

El Espectro de una Guerra no Evidente

DR. MARTIN C. LIBICKI, PhD*

LAS INNOVACIONES, tanto tecnológicas como organizativas, en las últimas décadas han creado un potencial de una guerra no evidente,¹ en la que la identidad del lado combatiente e incluso el mero hecho de la guerra son completamente ambiguos.

El gusano informático Stuxnet es solamente el ejemplo más reciente hecho público extensivamente. Se cree que este gusano ha infiltrado la instalación de centrífugas Natanz de Irán, haciendo que los equipos se destruyan a sí mismos en un período de semanas y produzcan la reducción prematura del 10 por ciento de la capacidad de enriquecimiento de uranio de Irán. Varios meses después de la divulgación pública del gusano (septiembre de 2010), las fuentes de inteligencia occidentales anunciaron que la fecha más próxima en la que Irán podía construir una bomba se había retrasado varios años. Hasta que se descubrió y examinó el gusano, los mismos iraníes no estaban seguros de la razón por la que sus equipos se desgastaban tan deprisa. De hecho, cuando se preguntó a Irán públicamente acerca de la posibilidad, primero negaron que había ocurrido dicho ataque, y dos meses más tarde dijeron lo contrario con rodeos.

Aunque la ciberguerra es el mejor ejemplo de guerra no evidente,² los estados pueden atacarse unos a otros de muchas maneras sin que la víctima sepa exactamente quién lo hizo o incluso qué se hizo. Algunas guerras, como la guerra electrónica (contra objetivos no militares) y la guerra espacial, aún no se han materializado de ninguna forma significativamente estratégica. Otros, como las minas navales/terrestres o el sabotaje, tienen largos antecedentes históricos. Lo que comparten es la ambigüedad. Entre una lista corta de tipos de guerra que *podría* llevarse a cabo plausiblemente de una manera no evidente se incluyen las siguientes

- ciberguerra;
- guerra espacial;
- guerra electrónica;
- guerra de drones;
- sabotaje, operaciones especiales, asesinatos, y minas;
- ataques de fuerzas sustitutas;
- armas de destrucción masiva; y
- respaldo de inteligencia para operaciones de combate.

La guerra no evidente ofrece un contraste claro, por ejemplo, con la invasión de carros de combate que tuvo lugar en la frontera entre Alemania y Polonia, un acontecimiento que con muy poca probabilidad planteara preguntas como, ¿qué carros de combate son esos, . . . y por qué están aquí? Por el contrario, los *usos* de guerra no evidente son limitados. Es bastante difícil capturar la capital de otro país de forma anónima (las fuerzas sustitutas pueden hacerlo pero a

*El Dr. Martin C. Libicki, PhD es un científico de gestión superior de RAND Corporation, que se concentra en los impactos de la tecnología de información en seguridad doméstica y nacional. Ha publicado *Conquest in Cyberspace: National Security and Information Warfare and Information Technology Standards: Quest for the Common Byte (Conquista en el ciberespacio: Seguridad nacional y Guerra de información y normas de tecnología de información)*, así como numerosas monografías. Anteriormente trabajó en la Universidad de Defensa Nacional, estado mayor de la Armada y la División de Energía y Minerales de GAO. El Dr. Libicki tiene un título de maestría y un doctorado de la Universidad de California–Berkeley. Este artículo fue anteriormente publicado en nuestra revista *Strategic Studies Quarterly*, Vol. 6, No. 3, Fall 2012.

esas alturas dejan de ser sustitutas y evolucionan hasta convertirse en dependientes o incluso independientes). La guerra defensiva es llevada a cabo casi siempre por el que posee lo que se defiende. Incluso la coacción requiere una autoidentificación *si* el “me” en—“no me pises”—no se comunica de forma adecuada. Pero hay algunos tipos de guerra que no se pueden llevar a cabo de forma satisfactoria o incluso de forma más ventajosa si hay duda de quién hizo qué. Nuevamente, Stuxnet constituye un ejemplo. Demorar el programa nuclear iraní benefició a Israel, tanto si alguien sabe o no con certeza si Israel (o alguien más) lo hizo. Además, si la finalidad de la guerra es hacer cambiar de ideas en la capital de la víctima, la incertidumbre puede concentrar la reflexión subsiguiente en lo que dice un ataque así sobre la seguridad y la potencia (reducida) de la víctima en vez de sobre la malevolencia del atacante sin determinar.

De forma correspondiente, este artículo explora el tema en varios pasos. Lo primero es desarrollar un sentido de lo que significa no ser evidente. Lo segundo es delinear varias formas de guerra que, en ciertas circunstancias, pueden ser no evidentes y por qué. Lo tercero es especular sobre cómo los estados (y los actores que no son estados) podrían hacer uso de la guerra no evidente. Lo cuarto es especular sobre cómo los estados víctima pueden responder a la amenaza de guerra no evidente.

¿Cuándo no es evidente la guerra?

La ambigüedad es la base de la falta de evidencia. Si la víctima no está segura de quién llevó a cabo una operación, puede tener dudas acerca de responder de la misma manera que si fuera cierto. De forma alternativa, el resto del mundo podría tener dudas incluso si la víctima tiene certeza, haciendo que la víctima se sienta insegura de responder como lo haría si *otros* estuvieran muy seguros de lo que pasa.

La falta de evidencia aumenta si los acontecimientos en cuestión pueden cuestionarse por sí mismos. Algunos podrían ser accidentes o misterios absolutos, por ejemplo, la falla inexplicable de un satélite. Otros podrían ser delitos, como robos a bancos por grupos con inclinación política, o actos de espionaje—muchos acontecimientos denominados ciberataques son realmente intentos de sustraer información. No obstante, algunos incidentes bélicos no evidentes serían claramente actos de guerra si fueran evidentes—en cuyo caso, la ambigüedad clave es el actor y no el acto.

Algunas formas de guerra no son evidentes porque la relación entre el atacante y un estado no es clara; por ejemplo, ¿en qué medida trabaja Hizbulá para sus propios fines, y en qué medida es una marioneta manipulada por Teherán? En algunos casos los perpetradores pueden ser empleados del estado que no están necesariamente trabajando, o al menos no probablemente, bajo el mando y control del propio estado. ¿El hecho de que alguien cercano a la estructura política rusa se atribuyera haber organizado ataques a instituciones estonias en Rusia significa que fue un ataque de Rusia?³ Se ha acusado a la agencia de inteligencia ISI de Pakistán de haber protegido a jefes militares talibanes; así pues, ¿está Pakistán en guerra con Afganistán? Si ambas preguntas pueden responderse con un “sí”, entonces estos los dos ejemplos anteriores son ejemplos de guerra no evidente.

Por último, muchas formas de guerra no evidente no presentan ningún riesgo personal para los combatientes—que tendrían que hacerlo, casi por definición, ya que la captura o identificación del perpetrador puede hacer que la fuente del ataque sea evidente. Pero nadie puede llegar a la conclusión de que los *estados* que empleen dichos combatientes estén desligados simplemente porque lo estén sus combatientes. Un método de guerra sin huellas digitales puede ser el siguiente paso lógico después de un método sin huellas de pisadas, pero los dos siguen siendo bastantes diferentes.

La falta de evidencia no es absoluta, y el umbral de respuesta dinámica para el estado víctima variará enormemente. El criterio principal es el grado de confianza que siente la víctima de que cierto estado llevó a cabo un ataque—sí, ciertamente, lo que ocurrió realmente *fue* un ataque. Esta probabilidad percibida va a ser casi siempre distinta de cero. Hay pocos estados que crean realmente que ningún otro estado quiera dañarles. Incluso lo que más adelante se demuestra que son accidentes (por ejemplo, la explosión del barco de EE.UU. *Maine*) se culpa a menudo a otros estados (por ejemplo, España). Si hay una crisis (por ejemplo, intento de España de sofocar una insurgencia cubana), la tendencia a creer que cualquier suceso dañino e inusual es un ataque será mucho más elevada.

Así pues, el atacante que atacara con impunidad debe preguntarse si la confianza con que la víctima cree que se llevó a cabo el ataque es probablemente mayor o menor que la confianza que requiere la víctima para responder al ataque. Todo depende de cuál es el umbral de la respuesta, y puede haber muchos tipos de respuestas. La evidencia suficiente para lograr una condena criminal en un tribunal de EE.UU. “fuera de toda duda razonable” es pocas veces el caso, aunque similarmente unos altos niveles de confianza pueden, de hecho, ser necesarios antes de que la víctima decida ir a la guerra. Por otra parte, la mera sospecha puede bastar para reducir o desaprobar presuntos planes de cooperación como ejercicios militares conjuntos, investigación conjunta o relaciones de redes homólogas. En el caso de algunas formas de guerra no evidente, el objetivo puede no estar seguro en lo que se refiere al patrocinio del estado pero puede convenirse a sí mismo de que dicho estado tiene que responsabilizarse de parte de la culpa si pudiera haber detectado y detenido u obstaculizado razonablemente dicho ataque y se hubiera negado a hacerlo.

También variará de qué forma aproximada el estado objetivo adquirirá la confianza de que otro estado específico llevó a cabo un ataque, pero uno no puede equivocarse mucho al considerar los medios, los motivos y la oportunidad. La oportunidad—en forma de algún vehículo de suministro identificable—a menudo distingue mejor la guerra evidente de la no evidente. Pero la oportunidad representa solamente un tercio. Considere, por ejemplo, cómo reaccionaría Estados Unidos ante la detonación de una llamada arma nuclear de maletín alrededor de, digamos, 1962. El maletín se incineraría, dejando poca evidencia forense. Pero en esa época, solamente otros tres estados disponían de los *medios* para llevar a cabo un ataque nuclear, y de esos tres, solamente uno, la URSS, tenía un *motivo* para hacerlo. En dichas circunstancias, la falta de un vehículo de suministro visible habría mellado poco la confianza de EE.UU. de creer que la URSS lo había hecho. De forma similar, para muchos tipos de guerra no evidente, dichos ataques a naves espaciales, la lista de sospechosos sería muy corta, ya que el número de naciones que navegan por el espacio es limitado (aunque, en ese caso, la víctima también debe distinguir con credibilidad entre accidentes y ataques).

Tipos de guerra no evidente

¿Qué es lo que hace que distintas formas de guerra evidente sean de hecho no evidentes? Examinémoslas una por una.

Ciberguerra

Los piratas pueden estar sentados en cualquier lugar y atacar sistemas de todo el mundo, alterando su funcionamiento, corrompiendo la información que tienen y los algoritmos que utilizan, y, según mostró Stuxnet, incluso descomponiendo máquinas al enviarles comandos dañinos desde sistemas pirateados. La atribución es particularmente difícil para un ciberataque. Los unos y ceros que constituyen el ataque no dejan los residuos físicos de sus operadores (especialmente si estos unos y ceros se copiaron de herramientas de otros). Los sistemas atacados con éxito, casi

por definición, no pueden distinguir un ataque de entradas completamente benignas en el momento (con un ataque de denegación de servicio distribuido, lo que importa es el volumen, no el contenido; los bytes de ataque generalmente proceden de máquinas “inocentes” que son manipuladas para bombardear a la víctima con mensajes no solicitados). Los métodos forenses como la identificación del ataque hasta sus orígenes pueden frustrarse fácilmente haciendo rebotar el ataque a través de suficientes portales, usando los servicios de una máquina inocente o pasando a una tercera conexión Wi-Fi. Las dificultades de atribución pueden ser inherentes al medio y es poco probable que mejoren en los años venideros. Los estados que deseen adivinar quién les atacó se dan cuenta de que deben fiarse de los medios y del motivo. Los medios ofrecen solamente poca ayuda en caso de un ataque poco refinado, ya que más de 100 países han investigado la ciberofensiva y la lista de piratas incluye grupos del crimen organizado, actores que no son estados e individuos. Por lo general, se cree que solamente un estado podría haber efectuado un ataque refinado como el de Stuxnet, con sus cuatro vulnerabilidades de días cero y dos certificados robados. Irán puede haber averiguado, una vez que se dio cuenta de que *había* sido atacado, que solamente Israel y Estados Unidos tendrían la razón y el talento para llevar a cabo un ataque de este tipo. Sin embargo, no es completamente imposible que Rusia o China hayan querido retrasar la carrera de armas nucleares de Irán.

Nadie sabe todavía si los ciberataques llevados a cabo de una manera no evidente demostrarán ser ventajosos para los que lo llevan a cabo. No está claro ni mucho menos que los ataques de Rusia (o rusos) a Estonia o Georgia le hicieran mucho bien. Si Israel atacara a Irán en el ciberespacio, lo que parecería un éxito podría considerarse como el principio de un nuevo conjunto de operaciones militares, o, de forma alternativa, un caso muy especial que nadie puede ni necesita duplicar.

Guerra espacial

Los satélites normalmente pierden capacidad de vez en cuando en la inmensidad y oscuridad del espacio. Un ataque a un satélite sin que se descubra el vehículo de ataque puede convertirse casi en el crimen perfecto. Los estados tal vez deseen saber lo que ocurrió, pero sacar un satélite de su órbita tal vez no sea necesariamente algo para lo que el satélite se diseñó, puede hacerse imposible debido a la naturaleza del ataque y requerirá gastos de una cantidad sustancial de combustible. Aunque el análisis posterior a la recuperación indicaría probablemente lo que ocurrió, tal vez se siga sin saber quién lo hizo. Una vez observado eso, salirse con la suya después de atacar a un satélite presenta dificultades. Estados Unidos tiene la capacidad de averiguar la plataforma de lanzamiento de todos los misiles terrestres suficientemente grandes y supuestamente puede hacer el seguimiento de objetos espaciales del tamaño de llaves (los detalles exactos serían indudablemente secretos). Como tiene una idea bastante buena de lo que está haciendo cada satélite, los que se emplean de otra manera son descubiertos necesariamente, pero la llegada de microsátélites, nanosatélites y picosatélites puede complicar la detección por sustracción en los años venideros. Los sistemas terrestres pueden cegar los satélites, pero los satélites tienen que mirar a lo que sea que les esté cegando (es decir, indicar de dónde procede el láser). El número de estados que pueden comprar una plataforma de lanzamiento es mucho mayor que los pocos que pueden lanzar objetos al espacio.

Guerra electrónica

A medida que nuestro mundo interconectado se hace cada vez más inalámbrico, el potencial de interferencias electrónicas crece por al mismo ritmo. Los dispositivos radiantes genéricos pequeños emplazados o dispersos de forma clandestina pueden bloquear señales de GPS (al menos para receptores comerciales) y causar estragos en las comunicaciones, que van desde comunicaciones de teléfonos móviles y de emergencia a controladores de máquinas. A veces puede ser

bastante difícil localizar dichos dispositivos pero no caracterizarlos (es poco probable confundir por mucho tiempo las interferencias deliberadas con causas naturales o accidentes). El uso de dispositivos genéricos puede frustrar la identificación, pero lo difícil en el anonimato es no ser sorprendido en el emplazamiento de dichos dispositivos. Una vez que empiecen a operar los dispositivos, su vida útil es limitada, porque son descubiertos o porque se agotan sus baterías.

Drones

En una serie de circunstancias relativamente limitadas, se puede llevar a cabo un ataque de drones sin una atribución firme. Los requisitos son muchos. El drone tiene que evitar que se estrelle (o debe recuperarse si se estrella); de lo contrario, existe una buena probabilidad de identificar incluso hasta el último comprador de un drone genérico. El país objetivo tiene que tener una cobertura de radar relativamente deficiente o ser contiguo a territorios u océanos donde no haya cobertura de radar. Si el drone procede del océano, la lista de posibles atacantes puede limitarse a los que tienen barcos en el área en ese momento. El drone mismo tiene que ser bastante genérico—de modo que su perfil a una distancia sea coherente con el inventario de muchos países diferentes—o ser furtivo. Por último, la posibilidad de que el ataque de un drone pueda ser un ataque no evidente de Estados Unidos debe esperar al desarrollo de drones de ataque por países *distintos* de Estados Unidos—si eso no ocurre, se asumirá que cualquier drone es estadounidense. Para estados en dificultades con Estados Unidos, la combinación de motivo y medios puede bastar.

Operadores especiales, sabotadores y asesinos

Al igual que con los drones, la clave para mantener el anonimato en operaciones especiales es evitar ser sorprendido. Irónicamente, la capacidad de llevar a cabo *muchas* operaciones especiales sin ser sorprendido requiere tantas destrezas organizativas y profesionales que el número de países capaces de hacer esto es pequeño—hacer acusaciones es mucho más creíble. De aquí que, la perfección puede ser delatora, a menos que el atacante muestre una moderación considerable. Esta categoría incluye minado por transporte encubierto (por ejemplo, submarinos), que, al menos, le da una resonancia histórica, pero también una resonancia contemporánea, como en los daños misteriosos—y disputados—a una embarcación irlandesa preparada para romper el bloqueo de Gaza.⁴

Ataques con fuerzas sustitutas

Esta amplia categoría incluye terroristas, insurgentes, milicias y corsarios. La atribución se dificulta porque generalmente requiere la captura de los perpetradores (o el uso de un método de operación reconocible) pero en su mayor parte porque requiere relacionar al perpetrador con un actor importante. No obstante, en la práctica la relación entre grupos insurgentes y estados realmente es ambigua, y no necesariamente, por diseño; facultar a individuos con organización, ideología y armamento tiende a hacerles creer que sus objetivos son importantes por sí mismos. El Vietcong, por ejemplo, puede haber sido establecido y sostenido por Vietnam del Norte pero tenían prioridades ligeramente diferentes.⁵ África proporciona un caso más pertinente en el que varios países que patrocinaron insurgencias contra sus vecinos se las arreglaron para encontrarse sitiados por insurgentes propios, respaldados de forma similar.

Ataques usando armas de destrucción masiva

A la llamada bomba del maletín de la época de la Guerra Fría se les ha añadido el uso de agentes biológicos y químicos—de los que hay muchos tipos—todos los cuales ofrecen, al menos en

teoría, un método de matar a personas sin que un estado se vea sorprendido haciéndolo. Por regla general, como las armas de destrucción masiva son relativamente pequeñas, es posible que su uso no requiera una inserción forzosa, y los componentes electrónicos modernos permiten detonarlas de forma remota. No obstante, dichos ataques se consideran particularmente infames, y casi todos los estados han firmado uno o más tratados internacionales contra eso. Por esa razón, más de esos ataques pueden identificarse a su último origen que un ataque similarmente encubierto por altos explosivos. Por supuesto, los agentes infecciosos, particularmente los que se puedan inventar por técnicas de recombinación de ADN, pueden suministrarse de una manera muy encubierta. No obstante, a menos que los ciudadanos propios de un estado sean de alguna manera inmunes a sus efectos, no está claro lo que ganaría ese estado al usarlos o, si se usan en una modalidad de “tipo fin del mundo”, por qué a un estado le gustaría ser no evidente en lo que respecta al asunto.

Apoyo de inteligencia a las operaciones de combate

Aunque técnicamente no es una guerra, un estado con un mecanismo refinado a distancia de recopilación de inteligencia y procesamiento/distribución puede proporcionar datos que pueden ser de gran ayuda para sus amigos. Si la asistencia no es interceptada directamente y su distribución es limitada, entonces otros tendrían dificultad en distinguir el origen de forma certera (aunque los estados pueden sospechar que los oponentes por debajo de sus posibilidades pueden haber tenido cierta ayuda, solamente un puñado de países podrían suministrarlo y lo suministrarían). A diferencia de otras formas de guerra no evidente, la ayuda con información no es particularmente infame, y las negaciones—o al menos “ni confirmar ni negar”—son normales en el mundo de la inteligencia. No obstante es posible que el estado proveedor no muestre su participación en el conflicto para no ser acusado de ser beligerante o si tiene un rival que pueda justificar entonces *su propia* asistencia al otro bando.

Merece la pena repetir que a menos que el ataque parezca un accidente completo—y el objetivo sea completamente creíble—no existe un ataque que sea completamente no atribuible. Cada estado tiene sus enemigos o amigos que no son de fiar, y si pasa algo desagradable, se sacarán a relucir los sospechosos normales para el examen. Por el contrario, la capacidad de negación plausible importa solamente si el estado víctima realmente necesita algo aproximado a una prueba judicial para tomar medidas o si se siente aliviado de que la autoridad del ataque no sea tan evidente que su negativa a responder no se considere una cobardía. Los perpetradores no tienen que ser sorprendidos con las manos en la masa para sufrir represalias en manos de los que pueden juntar medios, motivos y oportunidad para formar una base suficientemente robusta para llevar a cabo una acción.

Los usos de guerra no evidente

A menudo es más fácil afirmar lo que *no se puede* hacer con la guerra no evidente. Su falta de aplicabilidad para la conquista y la coacción específica ya se ha observado. Además, cualquier finalidad que requiera una serie sostenida de ataques no puede usar una técnica de guerra no evidente si la probabilidad de imputación de cada ataque no es cero y la probabilidad de imputar un acontecimiento es al menos algo independiente de la probabilidad de imputar otro. Esto descarta la guerra espacial, la guerra electrónica, los drones y las operaciones especiales. También puede descartar la ciberguerra pero es menos probable que se descarte la guerra de fuerzas sustitutas—donde la atribución debe inferirse en vez de descubrirse—y el apoyo de la inteligencia a la guerra.

Entonces, ¿qué *se puede* hacer con la guerra no evidente? Un uso es la coacción o disuasión generales. En vez de señalar, “si haces esto nosotros haremos eso”, la señal es, “si hace esto

entonces le pasarán cosas malas”. Como el acto de señalar mismo puede implicar al atacante, es útil si las señales proceden de alguien más. Otros pueden desear ayudar si hay múltiples estados con un interés común, como Vietnam, Indonesia y Filipinas que se oponen a la fanfarronería china en el Mar de China del Sur. Estos otros pueden ser también correligionarios o coideólogos (por ejemplo, “faltan al respeto a nuestra religión y le pasarán cosas malas”). El uso de guerra no evidente para obligar es más complicado que dé resultado, ya que es más fácil que entidades dispares se pongan de acuerdo en lo que se va a condenar que en lo que se debe hacer.

Otro uso muy evidente es el sabotaje, tipo Stuxnet, llevado a cabo para denegar a su objetivo cierta capacidad. La dificultad es que el sabotaje es bastante ineficaz a menos que tenga lugar a gran escala o esté de alguna forma relacionado con una operación (si es una operación de combate, el objetivo puede asumir que los sabotadores trabajan para los combatientes). Incluso si los daños son permanentes, los estados pueden recuperarse en general. El ataque a las centrífugas iraníes tenía sentido debido al fuerte deseo sentido por algunos países en hacer renquear el programa nuclear de Irán y ganar tiempo. Otra justificación del sabotaje es empujar un objetivo más allá de un punto crítico cercano, incluso si esto tiende a ser visible solamente desde un punto de vista retrospectivo. De lo contrario, las consecuencias de llevar a cabo lo que podría ser un acto de guerra pueden sobreponerse a las ganancias, incluso si ser sorprendido es poco probable.

Un ataque no identificable de suficiente magnitud también puede debilitar el objetivo antes de un ataque armado o al menos distraer tanto al objetivo que no pueda asignar los recursos, como sensores, armas in situ o atención de gestión, requeridos para prever y preparar lo que en verdad es, un ataque abierto inminente. Claramente, si no se produce un ataque, el precursor dejará de ser un ataque no evidente desde un punto de vista retrospectivo (a menos que el objetivo tenga múltiples enemigos ansiosos, todos ellos buscando indicios de debilidad, en cuyo caso, lo que parece evidente puede seguir siendo erróneo). Las ventajas de empezar en una modalidad no evidente son dobles. Primero, si el ataque inicial fuera evidente el objetivo podría efectuar una jugada defensiva de forma que dificulte la realización del ataque. Puede saber adónde apuntar sus defensas, por así decirlo; podría estimular a otros a ejercer presión sobre el atacante; o podría incluso contraatacar. En segundo lugar, si el ataque no cumple con sus objetivos, el atacante puede cancelar el ataque abierto y permanecer en la anonimidad con la esperanza de eludir el castigo.

De forma correspondiente, un ataque no evidente puede ser una prueba para ver si cierta técnica da resultado, cuáles son las defensas del objetivo, y donde deben buscarse las mejoras. Sería una prueba costosa si el objetivo mismo averiguara algo sobre sus vulnerabilidades y por lo tanto tuviera una causa para corregirlas y evidencia sobre cómo hacerlo.

Las operaciones no evidentes también pueden ayudar a ganar las guerras de terceros. Dicha ayuda puede ser no evidente si el *hecho* de la ayuda no es evidente o si el *origen* de la ayuda puede ser de cualquier país o entidad como grupos insurgentes o mercenarios. Esto plantea la cuestión de por qué un estado así querría dejar huellas dactilares. Una razón es que los ataques tienen lugar en un país distinto a otro que quería ayuda (por ejemplo, Siria ataca a Irak, y Estados Unidos ataca objetivos en Siria), convirtiéndose así en un acto de guerra por derecho propio y una excusa para que el país atacado llame a *sus* amigos para que le ayuden (por ejemplo, ataque a Irak). Sin embargo, lo más probable es que la asistencia respalde operaciones dentro del estado que está siendo atacado, ya sea por otro estado o por insurgentes, de modo que estos factores no entran en juego. Sin embargo, lo que *importa* es el aspecto de compromiso y cómo impide asumir un compromiso para tratar de obtener una victoria o perder crédito. La intervención y después la retirada prematura plantea dudas sobre la importancia del fin e incluso de la integridad del estado, incluso si dicho estado nunca se comprometió explícitamente a seguir como hasta ahora.

La guerra no evidente también puede llevarse a cabo para lograr un efecto narrativo. Normalmente, en la guerra, el atacante y el objetivo forman parte de la narrativa, y a menos que las

acciones del atacante sean totalmente infundadas, la disputa sobre las narrativas es probable que tenga dos vertientes donde los dos lados apoyan a su propio bando. No obstante, si el atacante es desconocido, o al menos no está claro, entonces el enfoque de la historia es necesariamente el objetivo, y el tema es probable que se concentre en por qué es atacado el objetivo—y puede muy bien extenderse en lo que el objetivo hizo para merecer el ataque o por qué el objetivo no pudo protegerse. Eso, de hecho, puede ser el motivo del atacante: crear una crisis de confianza en el estado objetivo, ya sea debilitándolo inmediatamente, creando fisuras en su cuerpo político, o al menos hacerle más proclive a hacer concesiones.

Por último, si un atacante puede persuadir al objetivo de que fue impactado por un tercero, puede catalizar el conflicto de modo que sea ventajoso para el atacante. Por ejemplo, un cibera-taque taiwanés no evidente a Estados Unidos durante una crisis con China podría poner a Estados Unidos en oposición creciente a China y de esta forma apoyar más probablemente a Taiwán. Un atacante que instigue una guerra entre dos socios comerciales anteriores podría forzar a ambos a comprar del otro país neutral relevante, el atacante. Por supuesto, si se sigue la atribución, el atacante se habrá hecho con un enemigo que no necesitaba y quizás también con un segundo enemigo—el país que el atacante esperaba que fuera acusado.

Las opciones de respuesta del objetivo

En algunos casos, la ambigüedad da resultado para ventaja del objetivo al dar una excusa para evitar la respuesta; afirma incertidumbre sobre quién lo hizo o lo qué de hecho se hizo. No saber ayuda a protegerse contra llamadas populares a combatir y redimir su honor. En algunos casos, el atacante mismo tal vez no piense necesariamente lo peor del honor del objetivo si no se produce una respuesta; en otros casos, se convencerá a sí mismo de que el objetivo sabía pero mentía para evitar una confrontación. Considere, de forma análoga, el arsenal nuclear fantasma israelí. Una vez que otros estados poderosos de Oriente Próximo reconozcan que Israel tiene armas nucleares, deben responder a la razón de por qué no las tienen ellos. Ningún gobierno resulta engañado, pero tampoco humillado.

No obstante, en su mayor parte, los objetivos querrán que se acaben dichos ataques —pero, ¿cómo hacerlo? La defensa es claramente una opción que lógicamente cobraría una mayor importancia cuanto menos pueda apoyarse en no responder, ya que no hay seguridad sobre quién lo hizo. Otra opción es ayudar a ejercer presión desde la comunidad mundial para terminar la posesión de la tecnología de ataque requerida, pero la mayoría de éstas no pueden prohibirse de forma efectiva. Las ciberarmas son en gran medida el anverso de las vulnerabilidades del sistema, es trivial ocultar el código de ataque y se requieren tecnologías de ataque básicas para la ciberdefensa. Las interferencias electrónicas son inherentes en su capacidad de generar energía de radiofrecuencia. El apoyo de la inteligencia a terceros es idéntico al apoyo de la inteligencia a operaciones militares en general. Las armas de sabotaje, las operaciones especiales y las insurgencias son armas pequeñas. Por el contrario, las armas de destrucción masiva y las minas terrestres (no las navales) ya están prohibidas por tratado. Las únicas armas no cubiertas por los tratados y que podrían prohibirse concebiblemente son las armas antisatelitales y los drones; ambas tienen finalidades militares legítimas (abiertas). Generalmente, es más cómo se usan dichas armas en vez de las armas mismas lo que determina las características de la guerra no evidente.

Una variante del segundo método es desarrollar un consenso global de que el uso encubierto de la guerra es mucho más infame que su uso abierto. Así, si dichas armas *se usan*—algo que no siempre es aparente—la comunidad mundial apoyaría los esfuerzos para ejercer presión sobre los usuarios potenciales para permitir investigaciones que clarificarían qué estado tiene la culpa. Después de todo, la mayoría de las formas de guerra son consideradas universalmente crímenes si son llevadas a cabo fuera de las fuerzas armadas; así, incluso el estado acusado debe tener

interés en localizar y extirpar a sus criminales peligrosos, suponiendo que desearan atribuir la culpa. En los casos en que el estado use fuerzas sustitutas y dichos actos *sean* crímenes, pueden sentir presión para cooperar con las investigaciones de la policía internacional. No obstante, la satisfacción para la parte afectada, supone que las acciones de la policía puedan establecer niveles razonables de certidumbre. Y lo que es más problemático, cuanto más se acerquen las vías de investigación a las puertas de los establecimientos militares o de inteligencia, mayor será la renuencia de los estados a que prosigan. Dicha renuencia no sería sin fundamento—si las supuestas acciones de guerra no evidente permiten a los investigadores escudriñar las operaciones encubiertas, los estados pueden en gran medida interpretar la necesidad de evidencia de forma que también les permitan descubrir los secretos de sus rivales.

El último recurso es que los estados víctima y sus aliados respondan a los estados combatientes sospechosos como si ciertamente lo hubieran hecho. Al hacer eso, deben tener en cuenta el grado de certidumbre de *otros* de que la acusación es correcta y, en cierta medida, si el supuesto estado atacante cree que es culpable. Muchas técnicas de guerra no evidente pueden ser llevadas a cabo por elementos descontrolados. Según se observó, algunas respuestas, como las malas relaciones entre el objetivo y el supuesto atacante, no requieren nada que se aproxime a una prueba conclusiva; la mera inquietud basta. Otras respuestas, como las represalias, requieren normalmente altos niveles de confianza. Al final, el estado víctima tiene que sopesar los riesgos relacionados con negativos falsos (no hacer nada ante la agresión) y positivos falsos (represalias contra inocentes). Observe además que la “denegación plausible” es apenas un absoluto en este caso. A menos que el estado víctima solamente pueda responder a través del sistema de tribunales—y los estados no puedan ir a juicio, solamente sus líderes—el balance entre responder y no responder pueden inclinarse mucho antes de que el medidor de confianza llegue al 100 por cien. Un estado relativamente pacifista rodeado por todas partes por amigos (por ejemplo, Bélgica) y que forme parte de alianzas puede desear una certeza casi absoluta y tal vez no reaccione incluso en ese caso; un estado ansioso bien armado rodeado por todas partes por adversarios potenciales (por ejemplo, Israel) puede ser menos quisquilloso.

La víctima también puede efectuar una represalia usando guerra no evidente usando guerra no evidente ella misma. Ostensiblemente, el compromiso mutuo de ambos lados para modular sus respuestas entre sí podría limitar el potencial de una guerra abierta, y por tanto, más destructora—siempre que ambos lados tengan cuidado de no descubrirse. Esto puede crear un conjunto de incentivos extraños donde las comunidades de ambos lados involucradas en una guerra no evidente se esfuerzan en no revelar las actividades de sus contrarios no sea que el poder y la influencia en ambos bandos se desplacen a comunidades cuyos métodos bélicos sean bastantes evidentes. Por el contrario, la percepción de que es aceptable intensificar las hostilidades de una manera no evidente en vez de llamar al otro bando puede hacer que aumente el costo destructor de la guerra no evidente hasta sus límites. Si los asuntos se hacen entonces evidentes, el nivel de guerra que forma la base del siguiente conjunto de amenazas empieza a un nivel mucho más elevado.

Evaluación y conclusiones

¿Sería buena la propagación de la guerra no evidente? Incluso si se esgrimiera únicamente para lograr buenos fines, dichas técnicas corroen tanto los valores militares como las normas diplomáticas. La guerra no evidente, casi por definición, tiene que ser el trabajo de pequeños equipos que deben aislarse de la comunidad más grande, de forma muy parecida a las agencias de inteligencia, por sí se descubren sus aventuras. Los esfuerzos de los equipos pequeños de guerra no evidente dejarían a la masa del establecimiento de seguridad nacional bastante

insegura acerca de lo que exactamente estaba pasando y quién estaba exactamente detrás de todas esas actividades (solamente algunas de ellas parecerían accidentes).

La guerra no evidente también se ajusta mal a los estados democráticos pero se adaptan mucho mejor a estados autoritarios o en decadencia en los que la comunidad de inteligencia se haya desacoplado de su estructura de gobierno legítimo. Es probable que los estados que tengan que gestionar reputaciones a largo plazo vean la desventaja de tener que mentir sobre las actividades bélicas cuando se vean preguntados.

La adopción universal o incluso amplia de la guerra no evidente probablemente produciría un mundo más sospechoso. Una vez que los ataques se hagan de forma que parezcan accidentes, se empezará a sospechar que muchos accidentes son ataques. Las naciones reaccionarían (incluso más que ahora) antes de sospechas en vez de la realidad; se podría atribuir/culpar a los atacantes de mucho más de lo que realmente merecen. En demasiados países, *cualquier* cosa que parezca rara se culpa a Estados Unidos (o a Israel) y a sus agencias de inteligencia ubicuas y omnipotentes. Parte de la madurez de sus gobiernos consiste en mejoras en su capacidad de distinguir realidades de fantasías; la evidencia de que dicha fantasía contenga un núcleo de verdad apenas facilitaría el proceso de madurez. De hecho, en circunstancias de crisis, es concebible que pueda iniciarse un conflicto aun cuando el acusado no haga nada.

Y por supuesto, una crisis podría empezar cuando un estado use dichas técnicas pensando en que nunca le iban a descubrir—y sea descubierto. □

Notas

1. El término *no evidente* tuvo una manifestación anterior en el producto de extracción de datos de Jeff Jonas, Non-Obvious Relationship Analysis (Análisis de relaciones no evidentes).

2. El término *guerra*, usado aquí, comprende operaciones llevadas a cabo para fines políticos por estados con el objeto de destruir, corromper o alterar de forma significativa haberes o intereses relacionados con el uso por parte de otros estados de medios que generalmente se consideran ilegales si no los llevan a cabo los estados. Nuestro debate se limita a los estados, porque los actores no estatales no siempre tienen remites ni siquiera identidades que no sean siempre ambiguas, y los individuos incluidos pueden estar sujetos a medidas legales en formas que los estados no pueden estar.

3. Sergei Markov, un diputado de la Duma estatal del Partido Rusia Unificada a favor del Kremlin, afirmó, “Acerca del ciberataque a Estonia . . . no se preocupen, ese ataque fue llevado a cabo por mi asistente. No les voy decir su nombre, porque entonces es posible que no pueda conseguir visados”. “Behind the Estonia Cyberattacks” (Detrás de los ciberataques a Estonia), *Radio Europa Libre/Radio Libertad*, 6 de marzo de 2009, http://www.rferl.org/content/Behind_The_Estonia_Cyberattacks/1505613.html.

4. Robert Mackey, “Irish Flotilla Activists Show Damage to their Boat” (Activistas de la flotilla irlandesa muestran daños en su barco), *The Lede: Blogging the News*, 1° de julio de 2011, <http://thelede.blogs.nytimes.com/2011/07/01/what-flotilla-activists-videos-look-like/>.

5. Qué se quedó en casi nada después de que los rangos originales se redujeran considerablemente en la ofensiva Tet de 1968.