# Cómo analizar la guerra en *Wi-Fi*

## De ciberguerra a Wikiguerra: la lucha por el ciberespacio

Paul Rexton Kan

*Paul Rexton Kan es Profesor de Estudios de seguridad internacional y el Presidente de Estudios Militares Henry L. Stimson de la Escuela Superior de Guerra del Ejército de EUA. Es autor de los libros Drugs and Contemporary Warfare y Cartels at War: Understanding Mexico's Drug-Fueled Violence and the Threat to US National Security. Su artículo reciente titulado, "Cyberwar in the Underworld", fue publicado en Yale Journal of International Affairs.*

*Este artículo fue publicado originalmente en la revista* Parameters *(en inglés), número de otoño de 2013*

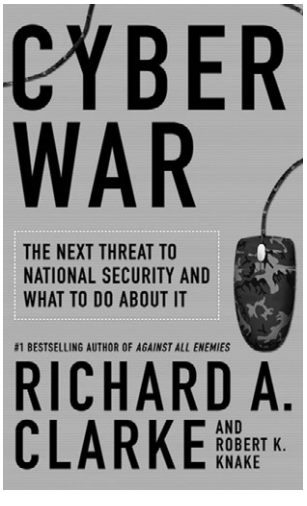
Resumen: Los líderes de la Nación advierten sobre una ciberguerra y ciberterrorismo que puede llevar a un posible ataque tipo "Pearl Harbor cibernético". A fin de evitar esta posibilidad, se requiere una defensa cibernética o, incluso, algún tipo de disuasión cibernética. Algunos formuladores de política aún quieren establecer el control de armas cibernéticas. Sin embargo, estos conceptos representan una modificación retroactiva de los conceptos usados en la esfera física para describir actos violentos y reacciones ante los mismos. ¿Estos conceptos ayudan a los formuladores de política, profesionales de seguridad nacional y eruditos a comprender los actos agresivos perpetrados en el ciberespacio?

Unos cuantos días después de los bombardeos en el Maratón de Boston en abril de 2013, la *Associated Press* (AP) reportó por medio de *Twitter*, "Noticias de última hora: dos explosiones en la Casa Blanca y Barack Obama herido". El índice industrial de Dow Jones perdió casi 150 puntos; US$ 136 billones en valores, repentinamente desaparecieron. La cuenta de *Twitter* de la AP, cuya alimentación había sido integrada en los algoritmos de reportaje de la Bolsa de Nueva York unos cuantos días antes, fue ilegalmente accedida (*hacked*) por un grupo que se llama el Ejército Electrónico Sirio, permitiendo enviar mensajes falsos por *Twitter* (*tweets*). Afortunadamente, la pérdida de riqueza nacional fue de corta vida ya que los valores se recuperaron en menos de tres minutos.

¿Cómo formamos un contexto sobre lo que pasó en estos tres minutos? ¿Fue esta una bala de salva en una ciberguerra comenzada por el régimen sirio, o una travesura realizada por un grupo no afiliado de "lulz" (una modificación de las siglas "lol", o "reírse con ganas")? No fue una pérdida permanente de activos y, aparte de los perpetradores, muy pocos, en realidad, se hubieran reído de esa manera. Sin embargo, todavía hay un sentido de seriedad con respecto a este episodio que revela los verdaderos límites de nuestra comprensión de la esfera cibernética en el ámbito de seguridad nacional. Dada la novedad de la esfera digital, sus orígenes manufacturados por el hombre y su carácter en constante evolución, debido a la manipulación de los seres humanos, no es de sorprender que los profesionales de seguridad nacional busquen modalidades cómodas y familiares. Los "ciberataques" son una ocurrencia diaria,

o más precisamente de nanosegundo a nanosegundo, que requiere "seguridad cibernética". Los líderes de la Nación advierten de una ciberguerra y ciberterrorismo que pueden llevar a un posible ataque tipo "Pearl Harbor cibernético". A fin de evitar esta posibilidad, se requiere una defensa cibernética, o incluso, algún tipo de disuasión cibernética. Algunos formuladores de política todavía quieren establecer el control de las armas cibernéticas para limitar los tipos de ciberataques que puedan ser perpetrados contra otro país. Sin embargo, estos conceptos representan una modificación retroactiva de los usados en la esfera física para describir actos violentos y las reacciones ante los mismos. ¿Ayudan estos conceptos a los formuladores de política, profesionales de seguridad nacional y eruditos a comprender los actos agresivos perpetrados en el ciberespacio?

En su libro titulado, *Cyber War: The Next Threat to National Security and What to Do About It*, Richard Clarke opina que estos conceptos no solo son relevantes, sino también consistentemente ignorados por los formuladores de política. En la opinión de Clark, la ciberguerra se refiere "a las acciones tomadas por una Nación-Estado para penetrar las computadoras o redes de otra nación a fin de causar daños o interrupción" (6). En su primer capítulo, Clarke describe las "pruebas experimentales", incidentes de la ciberguerra perpetrados más notablemente por los rusos, norcoreanos e israelíes. Hoy en día, estos episodios son bien conocidos —Israel al "adueñarse" del sistema de defensa antiaérea en 2007; los sospechosos ataques de negación distribuida de servicios (DDOS, por sus siglas en inglés) llevados a cabo por los rusos contra Estonia en 2007 y los ciberataques más sofisticados contra Georgia en 2008; y el ataque *botnet* contra páginas cibernéticas de EUA en 2009. De estos episodios, se derivan cuatro máximas: la ciberguerra existe; la ciberguerra ocurre a la velocidad de la luz; la ciberguerra es global y la ciberguerra ha comenzado. Estas máximas forman el corazón de su libro a medida que presenta más relatos de los "guerreros cibernéticos" en el "zona de combate" y cómo Estados Unidos debe prepararse, defenderse y tomar represalias.



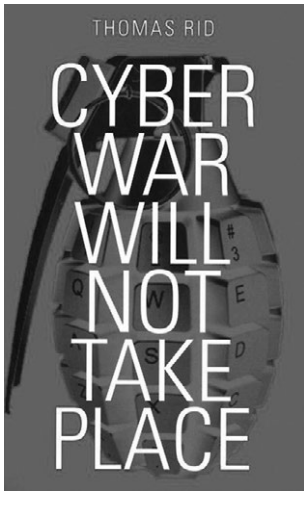

Clarke usa la mayor parte de su tiempo recalcando estas máximas en todo el libro con breves ejemplos. Clarke aparenta estar más preocupado de China, sostiene que está "haciendo sistemáticamente todas las cosas que haría una Nación, si contempla tener una capacidad de ciberguerra ofensiva y también se considera ser blanco de una ciberguerra" (54). La preocupación principal de Clarke es que Estados Unidos se quede rezagado en comparación con países tal como China. "De hecho, debido a su mayor dependencia de los sistemas controlados por medios cibernéticos y su incapacidad, hasta el momento, de crear defensas cibernéticas en el nivel nacional, Estados Unidos, actualmente, es mucho más vulnerable a la guerra cibernética que Rusia o China. Estados Unidos corre más riesgos de ser blanco de una guerra cibernética que los Estados menores tal como Corea del Norte" (155).

Dada la seriedad de la evaluación de Clarke y los ejemplos de graves consecuencias de los previos ciberataques, su libro merece un estudio detallado. La estrecha definición de Clarke en cuanto a lo que constituye una ciberguerra es problemática. ¿En realidad, constituye la guerra el sinnúmero de acontecimientos que él especifica? Ocasionar daños o interrupción es una gama bastante extensa de consecuencias —desde la desconfiguración de una página web hasta paralizar una red de energía eléctrica. En el mundo físico, un acto podría ser interpretado como vandalismo y otro podría ser considerado la destrucción maliciosa de la propiedad. ¿Sin una intención coercitiva para lograr una meta política, sería considerada la gama de ataques —cibernéticos o de otro tipo— un acto de guerra?

Es en este punto, el libro titulado, *Cyber War Will Not Take Place*, es especialmente útil para aclarar mucha ambigüedad conceptual en torno a la ciberguerra. En comparación con el libro de Clarke, el de Rid es una obra mucho más académica. Rid, profesor adjunto en King´s College en Londres, sostiene que todos los actos dañinos que se perpetran por medio del ciberespacio no constituyen una guerra o acción bélica, ni son especialmente violentos. "Ninguna ofensa cibernética jamás ha ocasionado la pérdida de vida humana. Ninguna ofensa cibernética tampoco ha herido a una persona. Ninguna ofensa cibernética ha derrumbado un edificio" (166).

Al usar la teoría de guerra de Clausewitz, Rid sostiene que "si el uso de la fuerza en la guerra es violento, instrumental y político, entonces no hay una ofensiva cibernética que satisfaga los tres criterios. Sin embargo, históricamente, hay muy pocos ataques cibernéticos que solo satisfacen uno de estos criterios (4, énfasis en el original). Según Rid, los acontecimientos a través del ciberespacio relatados por diversos profesionales de seguridad tal como Clarke se incluyen en las categorías de espionaje, sabotaje o subversión. "A pesar de las tendencias, la "guerra" en la "guerra cibernética", por último, tiene más en común con la guerra contra la obesidad que con la Segunda Guerra Mundial —tiene un valor más metafórico que descriptivo" (9).

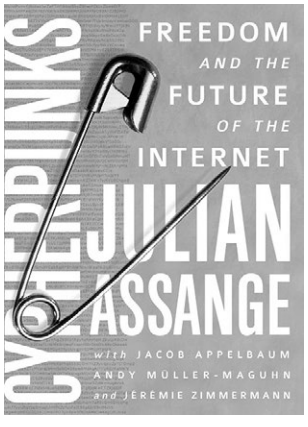
El punto de Rid en cuanto a tener cuidado con las metáforas y conceptos en un nuevo dominio es bien comprendido. La meta de su libro es "intentar ayudar a consolidar la discusión, menguar alguna parte de la exageración y adecuadamente enfrentar algunos de los desafíos de seguridad más urgentes" (ix). Muchas ideas se han centrado en la mecánica de los actos nefastos en el ciberespacio, sin embargo, en comparación, solo se ha invertido poco tiempo en establecer el contexto de los actos. Es necesario comprender las motivaciones de los grupos e individuos que actúan en el ciberespacio. El argumento principal y los subsecuentes capítulos de Rid sobre la "Violencia", "Sabotaje", "Espionaje" y "Subversión" son poderosos tónicos contra alguna parte de la literatura más alarmista sobre la ciberguerra. Su conclusión es tan interesante como provocadora —los ciberataques son un ataque con la violencia misma. Puesto que las actividades tales como el sabotaje, espionaje y subversión ahora pueden ser llevadas a cabo en el ciberespacio, se necesita un menor número para llevar a cabo estas actividades en el mundo físico. Antes, las Fuerzas especiales se desplegaban para destruir una instalación, se enviaban espías para robar secretos y turbas organizadas para hacer demostraciones contra las políticas del gobierno, hoy en día, los ciberataques pueden lograr, simple y clandestinamente, estas metas. Sin embargo, se debe tratar esta conclusión con mucha precaución. Es vagamente reminiscente de los rimeros teóricos del poder aéreo que previeron que el avión haría las guerras menos violentas porque acortaba su duración. En segundo lugar, si bien los ciberataques solo crean indirectamente la destrucción o interrupción en una nación objetivo, puede haber costes directos que pagar en el mundo físico. Las acciones digitales pueden ser enfrentadas con represalias cinéticas. Es posible que no se incluyan el sabotaje, espionaje y subversión en la definición de la guerra, pero han servido como el *casus belli* [motivo] para el comienzo de guerras en el pasado.




Si bien Rid ayuda a aclarar los parámetros de la discusión de la ciberguerra, al enfocarse en definiciones más precisas, conceptos más claros y metáforas más adecuadas, no hace un análisis suficientemente profundo de los ciberataques perpetrados por los grupos no estatales. En el capítulo de Rid sobre la "Subversión", solo se trata ligeramente el tema de grupos no estatales que usan el dominio digital para cambiar el comportamiento de Estados. Estos grupos deben ser ignorados porque otra pregunta en torno al *tweet* falso por la AP que causó una baja de la bolsa es, ¿quién es el Ejército Electrónico Sirio? ¿Es un grupo de "*hackers* [piratas] patrióticos" patrocinado por un Estado, una asociación no afiliada, una mezcolanza de personas que respaldan al régimen de Bashar Assad, o una combinación de todas estas posibilidades? Con el anonimato ofrecido por el ciberespacio, tanto Clarke como Rid concuerdan en el hecho de que el problema de atribución es difícil. Si el Ejército Electrónico Sirio es algún tipo de grupo no afiliado, el debate de la ciberguerra no capta la importancia de sus actividades. La ciberguerra entre países no ocupa todo el espacio en el debate, muy parecido a cómo la guerra interestatal no incluye todos los aspectos de la guerra. Grupos dispersos de *hacktivistas* [*hacker* activistas] toman parte en muchas de las mismas cibernéticas dañinas como hacen los Estado-Naciones. Esto demuestra una singularidad del domino cibernético. Gracias a la facilidad de entrada en el ciberespacio, los *hacktivistas* han cometido las mismas acciones en línea tales como la desconfiguración de sitios web, el robo de información privilegiada, ataques DDOS y el lanzamiento de *botnets* que forman parte del repertorio de los ciberataques realizados por países. En consecuencia,

los *hacktivistas* tienen casi el mismo poder en el ciberespacio que los hackers chinos infames del Ejército Popular de Liberación. Sin embargo, las directrices de los países que lanzan ciberataques por motivos políticos interrelacionados con la política exterior, los *hacktivistas* usan Internet para avanzar sus metas políticas y sociales que se centran en la misma Internet.

Los grupos tales como *Anonymous* y *Wikileaks* se consideran combatientes en una guerra para lograr la meta de libertad de Internet. Según ellos, la liberación humana comienza con la liberación de la información. En el libro de Julian Assange titulado, *Cypherpunks: Freedom and the Future of Internet*, este punto de vista pasa a ser el centro de atención. El nombre del libro proviene del movimiento *cypherpunks* que surgió a fines de la década de los años 80; sus integrantes eran partidarios de la disponibilidad y uso generalizado de la criptografía para proteger y fomentar la libertad humana contra la observación intrusiva del Estado. El libro es una recopilación de discusiones de sus creyentes colegas en el lema de los *cypherpunks* de "privacidad para los débiles, transparencia para los poderosos". Las discusiones ocurrieron con Assange, el fundador de *Wikileaks*, mientras el mismo estaba en arresto domiciliario en el Reino Unido esperando la extradición a Suecia, pero antes de que pidiera asilo político en la Embajada de Ecuador en Londres donde aún permanece. Las conversaciones revelan cómo el grupo se considera un participante en una lucha violenta contra lo que considera la "venidera distopia de observación constante", organizada por países y empresas poderosas. Sostienen que ellos y sus creyentes colegas han "tenido conflictos con casi todo Estado poderoso... Lo sabemos desde un punto de vista de combatiente, porque hemos tenido que proteger contra [ellos] a nuestro pueblo, nuestras finanzas y nuestras fuentes".

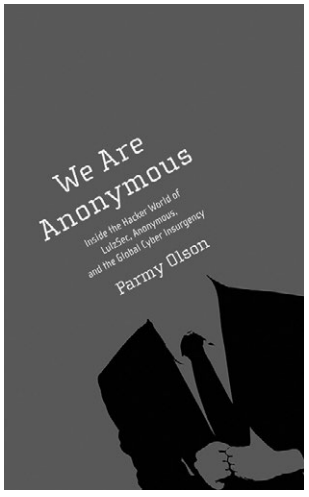



Sin embargo, no solo son los países el tema de estas discusiones. El motor de búsqueda *Google* es el tema del capítulo titulado "Espionaje en el sector privado". Hay un intercambio típico, pero que invita a la reflexión, entre dos integrantes del grupo:

> Jeremie: De hecho, la observación patrocinada por el Estado es un gran asunto que desafía la propia estructura de todas las democracias y cómo funcionan, pero también hay la observación privada y, posiblemente, la recolección de datos privada en masa. Considera, por ejemplo, a *Google*. Si eres un usuario estándar de *Google*, éste sabe con quién se comunica, a quién conoces, qué investigas, posiblemente tu inclinación sexual y tus creencias religiosas y filosóficas.
>
> Andy: [Google] sabe más de tí que tú mismo.
>
> Jeremie: Más que tu madre y, tal vez, más que tú. Google sabe cuándo estás y no estás en línea.
>
> Andy: ¿Saben lo que buscabas hace dos años, tres días y cuatro horas? Tú no te acuerdas; pero *Google* sí.

La retórica de las conversaciones puede ser demasiado dramática; se usan imprudentemente los términos como "campo de juventud Nazi" y "actos *Stasi* [seguridad del Estado de la antigua Alemania del Este]". El capítulo sobre "La Militarización del ciberespacio" comienza con Assange cuando sostiene que todas las comunicaciones vinculadas con Internet son vigiladas por las organizaciones de inteligencia militares. "Es como tener un tanque en su recámara. Es un soldado entre usted y su esposa mientras envía [textos]. Estamos viviendo bajo la ley marcial en cuanto a nuestras comunicaciones; pero no podemos ver los tanques" (33). El uso constante de metáforas, analogías y retórica de la guerra por el grupo, será desalentador para muchos. Sin embargo, es importante leer y hacerle frente a las implicaciones de sus argumentos en lugar de atracarnos con el uso (o abuso) del lenguaje. Lo más problemático es su ideología de libertad de Internet. Una ideología que se centra en el uso libre de la tecnología llega a ser irónica, especialmente, en el caso del Ejército Electrónico Sirio. Es incierto si el grupo de *cypherpunks* estaría de acuerdo con las actividades en línea hechas por otro grupo de *hacktivistas* en nombre del régimen tiránico en Damasco, un régimen que ha empleado el "kill switch" [interruptor de transmisiones] de Internet para controlar la salida de tráfico de Internet fuera de sus fronteras. Aunque Internet fuera completamente "liberada", las

actividades del Ejército Electrónico Sirio se permitirían ser perpetradas contra un Estado de vigilancia como Estados Unidos. En pocas palabras, no todo los casos de *hacktivismo* aportan a la liberación humana; es un arma de dos filos. Con el fin de parafrasear a un observador de tecnología, Farhad Manjoo, Internet solo es un conjunto de tubos sin ideología.

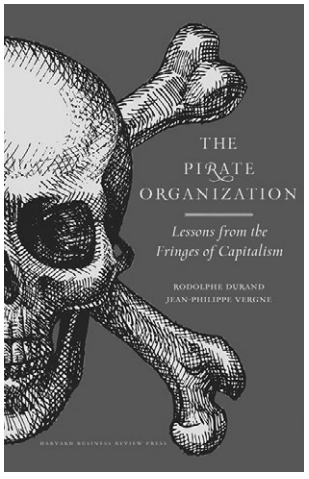



Si bien en el libro *Cypherpunks* se delinea la ideología adoptada por un núcleo de *hacktivistas*, el libro de Parmy Olson titulado, *We are Anonymous: Inside the Hacker World of LulzSec, Anonymous and the Global Cyber Insurgency*, es un relato periodístico ampliamente detallado de la historia de las acciones de un grupo cibernético que avanza esta ideología con sus ciberataques. A diferencia del núcleo de colaboradores de *Wikileaks*, en el libro de Olson se describe el auge del colectivo *hacktivista* que, hoy en día, se parece más a un movimiento social cibernético. Una de las más importantes observaciones de Olson es el concepto erróneo de que el grupo *Anonymous* es un "pequeño grupo de súper *hackers*". De hecho, solo unos cuantos en el colectivo eran *hackers* y los demás eran "solo jóvenes usuarios de Internet que querían hacer algo más que pasar el tiempo [en foros de chat anónimos]" (81). El llamamiento para el grupo *Anonymous* hizo eco del lema de los *cypherpunks*, "la información quiere ser libre".

Si los ataques contra Estonia y Georgia son el mejor ejemplo de la guerra cibernética en la esfera interestatal, los ataques llevados a cabo por *Anonymous* contra la Iglesia de Cienciología, PayPal y Sony son los mejores ejemplos del *hactivismo* en el mundo de *hackers*. Olson relata cómo *Anonymous* ganó notoriedad por sus operaciones en 2008 contra la Iglesia de Cienciología. En dicho año, la iglesia ejerció presión sobre el sitio web *YouTube* para quitar un vídeo que se filtró del integrante de la iglesia y actor Tom Cruise. Este tipo de presión ejercido por la Iglesia de Cienciología va en contra del principio de transparencia de *Anonymous*. En respuesta, el grupo *Anonymous* lanzó una operación para desplomar el sitio web de la iglesia que combinó ataques DDOS con travesuras tales como llamadas telefónicas con música repetitiva, constante envío de faxes de papel negro para agotar los cartuchos de tinta de la impresora y pedidos no solicitados de entregas de pizza y servicio de taxi. El grupo ha descubierto una causa común no solo con el fundador de *Wikileaks*, Julian Assange, sino también los movimientos *Occupy* y el informante convicto Bradley Manning. Olson también discute las numerosas operaciones de Anonymous dirigidas hacia las agencias e instituciones tales como PayPal, Mastercard y Visa, que rehusaron procesar los pagos por sitios web que recaudaban fondos para la defensa legal de Assange, Manning y las personas relacionadas con los movimientos *Occupy*.

Especialmente reveladora en el libro de Olson es la idea de que los principios del grupo también es cómo se estructura el grupo. La información en Internet es tan dispersa y descentralizada como *Anonymous*. Marshall McLuhan declaró que el "medio es el mensaje"; para los *hacktivistas*, el medio es el principio. La estructura del colectivo también es una reflexión de sus principios. Como grupo poco afiliado de activistas sociales en línea, *Anonymous* se enorgullece de no estar estructurado, sin jerarquía ni autoridad central. Esta estructura nebulosa tiene ventajas estratégicas, pero operacionalmente, según alega Olson en su capítulo "Guerra Civil", estas características han probado ser problemáticas. Debido a la estructura flexible, toda operación puede avanzar o ser cancelada de manera caprichosa. Además, como colectivo, los integrantes pueden hacer más que solo estar en desacuerdo con una operación planificada y optar por no respaldarla; pueden trabajar activamente contra la operación al lanzar contraataques contra las facciones con las cuales están en desacuerdo. También pueden prevenir que otros integrantes accedan los foros en línea, donde hay muchos integrantes. Las cismas internas han ocurrido entre integrantes de *Anonymous* que querían llevar a cabo operaciones de acuerdo con los principios *hacker*, otros querían ejecutar ataques motivados por principios contra organizaciones que suprimen la libertad humana en el mundo físico, e incluso otros, estaban completamente interesados en el *hacking* por "resentimiento y diversión".

Por último, a diferencia de un libro escrito para una audiencia popular, una obra académica, una colección de discusiones y una investigación periodística, *The*




*Pirate Organization: Lessons from the Fringes of Capitalism* es un ensayo escrito por Rodolphe Durand y Jean-Philippe Verne. Si bien los autores no se centran exclusivamente en el dominio cibernético, sí discuten la lucha histórica que existe entre los actores soberanos y los que buscan y sacan provecho de las áreas no gobernadas. Según ellos, una organización pirata—

> *…sin importar el tiempo, comparten las siguientes características: entran en una "relación" conflictiva con el Estado, especialmente si el Estado alega que es la única fuente de soberanía; operan de manera organizada, desde un conjunto de bases de apoyo ubicadas fuera del territorio sobre el cual el Estado normalmente alega el control soberano; desarrollan, en calidad de comunidades alternativas, un conjunto de normas discordantes que, según ellos, deben ser usadas para regular el territorio desconocido; y por último, representan una amenaza contra el Estado porque trastocan las propias ideas de la soberanía y territorio al oponerse al control del Estado y a las actividades de entidades legales que operaron bajo su jurisdicción, tales como empresas y monopolios.* (15)

Dada esta definición, *WikiLeaks* y *Anonymous* fácilmente se incluyen en los parámetros de una organización pirata. De hecho, los autores dejan claro que es erróneo concentrarse solo en la piratería marítima contemporánea. "Barbanegra, por ejemplo, tiene mucho más en común con un pirata cibernético que con un campesino somalí que usa un Kalashnikov para atacar un buque pesquero de una embarcación improvisada" (15) Con gran perspicacia, los autores documentan sucintamente la historia de las organizaciones piratas —los bucaneros de los siglos XVII y XVIII, los disyoqueis de radio en el mar, piratas cibernéticos en la web y piratas biológicos en el laboratorio. Según los autores, las organizaciones piratas surgen porque un nuevo territorio no gobernado está sujeto a la explotación. Como fue evidente en las críticas literarias de los cuatro libros previamente mencionados, el ciberespacio es el territorio sin gobernar más importante. Los *hacktivistas*, que se comprenden a través de la definición de una organización pirata, son, de distintas maneras, actores más centrales en el dominio cibernético que los Estado-naciones.

Los grupos tales como *Anonymous* y *Wikileaks*, sin duda alguna, representan un lado de la tensión entre la soberanía y los actores no estatales. Además, la manera usada por los autores para establecer la tensión entre este tipo de organización y el Estado, es un tónico útil para las personas como Clarke que consideran el *hacktivismo* una "forma bastante blanda de protesta en línea" (55). Las personas concentradas en una ciberguerra que ocurre entre Estado-naciones deben leer este libro para ganar una perspectiva más amplia sobre lo que les falta de la discusión más general de la ciberguerra.

Es una lástima que haya mucho que debatir en cuanto a la definición de las organizaciones piratas y su rechazo locuaz de la piratería marítima fuera del Cuerno de África; una comprensión más profunda demostraría que es una actividad más compleja que, de hecho, apoya su tesis. La piratería marítima contemporánea aprovecha las redes regionales y globales de financiación, seguros y transporte marítimo que ocurren muy lejos de los actos de secuestro en alta mar. La red es dispersa, bastante durable y resistente a la detección y eliminación.

Los cinco libros describen la creciente complejidad de la conceptualización de acciones maliciosas en línea. Muchas veces, los formuladores de política, profesionales de seguridad nacional y eruditos subestiman a los *hacktivistas* o piratas cibernéticos como grupos de descontentos socialmente torpes que derivan un sentido de pertenencia a través de hacer travesuras en línea. En su lugar, se concentran en la ciberguerra realizada o respaldada por Estado-naciones. Es fácil devolver los cambios complicados en el entorno de seguridad en el marco de Estado-naciones, pero hacerlo sería miope. Hemos hecho esto antes, no hace mucho y con efectos desastrosos. Cuando cayó el muro de Berlín y se perpetraron los ataques contra el Centro de Comercio Mundial, se ignoraban los actores no estatales a favor de los desafíos basados en Estado-naciones. Aún hoy en día, después de más de una década de guerra contra el Terrorismo y las guerras en Irak y Afganistán, nuestra comprensión de los temas tales como el terrorismo, insurgencia y guerra asimétrica no está completamente establecida.

Además, dada la novedad del dominio cibernético y su naturaleza rápidamente cambiante, sería erróneo hacer caso omiso de cualquier grupos que tenga como principio el deseo de definir el ciberespacio a través de actos en línea que desafían los elementos fundamentales de la seguridad nacional. Especialmente, si algunos de esos grupos se sienten acosados por gobiernos y rutinariamente usan la retórica de la guerra —"este dominio aparentemente platónico de ideas y flujo de información, ¿podría ser un concepto de la fuerza coercitiva? Una fuerza que podría modificar archivos históricos, intervenir las líneas telefónicas, separar a las personas, transformar la complejidad en escombros y construir muros, ¿como un Ejército ocupante?" (3). Los formuladores de política, profesionales de seguridad nacional y eruditos han subestimado a los grupos quienes piensan que actúan en defensa propia y que luego, atacan repentinamente, usando métodos imprevistos para nuestra sorpresa y detrimento.

Lo que está presente en varios grados en toda la literatura sobre el ciberespacio y la ciberguerra son los cinco debates distintos y constantes sobre este nuevo dominio y cómo actuar en el mismo. Los debates incluyen quién establece los límites del ciberespacio; cómo debe controlarse la información en línea; para quién debe estar disponible la información; pueden coexistir jerarquías y redes de personas en el ciberespacio; y cuál es la diferencia entre "la guerra" y "el crimen" en el ciberespacio.[1] En los libros revisados, es evidente que todo ataque cibernético o asalto cibernético no solo amplía los debates, sino también ayuda a dar más definición al dominio cibernético. Paradójicamente, los debates para definir el ciberespacio ocurren en el ciberespacio.

La paradoja probablemente llegará a ser cada vez más aguda con el avance de la tecnología cibernética y con la naturaleza cada vez más entrelazada de Internet en nuestras vidas cotidianas. Con la llegada de la "web portátil", tales como *Google Glass*, *Apple Iwatch* y, posiblemente, el *wi-fi* rociado, dicha naturaleza entrelazada llegará a ser personificada. No estaremos en el ciberespacio; seremos el ciberespacio. Estar preparado para este futuro hace de estos cinco libros una lectura esencial.

## Referencias bibliográficas

1. Hay una investigación muy sólida del debate sobre lo que es "la guerra", "crimen" y "violencia" en el dominio cibernético; véase la serie de artículos de John Stone, Gary McGraw, Dale Peterson, Timothy Junio, Adam Liff y Thomas Rid en el "Cyber War Roundtable" de la *Journal of Strategic Studies* 36, nro. 1 (febrero de 2013).