

El Derecho Internacional Consuetudinario del Ciberespacio

CORONEL GARY BROWN, USAF

MAYOR KEIRA POELLET, USAF

LO PRIMERO QUE hay que saber sobre el derecho internacional es que se parece muy poco a la clase de derecho con la que está familiarizada la mayoría de las personas. Las leyes nacionales de la mayoría de los países son promulgadas por cierta clase de institución soberana (como el Congreso) después de una consideración debida. Los estatutos están hechos cuidadosamente de modo que la ley tenga un efecto preciso. El derecho internacional no se parece en nada a eso. Contrariamente a lo que cree la gente, los tratados no son los medios principales de establecer el derecho internacional. El cuerpo de derecho internacional es una mezcla de práctica y tradición históricas así como de acuerdos firmados entre naciones.

Dentro de esta diversidad de guías, el derecho internacional consuetudinario ocupa una posición preeminente en el desarrollo de áreas del derecho—antes que tratados y convenciones.¹ El derecho internacional consuetudinario se desarrolla de la práctica general y uniforme de estados si la práctica va seguida por un sentido de obligación legal.² Cuando ocurre esto, el derecho consuetudinario se considera legalmente vinculante para las naciones-estado. En situaciones no tratadas por el consenso establecido en lo que constituye un comportamiento legal, las naciones pueden tomar medidas que consideren apropiadas.³ Este es el núcleo del ya bien establecido principio *Lotus*, llamado así por la decisión del Tribunal Internacional de Justicia donde se estableció.⁴

Solamente un puñado de acciones se considera que son normas perentorias del derecho internacional; es decir, cosas que universalmente se consideran erróneas y no permisibles.⁵ Son áreas excepcionales, incluida la piratería, el tráfico de personas y los secuestros. Una de las razones por las que hay tan pocas normas aceptadas universalmente se debe a la propia naturaleza del régimen legal internacional. Se establece según lo que las naciones hacen y creen que están obligadas a hacer, dificultando el consenso. Sin consenso, no hay ley, incluso en los casos que parecen sencillos, como la tortura. “La tortura o el trato o castigo crueles, inhumanos o degradantes” son reconocidos por la mayoría de los estados como una violación de los principios de los derechos humanos que ha llegado el estado de derecho internacional consuetudinario. No obstante, se continúan llevando a cabo acciones que se consideran tortura, y los estados que patrocinan esas acciones a menudo no son condenados, por lo que no se puede decir que exista un acuerdo internacional completo sobre este asunto.⁶

Aunque las pocas prohibiciones aceptadas como normas perentorias no tratan de la guerra, eso no quiere decir que el conflicto armado no esté completamente sin regular. Existe un cuerpo de derecho consuetudinario que refleja la amplia y prácticamente uniforme conducta de las naciones-estado durante la guerra tradicional que es ampliamente aceptada y bien entendida—el derecho de guerra. Desgraciadamente, la aplicación del derecho de guerra al ciberespacio es problemática debido a que las acciones y los efectos a disposición de las naciones y actores no estatales en el ciberespacio no corresponden necesariamente de forma clara con los principios de regulación del conflicto armado. El ciberespacio da a las naciones estado nuevas opciones, permitiéndoles tomar medidas no cinéticas que tal vez no hayan estado a su disposición antes. Las acciones que pueden haber requerido el uso de la fuerza militar en conflictos anteriores ahora pueden hacerse con técnicas cibernéticas sin usar la fuerza. Los estados también pueden tomar medidas en el ciberespacio que serían coherentes con el uso de la fuerza armada pero que

evitan más fácilmente asumir la responsabilidad de dichas acciones—pueden tomar cibermedidas “sin atribución”.

A falta de un régimen legal específico para el ciberespacio, el método lógico es guiarse por lo que existe para regular la guerra más convencional y determinar si se puede aplicar a las actividades del ciberespacio. La subsiguiente breve exposición es un examen general sobre cómo las prácticas nacionales se convierten en costumbres vinculantes en el cuerpo de derecho de las naciones como derecho internacional consuetudinario. Después de la exposición general hay una exposición más detallada de la forma en que el derecho internacional se puede aplicar a las cibermedidas de la nación-estado.

El desarrollo del derecho internacional consuetudinario

Es común que los estados no estén de acuerdo en lo que constituye una práctica general aceptada como ley. La forma más sencilla de prueba se encuentra en las acciones de los estados, los materiales gubernamentales publicados, las declaraciones gubernamentales oficiales, las leyes nacionales y las decisiones jurídicas que detallan la práctica real.⁷ Con el tiempo, se pueden desarrollar casos específicos de práctica estatal en una costumbre general.⁸

La segunda parte de la ecuación es más difícil. Para que una costumbre sea vinculante, los estados no solamente necesitan actuar de cierta manera; tienen que actuar de esa manera porque creen que están obligados legalmente a hacerlo.⁹ La aceptación de la práctica general como una obligación, que sea “aceptada por ley”, se denomina *opinio juris (deber jurídico)*.¹⁰ La evidencia de *opinio juris* se muestra principalmente mediante declaraciones de opinión, en vez de afirmaciones sobre la práctica del estado, como tratados o declaraciones.¹¹

No hay una fórmula matemática que regule cuántos estados deben aceptar una práctica o cuánto tiempo se necesita practicarla para que se convierta en una costumbre vinculante.¹² En su mayor parte, cuantos más estados practiquen una costumbre, mayor es la probabilidad de que evolucionen y se conviertan en ley, pero ni siquiera esa regla sencilla es completamente cierta. La práctica de estados potentes y activos políticamente tiene más peso que la de naciones menores, especialmente las que participen activamente en el área que se esté considerando. Por ejemplo, las acciones de Estados Unidos o Gran Bretaña tendrán más peso en el desarrollo del derecho internacional que regula las operaciones navales que las de Suiza.

Según se observó, el tiempo para desarrollar el derecho internacional consuetudinario puede variar considerablemente. El derecho de guerra es un buen ejemplo. El derecho consuetudinario de guerra se ha desarrollado durante miles de años, pero la práctica de conflicto limitado (por ejemplo, para proteger a los no combatientes) evolucionó principalmente en los últimos 150 años. Por ejemplo, los griegos empezaron a desarrollar el concepto de *jus ad bellum*, o guerra justa, en el siglo cuarto AC.¹³ Por el contrario, mientras que los principios que regulan la forma en que los combatientes participan en la guerra (*jus in bello*) también tienen enlaces históricos con esa época, no empezaron a asumir su forma actual hasta la década de 1860 durante la Guerra Francoprusiana y la Guerra de Secesión de EE.UU. Las atrocidades documentadas durante esas guerras condujeron al rápido desarrollo del régimen de derecho de guerra moderno, empezando por la primera Convención de La Haya de 1899.

A continuación citamos un ejemplo de derecho consuetudinario que se desarrolló rápidamente en ley espacial.¹⁴ En 1958, justo un año después del lanzamiento del *Sputnik*, la Asamblea General de Naciones Unidas creó un comité para establecer los usos pacíficos del espacio exterior. Hacia 1963, Naciones Unidas estableció la *Declaración de los principios legales que regulan las actividades de estados en la exploración y el uso del espacio exterior*, reconociendo formalmente lo que se había convertido en derecho consuetudinario aplicable a las actividades espaciales. Desde

entonces, la mayor parte de la ley espacial se ha generado a través de acuerdos internacionales, empezando por el primer tratado del espacio exterior firmado en 1967.

A veces incluso la *inacción* de un estado puede establecer la práctica. Por ejemplo, cuando un estado hace daño a otro, el silencio oficial del estado “víctima” puede ser evidencia de que la conducta en cuestión no constituye una violación del derecho internacional. Esta pasividad y falta de acción puede producir un efecto vinculante bajo lo que se llama doctrina de aquiescencia.¹⁵ Cuantas más veces un estado permita que se produzca una acción sin una protesta significativa, más probable es que la acción sea aceptada como una práctica legal del estado.

Desarrollo del derecho cibernético a través de la costumbre

El uso cada vez mayor de computadoras y redes de computadoras en los años 70 y 80 fue seguido rápidamente por la aparición de la “red de redes”, conocida como Internet a mediados de los 90¹⁶. Últimamente, Internet dio lugar a un dominio de operaciones completamente nuevo denominado *ciberespacio*. Es en este espacio virtual y a través de éste donde se producen las actividades cibernéticas. Así pues, no solamente las actividades en el ciberespacio son nuevas, sino que *donde* se producen las acciones cibernéticas es un lugar exclusivo.¹⁷

Como ha existido en un tiempo tan corto, no hay un cuerpo legal robusto para regular la conducta del estado en el ciberespacio.¹⁸ No obstante, hay casos documentados de práctica ciberestatal, y estos han empezado a establecer una pauta para establecer un derecho cibernético consuetudinario. Según se observó arriba, la ley común no aparece instantáneamente sino que se desarrolla mediante prácticas y justificaciones estatales. Se deben examinar las prácticas cibernéticas de los estados y la idea detrás de esas acciones durante los últimos más de 30 años para ver si hay una ley común en el ciberespacio. Si no se han desarrollado principios, según se expuso antes, el ciberespacio sigue sin tener limitaciones según el régimen internacional común predeterminado.

Aunque *opinio juris* es un elemento crítico, lo más fácil es analizar el desarrollo de la costumbre empezando por un examen de la acción del estado, que es más visible y fácil de documentar que la motivación. El análisis se complica con el secreto que rodea a la mayoría de las operaciones cibernéticas. El Departamento de Defensa (DoD) de EE.UU., asevera que sufre millones de estafas y miles de ataques en sus redes cada día.¹⁹ Con raras excepciones, no hay estado ni individuo que se atribuya estas acciones, por lo que evaluar la motivación de estos ciberactores desconocidos es difícil. Aunque complicado y difícil, se dispone de unos cuantos ejemplos de práctica estatal en el ciberespacio para su examen.

Podría decirse que el primer ciberataque ocurrió en la Unión Soviética. En 1982, estalló un oleoducto transiberiano. La explosión fue grabada por satélites estadounidenses, y un funcionario de EE.UU. dijo que “fueron la explosión y el incendio no nucleares más monumentales visto desde el espacio”.²⁰ Se ha informado que la explosión fue causada por malware informático que la Agencia Central de Inteligencia implantó en software canadiense, sabiendo aparentemente que el software sería adquirido ilegalmente por agentes soviéticos. Como la explosión se produjo en la remota Siberia, no ocasionó ninguna muerte. También avergonzó al Comité Ruso de Seguridad Estatal (la KGB), que creyó que habían robado la tecnología de software más reciente de Estados Unidos. En consecuencia, se ocultaron los hechos detrás de la explosión, y la URSS nunca acusó públicamente a Estados Unidos de causar el incidente.²¹

Se han producido múltiples ataques de software en computadoras contra sistemas de EE.UU. a medida que Internet ha ido creciendo exponencialmente durante los siguientes 25 años. Muchos de estos ataques fueron intentos de copiar información sensible o ataques de denegación de servicio relativamente sencillos pero potencialmente devastadores.²² Algunos de los más infames incluyen Moonlight Maze (1998–2001), que atacó los sistemas de computadoras del go-

bierno y académicos en Estados Unidos; Code Red (2001), que lanzó un gusano cuya finalidad fue llevar a cabo un ataque de denegación de servicio contra las computadoras de la Casa Blanca; y Mountain View (2001), un número de intrusiones en los sistemas de computadoras municipales de EE.UU. para reunir información sobre conducciones de servicio, oficinas gubernamentales y sistemas de emergencia.²³ Aunque había especulación sobre los orígenes, ninguno de estos incidentes pudo atribuirse definitivamente a un actor estatal.

En contraste con el hasta ahora poco conocido incidente siberiano, fue una serie muy pública de sucesos cibernéticos considerados por muchos como el anuncio del advenimiento de la ciber guerra. En abril de 2007, después de la retirada de una estatua rusa en Tallín, la capital de Estonia, un amplio ataque de denegación de servicio afectó a sus sitios web. En consecuencia, Estonia, uno de los países más interconectados, se vio obligada a cortar el acceso internacional a Internet. Rusia negó haberse involucrado en el incidente, pero los expertos especulan que el Servicio de Seguridad Federal Rusa (FSB) estaba detrás del suceso de denegación de servicio distribuido.²⁴

El año siguiente, tropas rusas invadieron la República de Georgia durante una disputa territorial en Osetia del Sur. En agosto de 2008, antes de que las fuerzas rusas cruzaran la frontera, los sitios web del gobierno georgiano se vieron sujetos a ataques de denegación y deterioro de servicio. Aunque existe la creencia extendida de que el incidente fue “coordinado e instruido” por elementos del gobierno ruso, nadie ha sido capaz de atribuir estas acciones definitivamente a Rusia.²⁵

El aviso a las fuerzas armadas de EE.UU. se produjo en 2008, aunque los detalles no se hicieron públicos hasta dos años después. La Operación Buckshot Yankee fue la respuesta del Departamento de Defensa a un gusano informático conocido como “agent.btz” que se infiltró en las redes informáticas secretas militares de EE.UU.²⁶ El gusano fue colocado en una unidad flash por una agencia de inteligencia extranjera, desde la que al final llegó a una red secreta. La finalidad del malware era transferir información de defensa sensible de EE.UU. a servidores informáticos extranjeros.²⁷ En lo que se considera una velocidad relámpago burocrática, se estableció el Cibercomando de EE.UU. menos de dos años después, con la misión, entre otras cosas, de dirigir las operaciones y la defensa de las redes informáticas del Departamento de Defensa.²⁸ Además de desenmascarar la extensión de las vulnerabilidades de la red, el suceso resaltó la falta de claridad en derecho internacional en la medida que se relaciona con los cibersucesos.

Merece la pena mencionar dos incidentes recientes antes de tratar la ley detalladamente. En 2010, Google informó que se habían infiltrado piratas chinos en sus sistemas y habían robado propiedad intelectual. A través de su investigación, Google averiguó que la exfiltración de su información no fue la única actividad nefaria; al menos otras 20 compañías han sido también objetivo de piratas chinos. Estas compañías cubrieron una amplia gama de usuarios de Google, incluidos los sectores informático, financiero, de medios de comunicación y químico. Los chinos también habían tratado de piratear las cuentas de Gmail de activistas de derechos humanos y lograron acceder a algunas cuentas mediante malware y estafas tipo “phishing”. Google publicó una declaración explicando que se descubrió a través de su investigación y qué pasos estaba dando como respuesta a la acción de China, incluidos la limitación de su negocio en China y con ese país.²⁹

Además en 2010, se detectó un gusano informático llamado Stuxnet en sistemas informáticos de todo el mundo. Stuxnet residía y se replicaba en computadoras usando el sistema operativo Windows de Microsoft pero su objetivo era un sistema de control de supervisión y adquisición de datos (SCADA) fabricado por Siemens. Los ciberexpertos determinaron que el gusano estaba diseñado para afectar los procesos automatizados de sistemas de control industrial y especularon que el plan de energía nuclear Bushehr de Irán o su instalación de enriquecimiento de uranio de Natanz era el objetivo deseado.³⁰ Después de que Stuxnet se hiciera público, Irán afirmó que la demora de la puesta en marcha de la planta de Bushehr se basaba en “razones técnicas” pero

no indicó que se debiera a Stuxnet.³¹ El subdirector de la Organización de Energía Atómica de Irán afirmó, “La mayoría de las reclamaciones hechas por agencias de medios de información [extranjeras] sobre Stuxnet son esfuerzos cuya finalidad era causar problemas entre los iraníes y personas de la región y demorar la puesta en marcha de la planta de energía nuclear de Bushehr”.³² El presidente iraní Ahmadineyad indicó en una rueda de prensa que un código de software malicioso dañó las instalaciones de centrífugas, aunque no afirmó específicamente que fuera Stuxnet o la instalación de Natanz.³³

Aunque no se tuviera en cuenta el incidente del oleoducto siberiano y considerando que Moonlight Maze fue el primer ciberincidente importante entre estados, han transcurrido unos 12 años de práctica general para considerar al determinar lo que constituye la ley común en el ciberespacio. Los incidentes que han ocurrido durante este período han sentado precedente para lo que los estados consideran un comportamiento cibernético aceptable. Lo que es notable es la ausencia de protestas de las naciones cuyos sistemas se han degradado de alguna manera debido a ciberactividades dañinas. Irán parecía rehusar incluso a admitir que las computadoras de su planta nuclear habían sido afectadas y aún no afirma haber sido ciberatacada.³⁴

Si los daños causados por el malware Stuxnet hubiera sido causados por un ataque cinético tradicional, como un misil de crucero, es probable que Irán hubiera respondido enérgicamente. Para empezar, en ataques más tradicionales es más fácil determinar el origen del ataque. Hay una variedad de razones por las que Irán pudo haberse abstenido de hacer una queja pública sobre el suceso Stuxnet; una posibilidad es que cree que la acción no estaba prohibida según la ley internacional. Sea cual sea la razón del silencio de Irán, sigue siendo cierto que ningún estado ha declarado que otro ha violado la ley internacional mediante un uso cibernético de la fuerza o de un ataque armado a través del ciberespacio. Aparte del suceso de Stuxnet, lo de Estonia y Georgia fueron los que más se le parecieron.

La situación en Georgia puede distinguirse porque la ciberacción fue llevada a cabo en concierto con las tropas rusas que cruzaban la frontera georgiana—un uso claro de la fuerza. La ciberactividad contra los sitios web georgianos no dio comienzo hasta después de que Georgia efectuara un ataque sorpresa al movimiento separatista en Osetia del Sur, el 7 de agosto de 2008. La ciberactividad comenzó más tarde ese mismo día, en la víspera en que Rusia llevó a cabo unos ataques de aviones para bombardear el interior del territorio georgiano. Parece como si fuera una táctica militar para cortar la capacidad de Georgia de comunicarse durante el ataque. No fue hasta el 9 de agosto de 2008 en que Georgia declaró un “estado de guerra” para el ataque armado que se estaba produciendo en su territorio. No declaró que la ciberactividad misma fuera un ataque o uso de la fuerza.³⁵

También se ha explicado que la masiva actividad distribuida de denegación de servicio de 2007 en Estonia fue un ciberataque. Sin embargo, después de deliberar, incluso el gobierno estonio concluyó que se trató de un acto delictivo en vez de un uso de la fuerza por parte de otro estado. Eso puede ser porque no pudieron atribuirlo con certeza al gobierno ruso (o a ningún otro gobierno), pero sigue habiendo un precedente. Los problemas de atribución seguirán importunando esta área de la ley. Es más difícil por costumbre desarrollar si la fuente de la acción es desconocida. Las acciones de bandas criminales o piratas aficionados no sienta el precedente de la ley internacional, y siempre que el actor siga siendo desconocido, los sucesos no tienen un valor precedente.

La ciberactividad y el espionaje

Mucho de lo ocurrido en el ciberespacio entre los estados pueden considerarse como meramente espionaje—simplemente intrusiones en los sistemas informáticos para recopilar datos de

inteligencia. No obstante, si estas acciones equivalen a espionaje, esto crea un dilema en el análisis del derecho cibernético.

Se ha venido espionando desde antes del derecho internacional consuetudinario. A pesar de la famosa afirmación, “Los caballeros no leen el correo de otros caballeros”, el espionaje ha existido desde los primeros días del conflicto armado.³⁶ Aunque el derecho de guerra trata del espionaje en tiempos de guerra y del tratamiento de los espías capturados, el derecho internacional consuetudinario no dice notablemente nada sobre la práctica de espiar en tiempos de paz. Los estados tienen leyes nacionales que prohíben el espionaje—incluido Estados Unidos, donde el espionaje es castigado con la pena de muerte—pero no hay ninguna ley internacional que prohíba el espionaje o insista en que se viola la soberanía.³⁷

A pesar de la ausencia de la guía específica, no se discute generalmente que el espionaje es realmente legal según la ley internacional. La mayoría de los abogados internacionales sostienen que el espionaje “no es ilegal” internacionalmente. Presuntamente, esto se debe a que sería impropio que los países observaran abiertamente que es aceptable llevar a cabo tanto espionaje como pudieran sin ser descubiertos. A pesar de la naturaleza “poco caballeresca” del espionaje, es un secreto a voces que los países espían a amigos y enemigos por igual. La mayoría de las veces, cuando se captura a un espía, la consecuencia es una declaración de persona non grata y la deportación o un intercambio por otros espías.³⁸

La práctica de las naciones en lo que se refiere al espionaje se limita a una aceptación tácita del espionaje. La actividad no está abiertamente aprobada sino que ocupa un espacio de política mal definido que permite que ocurra sin violar la ley internacional. Existe una prohibición general contra la violación de la soberanía territorial, pero como excepción que confirma la regla, la práctica del estado no prohíbe espionaje que pueda involucrar el cruce de fronteras internacionales sin permiso. Reflexionando sobre esta opinión general, un autor resumió lo siguiente, “La ley de espionaje es, por lo tanto, única en que consiste en una norma (integridad territorial), cuya violación puede ser castigada por los estados ofendidos, pero los estados han violado la norma de forma persistente, aceptando el riesgo de sanciones si son descubiertos”.³⁹

Esta afirmación ilustra apropiadamente la extraña posición que el espionaje tiene en la comunidad internacional. Años de práctica del estado aceptando las violaciones de la soberanía territorial para el espionaje han conducido aparentemente al establecimiento de una excepción a las reglas tradicionales de soberanía—parece haberse creado una nueva norma. Como las ciberactividades son frecuentemente parecidas al espionaje, incluso si se efectúan por otra razón, quizás no se exagera si se afirma que la mayoría de las ciberactividades pueden producirse también sin violar la soberanía territorial.

A medida que los estados han empezado a usar Internet y otras capacidades informáticas de almacenar, procesar y comunicar información, el uso de capacidades cibernéticas por parte de las agencias de inteligencia de todo el mundo ha aumentado de forma similar. “Los motivos para espiar [no han cambiado] en décadas. Lo que ha cambiado son los medios por los que espía la gente. El ciberespionaje se ha acelerado debido a mayores velocidades en la red y capacidades de procesamiento de chip refinadas”.⁴⁰ Uno podría pensar que esto significaría que todas las operaciones ciberespaciales nacionales no cinéticas estarían gobernadas por las normas internacionales indeterminadas de espionaje. Desgraciadamente, no es tan sencillo.

Manipular el ciberespacio en interés de la seguridad nacional empezó con el espionaje, pero el desarrollo continuo de las capacidades cibernéticas significa que podrían usarse en operaciones militares independientes de espionaje. Quizás por esta razón, las políticas y prácticas que regulan el ciberespionaje están más completamente desarrolladas que las que regulan las ciberactividades oficiales emprendidas por otras razones. Objetivamente, hay poca justificación para esta falta de relación, ya que la mayoría de las acciones militares en el ciberespacio no llegarían al uso de la fuerza. De hecho, muchas acciones militares en el ciberespacio no podrían distinguirse del ciberespionaje.

Por otra parte, en algunos casos hay diferencias importantes entre el ciberespionaje y los medios de espionaje más tradicionales. Entrar en otro país de forma furtiva y dejar un sensor para reunir y transmitir datos de inteligencia es una cosa. Pero, ¿qué pasaría si ese sensor contuviera también un potente explosivo que pudiera detonarse a distancia, causando una destrucción grave? Si un gobierno descubriera dicho dispositivo, se clasificaría como arma de guerra; eso incluiría cualquier idea que pudiera haber estado detrás de una actividad de espionaje. Esta segunda situación se parece más a algunas técnicas de ciberespionaje actuales. Los accesos a la red y las capacidades de ciberespionaje pueden utilizarse tanto para alterar sistemas como para borrar datos. Se puede dejar a la cibervíctima preguntarse si el código rebelde que descubre en su red es una herramienta diseñada para el espionaje o un ataque.

Un país que sufra ciberactividades de espionaje (como obtener acceso de forma ilícita a una red informática gubernamental) no dispone de un método seguro de distinguir entre la intención de una intrusión y puede tener poca noción de quien está detrás de eso. Cualquiera que sea el acceso no autorizado mediante medios nefarios, éste podría usarse para recopilar datos, destruir datos o incluso dañar o destruir equipos. “La diferencia entre ciberdelincuencia, ciberespionaje y ciberguerra es un par de pulsaciones del teclado. La misma técnica utilizada para robar dinero y obtener información patentada en planos o fórmulas químicas es la que una nación estado usaría para infiltrarse y destruir cosas”.⁴¹ Una vez que los usuarios ilegítimos tengan acceso a una red, pueden hacer las maldades que quieran, y las herramientas de software usadas por los espías puede ser las mismas que las usadas por delincuentes y saboteadores.

Así pues, incluso si el gobierno objetivo puede atribuir efectivamente la actividad a cierto estado, no sabría el “por qué” de la actividad. La naturaleza del ciberespacio no permite una distinción clara entre intrusiones para recopilar datos y las de una naturaleza más nefaria.

Por esta razón, podría deducirse que las operaciones ciberespaciales que no lleguen al uso de la fuerza deben estar cubiertas por la misma amplia ley internacional que regula el espionaje y que “no las consideran ilegales”. Después de todo, la mayoría de las ciberactividades militares son más similares al espionaje que las acciones militares tradicionales.⁴² Conceptualmente, hay poca diferencia entre entrar de puntillas en una oficina y robar un fajo de papeles de un archivo que entrar de puntillas electrónicamente en una computadora para robar un archivo. No obstante, hay una gran diferencia entre destruir algo y una acción reversible que haga que algo temporalmente sea menos funcional. En el reino cinético, se dispone de pocas opciones mínimamente invasoras. En el ciberespacio, las opciones varían desde cambiar un solo dígito a un colapso de una red eléctrica nacional. Considerar por igual que todas esas ciberactividades son “ataques” no es algo razonable.

Para facilitar la recopilación de inteligencia, se planta un código informático (malware) en sistemas gubernamentales. Ese código, en algunos casos, puede usarse para reunir inteligencia o de formas destructoras, por ejemplo, para introducirse en un sistema informático y controlar el correo electrónico en un cuartel militar. El acceso al sistema creado para fines de inteligencia también puede usarse para alterar sistemas informáticos a un nivel muy por debajo de lo que se consideraría un uso de la fuerza según la ley internacional. Aunque podría argumentarse que la intención del actor controla cómo debe analizarse un acción cibernética según el derecho internacional, esta forma de argumentar tiende a mezclar normas de conducta internacionales y nacionales.⁴³ La intención de una persona es clave para muchas imputaciones de delitos según la ley nacional, pero en el derecho de guerra, una nación que se sienta amenazada o como si estuviera siendo atacada tal vez no esté especialmente preocupada con la intención de la nación atacante.

No existe ninguna institución legal internacional a la que pueden acudir los estados para reunir evidencia y analizar con cuidado a fin de determinar la intención detrás de la ciberactividad de otro estado. Ni el Tribunal Internacional de Justicia ni ningún otro tribunal internacional pueden desempeñar esta función. Cualquier evidencia que existiera sería clasificada como se-

creta por la nación actor y sería también políticamente sensible. Los testigos serían en su mayoría oficiales del servicio de inteligencia y políticos. En otras palabras, el sistema se parece poco a un sistema de tribunal nacional, donde los oficiales de policía, los informes oficiales y los testigos serían escrutinizados completamente durante el transcurso de muchos meses para determinar la intención. Cuando un estado es consciente de una ciberintrusión, debe decidir rápidamente si es un preludio de un ataque o “meramente” espionaje. Incluso si el estado víctima quisiera de investigar el intento, tal vez no podría determinar el origen de la intrusión. Además, tal vez no quiera divulgar si se detectó la intrusión.

No se ha hablado mucho del asunto de intención internacional en lo que se refiere al derecho de guerra. Eso puede deberse, en el caso de ataques cinéticos, a que la intención del estado atacante generalmente no es ambigua.⁴⁴ Esto establece un enigma interesante. Si la intención no importa en las operaciones cibernéticas, y solamente unas pocas pulsaciones determinan si una ciberactividad constituirá espionaje o ataque, entonces cualquier intrusión para recopilar información es potencialmente una amenaza o un uso de fuerza. Si es así, el Consejo de Seguridad de Naciones Unidas podría prepararse para estar muy ocupado.⁴⁵

El sistema legal internacional opera según sus propias reglas, que se establecieron por consenso y son fundamentalmente diferentes que la ley nacional. El derecho de guerra es impulsado casi por completo por el efecto de las acciones en vez de por cierta clase de “mens rea nacional”.⁴⁶ La *intención* de un actor que tome medidas contra otro estado que podría interpretarse como hostil es, por razones prácticas, irrelevante para el análisis del derecho internacional.

Todo esto conduce de nuevo al régimen legal internacional actual que regula las ciberactividades. La cuestión es si la práctica del estado coincide con estas normas y si los estados cumplen por obligación legal. De otro modo, seguiría siendo el “Oeste Salvaje” en lo que respecta a comportamiento en el ciberespacio.

Por lo general, el ciberespacio es un régimen permisivo, análogo al conjunto de reglas de espionaje—poco está prohibido, pero los estados pueden seguir haciendo las cosas lo mejor que puedan para impedir que otros participen en la arena. Tampoco hay nada que impida que los estados prohíban el cibercomportamiento mediante leyes nacionales. Específicamente, siempre y cuando la ciberactividad siga estando por debajo del nivel de uso de la fuerza y no interfiera de otra manera con la soberanía de la nación objetivo, no estaría prohibido por la ley internacional, fuera cual fuera la intención del actor.

Es importante advertir que las ciberactividades agresivas que ocasionen efectos cinéticos (es decir, destrucción física, daños o lesiones) están cubiertos por la ley referente al uso de la fuerza y ataques armados. Son sucesos cinéticos regulados por el derecho de guerra tradicional justo como los efectos cinéticos por medios de guerra más tradicionales. Así, por ejemplo, un ciber-suceso que ocasione la destrucción física de una turbina de una central eléctrica sería un ataque militar sujeto a la ley internacional que regula cualquier otro ataque cinético.⁴⁷ No obstante determinar exactamente lo que constituye un efecto cinético no es siempre sencillo, esto es tan claro como otras cosas que regulan los rincones oscuros del derecho consuetudinario y es suficientemente clara para distinguir eficazmente los ciberataques de algo menos. Un ejemplo poco claro es una ciberacción contra una red eléctrica que haga que deje de funcionar temporalmente. Aunque no pueda producirse un suceso cinético real, la dependencia de las sociedades modernas de la electricidad para el cuidado de la salud, las comunicaciones y el suministro de servicios esenciales pone en claro que esto se consideraría como un efecto cuasicinético y por lo tanto constituiría un ataque militar si la alteración fuera durante un período significativo.⁴⁸

En lo que se refiere a áreas de ciberoperaciones que no adquieran el nivel de un ataque militar, hay pocas reglas. Pero *pocas* es diferente a *ninguna*, y se han establecido algunas guías para que los abogados internacionales evalúen el estado de los asuntos.

En 2003, durante los meses anteriores a la invasión de Irak, Estados Unidos planificó una ciberoperación que habría afectado considerablemente el sistema financiero de Irak y conge-

lado miles de millones de dólares durante las etapas iniciales de la guerra.⁴⁹ Por último, los oficiales de EE.UU. decidieron renunciar a esta opción. Según se dice, esto se debió a que estaban preocupados por que un ataque al sistema financiero de una nación afectaría la confianza internacional en el sistema financiero global, dañando a Estados Unidos y a sus aliados así como a Irak. Así pues, existe cierta interrogante sobre si se abstuvieron debido a *opinio juris* o por mero interés propio.

Al final, no hay gran diferencia. Los sistemas financieros de los estados modernos están inextricablemente entrelazados, más ahora que en 2003. Si la acción de cualquier nación dañara probablemente los sistemas financieros de muchas otras naciones, parece que este tipo de acción sería una violación del derecho internacional consuetudinario. Si por cualquier otra razón, estas acciones fueran tan cuestionables como indiscriminadas. Los sistemas financieros incluyen bancos y bolsas de valores, esencialmente cualquier actividad de “altas finanzas” relacionada con el sistema financiero internacional. La recesión mundial de 2007–08 demostró nuevamente cómo cuando una de las economías grandes del mundo estornuda, el resto es probable que se resfríe.⁵⁰

Existe cierta evidencia contraria potencial acerca de esta conclusión. En 2011, NASDAQ informó sobre una intrusión en sus sistemas informáticos.⁵¹ NASDAQ es una entidad financiera importante, y si se pone fuera de servicio, se consideraría ciertamente, según nuestra definición, un ciberataque; es decir, una ciberactividad que no es permisible según el derecho internacional. No obstante, en este caso, parece que la intrusión se detectó antes de que se causara cualquier daño, y Estados Unidos puede haber decidido que era una actividad delictiva que no merece un alboroto diplomático, o tal vez NASDAQ no haya podido determinar el origen de la penetración. Esto no afecta la conclusión aquí: la alteración a gran escala, o la destrucción, de las instituciones financieras de una nación constituye un ciberataque.

También parece que la penetración o alteración de sistemas de mando y control nucleares es una violación del derecho internacional consuetudinario. Esta afirmación se basa en la ausencia de práctica del estado de lo contrario y a la abundancia de *opinio juris* referente a la no proliferación y al monitoreo y control de armas nucleares.⁵²

Además de estas dos áreas, la ciberactividad del estado por debajo del nivel del uso de fuerza no está prohibida según el derecho internacional. Puede llevarse a cabo, lo mismo que el espionaje, sin sanciones de la comunidad internacional. Ciertos ejemplos de comportamiento permisivo, según lo ha demostrado la práctica estatal, están penetrando y manteniendo una presencia cibernética en sistemas informáticos gubernamentales (incluidos sistemas SCADA), exfiltración de datos del gobierno (incluidos los secretos militares más sensibles), y denegación de servicio o actividades similares que disminuyan el ancho de banda disponible para los sitios web gubernamentales.

Lo anterior se basa en la idea de que los países reaccionarían si fueran atacados. Como todas estas cosas han ocurrido pero no han dado lugar a recriminaciones significativas o una respuesta de autodefensa, la conclusión es que no son ataques. No obstante, los que toman estas medidas en sistemas gubernamentales corren el riesgo de una percepción equivocada de que su ciberespionaje es un ciberataque. Si no son ataques armados o usos de fuerza según el derecho internacional, no está regidos por el derecho de guerra consuetudinario. En consecuencia, estas ciberactividades perturbadoras están reguladas por el régimen general del derecho consuetudinario. Como se indicó antes, el régimen consuetudinario es permisivo en ausencia de normas, como es el caso aquí. La analogía existente más próxima es con el conjunto de reglas que regulan el espionaje. Según el régimen permisivo o de espionaje, las ciberactividades perturbadoras emprendidas por estados son permisibles como asunto de derecho internacional consuetudinario, con las dos excepciones (sistemas financieros y sistemas de mando y control nucleares) aquí indicadas.

Conformación de la estrategia de EE.UU. para el derecho cibernético internacional

Debido a su dependencia del ciberespacio, Estados Unidos debe crear de forma consciente una estrategia para influir en el desarrollo del derecho cibernético internacional consuetudinario en vez de observar meramente el desarrollo. El mejor método de hacer esto es mediante una práctica reconocida del estado. Debido al secreto de muchas ciberactividades, hay pocas que influyan realmente en el desarrollo de normas. Un examen prudente de medidas de EE.UU.—y la divulgación pública de algunas—ayudaría a establecer una referencia de lo que se consideraría un comportamiento aceptable.

Después de que Estados Unidos determine qué medidas cree que está autorizado a tomar en el ciberespacio, debe compartir abiertamente al menos ejemplos de las medidas que ha tomado. Además, debe buscar ciertamente la posibilidad de divulgar acciones tomadas contra él. Al proponer algunas de sus acciones como aceptables y reconocer las tomadas contra él como aceptables o inaceptables, Estados Unidos puede conducir un diálogo sobre cibernormas, llegando a conclusiones que serían beneficiosas para su seguridad nacional.

Además de la práctica del estado, Estados Unidos debe proporcionar materiales gubernamentales divulgables indicando lo que cree que son cibernormas. En mayo de 2011, el presidente publicó *Estrategia internacional para el ciberespacio*. Esta estrategia reconoce que “el desarrollo de normas para la conducta del estado en el ciberespacio no requiere una reinención de derecho internacional consuetudinario, ni convierte en obsoletas las normas internacionales existentes. Las normas internacionales vigentes desde hace tiempo que guían el comportamiento del estado—en tiempos de paz y conflicto—también se aplican al ciberespacio”.⁵³

Al reconocer que ciertos principios se aplican a actividades ciberespaciales de la misma forma que se aplican a actividades más tradicionales, Estados Unidos proporciona una estructura básica para las normas cibernéticas que espera que se desarrollen: defensa de libertades fundamentales, respeto a la propiedad, valoración de la privacidad, protección contra la delincuencia y el derecho a la defensa propia. Aunque en este momento la lista es más una aspiración que una realidad, puede servir como estructura en la que Estados Unidos puede poner futuros ejemplos de comportamiento cibernético real propios y ajenos.

Es importante observar que las normas establecidas en la *Estrategia internacional para el ciberespacio* no son reconocidas universalmente como derecho internacional consuetudinario (excepto el derecho a la defensa propia). Por ejemplo, aunque la estrategia trata de libertades fundamentales como libertad de expresión y privacidad, es aparente que la norma particular no se sigue en todo el mundo. Twitter, que ha sido una herramienta de comunicaciones importante para personas que protestaban contra el gobierno en muchos países, anunció que restringirá cierta libertad de expresión si parece violar una ley local al “retener como reacción contenido a usuarios de un país específico mientras lo poner a disposición del resto del mundo”.⁵⁴ Así pues, incluso si Estados Unidos no lo hace, Twitter reconoce que no todas las cosas son aceptadas como normas de comportamiento en todo el mundo en este momento.

El *Departamento de Estrategia de Defensa para la Operación en el Ciberespacio (DSOC)* reconoce los mismos principios y estimula el desarrollo y la promoción de normas ciberespaciales internacionales. El *DSOC* reitera el objetivo defensivo de *Estrategia internacional* para “oponerse a los traten de alterar redes y sistemas, disuadiendo a actores maliciosos, y reservándose el derecho de defender estos haberes nacionales vitales según sea necesario y apropiado”.⁵⁵ Ningún documento de estrategia incluye ejemplos reales de lo que sería necesario y apropiado y lo deja abierto a interpretación. Aunque es útil proporcionar la afirmación de que Estados Unidos tiene el derecho a defender sus haberes nacionales vitales, para la finalidad del derecho internacional consuetudinario también sería útil saber lo que Estados Unidos considera una amenaza a esos haberes. Por

otra parte, Estados Unidos puede haber dejado intencionadamente esta ambigüedad en su estrategia internacional para tener más flexibilidad en el tipo de respuesta relevante.

Conclusión

A falta de acuerdos internacionales formales, se está empezando a desarrollar una costumbre cibernética gracias a la práctica de los estados. La costumbre permite que la mayor parte de la ciberactividad por debajo del nivel del uso de fuerza, con serias acciones contra instituciones financieras importantes y acciones perturbadoras para los sistemas de mando y control nucleares son excepciones notables. Aunque ha habido cierto movimiento hacia las declaraciones, acuerdos, tratados y normas internacionales en el área, las afirmaciones prometedoras que se oyen más a menudo no coinciden con la práctica del estado actual. En una demostración práctica de política real, a los estados generalmente les gustaría prohibir a otros que emprendan la misma ciberactividad en la que están participando ya. La desconexión entre las afirmaciones prácticas y públicas crean un entorno deficiente para negociar acuerdos internacionales y un suelo poco fértil para que florezca el derecho consuetudinario positivo—normas. En este caso, para lo bueno y para lo malo, rige la opción predeterminada, es decir, el derecho internacional permisivo. A menos que los estados determinen positivamente que las ciberacciones perturbadoras deban tratarse de forma diferente al espionaje, esta área seguirá siendo un campo de batalla intelectual competitivo, donde los expertos cibernéticos hacen lo que hacen y los ingenios cibernéticos sufren.

Esta historia no es necesariamente mala. Reconocer la naturaleza permisiva de la costumbre cibernética animará a los estados a negociar acuerdos que moderen el comportamiento en el ciberespacio. Para negociar acuerdos, los estados tendrán que tratar los problemas cibernéticos críticos de atribución y responsabilidad estatal. A largo plazo, los acuerdos negociados y ejecutables que regulan el ciberespacio pueden ser una mejor opción que esperar al desarrollo necesariamente lánguido de la costumbre en un área que cambia a la velocidad del pensamiento. □

Notas

1. Vea *Estatuo del Tribunal Internacional de Justicia*, art. 38 (18 de abril de 1946), <http://www.icj-cij.org/documents/index.php?p1=4&p2=2&p3=0>.
2. John B. Bellinger III y William J. Haynes II, "A US Government Response to the International Committee of the Red Cross Study (Una respuesta del gobierno de EE.U. al Comité Internacional de la Cruz Roja), *Customary International Humanitarian Law*," *International Review of the Red Cross* 89, no. 866 (junio de 2007): 443–71, http://www.icrc.org/eng/assets/files/other/irrc_866_bellinger.pdf.
3. Lo contrario se puede mostrar, por ejemplo, mediante tratados bilaterales o una objeción coherente por otros estados.
4. Es un "principio negativo residual que proporciona eso [a falta de una ley], lo que no está prohibido en el derecho internacional está permitido". Anthea Roberts, "Traditional and Modern Approaches to Customary International Law: A Reconciliation" (Métodos tradicionales y modernos al derecho internacional consuetudinario), *American Journal of International Law* 95 (2001): 757–91. Aunque es posible que el principio *Lotus* pudiera inducir a los estados a tratar de regular cualquier asunto que pudiera afectarles negativamente, el derecho internacional espera que los estados "no puedan ejercer jurisdicción para prescribir derecho con respecto a otra persona o actividad que tenga relaciones con otro estado cuando el ejercicio de dicha jurisdicción no sea razonable". *Restatement of the Law, Third, Foreign Relations Law of the United States (Reformulación de la ley, tercera, Ley de relaciones exteriores de Estados Unidos)*, §403, 1987 [de ahora en adelante *Reformulación*].
5. "Una norma aceptada y reconocida por la comunidad internacional de estados en su totalidad como norma que no permite ninguna derogación y que puede modificarse solamente mediante una norma subsiguiente de derecho internacional general que tenga el mismo carácter". *Convención de Viena sobre tratados*, art. 53, 23 de mayo de 1969, http://untreaty.un.org/ilc/texts/instruments/english/conventions/1_1_1969.pdf.
6. Estados Unidos considera que prohibición de la tortura es *jus cogens*, pero según se observa, es posible que la práctica de las naciones no apoye esa conclusión. *Reformulación*, §702, comentario n.
7. *Reformulación*, §102, comentario b.
8. Roberts, "Traditional and Modern Approaches" (Métodos tradicionales y modernos), 757–58.

9. *Reformulación*, §102, comentario c, n. 4. Este comentario también sugiere que es posible que la evidencia explícita no sea siempre necesaria para establecer *opinio juris*; en algunos casos tal vez se infiera de la práctica del estado por sí sola.
10. Peter Malanczuk, *Akehurst's Modern Introduction to International Law (Introducción moderna al derecho internacional de Akehurst)*, 7a rev. ed. (Londres: Routledge, 1997), 39.
11. Roberts, *Traditional and Modern Approaches (Métodos tradicionales y modernos)*, 758, n. 4.
12. *Reformulación*, §102, comentario b.
13. Veá Polibio, *Las historias*, Libro V, 9 (debate sobre el derecho de represalias por las acciones sacrílegas cometidas por los etolianos), http://penelope.uchicago.edu/Thayer/E/Roman/Texts/Polybius/5*.html.
14. “El análisis de la práctica de los estados antes de la conclusión de del Tratado del Espacio Exterior de 1967 muestra que históricamente, la costumbre era la primera fuente del derecho internacional del espacio exterior”. Vladelen S. Vereshchetin y Gennady M. Danilenko, “Custom as a Source of International Law of Outer Space” (La costumbre como fuente del derecho internacional del espacio exterior), *Journal of Space Law* 13, no. 1 (1985): 22, 25.
15. Malanczuk, *Akehurst's Modern Introduction to International Law* (Introducción moderna de Akehurst al derecho internacional), 43, n. 10. Veá I. C. MacGibbon, “The Scope of Acquiescence in International Law” (El alcance de la aquiescencia en el derecho internacional), *1954 British Yearbook of International Law*, 143, 145–46; y MacGibbon, “Customary International Law and Acquiescence” (Ley internacional de costumbre y aquiescencia), *1957 British Yearbook of International Law*, 115, 138.
16. Harry Newton, *Newton's Telecom Dictionary (Diccionario de Telecomunicaciones de Newton)*, 23a ed. (New York: Flatiron Publishing, 2007), 502–3.
17. El Departamento de Defensa define el *ciberespacio* como un dominio de combate. Publicación Conjunta 1-02, *DoD Dictionary of Military and Associated Terms (Diccionario de términos militares y relacionados del Departamento de Defensa)*, 12 de abril 2001 (según la enmienda de abril de 2010), 121.
18. Para distinguirla de las acciones estatales que usan capacidades cibernéticas meramente como un medio de lograr un efecto más tradicional. Por ejemplo, usando correo electrónico para suministrar una nota diplomática no es legalmente diferente a enviar la nota con el embajador. La importancia de los “efectos” se trata a continuación.
19. Subsecretario de Defensa William J. Lynn III, “Remarks on Cyber” (Comentarios sobre el ciberespacio), Consejo de Relaciones Exteriores, 30 de septiembre de 2010, <http://www.defense.gov/speeches/speech.aspx?speechid=1509>.
20. Bret Stephens, “Long before There Was the Stuxnet Computer Worm, There Was the ‘Farewell’ Spy Dossier” (Mucho antes de que existiera el gusano informático Stuxnet, existió el dossier de espionaje ‘Farewell’), *Asian Wall Street Journal*, 19 de enero de 2010, 10. A principios de los 80, un oficial de la KGB pasó a la agencia de inteligencia francesa los nombres de los agentes soviéticos involucrados en el espionaje industrial. Esta información fue utilizada por Occidente para suministrar información engañosa a la URSS; los datos comunicados se denominan el Dossier Farewell.
21. William Safire, “The Farewell Dossier” (El Dossier Farewell), *New York Times*, 2 de febrero de 2004, <http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html?ref=williamsafire>.
22. Un ataque de denegación de servicio impide a un sitio web que responda resultando abrumado con miles de solicitudes (pings). A menudo estas solicitudes se originan a partir de una red robótica, denominada más comúnmente “botnet”. Los “bots” o robots informáticos son computadoras infectadas de malware que pertenecen a individuos que no son conscientes de lo que está ocurriendo. Los “bots” se convierten en parte de una “botnet”—agrupación de “bots”—controlada por un actor enemigo. Los “bots” pueden usarse para realizar una variedad de acciones desagradables, como enviar “spam” y recopilar datos para robar identidades. Las “botnets” normalmente están compuestas de computadoras de muchos lugares geográficos, por lo que la acción se llama denegación de servicio distribuida. Newton, *Newton's Telecom Dictionary*, 300, n. 16.
23. Un gusano es un tipo de virus informático que puede propagarse sin intervención humana y duplicarse a través de toda una red. Un gusano puede permitir a un usuario sin autorizar el acceso a una computadora desde un punto remoto.
24. William Ashmore, “Impact of Alleged Russia Cyber Attacks” (Impacto de los ciberataques rusos alegados) *Baltic Security and Defence Review* 11, no. 8 (2009).
25. Cooperative Cyber Defence Centre of Excellence (CCDCOE), *Cyber Attacks Against Georgia: Legal Lessons Identified (Los ciberataques contra Georgia: lecciones legales identificadas)* (Tallín, Estonia: CCDCOE, noviembre de 2008), 12.
26. Noah Shachtman, “Insiders Doubt 2008 Pentagon Hack Was Foreign Spy Attack” (Las personas con acceso a información privilegiada dudan que el ataque al Pentágono de 2008 fuera un ataque de espías extranjeros), *Wired: Danger Room*, 25 de agosto de 2010, <http://www.wired.com/dangerroom/tag/operation-buckshot-yankee/>; y Sergi Shevchenko, “Agent.btz: A Threat That Hit Pentagon” (Agent.btz: una amenaza que atacó al Pentágono), blog *Threat Expert*, 30 de noviembre de 2008, <http://blog.threatexpert.com/2008/11/agentbtz-threat-that-hit-pentagon.html>.
27. William J. Lynn III y Nicholas Thompson, “Defending a New Domain” (Defensa del nuevo dominio), *Foreign Affairs* 89, no. 5 (septiembre/octubre de 2010).
28. Cibercomando de EE.UU., “Mission Statement” (Declaración de objetivos), <http://www.stratcom.mil>.
29. Veá la afirmación de Google en <http://googleblog.blogspot.com/2010/01/new-approach-to-china.html>. Google ha reanudado ahora los negocios en China.
30. Yossi Melman, “Computer Virus in Iran Actually Targeted Larger Nuclear Facility” (El objetivo de los virus informáticos en Irán era una instalación nuclear más grande), *Haaretz.com*, 28 de septiembre de 2010, <http://www.haaretz.com/print-edition/news/computer-virus-in-iran-actually-targeted-larger-nuclear-facility-1.316052>.

31. Ministro de Asuntos Exteriores, República Islámica de Irán, orientación semanal, 5 de octubre de 2010, <http://www.mfa.gov.ir/cms/cms/Tehran/en/NEW/137891.html>.

32. “No Delay in Launch of Bushehr Power Plant Due to Stuxnet: Official” (No se retrasó la puesta en marcha de la central nuclear de Bushehr debido a Stuxnet), *Tehran Times*, 5 de febrero de 2011, http://www.tehrantimes.com/index_View.asp?code=23518.

33. Mark Clayton, “Stuxnet: Ahmadinejad Admits Cyberweapon hit Iran Nuclear Program” (Stuxnet: Ahmadinejad admite que una ciberarma atacó el programa nuclear de Irán), *Christian Science Monitor*, 30 de noviembre de 2010, <http://www.csmonitor.com/USA/2010/1130/Stuxnet-Ahmadinejad-admits-cyberweapon-hit-Iran-nuclear-program>.

34. Vea, por ejemplo, Bob Sullivan, “Could Cyber Skirmish Lead U.S. to War?” (¿Puede una ciberescaramuza hacer que EE.UU. declare una guerra), *Red Tape Chronicles*, 11 de junio de 2010, <http://redtape.msnbc.com/2010/06/imagine-this-scenario-estonia-a-nato-member-is-cut-off-from-the-internet-by-cyber-attackers-who-besiege-the-countrys-bandw.html>; and Gary D. Brown, “Why Iran Didn’t Admit Stuxnet Was an Attack” (Por qué Irán no admitió que Stuxnet fuera un ataque), *Joint Force Quarterly* 63 (4^o trimestre de 2011), <http://www.ndu.edu/press/why-iran-didnt-admit-stuxnet.html>. Tras Stuxnet, un oficial iraní observó que “se inició una guerra electrónica contra Irán”, pero nunca hubo una declaración oficial del gobierno aprobando esa opinión. Atul Aneja, “Under Cyber-Attack, Says Iran” (Ciberatacado, dice Irán), *Hindu*, 26 de septiembre de 2010, <http://www.thehindu.com/news/international/article797363.ece>.

35. CCDCOE, *Cyber Attacks against Georgia (Ciberataques contra Georgia)*, 4.

36. Cita de Henry Lewis Stimson, secretario de estado durante la administración de Herbert Hoover, que justifica el cierre del “Gabinete negro” en 1929, la oficina para descifrar códigos. Hay documentación de espionaje de hace miles de años. Egipto disponía de un servicio de inteligencia organizado hace 5000 años, y el espionaje es uno de los temas dominantes en *El arte de la guerra* de Sun Tzu hace 2500 años. Kurt D. Singer, *Three Thousand Years of Espionage (Tres mil años de espionaje)* (New York: Books for Libraries Press, 1948), vii.

37. Algunos expertos legales dicen que el espionaje es una violación de la soberanía, pero esta es la opinión de la minoría. Vea Manuel R. Garcia-Mora, “Treason, Sediton and Espionage as Political Offenses under the Law of Extradition” (Traición, sedición y espionaje como políticas de ataque según la ley de extradición), *University of Pittsburgh Law Review* 26, no. 65 (1964): 79–80; y Quincy Wright, “Espionage and the Doctrine of Non-Intervention in Internal Affairs” (El espionaje y la doctrina de no intervención en asuntos internos), en *Essays on Espionage and International Law (Ensayos sobre el espionaje y el derecho internacional)*, ed. Roland J. Stranger (Columbus: Ohio State University Press, 1962), 12. Vea 18 U.S.C., pt. 1, capítulo 37, “Espionage and Censorship” (Espionaje y censura) y 18 U.S.C., §§ 793–98, para el derecho nacional de EE.UU.

38. Por ejemplo, en julio de 2010 Estados Unidos y Rusia intercambiaron espías después de que el FBI descubriera una célula de espionaje rusa. Vea “U.S. Confirms Successful Exchange of Spies” (EE.UU. confirma el intercambio exitoso de espías), *CBS News*, 9 de julio de 2010, <http://www.cbsnews.com/stories/2010/07/09/world/main6661165.shtml>.

39. CDR Roger Scott, “Territorially Intrusive Intelligence Collection and International Law” (Recopilación de datos de inteligencia territorialmente inclusiva y el derecho internacional), *Air Force Law Review* 46 (1999): 217–18.

40. Josh Zachry, director asociado para operaciones de investigación, Institute for Cybersecurity, Universidad de San Antonio, dijo en “Cyber Espionage Threatens Global Security” (El ciberespionaje amenaza la seguridad global), *IntelligenceSearch.com*, <http://www.intelligencesearch.com/ia158.html>.

41. Tom Gjelten, “Cyber Insecurity: U.S. Struggles to Confront Threat” (Ciberinseguridad: EE.UU. lucha para confrontar las amenazas), *NPR.org*, <http://www.npr.org/templates/story/story.php?storyId=125578576>.

42. Vea el debate de los “efectos” a continuación.

43. Prescott Winter, “Cybersecurity—Governments Need to Cooperate” (Ciberseguridad—Los gobiernos necesitan cooperar), blog *Cyber Threat*, 8 de abril de 2010, <http://blogs.computerworlduk.com/cyber-threat/2010/04/cybersecurity-governments-need-to-cooperate/index.htm#>.

44. Una excepción notable es el caso de equivocación de hecho o por accidente, como ataques aéreos que impactan en objetivos equivocados u objetivos tergiversados de forma no intencionada, en cuyo caso el estado víctima y la comunidad internacional pueden evaluar la razonabilidad del error antes de caracterizar la acción según el derecho de guerra. Vea Daniel Williams, “NATO Missiles Hit Chinese Embassy” (Misiles de la OTAN impactan en la embajada china), *Washington Post*, 8 de mayo de 1999, A-1; y “US Warplanes ‘Bomb Afghan Wedding Party’,” (Aviones de combate de EE.UU. bombardean una fiesta de boda afgana), *Independent*, 6 de noviembre de 2008.

45. El artículo 2(4) de la Carta de las Naciones Unidas prohíbe incluso las amenazas de un uso de fuerza. Como los estados han demostrado que no desean abandonar el espionaje, es poco probable que a la prohibición de la “amenaza de fuerza” se le dé una interpretación amplia en el caso de las ciberactividades. Esto podría significar que los estados serán libres según la ley internacional de implantar un código de computadoras de uso doble y estar preparados para atacar, mientras que los estados defensores legalmente esperarían hasta que se convirtiera el código antes de actuar en defensa propia. Un debate más completo de este interesante asunto está fuera del alcance de este artículo.

46. *Mens rea* es un término legal que se refiere al elemento intencionado necesario para ser condenado por un delito.

47. En un ejercicio del Departamento de Seguridad Nacional de 2007 llamado Aurora, los ataques piratas controlados a una copia del sistema de control de una central nuclear permitieron a los investigadores cambiar la operación de un generador, produciendo su violenta destrucción física. “Staged Cyber Attack Reveals Vulnerability in Power Grid”

(Ciberataque ensayado revela vulnerabilidad de la red eléctrica), *CNN*, 26 de septiembre de 2007, http://articles.cnn.com/2007-09-26/us/power.at.risk_1_generator-cyber-attack-electric-infrastructure?_s=PM:US.

48. Se han recomendado otros factores para formar una prueba de uso de fuerza. El factor citado más común es la prueba de seis partes del Profesor Mike Schmitt para un ciberataque, que requiere la evaluación de ciberacciones en lo que se refiere a gravedad, necesidad primordial, carácter directo, capacidad de invasión, mensurabilidad y presunta legitimidad. Aunque se trata de una prueba racional para analizar las ciberacciones post facto, diríamos que solamente la primera—gravedad—es necesaria para determinar si el suceso puede considerarse un ataque. La velocidad relámpago de las ciberacciones hace que las decisiones rápidas sean cruciales, y es poco probable que las naciones tengan la información o el tiempo de considerar estos factores en el fragor de la batalla potencial. La prueba del profesor Schmitt podría ser muy útil para determinar si una ciberacción violó una norma internacional no basada en el uso de la fuerza, como el principio de no intervención. Vea Michael N. Schmitt, “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework” (Ataque a la red de computadoras y el uso de la fuerza en la ley internacional: ideas sobre una estructura de normativa), *Columbia Journal of Transnational Law* 37 (1998–99): 885; y *The Principle of Non-Intervention in Contemporary International Law: Non-Interference in a State's Internal Affairs Used to Be a Rule of International Law: Is It Still?* (*El principio de no intervención en la ley internacional contemporánea: la no interferencia en los asuntos internos de un estado solía ser una regla del derecho internacional: ¿sigue siéndolo?*), resumen de grupo de debate de Chatham House, http://www.chathamhouse.org.uk/files/6567_il280207.pdf.

49. John Markoff y Thom Shanker, “Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk” (El plan detenido de Irak de 03 explica el temor de EE.UU. al riesgo de una ciberguerra), *New York Times*, 1 de agosto de 2009.

50. Financial Inquiry Commission, *Final Report of the National Commission of the Causes of the Financial and Economic Crisis in the United States (Informe final de la comisión nacional de las causas de la crisis financiera y económica en Estados Unidos)*, enero de 2011, <http://www.fcic.gov/report>.

51. Devlin Barrett, Jenny Strasburg y Jacob Bunge, “NASDAQ Confirms a Breach in Network” (NASDAQ confirma una violación en la red); *Wall Street Journal*, 7 de febrero de 2011. Para ver un tratado general de la National Association of Securities Dealers Automated Quotation (NASDAQ), vea “NASDAQ Wiki,” *Motley Fool*, <http://wiki.fool.com/Nasdaq>.

52. Vea “U.S.-Soviet/Russian Arms Control” (Control armamentístico entre EE.UU. y Unión Soviética/Rusia), *Arms Control Today*, junio de 2002, http://www.armscontrol.org/act/2002_06/factfilejune02.

53. *International Strategy for Cyberspace: Prosperity, Security in a Networked World (Estrategia internacional: prosperidad y seguridad en un mundo interconectado por red)* (Washington: Casa Blanca, mayo de 2011), 9.

54. Gerry Shih, “Twitter to Restrict User Content in Some Countries” (Twitter restringirá el contenido del usuario en algunos países), *Reuters*, 27 de enero de 2012, <http://in.reuters.com/article/2012/01/26/twitter-idINDEE-80P0IR20120126>.

55. *International Strategy for Cyberspace (Estrategia internacional para el ciberespacio)*, 12; y *Department of Defense Strategy for Operating in Cyberspace (Estrategia del Departamento de Defensa para la operación en el ciberespacio)* (Washington: Departamento de Defensa, julio de 2011), 10.

El Coronel Gary Brown, USAF, ha sido auditor de guerra en el Cibercomando de EE.UU., Fort Meade, Maryland, desde su establecimiento en 2010. Anteriormente, fue auditor de guerra en el Comando de Componentes Funcionales Conjuntos—Guerra de redes. Se graduó en derecho en la Universidad de Nebraska.

La Mayor Keira Poellet, USAF, es una abogada de operaciones en el Cibercomando de EE.UU. Su asignación anterior fue la de auditora de guerra en el Campo de Aviación Lajes, Azores, Portugal. Recibió su maestría en derecho especial y de telecomunicaciones del Colegio de Derecho de la Universidad de Nebraska y su doctorado en jurisprudencia de la Escuela de Derecho Whittier.