Disuasión nuclear en Ciber-ia

Retos y controversias©

Dr. Stephen J. Cimbala (PhD)*

La edad de la información ha llegado, incluso a los asuntos militares, pero la teoría y la política relacionadas con la disuasión nuclear se están acelerando para mantenerse al día en un mundo impulsado por la cibernética. Los futuros conflictos militares, incluidos aquellos que comprenden la disuasión nuclear y gestión de crisis, incluirán un aspecto digital. La información de la guerra "cibernética" está aquí aunque no sea lo que impulse todos los conflictos. Existe en la vanguardia de cualquier ataque contra el cerebro y el sistema nervioso central del enemigo de mando, control, comunicaciones, computadoras, inteligencia, vigilancia y reconocimiento (C4ISR).[1] Por otra parte, con demasiada frecuencia los asuntos de disuasión nuclear y guerra cibernética se tratan como retos separados y diferenciados. Este separatismo cibernuclear es comprensible como asunto de división de trabajo entre expertos, pero resulta dudoso comparado con la realidad de la disuasión nuclear o gestión de crisis en condiciones cibernéticas intensivas.

Este artículo examina primero algunas de las amplias implicaciones teóricas del nexo nuclear-cibernético para estudiantes de política de seguridad nacional y conflictos bélicos. En segundo lugar, se concentra específicamente en disuasión nuclear estratégica y control de armas estadounidenses y rusos como ajustes relacionados con la política para relaciones nucleares y cibernéticas. En tercer lugar, analiza cómo la combinación de ataques nucleares y cibernéticos podría al menos afectar hipotéticamente la estabilidad de la disuasión nuclear. Por último, el artículo saca conclusiones pertinentes acerca de la interfaz nuclear-cibernética en lo que pueda referirse a un control, a la no proliferación y a la disuasión de armas en el futuro.

¿Cuánto les separa?

¿Cuáles son las implicaciones de una posible superposición entre conceptos o prácticas de guerra cibernética y disuasión nuclear?[2] La guerra cibernética y las armas nucleares parecen ser dos mundos completamente diferentes. Las armas cibernéticas deben atraer a los que prefieren un arco de desarrollo militar técnico no nuclear. La guerra en el dominio digital ofrece, al menos en teoría, un medio posible de paralizar o desactivar haberes enemigos sin la necesidad de un ataque cinético o de minimizar la destrucción física.[3] No obstante, las armas nucleares, son el verdadero epítome de destrucción "masiva"—tanto es así que se prefiere emplear para disuadir o evitar la guerra manipulando el riesgo antes que dispararla de forma real. Desgraciadamente, ni la disuasión nuclear ni la guerra cibernética podrán coexistir en distintos universos de políticas en un futuro próximo o distante.

Las armas nucleares, tanto si se retienen para disuadir como para dispararse de forma furiosa, deben incorporarse a sistemas de C4ISR. Las armas y sus sistemas C4ISR deben estar protegidos contra ataques de naturaleza cinética y digital. Además, los encargados de tomar decisiones que tengan que gestionar fuerzas nucleares durante una crisis idealmente deben disponer de la mayor información posible sobre el estado de sus fuerzas y sistemas de mando nucleares y cibernéticos, acerca de las fuerzas y C4ISR de los posibles atacantes, y acerca de las intenciones proba-

*Reconozco agradecidamente los ánimos de Paul K. Davis, RAND Corporation, para tratar este tema, así como sus detalles útiles. Él no es responsable de ningún argumento en este artículo.

bles y la aceptación de riesgo de posibles oponentes. En otras palabras, la tarea de gestionar una crisis exige pensar de forma clara y disponer de buena información. No obstante, el empleo de guerras cibernéticas en las primeras etapas de una crisis podría impedir una evaluación clara creando confusión en las redes y los canales de acción que dependan de esas redes.[4] La tentación de un ataque preventivo temprano de carácter cibernético podría "tener éxito" hasta el punto de que la gestión de la crisis nuclear se haría más débil en vez de más fuerte. Según ha observado Andrew Futter,

> Con las fuerzas de EUA y Rusia listas para ser utilizadas en cuestión de minutos e incluso segundos después de recibir una orden, está aumentando la posibilidad de que se puedan usar armas por accidente (como la creencia de que se estaba produciendo un ataque debido a una advertencia temprana usurpada o comandos de lanzamiento falsos), debido a cálculos erróneos (por comunicaciones arriesgadas, o mediante una escalada no intencionada), o por personas sin la autorización apropiada (como un grupo terrorista, un tercero o un comandante gamberro). En consecuencia, en este nuevo entorno nuclear, se está haciendo cada vez más importante asegurar las fuerzas nucleares y los sistemas de computadoras asociados contra un ciberataque, proteger contra una influencia externa maquiavélica y el "pirateo", y quizás lo que es más crucial, aumentar el tiempo que se tarda y las condiciones que deben cumplirse antes de lanzar armas nucleares.[5]

Irónicamente, aunque la reducción de arsenales nucleares estratégicos de EUA y rusos postsoviéticos desde el fin de la Guerra Fría es un desarrollo positivo desde los puntos de vista de control y no proliferación de armas nucleares, hace que el uso simultáneo de las capacidades de ataques cibernéticos y nucleares sea más alarmante. Los enormes y redundantes despliegues por parte de los estadounidenses y soviéticos de la Guerra Fría tenían al menos una virtud. Aquellos arsenales proporcionaban tanta redundancia contra la vulnerabilidad de los primeros ataques que bastaban los sistemas relativamente lineales para advertencia de ataques nucleares, comando y control (C2), y lanzamiento de respuesta durante o después de un ataque. Al mismo tiempo, las herramientas de la Guerra Fría para ocasionar daños cibernéticos militares eran primitivas comparadas con las disponibles ahora. Además, los países y sus fuerzas armadas dependían menos de la fidelidad de sus sistemas de información para la seguridad nacional. Así, la reducción de fuerzas de EUA, Rusia y posiblemente otras fuerzas al tamaño de "disuasiones mínimas" podría poner en peligro la flexibilidad y resistencia nucleares ante ataques cinéticos precedidos o acompañados de una guerra cibernética.[6] Por ejemplo, Bruce Blair, experto en política nuclear y autor de una serie de estudios sobre C2 nuclear, ha observado que

> las redes de comunicaciones y computadoras usadas para controlar fuerzas nucleares deben tener cortafuegos contra las dos docenas de naciones (incluidas Rusia, China y Corea del Norte) con programas de ataques por computadora especiales y de miles de intentos de intrusión hostiles llevados a cabo todos los días contra computadoras militares de EUA. No obstante las investigaciones de estos cortafuegos han puesto al descubierto una debilidad evidente.[7]

El debate anterior reconoce que las teorías relacionadas con ataques nucleares y cibernéticos, así como las prescripciones de políticas derivadas, tienen atributos exclusivos y señales de advertencia contra analogías fáciles. No obstante, el "dominio" cibernético atraviesa los otros dominios geoestratégicos para la guerra: tierra, mar, aire y espacio. Por otra parte, el dominio cibernético, comparado con los otros, carece de perspectiva histórica: el dominio cibernético "ha sido creado en un tiempo corto y no ha tenido el mismo nivel de escrutinio que otros dominios de combate", como ha expresado el Mayor Clifford S. Magee, Cuerpo de Infantería de Marina.[8] Brian M. Mazanec también señala el "secretismo relativo que rodea a la mayoría de las operaciones cibernéticas sin un registro extensivo de prácticas especiales de los estados".[9] James Wood Forsyth Jr. y el Mayor Billy E. Pope hacen hincapié en que el ciberespacio ha activado "una nueva forma de guerra que nadie puede ver, medir o supuestamente temer".[10] No obstante, los exper-

tos también esperan que como estamos en las primeras etapas del conflicto cibernético, podemos anticipar que se desarrollarán armas cibernéticas cada vez más numerosas y complejas, y que se integrarán en estrategias militares nacionales y guías de planificación operacional. Como argumentó Mazanec,

> Así, las capacidades de guerra cibernética desempeñarán una función cada vez más decisiva en los conflictos militares y se están integrando más profundamente en la doctrina de los estados y las capacidades militares. Más de 30 países han tomado medidas para incorporar las capacidades de guerra cibernética en su planificación y organizaciones militares, y es probable que aumente el empleo de la guerra cibernética como un arma de "fuerza bruta". Los planificadores militares están tratando activamente de incorporar capacidades de ofensiva cibernética en planes de guerra existentes, lo que podría conducir a operaciones de ofensiva cibernéticas desempeñando una función cada vez más decisiva en operaciones militares a niveles táctico, operacional y estratégico.[11]

La Tabla 1 resume la información sobre algunas de los ataques de redes de computadoras más publicados (CNA, por sus siglas en inglés) entre 2007 y 2013.

Tabla 1. Ataques de redes informáticas seleccionados

Nombre del ataque	*Fecha*	*Objetivo*	*Efecto*	*Perpetrador sospechoso*
Estonia	Abril–mayo de 2007	Servicios de web comerciales y gubernamentales (objetivo civil)	Ataque importante de denegación de servicios distribuido (DDOS, por sus siglas en inglés)	Rusia
Sistema de defensa aérea sirio (parte de la Operación Orchard)	Septiembre de 2007	Sistema de defensa aéreo militar (objetivo militar)	Degradación de las capacidades de defensa aérea permitiendo un ataque cinético	Israel
Georgia	Julio de 2008	Servicios de la web comerciales y gubernamentales (objetivo civil)	Ataque importante de DDOS	Rusia
Stuxnet	Fines de 2009–10, posiblemente desde 2007	Centrífugas iraníes (objetivo militar)	Destrucción física de centrífugas iraníes	Estados Unidos
Saudi Aramco	Agosto de 2012	Empresa comercial propiedad del estado (objetivo civil)	Destrucción de datos a gran escala e intento de interrupción física de la producción de petróleo	Irán
Operación Ababil	Septiembre de 2012 a marzo de 2013	Mayores instituciones financieras de EE.UU. (objetivo civil)	Ataque de DDOS importante	Irán

Adaptado de Brian M. Mazanec, "Why International Order in Cyberspace Is Not Inevitable" (Por qué no es inevitable el orden internacional en el ciberespacio) Strategic Studies Quarterly 9, no. 2 (verano de 2015): 81, http://www.au.af.mil/au/ssq/digital/pdf/summer_2015/SSQ_Summer_2015.pdf, Los CNA incluyen la explotación de redes informáticas.

Por supuesto, los CNA no son la única amenaza cibernética planteada por los adversarios potenciales de Estados Unidos u otros actores estatales o no estatales. Según Joel Brenner, antiguo inspector general y antiguo consejero superior de la Agencia de Seguridad Nacional,

> La Marina de EUA se gastó unos $5.000 millones para desarrollar un mando eléctrico silencioso para sus submarinos y barcos de modo que sean silenciosos y difíciles de rastrear. Unos espías chinos lo robaron. La marina gastó miles de millones más en desarrollar un nuevo radar para su crucero Aegis de última tecnología. Unos espías chinos también lo robaron. Los servicios de inteligencia electrónicos

> de chinos y rusos nos están dando una paliza —aprovechándose de redes porosas y de la indiferencia a la seguridad para robar miles de millones de dólares de secretos militares y comerciales. Algunos de nuestros aliados, como los franceses y los israelíes, también lo han intentado.[12]

Brenner afirma que el complejo militar-industrial de Estados Unidos "es el objetivo de espionaje más grande del mundo" y que más de 100 servicios de inteligencia extranjeros tienen como objetivo Estados Unidos.[13] Como recordatorio de esta carrera entre atacantes y defensores cibernéticos, el gobierno de EUA informó sobre grandes ataques por parte de piratas informáticos rusos contra el Internal Revenue Service (Servicio de Impuestos Internos) y por parte de piratas informáticos chinos contra la mayoría de las agencias federales de EUA durante la primera semana de junio de 2015.[14]

No obstante, el significado de los retos relacionados con la cibernética con la seguridad nacional de EUA, no se deduce necesariamente que los conceptos o métodos disuasorios se apliquen al ciberespacio. Según observa Dorothy E. Denning, los autores que comparan la disuasión militar con la disuasión cibernética "han encontrado generalmente que los principios que han hecho que la disuasión nuclear sea efectiva durante más de medio siglo dejan de ser válidos en el ciberespacio".[15] Nos avisa de que "al igual que no agrupamos todas las armas físicas en una sola estrategia de disuasión, tampoco debemos tratar de agrupar todas las armas cibernéticas es una sola estrategia. En vez de eso, necesitamos limitar nuestro tratamiento de disuasión en lo que se refiere al espacio cibernético".[16]

Denning sugiere dos métodos posibles de aplicación de la disuasión al ciberespacio. El primero consiste en concentrarse en tipos específicos de armas cibernéticas para las que la disuasión podría ser viable, como las armas de impulsos electromagnéticos nucleares. Un segundo método de disuasión en el ciberespacio, según Denning, podría ser la aplicación de regímenes de disuasión existentes para algunas actividades cibernéticas, incluidos regímenes internacionales que regulan el comportamiento de los estados o regímenes nacionales que se enfrentan a comportamientos criminales.[17] La Tabla 2 resume algunos de los principales marcadores genéticos que establecen identidades exclusivas para la guerra cibernética y la disuasión nuclear, incluso cuando se fuerza su acercamiento por medio de un avance tecnológico lento, por las demandas de la política y la estrategia, y por rivalidad internacional.

Tabla 2. Atributos comparativos de guerra cibernética y disuasión nuclear

Guerra cibernética	Disuasión nuclear
El origen del ataque puede ser ambiguo—son posibles las intrusiones de terceros haciéndose pasar por otros.	Es casi cierto que el origen del ataque que se puede identificar si el atacante es un estado, e incluso los materiales nucleares de los terroristas atacantes puede identificarse.
Los daños casi siempre se producen en los sistemas de información, redes y el contenido de sus mensajes aunque estos podrían tener efectos que tienen repercusiones en las operaciones de sistemas de combate militares, economía e infraestructura social. (Stuxnet fue un destructor excepcional, construido para ese fin de instalaciones nucleares objetivo).	La falta de disuasión puede conducir a daños históricamente sin precedentes y socialmente catastróficos incluso en el caso de una guerra nuclear "limitada" por las normas de las Guerra Fría.
La denegación de los objetivos del atacante es viable si las defensas son suficientemente robustas y si se pueden reparar las penetraciones en un buen momento.	La disuasión por medio de una amenaza para denegar al atacante de sus objetivos es menos creíble que la amenaza de castigo por represalia asegurada (aunque las defensas de misiles mejoradas tratan de cambiar esta situación).
El objetivo de los ataques cibernéticos es típicamente la destrucción o confusión en vez de la destrucción per se.	La disuasión nuclear se ha basado en su mayor parte en la amenaza creíble de una destrucción rápida y masiva de haberes físicos y poblaciones.

La guerra cibernética y los ataques de información pueden continuar durante un tiempo largo sin ser detectados y a veces sin producir daños evidentes o significativos—algunos no son informados ni siquiera después de haber sido detectados.	El primer uso de un arma nuclear desde 1945 por un estado o una organización no estatal con fines hostiles (distintos de una prueba) sería un evento transformador en la política mundial, sea cual sea el tamaño de la explosión y las consecuencias inmediatas.
El precio de entrada a la mesa de juegos para la guerra cibernética es comparativamente bajo—pueden jugar desde actores como piratas informáticos individuales a entidades estatales.	La construcción y operación de un freno disuasivo nuclear de segundo ataque requiere una infraestructura apoyada por un estado, conocimientos científicos y técnicos a gran escala y compromisos financieros a largo plazo.

Fuentes: Autor. Vea también Dorothy E. Denning, "Rethinking the Cyber Domain and Deterrence" (Reflexiones sobre el domino cibernético y la disuasión), Joint Force Quarterly 77 (2 trimestre de 2015): 8–15, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-77/jfq-77_8-15_Denning.pdf; Edward Geist, "Deterrence Stability in the Cyber Age" (Estabilidad de la disuasión en la era cibernética), Strategic Studies Quarterly 9, no. 4 (Invierno de 2015): 44-61; Timothy L. Thomas, Three Faces of the Cyber Dragon: Cyber Peace Activist, Spook, Attacker (Las tres caras del dragón cibernético: activista de paz cibernético) (Fort Leavenworth, KS: Foreign Military Studies Institute, 2012), 60–66; Martin C. Libicki, Crisis and Escalation in Cyberspace (Crisis y escalada en el ciberespacio) (Santa Monica, CA: RAND Corporation, 2012); y Libicki, Cyberdeterrence and Cyberwar (Disuasión y guerra cibernéticas) (Santa Monica, CA: RAND Corporation, 2009).

Gestión de crisis cibernética y nuclear

Como las armas nucleares se despliegan principalmente con el fin de evitar la guerra por medio de la disuasión, la relación entre la evolución de formas de guerra cibernética o de información y gestión de crisis nucleares se convierte en un componente importante de la agenda para analistas y planificadores militares. La información o la guerra cibernética tienen el potencial de atacar o alterar una gestión satisfactoria de las crisis en cada uno de los cuatro atributos importantes.[18] Primero, la guerra de información puede enturbiar las señales que se envían de un lugar a otro en una crisis. Este engaño puede hacerse de forma deliberada o inadvertida. Suponga que un bando introduce un virus o un gusano en las redes de comunicación de otros.[19] El virus o el gusano se activa durante la crisis y destruye o altera la información. La información carente o alterada puede hacer más difícil que la víctima cibernética organice un ataque militar. Sin embargo, la información destruida o alterada puede engañar a cualquiera de los bandos y llevar a pensar que su señal se ha interpretado correctamente cuando de hecho no es el caso. Así, el bando A puede tratar de enviar una señal de "firmeza" en vez de "cesión" a su oponente sobre cierto asunto. El bando B, al interpretar erróneamente un mensaje de "cesión", puede decidir continuar su agresión, encontrando una resistencia inesperada y permitiendo que se desarrolle una situación mucho más peligrosa.

La guerra de información también puede destruir o interrumpir los canales de comunicación necesarios para gestionar una crisis de forma satisfactoria. Puede hacerse alterando los enlaces de comunicación entre los encargados de la política y los comandantes militares durante un período de grandes amenazas y fuerte presión de tiempo. Son posibles dos clases de problemas que no se anticipan en estas condiciones, desde el punto de las relaciones cívico-militares. En primer lugar, los líderes políticos pueden haber delegado con antelación una autoridad limitada para un lanzamiento nuclear en condiciones restrictivas: solamente cuando se den estas pocas condiciones, según los protocolos de delegación por anticipado, estarían los comandantes militares autorizados a emplear armas nucleares distribuidas dentro de su comando. Las comunicaciones obstruidas, destruidas o alteradas podrían impedir a los líderes principales que supieran que los comandantes militares perciban una situación que fuera mucho más desesperada —y por lo tanto permisiva de una iniciativa nuclear— de lo que realmente era. Por ejemplo, durante la Guerra Fría, las comunicaciones interrumpidas entre el presidente de EUA y el secretario de defensa y los submarinos de misiles balísticos, una vez que estos últimos fueran atacados, podrán haber resul-

tado en una decisión conjunta de oficiales y tripulación del submarino para el lanzamiento en ausencia de instrucciones contrarias.

En segundo lugar, es casi cierto que la guerra informativa durante una crisis aumente la presión del tiempo bajo el cual operan los líderes políticos. Puede hacerlo literalmente, o puede afectar las líneas cronológicas percibidas dentro de las cuales el proceso de formular políticas puede tomar sus decisiones. Una vez que uno de los bandos vea que parte de su sistema de comando, control y comunicaciones se subvierta debido a información falsa o ruidos cibernéticos extraños, su sentido del pánico frente a la posible pérdida de opciones militares sería enorme. En el caso de planes de guerra nuclear de la Guerra Fría de EUA, por ejemplo, la interrupción de partes iguales del sistema estratégico de comando, control y comunicaciones podría haber prevenido la ejecución competente de partes del Plan Operacional Integrado Individual (el plan de guerra nuclear estratégica). El plan dependía de estimaciones muy bien organizadas de tiro de llegada simultánea y expectativas de daños precisos contra varias clases de objetivos. Las redes de centros de comunicación parcialmente mal informados o desinformados habrían conducido a ataques redundantes contra los mismos conjuntos de objetivos y, muy posiblemente, a ataques sin planificar a instalaciones amigas militares o civiles.

Un tercer efecto potencialmente alterador de la guerra de información sobre la gestión de crisis nucleares es que en dicha guerra se puede reducir la búsqueda de alternativas disponibles a unas pocas alternativas y de carácter desesperado. Los encargados de hacer política que buscan formas de escapar de los desenlaces de crisis necesitan opciones flexibles y resoluciones creativas de problemas. Las víctimas de la guerra informática pueden tener una capacidad disminuida para resolver problemas de forma rutinaria, y no digamos de forma creadora, una vez que las redes de información se llenen de despojos de todo tipo. Las preguntas a los operadores se plantearán malamente, y las respuestas (si es que están disponibles) serán impulsadas hacia el mínimo común denominador de procedimientos de operación estándar programados anteriormente. Los sistemas de represalia que dependen de alerta de lanzamientos al recibir un aviso en vez de supervivencia después de sufrir un ataque son especialmente vulnerables a ciclos reducidos y alternativas restringidas.

La tendencia a buscar la primera alternativa disponible que cumpla con las condiciones satisfactorias mínimas de alcance de objetivos es suficientemente fuerte en condiciones normales de organizaciones burocráticas no militares.[20] En sistemas C2 cívico-militares bajo la tensión de toma de decisiones de crisis militares, la primera alternativa disponible puede ser literalmente la última—o así se pueden persuadir a sí mismos los encargados de la política y sus consejeros militares. De forma correspondiente, el sesgo hacia soluciones prontas y adecuadas es fuerte. Durante la crisis de misiles cubana, por ejemplo, un número de miembros del grupo de consejeros presidenciales siguió proponiendo un ataque aéreo y la invasión de Cuba durante cada uno de los 13 días de deliberación durante la crisis. Si se hubiera dispuesto de menos tiempo para debatir y si el Presidente Kennedy no hubiera estructurado deliberadamente el debate de forma que surgieran alternativas, el ataque aéreo y la invasión podrían haber sido claramente la alternativa escogida.

En cuarto lugar —y finalmente sobre el problema de la gestión de crisis— la guerra de información puede causar la transmisión de imágenes deformadas de las intenciones y capacidades de un bando al otro, con unos resultados potencialmente desastrosos. Otro ejemplo de la crisis cubana de los misiles demuestra los posibles efectos secundarios de un simple malentendido y la falta de comunicación sobre la gestión de crisis de EUA. Durante el período más tenso de la crisis, un avión de reconocimiento U-2 se desvió de la ruta y se introdujo en el espacio aéreo soviético. Aviones caza de EUA y de la Unión Soviética despegaron de inmediato, y se avecinó una posible confrontación de las fuerzas aéreas en el Ártico. Jrushchov dijo después a Kennedy que las defensas aéreas soviéticas podrían haber inter-

pretado que el vuelo del U-2 era una misión de reconocimiento antes de un ataque o un bombardeo, lo que requería una respuesta de compensación por parte de Moscú.[21] Afortunadamente, el liderazgo soviético decidió dar el beneficio de la duda a Estados Unidos en este caso y permitir que los aviones caza de EUA escoltaran el U-2 extraviado de regreso a Alaska. Nunca se ha revelado por completo por qué no se eliminó esta misión programada del U-2 una vez que se inició la crisis; la respuesta puede ser tan simple como que la inercia burocrática se complicó debido a la falta de comunicación hacia abajo de la cadena de mando por parte de los encargados de la política que no supieron apreciar el riesgo de un reconocimiento "normal" en estas condiciones extraordinarias.

El debate y los ejemplos anteriores son subrayados por la evaluación del analista experto Martin Libicki en lo que se refiere a la relación entre la guerra cibernética y la gestión de crisis:

> Para generalizar, una situación en la que hay poca presión para responder rápidamente, en la que una desventaja o pérdida temporal es tolerable, y en la que hay motivos para conceder al otro bando cierto beneficio de la duda es una en la que hay tiempo para que dé resultado la gestión de la crisis. Por el contrario, si al no responder rápidamente se hace que la posición de un estado se erosione, una desventaja o un nivel de pérdida temporales es intolerable, y no hay motivos para disputar lo que ha ocurrido, quién lo hizo, y por qué —entonces los estados pueden llegar a la conclusión de que hay que tomar una decisión rápidamente.[22]

Esta vista general de las posibles disfunciones en la gestión de una crisis nuclear cuando se solapa con la guerra cibernética no es necesariamente totalmente pesimista. Las personas siguen a cargo, no las computadoras ni las redes de información. Si esas personas llevan a la mesa un conocimiento de la falibilidad humana, una apreciación del precedente histórico, y un sentido claro de proporción sobre el uso de tecnología en tiempos de paz, crisis y guerra, tienen todas las probabilidades de tener éxito. Por otra parte, los encargados de tomar decisiones con un exceso de confianza en sus habilidades, al no conocer precedentes históricos, y estar intoxicados con arrogancia técnica o sistemas militares por sí mismos pueden lograr una cantidad considerable de caso en un tiempo muy corto.

Conclusiones

Las herramientas cibernéticas no anulan la necesidad de una disuasión nuclear, y los modelos analíticos diseñados para el estudio de disuasión nuclear no pueden transferirse directamente al reino del conflicto cibernético sin crear un tumulto de paradigmas. No obstante, los planificadores militares y los formuladores de políticas encontrarán puntos comunes entre los problemas nucleares y cibernéticos. El problema de una guerra cibernética verdaderamente "estratégica" diferenciada de los ataques cinéticos plantea un problema menos inminente que la parte cibernética como facilitador (o desfacilitador) del éxito en la guerra convencional o la disuasión nuclear. El futuro de la tecnología digital, en la medida que se aplica a asuntos militares, es una guía misteriosa mágica de lo desconocido. Pero una apuesta más segura es que los futuros sistemas de C2 y comunicaciones nucleares, impulsados no obstante por mejoras digitales, tendrán que satisfacer los requisitos de política y estrategia para una respuesta temprana a comandos autorizados, evitar positivos falsos en advertencia y reacción tempranas, y mantener un espectro de opciones viables para los formuladores de política y comandantes, incluso en condiciones de guerra o de amenaza inminente de guerra.

La relación entre la gestión de la crisis nuclear y la edad de la información es un trabajo en curso, pero ahora pueden identificarse varias emboscadas potenciales de disuasión nu-

clear y estabilidad de crisis. En primer lugar, la guerra cibernética o el funcionamiento erróneo del software podrían interferir con una comunicación fiable. En segundo lugar, los ataques cibernéticos podrían tener lugar antes de que los encargados en tomar decisiones interpretaran los resultados y adoptaran una respuesta apropiada. En tercer lugar, la identidad de un atacante cibernético podría no ser clara durante una crisis; de hecho, un tercero podría "imitar" una comunicación estadounidense o rusa o crear un embolismo de información en cualquiera de las redes del estado. En un caso extremo, un pirata informático dirigido por un estado o un malware de un individuo descontento podría accionar una advertencia de ataque incorrecto o un comando de lanzamiento falso. Además, incluso si suponemos que los sistemas nucleares actuales y posibles estadounidenses y rusos son una prueba contra las advertencias erróneas o lanzamientos accidentales, la vulnerabilidad de los sistemas de C2 y lanzamiento nucleares de otros estados a la guerra cibernética es desconocida. ❑

Notas

1. P. W. Singer y Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know (Seguridad y guerra cibernéticas: lo que todos deben saber)* (New York: Oxford University Press, 2014), esp. 126–38.

2. La estrategia de defensa de EUA define tres misiones cibernéticas primarias del Departamento de Defensa (DOD): defensa de las redes, sistemas e información del DOD; defensa de intereses nacionales y en suelo estadounidense contra ataques cibernéticos de consecuencia significativa; y respaldo cibernético para operaciones militares y planes de contingencia. Vea el Departamento de Defensa de EUA, *The DOD Cyber Strategy (La estrategia cibernética del DOD)* (Washington, DC: Departamento de Defensa de EUA, abril de 2015), esp. 4–6, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf. Vea también Cheryl Pellerin, "DARPA's Plan X Gives Military Operators a Place to Wage Cyber Warfare" (El Plan X da a los operadores militares de DARPA un lugar para librar una guerra cibernética), Departamento de Defensa de EUA, 12 de mayo de 2016, http://www.defense.gov/News-Article-View/Article/758219/darpas-plan-x-gives-military-operators-a-place-to-wage-cyber-warfare; Edward Geist, "Deterrence Stability in the Cyber Age" (Estabilidad disuasoria en la era cibernética), *Strategic Studies Quarterly* 9, no. 4 (Invierno de 2015): 44–61; Robert Spalding III y Adam Lowther, "The New MAD World: A Cold War Strategy for Cyberwar" (El nuevo mundo de la destrucción mutua asegurada: una estrategia de la Guerra Fría para la guerra cibernética), *National Interest*, 22 de junio de 2015, http://nationalinterest.org/feature/the-new-mad-world-cold-war-strategy-cyberwar-13154; Singer y Friedman, *Cybersecurity and Cyberwar (Seguridad y guerra cibernéticas)*; Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling* (Sentido estratégico del poder cibernético: por qué no se nos cae el cielo en la cabeza) (Carlisle, PA: Instituto de Estudios Estratégicos, Colegio de Guerra del Ejército de EUA, abril de 2013); Martin C. Libicki, *Crisis and Escalation in Cyberspace (Crisis y escalada en el ciberespacio)* (Santa Monica, CA: RAND Corporation, 2012); Kamaal T. Jabbour y E. Paul Ratazzi, "Does the United States Need a New Model for Cyber Deterrence?" (¿Necesita Estados Unidos un nuevo modelo de disuasión cibernética?), capítulo 3 en *Deterrence: Rising Powers, Rogue Regimes, and Terrorism in the Twenty-First Century (Disuasión: potencias emergentes, regímenes gamberro en el siglo XXI)*, ed. Adam B. Lowther (New York: Palgrave Macmillan, 2012), 33–45; y Martin C. Libicki, *Cyberdeterrence and Cyberwar (Disuasión y guerra cibernéticas)* (Santa Monica, CA: RAND, 2009).

3. El virus "Stuxnet" es un ejemplo contrario ya que estaba diseñado específicamente y con el fin de la destrucción de centrífugas nucleares en Irán. Vea Singer y Friedman, *Cybersecurity and Cyberwar (Seguridad y guerra cibernéticas)*, esp. 114–20. Sobre los conceptos de operaciones de información de las potencias principales, vea Timothy L. Thomas, *Cyber Silhouettes: Shadows over Information Operations (Siluetas cibernéticas: sombras sobre las operaciones de información)* (Fort Leavenworth, KS: Oficina de Estudios Militares Exteriores, 2005), capítulos 5–6, 10, 14, y alusiones en diferentes partes de la publicación. Vea también Pavel Koshkin, "Are Cyberwars between Major Powers Possible? A Group of Russian Cybersecurity Experts Debate the Likelihood of a Cyberwar Involving the U.S., Russia or China" (¿Son posibles las guerras cibernéticas entre las grandes potencias? Un grupo de expertos de seguridad cibernética rusos debaten la probabilidad de una guerra cibernética en la que participaran Estados Unidos, Rusia o China), *Russia Direct*, 1 de agosto de 2013, http://russia-direct.org, en *Johnson's Russia List, 2013*, no. 143 (6 de agosto de 2013), davidjohnson@starpower.net.

4. Las armas cibernéticas no son necesariamente fáciles de usar efectivamente como instrumentos habilitadores para un efecto operacional/táctico o estratégico. Vea Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare (Conquista en el ciberespacio: la seguridad nacional y la guerra informática)* (New York: Cambridge University Press, 2007), esp. capítulos 4–5.

5. Andrew Futter, "Cyber Threats and the Challenge of De-alerting US and Russian Nuclear Forces" (Amenazas cibernéticas y el reto de dejar de alertar a las fuerzas nucleares estadodunidenses y rusas), NAPSNet Policy Forum,

15 de junio de 2015, http://nautilus.org/napsnet-policy-forum/cyber-threats-and-the-challenge-of-de-alerting-us-and-russian-nuclear-forces/. Vea también Franz-Stefan Gady, "Could Cyber Attacks Lead to Nuclear War?" (¿Podrían los ataques cibernéticos desencadenar una guerra nuclear?), *Diplomat*, 4 de mayo de 2015, http://thediplomat.com/2015/05/could-cyber-attacks-lead-to-nuclear-war/.

6. Existe una crítica experta de propuestas para una disuasión mínima de fuerza nucleares de EUA en la publicación del Dr. Keith B. Payne, director del estudio, y del Honorable James Schlesinger, presidente, Senior Review Group, titulada *Minimum Deterrence: Examining the Evidence (Disuasión mínima: examen de la evidencia)* (Fairfax, VA: Instituto Nacional de Política Pública, National Institute Press, 2013). Para obtener una evaluación experta favorable de las posibilidades de una disuasión mínima, vea James Wood Forsyth Jr.; Coronel B. Chance Saltzman, USAF; y Gary Schaub Jr., "Remembrance of Things Past: The Enduring Value of Nuclear Weapons" (Recuerdos de cosas del pasado: el valor duradero de las armas nucleares), *Strategic Studies Quarterly* 4, no. 1 (Primavera de 2010): 74–90.

7. Bruce Blair, "Could Terrorists Launch America's Nuclear Missiles?" (¿Podrían los terroristas lanzas misiles nucleares?), *Time*, 11 de noviembre de 2010, http://content.time.com/time/nation/article/0,8599,2030685,00.html. Un editor de este artículo objetó el argumento de Blair citado, respondiendo que su evaluación eran "claramente falsa".

8. Mayot Clifford S. Magee, USMC, "Awaiting Cyber 9/11" (A la espera de un cibertaque tipo 9/11), *Joint Force Quarterly* ejemplar 70 (3º trimestre de 2013): 76, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-70/JFQ-70_76-82_Magee.pdf.

9. Brian M. Mazanec, "Why International Order in Cyberspace Is Not Inevitable" (Por qué el orden internacional en el ciberespacio no es inevitable), *Strategic Studies Quarterly* 9, no. 2 (Verano de 2015): 80, http://www.au.af.mil/au/ssq/digital/pdf/summer_2015/SSQ_Summer_2015.pdf.

10. James Wood Forsyth Jr. y Mayor Billy E. Pope, USAF, "Structural Causes and Cyber Effects: Why International Order Is Inevitable in Cyberspace" (Causas estructurales y efectos cibernéticos: por qué es inevitable el orden internacional en el ciberespacio), *Strategic Studies Quarterly* 8, no. 4 (Invierno de 2014): 118, http://www.au.af.mil/au/ssq/digital/pdf/winter_14/forsyth.pdf. Vea también Mazanec, "International Order in Cyberspace" (El orden internacional en el ciberespacio) 96. El asunto sobre si el ciberespacio es un "dominio" u otra cosa es un debate epistemológico en el que aquí no se ha entrado.

11. Mazanec, "International Order in Cyberspace" (Orden internacional en el ciberspacio, 83.

12. Joel Brenner, *Glass Houses: Privacy, Secrecy, and Cyber Insecurity in a Transparent World (Casas de cristal: privacidad, secretos e inseguridad cibernética en un mundo transparente)* (New York: Penguin Books, 2013), 3.

13. Ibid., 73.

14. David E. Sanger y Julie Hirschfield Davis, "Hacking Linked to China Exposes Millions of U.S. Workers" (Pirateo informático conectado con China expone a millones de trabajadores de EUA), *New York Times*, 4 de junio de 2015, http://www.nytimes.com/2015/06/05/us/breach-in-a-federal-computer-system-exposes-personnel-data.html; y Chris Frates, "IRS Believes Massive Data Theft Originated in Russia" (El IRS cree que un robo masivo de datos se originó en Rusia), *CNN*, 4 junio de 2015, http://www.cnn.com/2015/05/27/politics/irs-cyber-breach-russia/.

15. Dorothy E. Denning, "Rethinking the Cyber Domain and Deterrence" (Reflexiones sobre el dominio y la disuasión cibernéticos), *Joint Force Quarterly* 77 (segundo trimestre de 2015): 11, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-77/jfq-77_8-15_Denning.pdf.

16. Ibid., 12.

17. Ibid., 13–15.

18. Para obtener definiciones útiles de *ataque cibernético* y g*uerra cibernética*, vea Paul K. Davis, "Deterrence, Influence, Cyber Attack, and Cyberwar" (Disuasión, influencia, ciberataque y guerra cibernética), *International Law and Politics* 47 (2015): 327–55, esp. 328.

19. Un virus es un programa que se reproduce automáticamente con la intención de destruir o alterar el contenido de otros archivos almacenados en discos flexibles o duros. Los gusanos corrompen la integridad de los sistemas de software e información de "dentro a afuera" de forma que crean puntos débiles que pueden ser aprovechados por un enemigo.

20. James G. March y Herbert A. Simon, *Organizations* (New York: John Wiley and Sons, 1958), 140, 146.

21. Graham T. Allison, *Essence of Decision: Explaining the Cuban Missile Crisis (Esencia de decisión: explicación de la crisis de misiles cubana)* (Boston: Little, Brown, 1971), 141. Vea también Scott D. Sagan, *Moving Targets: Nuclear Strategy and National Security (Objetivos móviles: estrategia nuclear y seguridad nacional)* (Princeton, NJ: Princeton University Press, 1989), 147.

22. Libicki, *Crisis and Escalation in Cyberspace (Crisis y escalada en el ciberespacio)*, 145.

Dr. Stephen J. Cimbala, PhD (BA, Penn State; MA, PhD, Universidad de Wisconsin–Madison) es un Profesor Distinguido de Ciencias Políticas en Penn State–Brandywine. El Dr. Cimbala, instructor ganador de un premio en Penn State, es autor de numerosas obras en los campos de control de armas nucleares, disuasión, policía de seguridad nacional y otros temas. Recientemente publicó su obra *The New Nuclear Disorder: Challenges to Deterrence and Strategy* (El nuevo desorden nuclear: retos de disuasión y estrategia) (Ashgate, 2015). El Dr. Cimbala ha servido en los consejos editoriales de publicaciones académicas, y ha sido consultor para varias agencias y contratistas del gobierno de EUA.