

Virtualmente Masivo: Comprendiendo la Concentración y el Poder de Combate en la Ciberguerra

CAPITÁN JOHN “STRIDER” COBB, FUERZA AÉREA DE LOS ESTADOS UNIDOS

La cantidad tiene una calidad totalmente suya.
—Atribuido apócrifamente a Josef Stalin,
discutiendo la producción de armamento ruso
durante la Segunda Guerra Mundial

LA FUERZA AÉREA DE EE.UU. define “masa” como “la concentración de los efectos del poder de combate en el lugar y el momento más ventajoso para lograr resultados decisivos”¹; en el Air Force Doctrine Document (Documento de Doctrina de la Fuerza Aérea) (AFDD) 3-12 se hace eco de esta definición a la vez que se destaca que las fuerzas cibernéticas “deben integrarse y sincronizarse con otras fuerzas”². Pero, ¿qué significa esto para la estrategia en el ámbito cibernético? Algunos han sugerido que el concepto de masa (concentración) ya no aplica en el ciberespacio y que un puñado de agresores podría lanzar ataques devastadores desde cualquier parte del mundo.³ El Col Gregory Rattray (USAF, Retirado) en “Strategic Warfare in Cyberspace” (Guerra estratégica en el ciberespacio) discute las funciones de apoyo, tales como inteligencia de la red, localización de blancos y desarrollo de herramientas, que pueden hacer que los ataques cibernéticos sean más eficaces. Esto sugiere otra perspectiva en cuanto a la concentración—una que incluye no tan solo los operadores iniciales atacando blancos, sino el resto de operadores que se requieren para organizar un equipo capaz de lanzar consistentemente ataques exitosos ya que él sugiere que los analistas y los programadores quizás tengan que sobrepasar la cifra de personas que realmente llevan a cabo los ataques.⁴ Esta es una diferencia significativa, y una pregunta importante que resolver, pero los temas de personal no son la única manera para comprender la concentración en la ciberguerra.

También podemos pensar sobre la concentración en términos de volumen del tráfico de ataque—al nivel más sencillo, en términos de cantidades de bits o paquetes que pasan hacia el blanco. En otras ocasiones una definición más significativa de volumen podría ser el número de virus que son liberados simultáneamente, típicamente desde la perspectiva de los firewalls (servidor de seguridad) y herramientas antivirus que tratarán de bloquear el malware (programas maliciosos). Lo que los agresores o investigadores consideran un virus podría utilizar un código que se modifica a sí mismo para que luzca como cientos de virus diferentes que tratan de colarse a hurtadillas. Por otro lado, los números de nodulos bajo ataque podría ser una definición útil de volumen—al nivel más bajo, la cantidad de dispositivos que están siendo atacados; a un nivel más elevado, la cantidad de ámbitos en la red o sitios físicos (por ejemplo, bases) bajo ataque. Esto es una simplificación excesiva, pero se puede pensar que estos aspectos diferentes de “volumen” son una versión ciberespacial de potencia de fuego. Una tercera manera de entender la concentración en la ciberguerra es en términos de la solidez o supervivencia de las redes que se están defendiendo. Una red con muchos dispositivos de repuesto, ancho de banda y rutas redundantes tendrá más posibilidades de supervivencia o al menos se recuperará más rápido contra una variedad de ataques. Asimismo, la cantidad y las destrezas de los técnicos que mantienen y defienden las redes bajo ataque es a menudo una manera de pasar por alto el tomar en cuenta la concentración. Por último, la mayoría de los países estarán más limitados durante ac-

ciones cibernéticas en tiempo de paz que cuando lanzan ataques cibernéticos en tiempo de guerra, de manera que la concentración puede que no adopte tantos aspectos durante acciones encubiertas durante tiempo de paz como en una guerra cibernética abierta.

En vista de que muchos lectores no están familiarizados con cómo los firewalls y el software antivirus protegen las redes, he aquí una explicación rápida. Típicamente un firewall explora el tráfico que entra o sale de una red local, mientras que el software antivirus explora el disco duro de una computadora en particular. Hay excepciones, tales como los Sistemas de Detección de Intrusión basados en la red o los filtros de la lista de control de acceso de enrutadores, pero la mayoría de los dispositivos que protegen una red son firewalls o antivirus tradicionales—y la mayoría de las herramientas alternativas utilizan reglas similares para sus exploraciones y filtros.⁵ Hay dos maneras principales que ellos utilizan para explorar en busca de virus, firmas y heurísticas. La manera más común para las defensas de una red de buscar malware es verificando firmas, por lo regular apareando parte de, o de todo un archivo (o paquete de red) contra una lista de malware conocido. Esto puede ser bastante eficaz contra ataques conocidos, pero obviamente no detecta la mayoría de ataques nuevos, y a menudo no detectan ataques conocidos que han recibido cambios inclusive menores.⁶

La otra manera como las defensas de la red encuentran malware es empleando “heurística”—en lugar de buscar un texto específico o archivos que se sabe son maliciosos, buscan patrones o comportamientos sospechosos. Esto es más eficaz, aunque no es perfecto, para encontrar ataques nuevos (“día cero”) y mucho mejor para atrapar variaciones nuevas de ataques antiguos. Sin embargo, la mayoría de los algoritmos heurísticos tienen índices positivos falsos elevados. En vista de que con frecuencia muestran o bloquean aplicaciones y tráfico legítimo más a menudo que ataques reales, pueden demandar mucho más tiempo y ser frustrantes de operar. Estos filtros enfrentan problemas estadísticos similares a algunas detecciones de cáncer⁷—en vista de que la gran mayoría del tráfico en la red no es malicioso, mostrando 95% de virus y 1% de tráfico legítimo resultarán en más positivos falsos que virus reales.⁸ Muchos productos comerciales emplean una combinación de ambos métodos, y los investigadores de seguridad están trabajando en varias maneras alternativas de detectar ataques, pero hoy todas, salvo la mayoría de las redes más importantes y seguras, tienden a depender en gran medida en la detección basada en la firma ya que la falta de recursos hace que otros métodos no sea factibles.⁹ Como resultado, en muchas redes militares e industriales grandes los ataques nuevos no se detectarán hasta que sea demasiado tarde y ya hayan invadido la red.

A causa de estas limitaciones, en el estado actual del ciberespacio los efectos de un ataque no son siempre en proporción a su sofisticación. El tamaño, complejidad, defensas e interconexión del blanco determinan cuán sofisticado debe ser un ataque para tener éxito. Las limitaciones políticas de un agresor, tales como exigir furtividad y no atribución—o atribución falsa—a menudo aumenta el nivel de sofisticación requerido, al igual que la carga de trabajo para los agresores. Sin embargo, en vista de que esos factores varían entre blancos militares y de infraestructura importantes, algunos blancos críticos son prácticamente imposibles de asegurar sin paralizar su capacidad de funcionar, mientras que otros—principalmente blancos más pequeños—aún si son menos críticos, puede que requieran ataques sumamente sofisticados. Los ataques de DoS (negación de servicio) pueden a menudo darse el lujo de ser menos sofisticados que los intentos de espionaje; las redes grandes, distribuidas geográficamente y de nodulos múltiples ofrecen más oportunidades para introducir un ataque y hacer que la labor de vigilar las defensas sea más difícil. Hardware y software disponible en el mercado (COTS por sus siglas en inglés) se puede atacar con entrenamiento y herramientas estándar, mientras que los sistemas especializados que a menudo se encuentran en contextos de inteligencia, nuclear o infraestructura puede que requieran reconocimiento extenso y ataques hechos a la medida.¹⁰

Aunque en su obra hay suposiciones sumamente dudosas, Thomas Rid¹¹ está correcto al destacar que ataques furtivos, sumamente precisos y “estratégicos” como el Stuxnet¹² requieren re-

cursos significativos para prepararlos y no se pueden volver a usar fácilmente. Este tipo de ataque requiere docenas de analistas de inteligencia, programadores y operadores para diseñarlo, montarlo y lanzarlo. Mientras que grupos diferentes pueden que combinen algunas o todas esas funciones en el adiestramiento que recibe un guerrero cibernético, este tipo de ataque contra un blanco sumamente defendido aún requerirá meses de trabajo de docenas de personal bien entrenado. En la medida en que una campaña cibernética trata de corromper o desactivar grandes cantidades de blancos protegidos y autónomos, claramente necesitará inversiones significativas y esas inversiones aumentan si se necesitan furtividad y no atribución—particularmente en vista de que los equipos que trabajan en el blanco autónomo no estarán disponibles para trabajo de ciberinteligencia de “rutina” que supuestamente aún será necesario.

Sin embargo, también hay muchos blancos ciberespaciales que son defendidos menos vigorosamente y algunos de ellos pueden ser blancos de gran valor. Si bien las instalaciones nucleares como las que fueron atacadas por Stuxnet probablemente permanecerán muy protegidas y defendidas cuidadosamente, muchos sistemas militares e industriales requieren un acceso más amplio para ser eficaces. Por ejemplo, las redes de energía no pueden funcionar eficazmente a menos que estaciones de energía se estén comunicando entre sí constantemente. Puede que no estén en “en línea” en el sentido de enviar tráfico no codificado directamente por la Internet, pero esta interconexión aún se puede emplear para controlar, degradar o destruir toda la red con un solo ataque—aunque se debe destacar que en países grandes como Estados Unidos o Rusia, “la red de energía” es en realidad un conjunto de redes regionales sin conexión directa: por ejemplo, EE.UU. cuenta con tres redes regionales¹³ y Rusia, aunque más centralizada que la de EE.UU., cuenta con siete regiones con interconexiones limitadas.¹⁴ Muchas redes militares enfrentan la misma situación—tienen que unir un gran número de unidades y bases para proveer los efectos de multiplicador de fuerza de la que todos los militares modernos dependen, lo que dificulta evitar que ataques sofisticados se esparzan una vez que comprometen un nódulo en la red.

En este entorno, la segunda definición es probablemente una mejor manera para entenderlo. Algunos blancos son vulnerables a los ataques que pueden ser creados por un solo equipo y luego lanzados contra toda una red y, si tienen éxito, pueden obstaculizar toda una región. Los servicios públicos enlazados son un ejemplo, particularmente las redes de energía, que tienden a ser redes más grandes y más interdependientes que otras redes de servicios públicos. Otras podrían ser las redes militares para C2, logística y concienciación de la situación operacional. Esas funciones son necesarias al nivel táctico u operacional, y por lo tanto requieren típicamente una red compartida a lo largo de una gran cantidad de nódulos críticos. Al extremo sumamente sencillo del espectro de posibles ataques cibernéticos, la concentración en un ataque de negación de servicio distribuido (DDoS, por sus siglas en inglés) es sencillamente la cantidad de ancho de banda empleado para intentar abrumar la red objetivo. A medida que progresamos en el espectro, si un ataque emplea un código que se auto modifica, el defensor puede que necesite bloquear no una sino cientos de firmas nuevas de virus en docenas y hasta miles de perímetros de la red (cada firewall protegiendo el área o la red local tiene que ser actualizada con todas las firmas de virus relevantes para poder bloquearlas). En algunos casos, la cantidad de aprovechamientos a la vulnerabilidad (exploit) que los virus están utilizando puede que sea más relevante que cómo un virus se muta para colarse a hurtadillas a través de los filtros—una activación es el código malicioso que emplea un error en el software de un blanco para controlar el sistema; cuando se explotan más vulnerabilidades, es más probable que el virus tenga éxito.¹⁵ La mayoría de las redes militares cuentan con técnicos que invierten grandes cantidades de tiempo intentando corregir las vulnerabilidades conocidas antes de que un ataque se aproveche de ellas, a sabiendas que las firewalls y los antivirus no impiden todos los ataques. Un ataque que solamente emplea un aprovechamiento fracasará si la vulnerabilidad correspondiente está completamente reparada. Si bien reparar rápida y completamente es un problema muy difícil¹⁶, hay herramientas que permiten que las redes modernas grandes reparen la mayoría de los sistemas en cuestión

de días.¹⁷ Si un ataque emplea más de un aprovechamiento de la vulnerabilidad (exploit), aumenta el reto al defensor; sin embargo, los aprovechamientos, particularmente aprovechamientos de día cero, pueden ser recursos de inteligencia valiosos, y muchas autoridades advierten contra revelarlos arbitrariamente.¹⁸ Por otra parte, estos aprovechamientos son más numerosos de lo que las personas se imaginan; por ejemplo, entre enero y mayo de 2012, Microsoft anunció—y difundió parches—para 31 vulnerabilidades graves en el sistema operativo Windows 7 y sus aplicaciones comunes (por ejemplo, Microsoft Office).¹⁹

En cambio, hay ataques en los que la concentración se entiende mejor como el número de redes señaladas para ser atacadas por un ataque o series de ataques. En la obra anterior del autor se discuten ataques que pueden desconectar las redes locales del control centralizado o respuesta²⁰; en esos tipos de ataques la cantidad de lugares geográficos o las redes locales puede que tengan más significado que el personal utilizado para crear los ataques o la variedad de ataques empleados. Esto aplica principalmente a los ataques de negación de servicio (DoS) y de negación de servicio distribuido (DDoS)²¹, o defensas de la red sumamente centralizadas—si hay defensores de la red experimentados en cada lugar, ellos deben poder resolver ataques sencillos relativamente fácil, particularmente ataques DDoS, mientras que un método más centralizado en cuanto a la defensa de la red puede que conlleve en desconectar a los defensores de las redes debajo de ellos, o a que los defensores abarquen demasiado como para poder reaccionar en todos los lugares simultáneamente.

Por otra parte, en estos tipos de ataques el personal puede ser un elemento crítico de concentración para los defensores; a diferencia de ataques sumamente selectivos, estos tipos de ataques DoS pueden ser sumamente asimétricos. Aunque están sujetos a la carrera armamentista entre agresores y defensores, a medida que los filtros, exploraciones y herramientas de la red se apresuran para ponerse al día con las técnicas de piratería, estos ataques DoS los pueden lanzar equipos bastante pequeños, y pueden requerir un gran número de defensores para arreglar y limpiar cada red local bajo ataque.

La medida relevante del poder de combate en el ciberespacio varía dependiendo de los tipos de ataque en juego y las redes que necesitan defensa. Si bien los técnicos y los operadores duchos siempre son importantes²², el balance adecuado entre calidad y cantidad depende de los ataques y herramientas que un militar anticipa usar y enfrentar. En vista de los límites presupuestarios que todos los militares enfrentan, y la amplia gama de posibles ataques cibernéticos, estos son compromisos que todos los militares deben hacer. Si la amenaza principal es de ataques furtivos similares al Stuxnet, cuya intención es dañar datos furtivamente o dañar invisiblemente instalaciones específicas, entonces los defensores de la red tienen que estar bien capacitados, especialmente en técnicas forenses. Sin embargo, puede que no necesiten ser más numerosos que sus agresores, y las defensas de la red a menudo pueden darse el lujo de atrapar ataques después que el ataque ha tenido éxito, al menos en parte, ya que los ataques a menudo se esparcirán lentamente y causarán el daño lentamente para evitar ser detectados. En cambio, si la amenaza principal son ataques concebidos para interrumpir o aislar rápidamente los sistemas críticos, los defensores de la red tendrán que ser más numerosos y sus destrezas deben enfocarse en contrarrestar ataques ocultos y reconstruir los sistemas que un agresor dismantela exitosamente. Para poder contar con suficientes conocimientos acerca de posibles adversarios para saber cuál caso aplica, por lo regular requiere una inversión significativa en personal de inteligencia enfocado en cibernética; más personal de ese tipo será necesario para poder llevar a cabo ataques exitosos en respuesta.²³ Es posible que ambos tipos de ataque se puedan lanzar simultáneamente, pero en la mayoría de los casos si estos ataques van dirigidos a las mismas redes y sistemas interferirán entre sí, a menudo resultando en un agresor perdiendo el control de los ataques más precisos; lo que es más probable es que los ataques encubiertos DoS o DDoS ataquen un área mientras que una red o sistema diferente es atacado más cuidadosa y furtivamente, lejos del ataque obvio. Por supuesto, en cualquier conflicto hoy en día coordinar y ar-

monizar ataques cibernéticos—entre sí y de ataques cinéticos en la proximidad—es un esfuerzo de planificación crítico.²⁴

Un vistazo a la historia del poderío aéreo podría ayudar a aclarar estos métodos diferentes—de alguna manera, los agresores cibernéticos enfrentan un problema similar al que enfrentaron la USAAF y la RAF en sus campañas de bombardeo contra el sistema industrial de Alemania durante la Segunda Guerra Mundial. Los ataques sumamente específicos (al estilo Stuxnet)—eliminar un puñado de blancos aislados de gran valor con un solo ataque elaborado con precisión, a menudo lenta y furtivamente—pueden ser considerados similares al método de bombardeo estratégico empleado por EE.UU. durante la Segunda Guerra Mundial. En este método, el agresor encuentra un puñado de nodulos críticos e invierte grandes cantidades de personal, tiempo y poder de combate para derribar esos sistemas²⁵, confiando de que el enemigo no podrá funcionar sin esos nodulos críticos. En comparación, las diferentes formas de ataques DoS pueden considerarse similares al método británico de atacar—en lugar de atacar directamente sistemas críticos, y a menudo sumamente defendidos, el agresor intenta derribar algún aspecto de la red local o regional de la cual esos sistemas críticos dependen. El método para atacar de la RAF durante la Segunda Guerra Mundial se basaba inicialmente en atacar fábricas claves, pero después de fracasos iniciales y grandes pérdidas, la RAF cambió a sencillamente bombardear las ciudades industriales principales, atacando todo el ecosistema industrial en lugar de una serie de “nódulos claves” discretos. A pesar de un inicio desalentador similar, la USAAF atacaba lo que consideraba nodulos vitales—principalmente la fabricación de aeronaves, combustible, transporte y rodamiento de bolas—desde 1943-1945, intentando aplastar el sistema industrial alemán destruyendo o desactivando un puñado de nodulos claves (tales como la fábrica de rodamientos de bolas en Schweinfurt y la refinería en Ploesti).²⁶ Por supuesto, en ejecución, ni el método de la USAAF ni el de la RAF no siempre eran tan diferentes, los B-17 y B-24 de la USAAF a menudo no podían lanzar bombas en el blanco con la interferencia del clima y las defensas alemanas²⁷, pero los dos métodos de ataque tienen similitudes con los equivalentes cibernéticos discutidos anteriormente. Desde luego, las PC y los interruptores en una red militar son blancos menos controvertidos que la población de ciudades industriales, pero muchos ataques DoS son menos precisos y más probables de extenderse tener consecuencias no intencionales en el ciberespacio civil. Resulta importante destacar que, dependiendo de la situación, ambos tipos de ataque pueden ser muy eficaces; los ataques DDoS en Estonia en el 2007 constituyen un ejemplo de un ataque DDoS que tuvo impactos significativos²⁸, mientras que los supuestos ataques DoS coordinados por Rusia dañaron la capacidad de Georgia de responder a ataques armados rusos en el 2008.²⁹

Por consiguiente, si bien destruir un solo reactor es extremadamente difícil y típicamente requiere planificar cuidadosamente un ataque completamente nuevo, interrumpir el C2 o la logística militar es a menudo práctico empleando herramientas “comerciales” para la piratería con el fin de organizar un ataque relativamente no refinado. A diferencia de la mayoría de los demás ámbitos, en el ciberespacio un blanco más distribuido y más grande es mucho más fácil de atacar y paralizar. En discusiones recientes sobre la ciberguerra a menudo se ha confundido el espionaje con la guerra, y como resultado algunos comentaristas han dado por sentado que el aprovechamiento de las vulnerabilidades es más valioso de lo que sería en tiempo de guerra, que la furtividad es más necesaria de lo que sería en tiempo de guerra y que las redes grandes de la milicia o infraestructura poseen las mismas defensas de los que a menudo poseen sistemas pequeños de inteligencia o nucleares.³⁰ Estas malas interpretaciones distorsionan la naturaleza de la concentración en la ciberguerra, y pueden resultar en errores graves al organizar unidades de ciberguerra o crear defensas de la red. Si bien el espionaje cibernético—inclusive ataques cibernéticos encubiertos en tiempo de paz—tienden a incluir ataques furtivos y sumamente precisos, los ataques cibernéticos en una guerra abierta pueden abarcar todas las diferentes formas de concentración y poder de combate discutidos anteriormente. Las limitaciones diplomáticas y políticas puede que varíen de un conflicto “solamente cibernético” a una guerra tradicional (ci-

nética) que incluye ataques cibernéticos, pero ambos probablemente incluirán ataques abiertos que sacrifican la furtividad para atacar más fuerte y más rápido, permitiendo ataques generalizados con recursos limitados.

La concentración es importante en la ciberguerra, pero su significado varía dependiendo de la naturaleza del ataque y del blanco. Si bien el nivel táctico no siempre será impactado muy severamente, particularmente en las milicias o fuerzas terrestres que no son estadounidenses donde las redes no se emplean demasiado, al nivel operacional las milicias modernas dependen en gran medida de sus redes para la logística y la concienciación de la situación. Estas redes son “centros de gravedad”, y si se pueden interrumpir pueden reducir significativamente la eficacia de las fuerzas que dependen de ellas. Aunque ataques sumamente precisos pueden ser devastadoramente eficaces, también hay alternativas DoS que pueden paralizar cuando se llevan a cabo correctamente. Las definiciones correctas de concentración y poder de combate en la ciberguerra son fluidas, al igual que el ciberespacio en sí, y las milicias que se limitan a una fase corren el riesgo de la derrota cuando un adversario ataca en maneras que no son iguales ni a su doctrina ni a su organización. □

Notas

1. Air Force Doctrine Document (Documento de Doctrina de la Fuerza Aérea) (AFDD) 1, pág. 32.
2. AFDD 3-12, Cyberspace Operations (Operaciones Ciberespaciales), pág. 16.
3. Martin Libicki, *Cyberdeterrence and Cyberwar* (Ciberdisuasión y Ciberguerra) (Santa Monica, CA: RAND Corp, 2009), pág. 59. Disponible en <http://www.rand.org/pubs/monographs/MG877.html>.
4. Gregory J. Rattray, *Strategic Warfare in Cyberspace* (La guerra estratégica en el ciberespacio) (Boston: MIT Press, 2001), págs. 100, 464.
5. Consultar Edward Skoudis, ed. Franklin D. Kramer, Stuart H. Starr y Larry K. Wentz, “Information Security Issues in Cyberspace” (Temas sobre seguridad en el ciberespacio), *Cyberpower and National Security* (Ciberpoder y la seguridad nacional) (Dulles, VA: Potomac Books, 2009).
6. “Antivirus Software” (Software antivirus), Wikipedia, http://en.wikipedia.org/wiki/Antivirus_software. Consultado el 30 de mayo de 2012.
7. Maia Szalavitz, “Why People Stick with Cancer Screening, Even When it Causes Harm” (Por qué las personas continúan con las pruebas de cáncer inclusive cuando son dañinas), *Healthland*, Time.com, <http://healthland.time.com/2012/05/25/why-people-cling-to-cancerscreening-and-other-questionable-medical-interventions-even-when-they-cause-harm/>.
8. “Antivirus Software”, Wikipedia.
9. Para más información, consultar, see Shon Harris, *CISSP All in One Exam Guide* (Guía para examen CISSP), 4th ed. (New York: McGraw Hill, 2008), págs. 250-257.
10. Sin embargo, esos sistemas especializados puede que sean más débiles y vulnerables que sus contrapartes estándar COTS una vez que los agresores los entienden—especialmente sistemas de infraestructura, que a menudo fueron concebidos sin pensar en lo absoluto en la seguridad.
11. Thomas Rid, “Think Again: Cyberwar” (Piense nuevamente: Ciberguerra), *Foreign Policy* (Política Exterior), 27 de febrero de 2012, <http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=0,2>.
12. Stuxnet fue un virus troyano sumamente significativo que se propagó en unidades de memoria flash (thumb drives) que infiltraron y sabotearon instalaciones nucleares iraníes en el 2010 por varios meses antes de ser detectados. Consultar “The Stuxnet Outbreak” (La epidemia Stuxnet), *The Economist*, 30 de septiembre de 2010. <http://www.economist.com/node/17147818>.
13. Richard A. Clarke y Robert K. Knake, *Cyberwar: The Next Threat to National Security and What to Do about It* (La próxima amenaza a la seguridad nacional y qué hacer) (New York: HarperCollins, 2010), 167.
14. Rinat Abdurafikov, “Russian Electricity Market: Current State and Perspectives” (El mercado de la electricidad rusa: Estado actual y Perspectivas), VTT Technical Research Centre of Finland (Centro Técnico VTT de Finlandia), 2009. <http://www.vtt.fi/inf/pdf/workingpapers/2009/W121.pdf>.
15. “Exploit” (Aprovechamiento de la vulnerabilidad), Wikipedia, [http://en.wikipedia.org/wiki/Exploit_\(computer_security\)](http://en.wikipedia.org/wiki/Exploit_(computer_security)), consultado el 27 de mayo de 2012. Consultar también a Harris, pág. 62.
16. Ver Stephen Northcutt, et al, *Inside Network Perimeter Security*, 2nd ed. (Dentro de la seguridad del perímetro de la red, 2a Edición) (Indianapolis: Sams Publishing, 2005), págs. 257-258 para una discusión de los factores que hace que la reparación (patching) sea una dificultad grande en la red.
17. *Microsoft Security Update Guide*, 2nd ed. (Guía para actualización de seguridad Microsoft), Microsoft, 2011 <http://www.microsoft.com/en-us/download/details.aspx?id=559> Para un breve resumen de un sistema de patching, consultar “WSUS Overview”, Microsoft Technet, <http://technet.microsoft.com/en-us/library/cc539281.aspx>.

18. Libicki, p. 57.
19. "Patch Tuesday (January-May 2012)" Microsoft Technet, <http://technet.microsoft.com/en-us/security/bulletin/ms12-jan>, <http://technet.microsoft.com/en-us/security/bulletin/ms12-feb>, <http://technet.microsoft.com/en-us/security/bulletin/ms12-mar>, <http://technet.microsoft.com/en-us/security/bulletin/ms12-apr>, <http://technet.microsoft.com/en-us/security/bulletin/ms12-may>.
20. John Cobb, "Centralized Execution, Decentralized Chaos: How the Air Force is Poised to Lose a Cyber War" (Ejecución centralizada, caos descentralizado: Cómo la Fuerza Aérea está destinada a perder una ciberguerra), Air and Space Power Journal, Verano 2011, http://www.au.af.mil/au/cadre/aspj/airchronicles/apj/2011/2011-2/2011_2_16_cobb.pdf.
21. DoS se refiere a cualquier ataque enfocado en desmantelar un sistema o red sobrecargándola. EL DDoS es un tipo de DoS específico donde cantidades masivas de tráfico de la red proveniente de computadoras alrededor del mundo se envían para abrumar el servidor o la red objetivo, causando que se congele y deje de responder al tráfico legítimo. Ver Harris págs. 1010-1013.
22. Para una discusión más profunda sobre este tema, consultar Kamal Jabbour, "Cyber Vision and Cyber Force Development" (Visión cibernética y desarrollo de la fuerza cibernética), Strategic Studies Quarterly, Primavera 2010, www.au.af.mil/au/ssq/2010/spring/jabbour.pdf.
23. Rattray, pág. 142.
24. Consultar el AFDD 3-12, págs. 25-26 para una discusión adicional sobre cómo armonizar ataques cibernéticos.
25. Elinor Mills, "Expert: Stuxnet was Built to Sabotage Nuclear Plant" (Experto: Stuxnet fue creado para sabotear una planta nuclear). Insecurity Complex, CNET.com, http://news.cnet.com/8301-27080_3-20017201-245.html?tag=mncol;1n.
26. Geoffery Perret, *Winged Victory* (New York: Random House, 1993), págs. 240-244.
27. Rattray, pág. 280.
28. Los ataques DDoS que supuestamente fueron coordinados por Rusia ocasionaron interrupciones significativas a los bancos y gobierno de Estonia (Rusia negó cualquier participación oficial). Ver Clarke y Knake, págs. 11-16.
29. David Hollis, "Cyberwar Case Study: Georgia 2008" (Estudio sobre la ciberguerra: Georgia 2008). Small Wars Journal, 6 de enero de 2012, <http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008>, p. 5.
30. Ejemplos de estas suposiciones erróneas incluye Rid (especialmente pág. 5) y Libicki (ver págs. 56-59, y compare a las guías de la industria sobre el patching mencionado anteriormente, particularmente Northcutt, et al—una red grande de reparación requiere un esfuerzo significativo durante el transcurso de días, a menudo semanas, y cuando se hace muy rápido el patch en sí puede dañar sistemas críticos).



EL Capitán John M. Cobb, USAF (BS, USAFA) es Jefe, Ingeniería de Informática para la Dirección de Educación en Logística y Comunicaciones en el Cuartel General de la Universidad del Aire, Base Aérea Maxwell, Alabama. En este puesto, él es responsable de crear el software educativo que se emplea en la Fuerza Aérea, asesorar a los líderes de la dirección sobre la tecnología educativa y asesorar a los suboficiales programadores. Antes de desempeñar su cargo actual, el Capitán Cobb se desempeñó en calidad de Oficial a Cargo, Operaciones de la Red en la Base Aérea Misawa, Japón, donde estuvo a cargo de mantener y asegurar una red base para más de cuatro mil miembros del servicio conjunto. El Capitán Cobb fue desplegado en apoyo a las operaciones Nuevo Amanecer y Paz Duradera, y es egresado de la Escuela Superior para Oficiales de Escuadrón.