" cuando sea posible no solo en la ley o la ética, per se, sino también en la lógica práctica de la lucha de guerra. En el caso del ciberespacio, esto no es particularmente difícil de hacer, especialmente si los guerreros actuales no perciben una asimetría entre lo que la ley y la ética pueden requerir, y lo que creen que necesitan para cumplir su misión.

No obstante la afirmación del Sr. Baker de que las maquinaciones legales han dejado a las fuerzas armadas "incapaces de luchar, o incluso planear para una guerra en el ciberespacio", el General de la Fuerza Aérea Robert Kehler, comandante del Comando Estratégico de los Estados Unidos cuya organización subordinada el Cibercomando Estadounidense es el principal proponente de planeamiento y operaciones ciberespaciales militares, parece discrepar. En noviembre de 2011 declaró que "no creía que necesitemos nuevas autoridades explícitas para realizar operaciones ofensivas de cualquier clase". [26] Además, dijo que "no pensaba que hubiera ningún problema sobre autoridad para realizar [ciber] operaciones".[27] En otras palabras, los combatientes de guerra aparentemente no ven incompatibilidad entre las restricciones legales y éticas y su capacidad de "planear efectivamente para una guerra en el ciberespacio".

El respeto del estado de derecho es especialmente importante en el ámbito ciberespacial porque casi todos los expertos concuerdan en que la confrontación de la amenaza requiere de la cooperación de otros países a fin de rastrear y neutralizar las ciberamenazas -en tiempo de paz o de guerra.[28] Las naciones vitales para este esfuerzo, incluyendo especialmente las grandes democracias del mundo, indudablemente no estarían dispuestas a cooperar con ningún país que rechace límites en las operaciones militares, ciberespaciales o de cualquier otra forma. Los profesores Michael Riesman y Chris T. Antoniou señalan en su libro de 1994, The Laws of War (Las leyes de la guerra):

> En las democracias populares modernas, incluso un conflicto armado limitado requiere una base importante de apoyo público. Ese apoyo puede reducirse e incluso revertirse rápidamente, sin importar lo digno que sea el objetivo político, si la gente cree que la guerra se está llevando a cabo de una manera injusta, inhumana o indigna.[29]

Sin embargo, un rechazo del concepto del Sr. Baker para la ciberguerra no sugiere que las preocupaciones éticas y legales acerca de la ciberguerra se pueden desestimar. Por ejemplo, uno de los temas más serios tiene que ver con el papel de los civiles en las ciberoperaciones.

Ciberguerreros civiles

Casi se deja de mencionar que hay enorme especialización ciberespacial en la comunidad civil, y que es esencial que las fuerzas armadas tengan acceso a ella. Dicho esto, la extensión de tal acceso, y precisamente lo que significa–-o debe significar–- el acceso, es propiamente el tema de escrutinio legal y ético.

Los fundamentos no son difíciles. Para disfrutar del privilegio del combatiente, es decir una "licencia"–por así decirlo- para emprender actos destructivos legales contra la persona o propiedad del enemigo sin temor de enjuiciamiento, hay que ser miembro de las fuerzas armadas

propiamente constituidas de un beligerante en un conflicto armado.[30] A menudo esto se ha confundido con la creencia de que un civil no puede participar directamente en las hostilidades. En realidad, los civiles pueden hacerlo sin necesariamente cometer un crimen de guerra, pero hay consecuencias.

Entre las principales se encuentra el hecho de que si caen en manos del enemigo, podrían quedar sujetos a la ley criminal doméstica del enemigo por actos que, si los realizara un miembro de los militares oponentes, quedarían exentos de acusación. Lo que es más, según la ley de guerra, los civiles pueden ser objetivos adecuados -cinética o ciberespacialmente- cuando participan directamente en las hostilidades. En el contexto del ciberespacio, se debe entender que incluso el Comité Internacional de la Cruz Roja explícitamente utiliza como ejemplos de participación directa actos que son la clase de cosas que se esperaría del ciberguerrero, es decir, "Interferir electrónicamente con redes de computadoras militares (ataques de redes de computadoras) y transmitir inteligencia de selección táctica de objetivos para un ataque específico".[31]

¿Qué significa todo esto desde una perspectiva ética? Por un lado es esencial que los civiles entiendan las consecuencias potenciales, especialmente cuando el civil está lejos del sitio de trabajo, como en casa con su familia. Aunque hay debate en la comunidad internacional sobre lo que es necesario para que un civil sea considerado objetivo en la misma base que un miembro de las fuerzas armadas, el Comité Internacional de la Cruz Roja concuerda en que los civiles que asuman una "función de combate continua" (en oposición a simplemente "participar en hostilidades de forma espontánea, esporádica o desorganizada") pueden ser seleccionados como objetivos en una base similar a los miembros de las fuerzas armadas.[32]

Miembros de las fuerzas armadas–junto con los civiles que regularmente participan en una "función de combate continua" como ataques a redes de computadoras–pueden ser atacados con cualquier arma legal en cualquier lugar y en cualquier momento, independientemente de si en ese momento en particular el individuo presenta una amenaza inminente o esté realizando una función militar. Esto quiere decir, por ejemplo, que un ciberguerrero civil que participa regularmente en operaciones de ataque a redes de computadoras podría ser legítimamente atacado por un beligerante (no terroristas) en su hogar en un suburbio de Washington. Y no solo con ciber-armas; se puede usar cualquier arma legal si cumple con la ley de la guerra.

Por consiguiente, si el civil es suficientemente importante para las ciberoperaciones militares, se le podría asaltar con gran violencia donde se encuentre, siempre y cuando la muerte y lesiones incidentales de civiles inocentes–como la propia familia del ciberguerrero–que pudieran ocurrir en el ataque no "fueran excesivas en relación a la ventaja militar concreta y directa anticipada" (siendo esa "ventaja militar", por supuesto, la eliminación o neutralización del ciberexperto).[33]

Por tanto, el tema ético para los ciberguerreros puede ser la medida en que sea apropiado pedir a los civiles exponerse a esta clase de riesgos. Una cosa es que los miembros de las fuerzas armadas asuman voluntariamente el proverbial "contrato de responsabilidad ilimitada" del servicio militar para ponerse en peligro; otra cosa es, sin embargo, pedir que los civiles hagan eso, y aún más esperar que sus familiares acepten que pueden convertirse en daño colateral en un conflicto que tiene expresiones violentas junto con ciber-efectos no cinéticos. En la ciberguerra, los "frentes de batalla" pueden estar lejos de lo que cualquiera podría reconocer como el campo de batalla tradicional.

Es imposible saber lo real que puede ser esta clase de amenaza. Sin embargo, en una era de "celdas durmientes" y la proliferación de fuerzas de operaciones especiales clandestinas de otros entre muchos países, esta clase de contrarresto a las capacidades ciberespaciales de Estados Unidos podría no ser tan extravagante como algunos podrían pensar. En cualquier caso, esta discusión del riesgo personal que podrían ocasionar las ciberoperaciones hace irónico que los ciberguerreros tengan que fortificarse para resistir el cruel asalto de algunos críticos sobre su ética y profesionalismo.

¿Desafíos a la ética marcial de los ciberguerreros?

Tal vez una de las críticas más desconcertantes que ha acompañado al uso creciente de tecnologías avanzadas en la guerra es la tendencia de algunos comentaristas contemporáneos a suponer que su empleo es "impropio de un hombre" o "poco digno". Considérese la experiencia de los operadores de vehículos teledirigidos que, como los cibercombatientes, luchan la guerra desde consolas de computadora. Un artículo muy reciente de un experto titulado "Con sus mortales vehículos teledirigidos, Estados Unidos está luchando una guerra de cobardes" es un ejemplo de la clase de retórica desagradable que se usa.[34] Aunque tales calumnias aún no se han formulado contra los ciberguerreros, parecería que es solo cuestión de tiempo antes de que se les someta a la misma clase de insulto a su ética profesional.

¿Cómo comenzó todo esto? Puede remontarse a los comentarios de hace algunos años del Dr. David Kilcullen, un Teniente Coronel retirado del Ejército Australiano que se ha convertido en uno de los más destacados proponentes de la forma de contrainsurgencia centrada en tierra con utilización intensiva de personal que encontró lugar en el Manual de Contrainsurgencia del Ejército y la Infantería de Marina, (FM 3-24) publicado en 2006.[35] Es importante entender que el Manual es más bien hostil a las operaciones aéreas en general, y les dedica sólo cinco páginas en un documento de 300 páginas, por lo que la crítica del Dr. Kilcullen a los vehículos teledirigidos no parece incoherente con su visión más amplia del poderío aéreo.

En cualquier caso, el Dr. Kilcullen afirmó ante el Congreso en 2009 que los ataques con vehículos teledirigidos contra terroristas eran "contraproducentes".[36] "En la cultura tribal Pashtun de honor y revancha", dijo, "el combate frente a frente es visto como valiente; disparar a la gente con misiles desde 6.500 metros no lo es".[37] Según Kilcullen, "usar robots desde el aire ... parece cobarde y débil."[38] Es obvio que su tesis podría fácilmente aplicarse a las ciberoperaciones y a quienes la realizan.

Lo que hace espectaculares estas declaraciones en su ironía es que el adversario al que se refiere Kilcullen no solo usa dispositivos explosivos improvisados detonados a control remoto para asesinar fuerzas estadounidenses al resguardo de la distancia, sino que también emplean niños para implantarlos. ¿No los convertiría eso, según sus propios estándares de "cultura de honor", en "cobardes y débiles"? No obstante, toda esta discusión, desmoralizadora o inexacta, es –en términos de la lucha de guerra actual– más bien inmaterial. El "objeto de la guerra", como el General Patton lo puso gráficamente, "no es morir por su país sino hacer que el otro individuo muera por el suyo".

El coraje físico, por muy admirable que sea, no es la única cualidad que se necesita para la victoria en el siglo 21, y quizás siempre. Por ejemplo, los nativos estadounidenses, lucharon una guerra con extraordinaria valentía. En la edición de Abril de 2012 del Journal of Military History el historiador Anthony R. McGinnis señala que la forma individualizada y estilizada de guerra de los nativos estadounidenses no era rival para "una nación moderna tecnológicamente avanzada" que tiene la "victoria final como meta".[39] Por supuesto, no hay nada malo en ser "una nación moderna tecnológicamente avanzada" que tiene la "victoria final como meta" siempre y cuando esos avances tecnológicos se utilicen en una forma legal y éticamente apropiada.

La verdad es que no solo no hay nada poco ético en luchar una guerra desde lejos, en realidad no hay nada especialmente inusual en ello. Desde tiempos inmemoriales, los guerreros han buscado combatir a sus adversarios en formas que negaban a sus oponentes la oportunidad de poder usar sus armas. Por ejemplo, como este escritor dijo en alguna otra parte:

> David mató a Goliat con un proyectil antes de que el gigante pudiera usar sus armas; las lanzas de 16 pies de las falanges de Alejandro el Grande alcanzaron sus objetivos mucho antes que las lanzas de 12 pies que llevaban sus oponentes; los arqueros ingleses destruyeron lo mejor de los caballeros franceses de Agincourt desde lejos cuando hicieron llover flechas sobre los jinetes; y, más recientemente, los tanques estadounidenses y británicos destruyeron el núcleo de las fuerzas blindadas de Saddam durante la "Ba-

> talla de 73 Easting" en 1991 principalmente porque sus cañones tenían más alcance que los tanques T-72 de Irak. No hay nada nuevo acerca de matar a distancia.[40]

Pero hay algo acerca de la guerra computarizada que atrae escarnio de algunos, no obstante equivocada e injustamente. Por ejemplo, Phillip Altson, un profesor de leyes de la Universidad de Nueva York fue nombrado por las Naciones Unidas como "Relator especial" para redactar un informe sobre homicidios selectivos. El documento que produjo también incluyó sus opiniones sobre los operadores de vehículos teledirigidos.[41] En él, sostiene que debido a que las operaciones con vehículos teledirigidos se pueden realizar "enteramente desde pantallas de computadora y enlaces de audio remotos, hay un riesgo, "dice él, "de desarrollar una mentalidad 'PlayStation' para matar".[42]

¿Mentalidad 'PlayStation' para matar? La simple sugerencia de que tal falta insultante de profesionalismo aparezca en un informe oficial de las Naciones Unidas, de por sí, es inquietante. La evidencia principal del hallazgo del profesor Alston parece ser sus propias especulaciones acerca del esquema mental de quienes realizan una tarea que él nunca ha realizado. Sin embargo, la evidencia real apunta en una dirección diferente a la sugerida por Alston, y refuerza la idea de que estos oficiales difícilmente consideran sus obligaciones un juego. De hecho, el Dr. Peter Singer del Brookings Institution dijo en 2010 que en sus estudios encontró "niveles de tensión de combate más altos entre [algunas unidades de vehículos teledirigidos] que entre algunas unidades en Afganistán".[43] Concluyó que los operadores sufrían "fatiga, cansancio emocional y agotamiento crecientes".[44] Estos malestares son poco indicativos de "jugadores".

Más recientemente, el Air Force Times citó a un oficial de la Fuerza Aérea que respondió directamente a la acusación de "juego de video" señalando que las responsabilidades de los operadores de vehículos teledirigidos eran tremendamente estresantes, y que las operaciones eran un "evento profundamente emocional. No es un acto despreocupado. No es un juego de video".[45] Aunque el debate aún causa agitación,[46] demuestra la rapidez con la que algunos críticos ridiculizan el profesionalismo de gente de principios que hacen lo que su misión les pide hacer. Ciertamente, la comparación con las ciberoperaciones no es similar, pero–en cualquier caso–los ciberoperadores están en el asunto muy serio de defender su patria y, al hacerlo, se les puede pedir que hagan estragos mediante ciber-metodologías en cualquier adversario. Aunque los medios de hacerlo pueden ser diferentes, el profesionalismo que demandan las operaciones es muy alto, y las cargas psicológicas sobre aquellos que las realizan son igualmente muy grandes.

Ha surgido otro aspecto de las campañas con vehículos teledirigidos que podría encontrar analogía en la ética y el profesionalismo que deben demostrar los ciberoperadores. Se expresa en el artículo del 29 de abril de 2012 en Rolling Stone del controversial escritor Michael Hastings). En él, Hastings declara:

> La naturaleza de control remoto de las misiones no tripuladas habilita...al Pentágono y la CIA a lanzar ahora ataques militares u ordenar asesinatos sin poner una sola bota en el terreno–y sin preocuparse de una reacción pública contraproducente respecto a soldados estadounidenses que vuelven a casa en bolsas mortuorias. La inmediatez y lo confidencial de los vehículos teledirigidos hacen más fácil que nunca que los líderes desaten el poder militar estadounidense–y más difícil que nunca evaluar las consecuencias de tales ataques clandestinos.[47]

Por todas sus bravatas, Hastings tiene algo de razón cuando dice que "la inmediatez y lo confidencial de los vehículos teledirigidos hacen más fácil que nunca que los líderes desaten el poder militar estadounidense". La experiencia de este escritor es que los elementos decisorios principales están muy conscientes de que cualquier operación militar puede tener consecuencias no intencionadas–no importa el 'poco costo' que pareciera tener durante la planificación. Sin embargo, lo que dice respecto a los vehículos teledirigidos podría encontrar un paralelo con las ciberoperaciones, y podría exigir que los ciberguerreros exhiban virtudes éticas, incluyendo especialmente candor y coraje.

La necesidad de consejo franco, holístico

La novedad de las ciberoperaciones, la incertidumbre de su efecto preciso, y la pura dificultad de su ejecución no siempre pueden entenderlas todos los participantes en la cadena de decisión, y estas condiciones pueden dar lugar a otra responsabilidad ética, que es prestar consejo franco, holístico. No es imposible que en una situación dada los involucrados en el proceso tengan que salirse de su carril, por así decirlo, para hacer las preguntas difíciles, o señalar hechos inconvenientes. Si debe "desencadenarse" el ciberpoderío estadounidense como diría Hastings, es imperativo que se haga con el mismo cuidado que se haría en cualquier operación militar tradicional. Esto podría exigir que alguien haga más de lo que requiere la norma, solo para cerciorarse que se toman en cuenta todas las consideraciones correctas–incluyendo éticas y legales–de manera que se tomen las mejores decisiones.

Afortunadamente, para los abogados, el Código Modelo de Conducta Profesional de la Asociación Americana de Abogados -la "biblia" de los abogados- específicamente permite tal consejo holístico. La Regla 2.1 del Código exige que los abogados "ejerzan juicio profesional independiente y produzcan consejo cándido".[48] Además, los abogados no están limitados a proporcionar asesoramiento legal como continúa diciendo la Regla que al "brindar asesoramiento un abogado se puede referir no solo a la ley sino a otras consideraciones tales como factores morales, económicos, sociales y políticos, que puedan ser pertinentes a la situación del cliente".[49] En realidad, ésta es la guía apropiada no solo para los abogados, sino para todos los profesionales civiles y militares que participan en ciberoperaciones porque su éxito depende de una amplia gama de factores, y corresponde a todos los involucrados trabajar juntos para asegurar que se identifiquen y consideren.

La regla menciona candor. Esto no es algo simplemente para los abogados, es una virtud ética fundamental para todos los profesionales de defensa.[50] Entre otras cosas, es un rasgo importante que se debe tener en cuenta al evaluar la amenaza potencial que representa el ciberespacio. Falsear, o peor aún, tergiversar deliberadamente la amenaza, puede dar lugar a deficientes asignaciones de recursos y otros errores de juicio. Las opciones acerca del ámbito y la naturaleza de la amenaza difieren ampliamente; en una entrevista en PBS Newshour en la primavera de 2012, Terry Benzel del Instituto de Investigación de la Información insiste que "todos en la cibercomunidad, hablamos sobre ciber-Pearl Harbor. Y no se trata de si va a suceder. Es cuándo va a suceder".[51] Similarmente, un "importante experto en ciberseguridad europea dice que se necesita acción internacional para evitar una ciberguerra y ciberterrorismo catastróficos".[52]

Sin embargo, no todos están de acuerdo. En abril de 2012 el Contralmirante Samuel Cox, director de inteligencia del Cibercomando Estadounidense, supuestamente "restó importancia al prospecto de que un enemigo de los Estados Unidos pudiera inhabilitar la red de energía eléctrica de la nación o interrumpir la Internet, diciendo que esos sistemas están diseñados para resistir ciberataques serios".[53] Más punzante es un artículo de febrero de 2012 de Wired, en que los investigadores Jerry Brito y Tate Watkins refutan gran parte del discurso histriónico acerca de la amenaza de la ciberguerra.[54] Según Brito y Watkins, "la evidencia para sustentar graves advertencias [sobre la ciberguerra] brilla por su ausencia".[55]

Congruente con las conclusiones de Brito y Watkins es un informe de 2011 de la Organización para Cooperación y Desarrollo Económico.[56] Al tiempo que afirma que los gobiernos "necesitan hacer preparaciones detalladas para resistir y recuperarse de una amplia gama de cibereventos indeseados, tanto accidentales como deliberados",[57] los autores de ese estudio concluyen "que muy pocos eventos relacionados con el ciberespacio tienen la capacidad de causar una conmoción global".[58] Escribiendo en Foreign Policy el analista Thomas Rid sostiene que la ciberguerra es "aún más ruido que peligro".[59]

Todo esto plantea inquietudes porque Brito y Watkins dicen que "en muchos aspectos, la retórica sobre la ciber-catástrofe se asemeja a la exageración de la amenaza que vimos en el pe-

ríodo previo a la Guerra de Irak".[60] También señalan que la "ciberseguridad es una industria grande y floreciente" y que "en Washington abunda gente que tiene intereses particulares en combinar y exagerar las amenazas a nuestra seguridad digital".[61] Aunque no llegan a acusar realmente a nadie de empujar temores de ciberguerra por beneficio personal, piden un "alto" en la "retórica apocalíptica" e insisten que los "escenarios alarmistas que dominan el discurso político pueden ser buenos para el complejo de ciberseguridad industrial, pero no hacen ningún favor a la seguridad real".[62]

El ámbito y la inmediatez de la amenaza se debate con razón, pero todos podrían estar de acuerdo en que, en cualquier caso, la exageración deliberada (o subestimación) de la amenaza, aunque sea por razones de apoyo activo bien intencionadas, puede plantear cuestiones de ética y profesionalismo. Como Brito y Watkins sugieren, al considerar el período previo a la guerra con Irak en 2003 es claro lo que puede pasar cuando se malinterpreta una amenaza, lo que puede explicar el título de su polémica "Cyberwar Is the New Yellowcake (La ciberguerra es el nuevo óxido de uranio concentrado)." En resumen, candor–y retórica moderada si procede–son cualidades críticas de los ciberguerreros. El lenguaje mesurado del Presidente Obama que urge a la gente a tomar "seriamente" la ciberamenaza y planear para ello como una "prioridad", representa un enfoque responsable que resalta los peligros sin caer víctima de la exageración contraproducente y engañosa.[63]

La virtud de competencia

Finalmente, una de las responsabilidades éticas de los ciberguerreros es la competencia. Las Reglas Modelo de Conducta Profesional de la Asociación Americana de Abogados proporcionan pautas que todos los profesionales del ciberespacio deberían considerar en analogía a sus responsabilidades. La Regla 1.1 de ese Código dice que "la representación competente requiere el conocimiento legal, habilidades, escrupulosidad y preparación razonablemente necesarios para la representación".[64] Para quienes se preocupan de los aspectos legales y éticos de la ciberguerra, el mandato ético de competencia va más allá del conocimiento y entendimiento de la ley y/o la ética, per se.

Sin duda hay muchos aspectos de las ciberoperaciones que son extraordinariamente complejos. Por tanto, les incumbe a los asesores legales y de otro tipo familiarizarse lo más que sea posible con el "negocio" del cibercliente para incluir sus aspectos técnicos. Un conocimiento práctico de la tecnología no solo ayudará a los asesores a entender los hechos de manera suficiente para aplicarles principios legales y éticos; también les dará gran credibilidad con aquellos que buscan su asesoramiento. Los elementos decisorios en el ámbito ciberespacial–y los que buscan asesoramiento en otras actividades–naturalmente gravitarán hacia los que muestren un entendimiento genuino de las muchas complejidades de su disciplina.

Esto no es una tarea fácil. Mantenerse actualizado con la tecnología en este campo tan complicado es un trabajo que tarda mucho y nunca termina. Pero se debe realizar con bastante anticipación de la necesidad, ya que no hacerlo puede dar lugar a una vida de lamentos. Winston Churchill observó una vez:

> Para todo hombre llega una vez en su vida ese momento especial en que figurativamente se le da una palmada en el hombro y se le ofrece una oportunidad para hacer algo muy especial, exclusivo para él y adaptado a sus talentos. Qué tragedia si ese momento lo encuentra desprevenido o sin la calificación para el trabajo que podría ser su mejor momento.[65]

Observaciones finales

Este ensayo busca ilustrar solo algunos ejemplos de cómo se podrían cruzar la ley y la ética. Este esfuerzo puede suscitar la pregunta: ¿cuáles de estos imperativos funcionará mejor para imponer los límites en la ciberguerra que gente honorable, y aún práctica, demanda? Kenneth Anderson, un profesor de leyes en la American University, tuvo recientemente la ocasión de considerar uno de sus primeros escritos sobre la eficacia de la ley y el honor como "motores" para el comportamiento correcto en el conflicto. El profesor Anderson sostiene que:

> La fe en la legalidad como el motor que impulsa tal adhesión a las leyes de la guerra me parece, no obstante, totalmente equivocada; es una fantasía hecha a la medida para los abogados, y especialmente para los abogados estadounidenses. Los abogados creen que el problema es uno de imposición, mientras que en realidad es uno de lealtad. Las codificaciones de la ley internacional son una plantilla útil para organizar las categorías de los deberes de un soldado. Pero, al final, la cultura pertinente al respeto de la ley humanitaria internacional no es la cultura de la legalidad y al culto de los abogados, sino más bien es la cultura del honor profesional de soldados, y lo que están dispuestos a hacer o no hacer en el campo de batalla.[66]

El que el "honor" colinde con la ética, o un subconjunto de la misma, puede ser apropiado para un debate activo en la universidad. Sin embargo lo que es más importante observar, como lo hace Anderson, es que John Keegan, quizás el historiador militar más eminente de la era moderna, no tuvo reservas para decir que "no hay sustituto para el honor como medio de imponer decencia en el campo de batalla, nunca lo ha habido, y nunca lo habrá".

Los "campos de batalla" del ciberespacio no se parecen mucho a los que se refiere Keegan, pero su punto de vista ciertamente tiene igual aplicabilidad. Al final, el honor y la mentalidad ética que implica, es indispensable. Pero la discusión no puede terminar allí, porque el simple hecho de haber desarrollado el carácter para llegar a la respuesta correcta no es suficiente, ya que se puede requerir coraje para insistir en ella.

El coraje que necesitan los ciberguerreros no es necesariamente el coraje físico que deben demostrar los combatientes del campo de batalla. Más bien, es mucho más probable que los cibercombatientes tengan que demostrar coraje moral. Esto es particularmente cierto a medida que se desarrollan las normas para las ciberoperaciones. Puede ser un gran reto hacer lo correcto, particularmente en circunstancias de extrema urgencia donde no hay orientación explícita salvo referencias a los principios clásicos de la ley y la ética.

Los cibercombatientes quizás deseen considerar que Max Hastings, otro historiador británico, en su estudio clásico del heroísmo militar concluye que "la bravura física se encuentra [en los militares] con más frecuencia que la variedad espiritual".[67] "El coraje moral", insiste "es raro."[68] Sin embargo es exactamente esta clase rara la que más necesitan demostrar los ciberguerreros. La ley puede proporcionar una arquitectura, pero es solo cuando se cruzan el honor y el coraje moral que podemos estar realmente seguros que los principios éticos dignos de defender son los que se conservan. ❑

Notas

1. Barack Obama, Taking the Cyberattack Threat Seriously (Tomar en serio la amenaza del ciberataque), WALL STREET JOURNAL, 19 de julio de 2012, http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html. Barack Obama, Taking the Cyberattack Threat Seriously (Tomar en serio la amenaza del ciberataque), WALL STREET JOURNAL, 19 de julio de 2012, http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html.

2. Por ejemplo, la División de Ley Internacional del U.S. Naval War College organizó una conferencia dedicada a los aspectos legales de la ciberguerra en junio de 2012, http://www.usnwc.edu/ILDJune2012.

3. Véase por ejemplo, Randall R. Dipert, The Ethics of Cyberwar (La ética de la ciberguerra), J. OF MIL. ETHICS, Vol. 9, No. 4 (2010), en 384, 385 (no hay discusiones informadas, abiertas, públicas o políticas de lo que sería una política ética y acertada para el uso de tales ciber-armas.").

4. Stockdale Center for Ethical Leadership de la Academia Naval de los Estados Unidos, Warfare in a New Domain: The Ethics of Military Cyber Operations (La guerra en un nuevo dominio: La ética de las ciberoperaciones militares), 26-27 de abril de 2012 http://www.usna.edu/ethics/publications/mccain2012.php. Gran parte de este ensayo viene de una presentación que hizo el autor en esa conferencia.

5. Patrick Lin, Fritz Allhoff, y Neil Rowe, Is it Possible to Wage a Just Cyberwar? (¿Es posible luchar una ciberguerra justa?), THE ATLANTIC, 5 de junio de 2012, http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/.

6. Geoffrey Best, Law and War Since 1945 (La ley y la guerra desde 1945), 1994, p. 289

7. Teniente Gabriel Bradley, Honor, Not Law, (Honor, no ley) ARMED FORCES JOURNAL, marzo de 2012, disponible en http://www.armedforcesjournal.com/2012/03/9563756 (consultada por última vez el 23 de abril de 2012).

8. Id.

9. Id.

10. Program on Humanitarian Policy and Conflict Research, Manual on International Law Applicable to Air and Missile Warfare (2009) (Programa sobre política humanitaria e investigación de conflicto, Manual sobre ley internacional aplicable a la guerra aérea y con misiles) http://ihlresearch.org/amw/HPCR%20Manual.pdf [de aquí en adelante el Manual AMW].

11. Véase por ejemplo, Roger Crisp, Cyberwar: No New Ethics Needed (La ciberguerra: No se necesita nueva ética), PRACTICAL ETHICS (blog), 19 de junio de 2012, http://blog.practicalethics.ox.ac.uk/2012/06/cyberwarfare-no-new-ethics-needed/.

12. Estos términos se usan, por ejemplo, en el Artículo 2 y el Artículo 52, respectivamente de la Carta de las Naciones Unidas, http://treaties.un.org/doc/Publication/CTC/uncharter.pdf.

13. Véase la nota 5, supra.

14. Si, por ejemplo, se puede hacer un caso objetivo para la aplicación correcta de la doctrina de autodefensa preventiva por una nación-estado, no habría base legal o moral para que Irán responda. Para una discusión de la autodefensa preventiva, consulte en general, Kinga Tibori Szabó, ANTICIPATORY ACTION IN SELF-DEFENCE: ESSENCE AND LIMITS UNDER INTERNATIONAL LAW (ACCIÓN PREVENTIVA EN DEFENSA PROPIA: ESENCIA Y LÍMITES SEGÚN LA LEY INTERNACIONAL) (2011).

15. Id.

16. Id.

17. Véase por ejemplo, Crisp, supra nota 11.

18. Véase supra nota 5.

19. Harold Koh, el asesor legal del Departamento de Estado de los Estados Unidos, explica los términos:

> Primero, el principio de distinción, que requiere que los ataques se limiten a objetivos militares y que los civiles o los objetos civiles no deben ser objeto del ataque; y Segundo, el principio de proporcionalidad, que prohíbe los ataques que podrían causar pérdidas incidentales de vidas civiles, lesiones a civiles, daño a objetos civiles, o una combinación de ellos, que serían excesivos en relación a la ventaja militar concreta y directa anticipada.

Harold Koh, The Obama Administration and International Law (La administración Obama y la ley internacional), discurso, American Society of International Law, 25 de marzo de 2010, http://www.state.gov/s/l/releases/remarks /139119.htm.

20. Stewart A. Baker y Charles J. Dunlap Jr., What Is the Role of Lawyers in Cyberwarfare? (¿Cuál es la función de los abogados en la ciberguerra?), ABA JOURNAL,1 de mayo de 2012, http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare/.

21. Id.

22. Id.

23. Id.

24. Id. (se añaden las cursivas).

25. Id.

26. Jim Wolf, "U.S. Military better prepared for cyber warfare: general (Militares estadounidenses mejor preparados para la ciberguerra: general)", Reuters (16 de noviembre de 2011) http://www.reuters.com/article/2011/11/17/us-usa-cyber-military-idUSTRE7AG03U20111117?feedType=RSS&feedName=everything&virtualBrandChannel=11563

27. Id.

28. Véase por ejemplo, Department of Defense Strategy for Operating in Cyberspace (Estrategia del Departamento de Defensa para operar en el ciberespacio) del Departamento de Defensa de los Estados Unidos, 2011, en 9, http://www.defense.gov/news/d20110714cyber.pdf ("El ciberespacio es una red de redes que incluye miles de proveedores de servicio Internet (ISP) en el mundo; ningún estado u organización puede mantener ciberdefensas efectivas por su cuenta".).

29. W. Michael Riesman y Chris T. Antoniou, THE LAWS OF WAR (LAS LEYES DE LA GUERRA) (1994), en xxiv.

30. Véase en general, Gary D. Solis, THE LAW OF WAR (La ley de la guerra) (201), en 41-42.

31. Direct Participation in Hostilities: Questions and Answers (Participación directa en hostilidades: Preguntas y respuestas), Comité Internacional de la Cruz Roja, 6 de febrero de 2009, http://www.icrc.org/eng/resources/documents/faq/direct-participation-ihl-faq-020609.htm.

32. Id.

33. Véase Koh, supra, nota 19.

34. George Monbiot, With its deadly drones, the US is fighting a coward's war (Con sus mortales vehículos teledirigidos, Estados Unidos está luchando una guerra de cobardes), The Guardian (U.K.), 30 de enero de 2012, http://www.guardian.co.uk/commentisfree/2012/jan/30/deadly-drones-us-cowards-war.

35. Departamento del Ejército de los Estados Unidos, Manual de Campo 3-24, 2006, http://www.fas.org/irp/doddir/army/fm3-24.pdf.

36. Doyle McManus, U.S. drone attacks in Pakistan 'backfiring,' Congress told (Los ataques con vehículos teledirigidos en Paquistán son 'contraproducentes', se le advierte al Congreso), LOS ANGELES TIMES, 3 de mayo de 2009, http://articles.latimes.com/2009/may/03/opinion/oe-mcmanus3

37. Id.

38. Id.

39. Anthony R. McGinnis, When Courage Was Not Enough: Plains Indians at War with the United States Army (Cuando el coraje no era suficiente: Los Indios de las Llanuras en guerra con el Ejército de los Estados Unidos), J. OF MIL. HISTORY, abril de 2012, en 473.

40. Charles J. Dunlap, Jr., Does Lawfare Need an Apologia, Does Lawfare Need an Apologia? (¿Necesita la ley de la guerra una apología? 43 CASE WES. RES. J. INT'L L. (2010), en 121.

41. Relator especial sobre ejecuciones extrajudiciales, sumarias o arbitrarias, Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Execution: Study on Targeted Killings, entregado al Consejo de Derechos Humanos, U.N. Doc. A/HRC/14/24/Add.6 (28 de mayo de 2010), disponible en http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.24.Add6.pdf (consultado últimamente el 2 de septiembre de 2010).

42. Id., en 25.

43. Marc Pitzke, Interview with Defense Expert P.W. Singer (Entrevista con el experto en defensa P.W. Singer), SPIEGEL ONLINE INTERNATIONAL, 12 de marzo de 2010, thttp://www.spiegel.de/international/world/0,1518,682852,00.html.

44. Id..

45. Jeff Schogol y Markeshia Ricks, Demand grows for UAV pilots, sensor operators (Aumenta la demanda de pilotos de UAV, operadores de sensores), Air Force Times, 21 de abril de 2012,

46. Véase por ejemplo, Kenneth Anderson, Laurie Blank on Mark Mazzetti's 'The Drone Zone'–Último en una serie de Lewis, Dunlap, Rona, Corn, y Anderson, LAWFARE, 21 de julio de 2012, http://www.lawfareblog.com/2012/07/laurie-blank-on-the-mazzetti-the-drone-zone-last-in-series-from-lewis-dunlap-rona-corn-and-anderson/.

47. Michael Hastings, The Rise of the Killer Drones: How America Goes to War in Secret (El auge de los vehículos teledirigidos asesinos: Cómo va Estados Unidos a la guerra en secreto), ROLLING STONE, 16 de abril de 2012, http://www.rollingstone.com/politics/news/the-rise-of-the-killer-drones-how-america-goes-to-war-in-secret-20120416#ixzz22VDkfR00.

48. Regla modelo de conducta profesional de la ABA 2.1, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_2_1_advisor.html.

49. Id.

50. Compare lo siguiente de la lista de "Valores éticos primarios" encontrados en el Reglamento Conjunto de Ética del Departamento de Defensa (se añaden las cursivas):

> a. Honestidad. Ser veraz, simple y cándido son aspectos de la honestidad.
>
> (1) La veracidad es obligatoria. Los engaños se descubren con facilidad y usualmente lo son. Las mentiras erosionan y socavan la confianza del público. Las falsedades dichas por razones aparentemente altruistas (para no herir sentimientos, fomentar la buena voluntad, etc.) las resienten los recipientes.
>
> (2) La simpleza añade franqueza a la veracidad y usualmente es necesaria para fomentar confianza pública y asegurar la conducción efectiva y eficiente de las operaciones del Gobierno Federal. Las verdades que se presenten de tal manera que lleven a los recipientes a la confusión, interpretación errónea o conclusión inexacta no son productivas. Tales engaños indirectos pueden fomentar mala voluntad y erosionar la apertura, especialmente cuando hay una expectativa de franqueza.
>
> (3) Candor es el ofrecimiento directo de información no solicitada. Es necesario de acuerdo con la gravedad de la situación y la naturaleza de las relaciones. Se requiere candor cuando una persona razonable se sentiría traicionada si se retiene información. En algunas circunstancias, el silencio es deshonesto, y en otras circunstancias, revelar información sería incorrecto y quizás ilegal.

Reglamento 5500.07-R del Departamento de Defensa de los Estados Unidos, Joint Ethics Regulation (Reglamento Conjunto de Ética), 17 de noviembre de 2011, para 12-401a, http://www.dtic.mil/whs/directives/corres/pdf/550007r.pdf.

51. Preventing a 'Cyber-Pearl Harbor' (Evitar un 'Ciber-Pearl Harbor'), PBS NEWSHOUR, 16 de abril de 2012, http://www.pbs.org/newshour/bb/science/jan-june12/deterlab_04-16.html.

52. Expert warns on cyberwar threat (Experto advierte sobre la amenaza de la ciberguerra), UPI.COM, 16 de marzo de 2012, http://www.upi.com/Science_News/2012/03/16/Expert-warns-on-cyberwar-threat/UPI-33781331937216/#ixzz1sRYZauJc (cita a Eugene Kaspersky, director ejecutivo y cofundador de Kaspersky Lab, que dice ser la empresa antivirus más grande de Europa).

53. Richard Lardner, US Needs Top-level Approval to Launch Cyberattacks (EE.UU. necesita aprobación del más alto nivel para lanzar ciberataques), SALON.COM, 24 de abril de 2012, http://www.salon.com/2012/04/24/us_needs_top_level_approval_to_launch_cyberattacks/.

54. Jerry Brito y Tate Watkins, Cyberwar is the New Yellowcake (La ciberguerra es el nuevo óxido de uranio concentrado), WIRED, 14 de febrero de 2012, disponible en http://www.wired.com/threatlevel/2012/02/yellowcake-and-cyberwar/.

55. Id.

56. Peter Sommer y Ian Brown, Reducing Systemic Cybersecurity Risk (Reducción del riesgo sistémico de ciberseguridad), Organización para Cooperación y Desarrollo Económico, 14 de enero de 2011, en 5, http://www.oecd.org/dataoecd/57/44/46889922.pdf.

57. Id.

58. Id.

59. Thomas Rid, Think Again: Cyberwar (Repensar la ciberguerra), FOREIGN POLICY, Marzo/Abril de 2012, en 80, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=full.

60. Brito and Watkins, supra note 54.

61. Id.

62. Id.

63. Véase nota 1, supra.

64. ABA Model Rule of Professional Conduct 1.1 (Regla modelo de conducta profesional de la ABA 2.1), http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence.html.

65. Según cita del Mayor General Stephen R. Lorenz, Lorenz on Leadership (Liderazgo según Lorenz), AIR & SPACE POWER JOURNAL, Verano de 2005, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj05/sum05/lorenz.html

66. Kenneth Anderson, Sir John Keegan, Ave Atque Vale, LAWFARE, 3 de agosto de 2012, http://www.lawfareblog.com/2012/08/sir-john-keegan-ave-atque-vale/.

67. Max Hastings, WARRIORS: PORTRAITS FROM THE BATTLEFIELD (GUERREROS: RETRATOS DEL CAMPO DE BATALLA), (2005), en XVII.

68. Id.

El Mayor General Charles J. Dunlap, Jr., USAF (Ret.) es el Director Ejecutivo del Centro de Ley, Ética y Seguridad Nacional en la Escuela de Leyes de Duke University. Su carrera de 34 años como abogado militar incluyó asignaciones en el Reino Unido y Corea, y participó en operaciones militares en África y Oriente Medio. Un graduado distinguido del National War College, las publicaciones recientes del General Dunlap relacionadas con el ciberespacio incluyen Perspectives for Cyber Strategists on Law for Cyberwar (Perspectivas para ciber-estrategas sobre la ley de la ciberguerra), en Strategic Studies Quarterly (2011) y Towards a Cyberspace Legal Regime in the 21st Century: Considerations for American Cyberwarriors (Hacia un régimen legal en el ciberespacio en el siglo 21: Consideraciones para los ciberguerreros estadounidenses), en la publicación Law Review de la University of Nebraska (2009). El General Dunlap y Stuart Baker debaten temas legales del ciberespacio en Patriot Debates, publicado en 2012 por la Asociación Americana de Abogados.