Guerra cibernética y disuasión

Aplicación de un marco teórico general

Capitán Isaac Nacita, Fuerza aérea de EE.UU.
Teniente Coronel Mark Reith, PhD, Fuerza aérea de EE.UU.

Introducción

La historia militar, cuando se estudia superficialmente, da argumentos en apoyo de cualquier teoría u opinión.

—Paul Bronsart von Schellendorf

En septiembre de 1870, después de solo seis semanas de lo que muchos pensaban que iba a ser una guerra prolongada, los espectadores prusianos abuchearon a Louis-Napoléon Bonaparte cuando fue llevado cautivo a lo que ahora es Kassel, Alemania. Era una descripción apropiada de la desgracia nacional francesa.[1] Sus estructuras militares antes de la guerra y la falta de planificación estratégica tenían parte de la culpa. El archivador nacional Dallas D. Irvine apunta, "(el sistema francés) fue casi completamente efectivo en excluir la inteligencia del ejército del estado mayor y del alto mando. La consecuente falta de inteligencia a nivel superior puede atribuirse a todos los defectos inexcusables de la política militar francesa".[2] No obstante, las fuerzas armadas, influidas por la idea de que Francia había perdido debido a la falta de moral que un método ofensivo habría proporcionado, se reagruparon y se volvieron a concentrar, esta vez adoptando un "ataque a ultranza". Esta doctrina fue la estrategia militar francesa al entrar en la Primera Guerra Mundial, y se demostró casi de inmediato que estaba espectacularmente equivocada. Los franceses perdieron 300.000 soldados durante el primer mes de la guerra. No obstante "el legado de la adopción de la ofensiva fue incluso más terrible en otro sentido. La matanza arbitraria que engendró produjo una reacción similar en todos los que la vivieron, una determinación nefasta para impedir que nunca se volviera a producir una matanza así".[3] Una vez más, pasaron a la defensiva, y en los años anteriores a la Segunda Guerra Mundial construyeron la línea Maginot. Los alemanes simplemente no pasaron por sus puntos fuertes, sino que se abrieron paso por una línea francesa más débil en un terreno inesperado. La línea Maginot es ahora una metáfora de algo que crea una falsa sensación de seguridad.

Hay un dicho por el que los políticos y generales están luchando siempre la última guerra, que se enfatiza cuando cambian rápidamente las armas y características de la guerra. Sin embargo, si esto es cierto, a menudo no se debe a una incapacidad de aprender lecciones de conflictos anteriores, sino de "aprender excesivamente" o compensar en exceso por los fracasos y experiencias del pasado. En realidad, este no es un problema de aprendizaje, sino de sacar malas consecuencias de casos históricos, lo que lleva a aplicar mal la doctrina la próxima vez.

El Departamento de Defensa reconoce ahora que la guerra se ha extendido al ciberespacio, y mi tesis central es que las fuerzas armadas a menudo sufren de una falta de conversaciones significativas referentes a los problemas a los que se enfrenta en ese dominio. La falta de discurso se debe parcialmente a metáforas y analogías mal adoptadas extraídas de otros dominios bélicos y ejemplos históricos, y en general a una falta de enmarcado estratégico riguroso del problema y sus soluciones potenciales.

El problema

¿A qué problema no se enfrena Estados Unidos en el ciberespacio? El mundo en línea refleja la totalidad de los temas sociales humanos. ¿Está teniendo lugar una guerra cibernética? El ciberespacio es un "entorno disputado", pero también lo es el mercado comercial global. Karl von

Clausewitz llamó a la guerra un conflicto de voluntades, una acción política llevada a cabo por otros medios, pero también la caracteriza con una fuerza física que parece requerir un dominio físico.[4]

Algunos, por lo tanto, razonan que se producen actos de sabotaje, espionaje y subversión, y que se llevan a cabo a través de un medio diferente, pero no mediante una guerra.[5] Martin C. Libicki sugiere la posibilidad de una guerra "clandestina", implicando que es posible que la población general no esté completamente al tanto de lo que está ocurriendo.[6] Otros restan importancia a la terminología porque se han exagerado mucho las cosas a las que nos hemos enfrentado hasta ahora y no merecen este título. En muchos casos los efectos reales debidos a ataques ciberespaciales maliciosos son menores que los que ocurren debido a eventos naturales o accidentales. Existe un caso algo humorístico en que, un año después de unos presuntos ciberataques rusos en Georgia, una mujer de 75 años cortó por accidente un cable con una pala e impidió el acceso a internet en toda Armenia, superando a Rusia en términos de efecto total.[7] Todo esto se complica también por la tendencia a tratar todos los problemas sociales de EE.UU. usando una terminología bélica. Estamos luchando una "guerra contra la pobreza" y una "guerra contra las drogas". Hay victorias y hay derrotas, pero raramente hay un ganador y un perdedor claros.

A pesar de estas cosas, el Departamento de Defensa ya ha reconocido el ciberespacio como un dominio bélico. Pero la naturaleza del problema es central a la cuestión de disuadir o imponerse en el ciberespacio. Una fuente dice, "¡dejen de debatir cómo llamar al problema y ayúdennos!"[8] El punto se entiende, pero si el problema no se entiende, no debemos esperar ninguna ayuda significativa.

El Consejo Científico de Defensa (DSB) presenta algunos ejemplos de ciberataques que podría usar para enmarcar el problema. Apunta a los ataques de negación de servicio de Irán en Wall Street en 2012–13, al pirateo informático de Corea del Norte de Sony Pictures, al robo de propiedad intelectual chino y a la presunta participación de Rusia en las elecciones presidenciales de 2016. El documento también se refiere a ataques por actores no estatales como Anonymous o New World Hackers, reconociendo que todos esos representan solamente una pequeña muestra. Entre los temores se incluye la capacidad de estas naciones de poner en riesgo la infraestructura crítica de EE.UU., para frustrar la respuesta militar de EE.UU. por miedo de un dominio cibernético, y usar una amplia gama de ataques de menor intensidad que colectivamente pasan factura a las bases del poder nacional.[9]

Las recomendaciones del DSB para una disuasión cibernética son un compendio de disuasión de la Guerra Fría y no sin reconocimiento. Su primera iniciativa, planificación de campañas disuasorias adaptadas para hacer frente a una gama de ataques, inequívocamente se asemeja a una respuesta flexible, el concepto que alejó la política nuclear de EE.UU. de la represalia masiva hacia algo más proporcional. Su segunda iniciativa, crear una "línea delgada" resistente a la cibernética contra sistemas de ataque clave de EE.UU., incluso usa el término "segundo ataque" como reconocimiento clave de sus antecedentes de disuasión nuclear. Incluso "contrarrestar" aparece en el documento, término usado durante los años de la administración Carter para transmitir una cierta estrategia de disuasión nuclear.[10] La analogía no se limita al DSB, debido presuntamente a que la propia Guerra Fría se invoca a menudo en debates de la relación entre países sobre sus interacciones en el ciberespacio.[11] Un caso recientemente citado describió la sugerencia de filtrar nuestras capacidades ofensivas cibernéticas, que adopta la idea de disuasión nuclear, es decir, un arma secreta no puede ser disuasoria.[12] Incluso la cuestión planteada por

este artículo parece imitar los discursos del presidente Reagan sobre "imponerse" sobre las fuerzas del comunismo y la Unión Soviética.

En 2012, el secretario de Defensa Leon Panetta usó el término "Pearl Harbor cibernético" para transmitir el peligro al que se enfrentaba EE.UU. en el ciberdominio;[13] otros han usado similarmente la "cibernética continua". Por el contrario, John Arquilla y David Rondfeldt sugirieron (más de una década antes) un "destino manifiesto para la edad la información".[14] Otros llaman al ciberespacio el nuevo "oeste salvaje" o evocan la era de piratas y corsarios, gobiernos débiles y normas internaciones no explícitas o que no se hacían cumplir.[15] Todo esto tienen algo en común: el deseo de explicar algo nuevo en términos comprensibles haciéndonos recordar el pasado. La guerra cibernética es complicada porque cubre una gama de ataques; los ataques de negación de servicio y las filtraciones de documentos del Partido Nacional Democrático representan dos tipos muy diferentes de ataques y dos estrategias muy diferentes. Lo único que tienen en común ambas cosas es que se llevaron a cabo usando herramientas de dominio cibernético y se dirigieron a EE.UU.

Expertos académicos de EE.UU. han observado que la metáfora es una parte esencial de cómo las personas justifican y entienden el mundo, no solo en el lenguaje, sino también en los procesos de razinamiento.[16] Christopher R. Paparone indica que la "gestión del significado" es una tarea principal de los líderes.[17] A menudo son la mejor forma de enmarcar la narrativa, pero con el problema obvio de un exceso de simplificación. Así, una traducción ingenua de los principios de disuasión nuclear en el ciberespacio oscurece los problemas reales a los que nos enfrentamos.[18] Las metáforas "llevan consigo, a menudo de modo furtivo e insidioso, 'soluciones' naturales".[19] Los virus informáticos se asemejan a virus biológicos, por lo que algunos han sugerido una versión cibernética del Centro de Control de Enfermedades.[20] El pirateo informático en línea, como la piratería real, es un problema de establecer normas internacionales y obligar a las naciones a hacerlas cumplir.[21] Estas son quizás dos de las mejores ideas, pero también muestran que el método de enmarcar el problema afecta la forma en que se formulan las decisiones. La descripción del telón de acero de Winston Churchill ofrecía una imagen visceral en las mentes occidentales que contribuyeron a conformar la política de contención bajo la administración Eisenhower. Las referencias a un "telón de información" o "echen abajo ese muro cortafuegos" no tienen la misma vitalidad.[22]

Paparone habla de categorías de metáforas usadas por los líderes: newtoniana, posnewtoniana y de las artes y humanidades.[23] Las metáforas newtonianas se basan en ciencias exactas, y tienden a ser deterministas en carácter. La doctrina militar deriva muchos de sus conceptos de la terminología newtoniana, como masa, fricción, centro de gravedad y poder, que tienen una calidad cuantitativa. Por el contrario, las metáforas posnewtonianas aluden a la complejidad e interacción mutua de un sistema, basado en campos como la biología, la medicina, y la mecánica cuántica, en los que los efectos de probabilidad caracterizan los resultados en vez otros lineales, deterministas. Los términos se usan ampliamente en el ciberdominio; red, virus, infección y gusano establecer paralelos con el mundo "posnewtoniano". También se usan para explicar cosas como el terrorismo y la insurgencia. Por último, las artes y humanidades proporcionan metáforas y analogías de referencias históricas, literarias y culturales. Una de las mejores metáforas de la guerra se debe a Clausewitz cuando la comparó a dos luchadores tratando de dominarse entre sí.[24]

En resumen, el debate de la guerra cibernética está teniendo lugar dentro del contexto de un lenguaje que está tan congestionado como la internet misma. Este problema tiene algún precedente. El Teniente Coronel Peter Faber, USAF, retirado, indicó que la teoría y la doctrina del poder aéreo sufrieron de una "prisión del lenguaje" similar durante su desarrollo que mezclaba ideales racionales mixtos, pensamiento antirracional y terminología militar.[25] Como respuesta, el Teniente Coronel Faber sugirió un marco concebido originalmente por el Dr. Robert Pape y expandido por ciertos trabajos en la Universidad de Aire.[26] Este marco tenía como fin generalizar las ideas del poder aéreo, pero sin bloquearlo en un contexto lingüístico particular. Particu-

larmente, el objetivo de cualquier estrategia es vincular los fines con sus medios. Este es el marco que propongo que puede utilizarse para entender cómo tratar las amenazas cibernéticas específicas a la seguridad nacional a las que se enfrenta EE.UU.

Un marco estratégico

El marco adopta la forma de seis cuestiones clave en anticipación de cualquier estrategia que utiliza fuerzas militares:[27]

1. ¿Qué resultado busco?
2. ¿Cuáles son las capacidades político-militares específicas y las del adversario?
3. ¿Qué tipo de estrategia debo seguir?
4. ¿Qué metas u objetivos son los más importantes?
5. ¿Qué mecanismos espero que active mi operación?
6. ¿Cómo debo regular mis acciones en el tiempo?

Empezando por la primera cuestión, el resultado buscado es principalmente de naturaleza política. No obstante, no tiene que estar orientado a la destrucción. En este caso, el objetivo es detener acciones agresivas en el ciberespacio. No obstante, esto requiere una mayor aclaración. El resultado debe considerarse con respecto a algún receptor.[28] ¿Quién debe llevar a cabo acciones agresivas en el ciberespacio, y qué acciones debe detener? ¿El resultado político es que China reduzca el robo de propiedad intelectual de las corporaciones estadounidenses? ¿O reducir la vulnerabilidad de infraestructura crítica de EE.UU.? El cambio de formulación de este resultado puede cambiar el sentido de la estrategia. Por ejemplo, el resultado puede indicarse en términos de impedir que un estado nación particular tome medidas cibernéticas hostiles contra nuestra red eléctrica. De forma alternativa, puede indicarse en términos de minimizar los *efectos* de un ataque cibernético a un sistema eléctrico en el funcionamiento de la sociedad. En el último caso, quizás el receptor no es el adversario, sino los propietarios o gerentes privados de infraestructura crítica de EE.UU. Debemos evitar la tentación de grandes objetivos disuasorios estratégicos unificados para cubrir todos los actores cibernéticos posibles; esto es similar a una disuasión "terrestre" o "marítima".[29]

A continuación, comparamos las capacidades político-militares. La política, la preparación, el adiestramiento, la cultura doméstica, los equipos, las tácticas y la atribución son aplicables al ciberdominio como a cada dominio. Tal vez, EE.UU. tiene una ventaja bélica convencional, pero ¿cómo están de preparadas las fuerzas para defender redes o llevar a cabo acciones ofensivas en el ciberespacio? ¿Qué pasa con la fuerza cultural, la capacidad de respuesta de la población general a una campaña de información que solicita una narrativa particular, como el presunto entrometimiento en una elección? Sun-Tzu puede haber resumido la importancia de esta cuestión de forma sencilla: conózcase a sí mismo, y conozca a su enemigo.[30]

La tercera cuestión clave pide considerar una cierta estrategia. El Teniente Coronel Faber sugiere varias:

- castigo—empujar a una sociedad pasado su punto de ruptura económico o sicológico
- riesgo—igual que un castigo, pero con una escalada gradual
- negación—capacidad neutralizadora de librar una guerra
- decapitación—destruir o aislar el liderazgo, las comunicaciones nacionales u otros centros de poder
- desactivación—alterar las capacidades ofensivas

- demora—usar un método de amenazas o disuasión para conservar el statu quo
- activación—creación de estabilidad donde sea débil

Ahora se hace más claro por qué los problemas del lenguaje a menudo han sido dañinos para los debates cibernéticos. Las analogías de disuasión nuclear, que se han usado, pero que han demostrado ser insuficientes en la mayoría de los casos, no se adaptan normalmente porque se formularon para resultados políticos específicos y evaluaciones específicas de capacidad. Por supuesto es cierto que las armas cibernéticas no son bombas nucleares, pero las bombas no son el objetivo de la disuasión, sino los medios que se adaptan a la evaluación. Una lección más importante ahora es cómo se aplicaba la estrategia dadas las opciones y no qué estrategia. Las estrategias de demora o castigo pueden haber dado resultado entonces; tal vez ahora sea más apropiada una estrategia de negación o activación. Un posible ejemplo de una estrategia de decapitación "cibernética" fue la publicación del informe Mandiant, que simplemente usaba una exposición bien documentada de la PLA para aislarla en la comunidad internacional.[31] Esto condujo a acuerdos internacionales, con reducciones observadas en el número de intrusiones cibernéticas desde entonces.[32]

La cuarta cuestión clave tiene en cuenta los objetivos críticos y su importancia. El Teniente Coronel Faber señala temas que deben considerarse:

1. ¿Qué aspectos del poder del receptor deben seleccionarse como objetivos?[33]
   - Fuentes – militares, industriales, culturales
   - Manifestaciones – gobierno, ideológicas
   - Vínculos – redes humanas y materiales
2. ¿Cuál es la estrategia genérica?
   - Directa – asalto "frontal", confrontación o apoyo
   - Indirecta – reducir la voluntad de luchar o alterar la toma de decisiones
3. ¿Qué nivel de destrucción deseo?

Claramente, los adversarios mencionados anteriormente hacen mismas consideraciones.

A menudo, se supone la estrategia indirecta en el ciberespacio, lo que a veces se traduce en negación, degradación, alteración, destrucción o manipulación de información.[34] No obstante, en sentido general, se puede escoger un objetivo para fortalecer o debilitar, dependiendo de las formulaciones anteriores.[35] La teoría de selección de objetivos forma una gran parte de la teoría del poder aéreo y es un aspecto clave de la estrategia nuclear. EE.UU. también usa a menudo una influencia económica para seleccionar fuentes de poder. La selección de objetivos cibernéticos es un concepto menos desarrollado, pero fue considerado recientemente en una tesis en la Universidad del Aire.[36] Al igual que con el poder aéreo, los objetivos son interminables. No obstante, el vínculo entre este paso y el siguiente es lo que Teniente Coronel Faber llama el "santo grial" del poder aéreo, algo que aún no se ha logrado completamente.

La quinta cuestión clave es preguntar qué mecanismos esperan ser activados por la opción de selección de objetivos anterior. ¿Qué cambios o resultados deben esperarse? ¿División política? ¿Confusión, revuelta o rendición masivas? ¿Mayor voluntad de lucha? Un recordatorio clave de los primeros defensores del poder aéreo es que a menudo estaban equivocados; bombardear ciudades a veces resultaba en caos o rendición y a veces fortalecía la voluntad popular de resistir. De modo similar, los efectos del poder cibernético son difí-

ciles de predecir. Los ataques de negación de servicio de 2007 en Estonia no parecen haber logrado ningún efecto duradero. Stuxnet demoró, pero no pareció alterar finalmente la dirección de los programas nucleares iraníes. Por otra parte, entender el efecto real de las campañas de información durante la elección de 2016 sigue siendo elusivo. Los efectos de primer orden en el ciberespacio son más fáciles de calcular, como era en los bombardeos estratégicos, o tal vez no sean el propósito principal en absoluto. Son los efectos de primer, segundo, tercer y cuarto orden los que han sido siempre difíciles, y estos dependen considerablemente de si se ha prestado atención apropiada a la pregunta dos.

Por último, la disuasión no es un asunto de frustrar la tecnología, sino de influir en decisiones. Estas decisiones normalmente son específicas y limitadas. La política nuclear de EE.UU. quizás influyó en las decisiones soviéticas de no lanzar armas nucleares, pero no pudo impedir todas las acciones militares soviéticas no deseables porque no hay forma de garantizar el comportamiento humano en cada situación. No obstante, se puede usar el razonamiento crítico y el sentido común para buscar soluciones si el problema está bien enmarcado, el resultado deseado está claramente definido y si se ha hecho el trabajo de conocernos y conocer a nuestros adversarios de forma suficientemente buena para hacer estimaciones razonables de sus respuestas.

Por último, el Teniente Coronel Faber considera el momento oportuno. ¿Deben ser acciones individuales o múltiples? ¿Incrementales, secuenciales, acumulativas o simultáneas? Una vez más, esto está unido al mecanismo deseado. ¿Será suficiente una sola respuesta para disuadir a un actor particular de un cierto comportamiento? ¿O acciones tomadas de forma regular? La política declaratoria puede funcionar en algunos casos y tal vez no en otros.

Afirmo que esta estructura proporciona una manera útil no prescriptiva en la que medir la cuestión de estrategia para la guerra y disuasión en el ciberespacio. No es prescriptivo porque la guerra no es finalmente una ecuación matemática determinista, y ha quedado demostrado que vincular medios y extremos siempre es difícil. No obstante, nos recuerda unas cuantas lecciones importantes, y ayuda a liberarnos de las trampas de comunicarnos según un conjunto de referencias limitadas.

Algunas recomendaciones finales

Entonces, ¿debe EE.UU. prepararse mejor para la disuasión y, si fracasa, imponerse en el ciberespacio? Hay al menos tres ideas que debemos inferir de este ejercicio.

1. El razonamiento y el juicio críticos deben sustituir a las lecciones aprendidas.

> *Los naturales de nuestro país consideran, y con razón, que para buscar la puerta necesitan dar un gran rodeo, y les es más corto y más fácil saltar por la pared.*
>
> —John Bunyan, Pilgrim's Progress (El progreso del peregrino)

La idea central de este artículo ha sido que un uso deficiente del lenguaje y no enmarcar el problema ha complicado e inutilizado el debate de la guerra cibernética y la estrategia disuasoria. Los líderes superiores no rechazarán ni deberán rechazar todo el lenguaje metafórico y las referencias históricas. Nuestro lenguaje y nuestra historia forman parte de la fuerza de nuestro país. Por lo tanto, la comunicación de las imágenes adecuadas y las lecciones históricas adecuadas con el fin de formular la estrategia de hoy sigue siendo la meta. Esto ocurrirá en un mayor grado cuando nos comprometamos a la tarea difícil de razonar de forma crítica en vez de tomar el atajo de un método simplificado de lecciones aprendi-

das. Debemos aprender de quienes tuvieron en cuenta la guerra nuclear en la década de 1960, o la guerra asimétrica en Oriente Medio, pero no debemos tratar de tomar atajos en nuestras soluciones. Debemos considerar los problemas por su propio mérito, además de reconocer el trabajo de aquellos que nos han precedido, y cosechar el beneficio de pensadores estratégicos que ayudaron a proporcionar un marco para razonar bien hoy.

2. Se necesitará un liderazgo valeroso.

> *No desprecie nunca las dimensiones sicológicas, culturales, políticas y humanas de la guerra, que es inevitablemente trágica, ineficiente e incierta. No crean en análisis de sistemas, modelos informáticos, teorías de juegos o doctrinas que sugieran otra cosa.*
>
> —Secretario de Defensa Robert Gates, 2008

Las decisiones en guerra y paz se basan a menudo en inteligencia insuficiente, probabilidades y principios generales. Podemos reducir la probabilidad de establecer relaciones fundamentalmente débiles entre nuestros fines y nuestros medios pensando de forma clara y crítica y teniendo en cuenta un conjunto amplio de perspectivas. No obstante, al final del día, nuestros líderes tendrán que tener el coraje suficiente para escuchar y para actuar o no actuar. No debemos esperar menos. La guerra es fundamentalmente incierta, y siempre se necesitará el coraje de decidir.

3. La humildad es clave.

> *Una forma generalmente útil de concluir una discusión desagradable de esta clase sería afirmar que tenemos los recursos, la inteligencia y el coraje de tomar las decisiones correctas. Este es por supuesto el caso. Y existe una buena probabilidad de que hagamos eso. No obstante, quizás, como una pequeña ayuda para hacer que sea más probable que tomemos dichas decisiones, debemos contemplar la posibilidad de que tal vez no se tomen. Son difíciles, conllevan sacrificio, se ven afectadas por grandes incertidumbres, asuntos de importancia en que se desconoce mucho y mucho más debe eludirse por secretismo; y, sobre todo, implican una nueva imagen de nosotros mismos en un mundo de peligro persistente. No es ni mucho menos cierto que debemos enfrentarnos a la prueba.*
>
> —Albert Wohlstetter, The Delicate Balance of Terror (El delicado balance del terror)

La humildad nos permite hacer varias cosas. Nos permite considerar el pasado y reconocer que no somos los únicos en afrontar problemas y retos de la humanidad. Insiste en que reconozcamos y aceptemos cálculos estratégicos equivocados y cambiemos nuestro curso de acción. Nos permite la capacidad de trabajar con otros desde distintos campos y con diferentes antecedentes para resolver un problema común. Nos dice que demos la iniciativa a otros que son más capaces, más conocedores y están más informados en el caso de ciertos temas que tendremos que tener en cuenta. Hace que nos demos cuenta de que las respuestas completas y las soluciones completas no forman parte del dominio de la guerra y de la disuasión. Por último, la humildad nos recuerda que no es cierto que vayamos a tener éxito y entonces nos muestra que nosotros también debemos hacer el trabajo difícil que cada generación anterior ha afrontado a su manera. ❑

Notas

1. Charles W. Sanders Jr., *No Other Law: The French Army and the Doctrine of the Offensive (Sin ninguna otra ley: el Ejército de Francia y la doctrina de la ofensiva),* Informe de investigación no. P-7331 (Santa Monica, CA: The RAND Corporation, 1987), https://www.rand.org/content/dam/rand/pubs/papers/2005/P7331.pdf.

2. Dallas D. Irvine, "The French and Prussian Staff Systems Before 1870" (Los sistemas de estado mayor franceses y prusianos antes de 1870*), The Journal of the American Military Foundation* 2, no. 4 (Invierno de 1938): 192–203.

3. Sanders, "No Other Law" (Sin ninguna otra ley), 192–203.

4. Karl Von Clausewitz y Sun-Tzu, El libro de la guerra: "*El arte de la guerra" de Sun-Tzu y "De la guerra" de Karl von Clausewitz* (New York, NY: Random House, Inc., 2000).

5. Thomas Rid, "Cyber War Will Not Take Place" (La guerra cibernética no tendrá lugar*), Journal of Strategic Studies* 35, no. 1 (2012): 5–32, doi: 10.1080/01402390.2011.608939.

6. Martin C. Libicki*, Cyberdeterrence and Cyberwar (Disuasión y guerra cibernéticas)* (Santa Monica, CA: RAND Corporation, 2009),

https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

7. Peter W. Singer y Noah Shachtman, "The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity is Misplaced and Counterproductive" (La guerra equivocada: la insistencia sobre la aplicación de metáforas de guerra fría a la ciberseguridad es inapropiada y contraproducentre), *Brookings Institute,* agosto de 2011, https://www.brookings.edu/articles/the-wrong-war-the-insistence-on-applying-cold-war-metaphors-to-cybersecurity-is-misplaced-and-counterproductive/.

8. Jason Andress y Steve Winterfield*, Cyber Warfare: Techniques, Tactics, and Tools for Security Practitioners (La guerra cibernética: técnicas, tácticas y herramientas para los practicantes de seguridad),* 2ª edición (Waltham, MA: Syngress, 2014).

9. Departamento de Defensa, Consejo Científico de Defensa, *Task Force on Cyber Deterrence (Fuerza de tarea sobre la disuasión cibernética*) (Washington, DC: Subsecretaría de Defensa para adquisición, tecnología y logística, 2017), http://www.dtic.mil/docs/citations/AD1028516.

10. Laboratorios Nacionales de Sandia*, U.S. Strategic Nuclear Policy: A Video History, 1945–2004 (Política nuclear estratégica de EE.UU.: una videohistoria,* 1945-2004) (Albuquerque, NM: Laboratorios Nacionales Sandia, 2012), https://archive.org/details/U.s.StrategicNuclearPolicy.

11. David Ignatius, "Cold War Feeling on Cyberspace" (Sentimiento de la guerra fría en el espacio cibernético*) RealClearPolitics*, 26 de agosto de 2010, https://www.realclearpolitics.com/articles/2010/08/26/cold_war_feeling_on_cybersecurity_106900.html.

12. Peter W. Singer y Allan Friedman*, Cybersecurity and Cyberwar: What Everyone Needs to Know (La seguridad y la guerra cibernéticas: lo que todos deben saber*) (New York, NY: Oxford University Press).

13."Comentarios por el secretario Panetta sobre la ciberseguridad a ejecutivos comerciales para la seguridad nacional", Operaciones de Prensa del Departamento de Defensa, transcripción de noticias, 11 de octubre de 2012, http://archive.defense.gov

/transcripts/transcript.aspx?transcriptid=5136.

12-SAW-Nacita & Reith.indd 125 3/23/2018 10:05:15 AM

14. John Arquilla y David Ronfeldt*, The Emergence of Noopolitik: toward an American Information Strategy (La emergencia de la "noopolitik": hacia una estrategia de información estadounidense)* (Santa Monica, CA: RAND Corporation, 1999).

15. Singer y Friedman*, Cybersecurity and Cyberwar (Seguridad y guerra cibernéticas).*

16. Sean Lawson, "Putting the 'War' in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States" (Poner la guerra en la guerra cibernética: metáfora, analogía y discurso de seguridad cibernética en Estados Unidos), *First Monday* 17, no. 7: (2 de julio de 2012), http://firstmonday.org/ojs/index.php/fm/article/view/3848/3270&sa=U&ei=E9hVU4_PBKrw8AGmhIDQC#p6.

17. Christopher R. Paparone, "On Metaphors We Are Led By" (Nos lideran las metáforas), *Military Review* (Noviembre–diciembre de 2008), http://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/2008-Archive/#novdec.

18. Singer y Shachtman, "The Wrong War"(La guerra equivocada).

19. Lawson, "Putting the 'War' " (Poner la guerra).

20. Singer y Friedman*, Cybersecurity and Cyberwar (La seguridad y la guerra cibernéticas*); y Lawson, "Putting the 'War.' " (Poner la guerra).

21. Singer y Friedman, *Cybersecurity and Cyberwar (La seguridad y la guerra cibernéticas).*

22. Nathan Hodge, "Hillary on Net Freedom: Tear Down This Firewall" (Hillary sobre la libertad en la red: echen abajo ese muro cortafuegos), *Wired,* 21 de enero 2010,

https://www.wired.com/2010/01/secstate-clinton-on-net-freedom-tear-down-this-virtual-wall/.

23. Paparone, "On Metaphors" (Sobre metáforas).

24. Clausewitz y Sun-Tzu*, Book of War (Libro de la guerra).*

25. Teniente Coronel Peter R. Faber, *Competing Visions of Aerospace Power: A Language for the 21st Century (Visiones rivales del poder aeroespacial: un lenguaje del siglo* XXI), informe de investigación (Newport, RI: Departamenteo de Investigación Avanzada, Colegio de Guerra Naval, 21 de febrero de 1997), http://www.au.af.mil/au/awc/awcgate/theorists/faber-full.pdf.

26. La descripción del desarrollo de esta estructura, así como de alternativas, se da en el artículo siguiente: Thomas P. Ehrhard, Making the Connection: An Air Strategy Analysis Framework (Hacer la conexión: un marco de análisis de estrategia aérea), Escuela de Estudios Avanzados del Poder Aéreo (Base de la Fuerza Aérea Maxwell, AL: Air University Press, 1997), http://www.au.af.mil/au/aupress/bookinfo.asp?bid=438&type=papers.

27. Lawson, "Putting the 'War'" (Poner la guerra).

28. Aquí es importante una nota: estas estrategias fueron formuladas en el contexto del poder aéreo. No obstante, los fines del poder aéreo se han considerado siempre estratégicos. La disuasión es un concepto inherentemente estratégico, y las consideraciones generales deben aplicarse, no solamente con un enfoque ofensivo, sino también defensivo.

29. El objeto de la disuasión o de la acción ofensiva es una persona, no una tecnología ni un dominio, según se describió con detalle en este artículo. Faber cita varias: una organización internacional, un estado nación, una organización no gubernamental, una red terrorista y así sucesivamente. No obstante, nuestro receptor no tiene que ser el adversario; podría bien ser un aliado. Un ejemplo de esto es el puente aéreo de Berlín, que trató de asegurar que Berlín Occidental no cayera ante las presiones económicas soviéticas. En este caso, el adversario era la Unión Soviética, pero el receptor era el pueblo de Berlín. Se presume, que hay algún adversario, pero nuestro resultado no necesita formularse en sus términos solamente.

30. Clausewitz y Sun-Tzu, *Book of War (Libro de la guerra).*

31. Dorothy E. Denning, "Rethinking the Cyber Domain and Deterrence" (Razonar el dominio cibernético y la disuasión). *Joint Force Quarterly* 77, (Verano de 2015), http://ndupress.ndu.edu/JFQ/JointForceQuarterly77/tabid/12113/Article/581864/re

thinking-the-cyber-domain-and-deterrence.aspx.

32. Mandiant, APT1*: Exposing One of China's Cyber Espionage Units (Exposición de una de las unidades de espionaje cibernético de China)* (Alexandria, VA: Mandiant, 2013),

https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf; and Fire-Eye iSight Intelligence (2016). *Redline Drawn: China Recalculates Its Use of Cyber Espionage (Línea roja trazada: China recalcula su uso de espionaje cibernético) (Milpitas, CA: FireEye iSight Intelligence*, 2016), https://www.fireeye.com/content/dam/fireeye-www./current-threats/pdfs/rpt-china-espionage.pdf.

33. Una vez más, este es el receptor, que no es necesariamente equivalente al adversario.

34. Centro de Desarrollo de Doctrina y Educación Curtis E. Lemay, 30 de noviembre de 2011, Annex 3-12—*Cyberspace Operations: Introduction to Cyberspace Operations (Anexo 3-12-Operaciones ciberespaciales: introducción a las operaciones ciberespaciales),* http://www.doctrine.af.mil/Doctrine-Annexes/Annex-3-12-Cyberspace-Ops/.

35. Por ejemplo, si el receptor es el adversario, su poder militar puede ser seleccionado como objetivo directamente mediante fuerza cinética o por medios cibernéticos. En el caso de la infraestructura crítica, se puede tratar de mejorar las prácticas de seguridad de la red de las compañías que gestionan esas instalaciones incentivando o motivando mejores prácticas defensivas.

36. Steven Anderson, "Airpower Lessons for an Air Force Cyber-Power Targeting Theory" (Lecciones del poder aéreo para una teoría de selección de objetivos de poder cibernético de la Fuerza Aérea*), Drew Paper* No. 23 (Base de la Fuerza Aérea Maxwell, AL: Air University Press, 2016), http://www.au.af.mil/au/aupress/digital/pdf/paper/dp_0023_anderson_airpower_lessons.pdf.

Capitán Isaac Nacita, Fuerza Aérea de EE.UU. (BS, Universidad de California en Los Angeles) es un estudiante de maestría en el Instituto de Tecnología de la Fuerza Aérea, donde está estudiando sistemas espaciales. Antes, era un analista en el 746º Escuadrón de Pruebas de la Base de la Fuerza Aérea Holloman, Nuevo México, donde lideró un elemento responsable de probar los sistemas de navegación y guía.

Teniente Coronel Mark Reith, PhD, Fuerza Aérea de EE.UU. (PhD, Universidad de Texas en San Antonio) sirvió antes como subcomandante del 26º Grupo de Operaciones Ciberespaciales y comandante del 690º Escuadrón de Soporte de la Red, liderando las fuerzas de la empresa de ciberdefensa y de la Red de Información del Departamento de Defensa respectivamente. Sirve actualmente como director del Centro de Investigación Ciberespacial y es profesor ayudante de Ciencias Informáticas en el Instituto de Tecnología de la Fuerza Aérea.