El boxeo con un contrincante imaginario
La guerra cibernética y el ataque económico estratégico

Soren Olson

Primero atacar la estrategia del enemigo, después, su alianza, luego, su ejército y, por último, sus ciudades.

—Sun Tzu, El Arte de la Guerra

LOS RECURSOS E infraestructuras críticas de Estados Unidos están expuestos al asalto de "inteligentes y persistentes" ataques cibernéticos. Tales ataques podrían dramáticamente afectar la cadena de suministro de nuestro recurso más estratégico, el petróleo. Dos décadas de advertencias relativas a las inherentes vulnerabilidades cibernéticas en la infraestructura estadounidense, han sido efectivamente ignoradas. Las estructuras burocráticas como el Comando Cibernético de Estados Unidos (*USCYBERCOM*, por sus siglas en inglés) crean la ilusión de seguridad pero no abordan el verdadero problema. Mientras nos enfocamos en crear efectos en el enemigo, en gran medida, ignoramos los efectos que el enemigo puede crear en nosotros. Nuestra cultura de modas estratégicas (por ejemplo, guerra híbrida, guerra de cuarta generación, guerra irregular, contrainsurgencia y contra terrorismo) y nuestra evaluación de amenaza centrada en la fuerza, indican que los cambios en el carácter de la guerra y las correspondientes consecuencias pueden perderse. En la actualidad, el carácter de la guerra, sin lugar a dudas, implica que los ataques contra la infraestructura económica y nacional y los métodos cibernéticos, serán las armas de elección.

Sin el carácter llamativo de los sistemas de armas, la protección de la infraestructura nacional y los sistemas económicos no exigen una prioridad lo suficientemente alta en la planificación estratégica. Si bien, el Departamento de Defensa (DoD), el Departamento de Seguridad Nacional y otros sectores de la comunidad estratégica estadounidense, han comenzado a responder ante la amenaza de la guerra cibernética, se necesita hacer más. Deben tomarse medidas, a pesar de la infraestructura nacional y contar con sistemas económicos administrados por civiles y fuera de la jurisdicción tradicional del DoD.

Lo que complica aún más la cuestión de la jurisdicción es el programa de Stuxnet. El Stuxnet, concluyentemente, ha demostrado que las armas cibernéticas desarrolladas a nivel nacional están siendo dirigidas a objetivos civiles para lograr efectos estratégicos. Por otra parte, en vista de que dos de los tres principales explotadores en el software Siemens que atacó el Stuxnet, siguen sin parches de protección varios años más tarde, se cuestiona la disposición de las empresas privadas de proteger los sistemas de infraestructura crítica.[1] Estas dos observaciones se combinan para sugerir que la guerra cibernética no respetará las responsabilidades institucionales tradicionales. De hecho, se debería cuestionar si sería prudente dejar la defensa contra los ataques de tipo estratégico —y otros— a empresas privadas y al aparato de seguridad nacional.

El Teniente Segundo Soren Olson, Fuerza Aérea de EUA, es egresado del Departamento de Estudios Militares y Estratégicos de la Academia de la Fuerza Aérea de EUA. Actualmente está en entrenamiento de vuelo en la Base Aérea Columbus.

NASA-JSC

Los recursos subterráneos de petróleo y agua cerca de Denver City, estado de Texas, muestran patrones distintivos con respecto al uso del terreno.

Muchos autores utilizan el pre y post 11-S para caracterizar un cambio de cómo se percibía el terrorismo. Antes de septiembre de 2001, el terrorismo, en gran medida, se consideró un comportamiento delictivo.[2] Luego de quedar demostrado el impacto del terrorismo, el mismo se convirtió en un asunto de defensa nacional. Asimismo, la seguridad cibernética debe pensarse en términos de antes y después del programa Stuxnet; la tendencia a considerar el uso de armas cibernéticas como un acto delictivo debe ser remplazada con el concepto de que su uso contra los intereses de Estados Unidos es un acto de agresión.

La evolución de un arma

De los retos que enfrentan los estrategas estadounidenses, la tendencia a descartar las vulnerabilidades inherentes a la infraestructura interna probablemente es la más insidiosa. La arrogancia con la que se consideran las vulnerabilidades cibernéticas se demuestra en lo siguiente:

> Los ataques cibernéticos juegan un rol potencialmente importante contra adversarios desprevenidos y desafortunados que cuentan con la suficiente sofisticación para adquirir y depender de sistemas de información, pero no lo suficiente para defenderse contra un ataque inteligente y persistente.[3]

La infraestructura nacional de Estados Unidos depende de tecnologías cibernéticas[4] y el desestimar o limitar la amenaza cibernética de los actuales conceptos de guerra, asegurará que no estemos preparados y seamos desafortunados.

Muchos afirman que los avances en la tecnología fundamentalmente cambian nuestro mundo. Del mismo modo, cuando se observan las nuevas tecnologías, armas y tácticas, muchos estrategas las llaman revoluciones en asuntos militares (*RMA*, por sus siglas en inglés). Estas *RMA* son afirmadas para cambiar cómo se lleva a cabo la guerra.[5] Independientemente de la utilidad de las *RMA* como concepto, algunos desarrollos

en la guerra como la tecnología, las armas o los métodos, han alterado el carácter de la guerra. La guerra cibernética es uno de ellos.

El cambio en el carácter de la guerra siempre se puede apreciar después del hecho, pero no así el desarrollo de las tecnologías y métodos que son la base del cambio. Las raíces de los cambios en la guerra, a menudo, están presentes y se desarrollan por años antes de su primer empleo decisivo. El uso de los ferrocarriles, las comunicaciones telegráficas y los asaltos directos contra posiciones fortificadas durante las operaciones de la Guerra Civil previeron las operaciones de la Primera Guerra Mundial.[6] Los alemanes pusieron a prueba la coordinación de elementos terrestres y aéreos en la Guerra Civil española, años antes de que fuera empleada en gran escala contra los polacos y franceses en la Segunda Guerra Mundial.[7] Del mismo modo, la guerra de Yom Kippur en 1973, utilizó el poder aéreo para enclavar y golpear las formaciones terrestres, una técnica que se utilizaría casi 20 años más tarde en la Operación *Desert Storm*.[8] En cada ejemplo, los años transcurridos entre el desarrollo inicial y la implementación a gran escala solo sirvieron para aumentar la letalidad del producto final. La guerra cibernética ha sido desarrollada y probada de manera similar a estos ejemplos y los informes constantemente han advertido el peligro que tal guerra representa.

En 1991, el Consejo Nacional de Investigación, afirmó lo siguiente: "Muchos desastres pueden resultar de ataques intencionales en los sistemas, los cuales pueden ser prevenidos, detectados o recuperados a través de una mejor seguridad".[9] En el informe se pedía una estrategia coherente. Seis años después, una Comisión presidencial señaló que aún no había ningún organismo de coordinación, según lo que se había recomendado anteriormente. Curiosamente, afirmó que contrario al informe de 1991, la naturaleza de las amenazas cibernéticas todavia se comprendía adecuadamente. En 2001, los argumentos sobre la fuerza relativa de defensa y ataque en este nuevo dominio[11] eran tan contradictorios, que un Subcomité del Congreso recomendó dejar el manejo de la seguridad cibernética de la infraestructura crítica estadounidense y redes al sector privado.[12]

Los defensores de depender de la industria privada para defender la infraestructura crítica deberían recordar que no siempre se puede confiar que las empresas sirvan los intereses nacionales. Las empresas privadas son, sin duda alguna, patrióticas y responsables, sin embargo, los estrategas no deben olvidar los nombres de proyectos, empresas y personas sinónimas de enfoques a corto plazo; el Ford Pinto, Enron, Fannie Mae y Freddie Mac y, Bernie Madoff. Los estrategas tampoco pueden descartar la posibilidad de que una empresa privada intencionalmente deje las vulnerabilidades cibernéticas para su propio beneficio o, bajo la dirección de otro poder nacional. En virtud de estas preocupaciones, no parece prudente ubicar el mandato de la defensa nacional en la industria privada, particularmente, cuando los riesgos son altos y la capacidad o la voluntad de las empresas para defenderse de las armas cibernéticas, tales como Siemens en el caso de Stuxnet, es cuestionable.

A pesar de los pasados errores, no cabe duda de que las capacidades cibernéticas de Estados Unidos están aumentando, especialmente con la reciente creación de *USCYBERCOM*. Sin embargo, los partidiarios de las actuales iniciativas de defensa cibernética deben tomar en cuenta la siguiente reciente evaluación de las iniciativas en esta materia en EUA, hecha por la Oficina de Responsabilización del Gobierno:

> El Comando estratégico de EUA ha identificado que la fuerza de trabajo cibernética del Departamento de Defensa es pequeña y no está preparada para enfrentar la amenaza actual... No queda claro si estas brechas serán tratadas, ya que el DoD no ha llevado a cabo una evaluación más amplia del departamento sobre la existencia de estas en las capacidades relacionadas a la cibernética, ni ha establecido un plan o estrategia de financiación para resolver aquellas que pueden ser identificadas.[13]

Veinte años de desastres, investigaciones y cambios de políticas, han llevado, en varias ocasiones, a los mismos lamentables resultados.

El perfeccionamiento de la guerra cibernética continuó, incluso, cuando esta comedia de humor negro de preocupación e inacción tomó lugar. En 1999, un funcionario de defensa declaró que la Oficina Federal de Investigaciones (FBI) estaba investigando unos 6.080 ataques diarios que se grabaron en los sistemas informáticos del DoD.[14] En 2001, los investigadores en la Universidad de Dartmouth predijeron que los ataques cibernéticos sería el arma asimétrica de elección para los grupos y países hostiles en el futuro.[15] En 2003, el *Guardian* comentó que las organizaciones federales de Estados Unidos experimentan un número asombroso de ataques cibernéticos contra redes críticas y que los ataques fueron codificados con el nombre "*Titan Rain*".[16] En este punto, el Gobierno Federal comenzó a analizar si las redes cibernéticas comerciales debían considerarse infraestructuras críticas y por lo tanto debían ser protegidas, pero no se hizo nada significativo al respecto. En 2005 un Comité presidencial encontró que las computadoras que administran las instalaciones, infraestructura críticas y servicios esenciales de EUA, pueden ser objetos de ataque orientado a crear fallas generales en el sistema; estas computadoras, a menudo, son prácticamente accesibles desde cualquier parte del mundo, a través de Internet.[17]

En marzo de 2009, *Forbes* describió un grupo de espionaje cibernético conocido como "GhostNet". Se piensa que el GhostNet infiltró las redes del Gobierno de 117 países.[18] Dichas intrusiones demuestran la capacidad de los atacantes extranjeros para penetrar las redes críticas defendidas durante largos períodos. Por último, el gusano Stuxnet fue descubierto en julio de 2010 y constituye un ejemplo de la época de guerra cibernética. En una condición donde el ataque militar tradicional era políticamente poco práctico, esta compleja serie de unos y ceros, se asevera, han gravemente dañado o incluso retrasado el programa nuclear iraní.[19]

DoD (Cherie Cullen)

Comandante, Comando Estratégico de EUA, el General C. Robert Kehler

A pesar de su capacidad demostrada para producir efectos cinéticos, la verdadera importancia de la guerra cibernética radica en su aplicación estratégica. La guerra cibernética es ideal para la orden definitiva de ataque de Sun Tzu, al enfrentar a un enemigo: "Primero, atacar la estrategia del enemigo, después, su alianza, luego, su ejército y, por último, sus ciudades".[20]

Un adversario que intenta atacar la estrategia de Estados Unidos, primero debe determinar qué el país pretende proteger. El suministro de energía es la prioridad impulsora de la actual política exterior de EUA y se han invertido millones de millones de dólares de la defensa para mantener el acceso a suministros de petróleo del Medio Oriente.[21] Es una cruel ironía que, a pesar de esta inversión, persisten vulnerabilidades en la cadena de suministro de petróleo, lo cual demuestra que el compromiso de Estados Unidos con la defensa de los recursos críticos sigue deficiente.[22]

La cruda amenaza

Como el mayor consumidor mundial de petróleo, Estados Unidos no puede suministrar sus demandas de los recursos internos. En consecuencia, alrededor del 36 por ciento de las importaciones provienen de rutas de ultramar concentradas y otro 27 por ciento es transportado al territorio continental de Estados Unidos a través de oleoductos terrestres.[23] Incluso, el petróleo interno depende del sistema de oleoductos interno. La capacidad de atacar o defender esta red de suministro de petróleo mundial y nacional descansa en los sistemas de computadoras.[24] Los guardianes comerciales de los recursos críticos, como la infraestructura del petróleo, incluso han podido mantenerse al día con las vulnerabilidades reveladas en cuanto al control de supervisión y sistema de adquisición de datos (*SCADA*, por sus siglas en inglés).[25] No están preparados para la avalancha que la historia dice será de una magnitud mayor que cualquier ataque cibernético usado anteriormente.

Históricamente, a los países que importan energía de fuentes propensas a ataques invisibles no les va muy bien, por así decirlo. En la Segunda Guerra Mundial, los submarinos estadounidenses intencionalmente atacaron las importaciones japonesas de petróleo.[26] Luego de dos años de asaltos invisibles, menos de 28 por ciento del petróleo enviado llegó a Japón.[27] Además, la pérdida de materias primas y petróleo y la incapacidad de transportar artículos a las líneas del frente, fue la principal razón del debilitamiento de la capacidad de Japón para mantener la fuerza militar efectiva.[28] Ante un ataque coordinado y sostenido, es casi imposible defender completamente una amplia red contra un enemigo invisible.

Con la guerra cibernética, el verdadero peligro radica en la capacidad del enemigo para coordinar diferentes actores anónimos y usarlos para atacar intereses globales mientras, simultáneamente, ataca la infraestructura nacional de petróleo de Estados Unidos. A finales del siglo XVI, Inglaterra utilizó a los corsarios para atacar la economía española, los que asaltaban los buques llenos de oro que salían de Centroamérica. Entre los ejemplos más recientes se encuentran el uso estadounidense de los Contras y muyahidines durante la guerra fría, así como el apoyo por parte de los soviéticos de guerrilleros centroamericanos. Entre los usos más recientes de intermediarios se encuentran los rusos, con los piratas (*hackers*) "patrióticos" contra los sistemas bancario y de comunicación georgianos en 2008.[29] Cada ejemplo señala la flexibilidad de grupos independientes, para lograr la mayor potencia.

El valor de los intermediarios en la guerra cibernética es que ellos complican aún más la responsabilidad de los ataque. Una potencia puede encontrar e identificar las vulnerabilidades y luego, coordinar ataques por medio de intermediarios. Los últimos trazados de vulnerabilidades de redes e infraestructuras, no han sido tratados como un acto de guerra. Por consiguiente, si bien la fuente de información que capacita los ataques puede conocerse, siempre que la potencia hostil originaria utilice a intermediarios, hay poca acción directa que pueda tomar Estados Unidos.

Hoy en día, la propagación de los afiliados a al Qaeda y otros grupos armados, resulta en más intermediarios dispuestos a atacar los intereses

estadounidenses. Esta es la oportunidad que un Estado-Nación coordinador ofrece a estos grupos:

> Debe quedar claro que la infraestructura de energía de los Estados Unidos es su alma y, como tal, es una de las más críticas de todas las infraestructuras. Los recursos de la industria de petróleo y gas son objetivos claros para un yihad económico.[30]

Los piratas somalíes ya están utilizando información de las compañías navieras para apoderarse de los buques en las costas del Cuerno de África.[31] Estos grupos de piratas han demostrado una voluntad de actuar basados en la información recibida, acerca de las vulnerabilidades de las compañías navieras occidentales. Los piratas modernos, armados con información privilegiada, han ocasionado gran cantidad de daños, comparables con los estragos que podría generar un actor estatal anónimo malintencionado, con una campaña coordinada. Sin embargo, dirigir ataques físicos, aumentados por la información que obtienen de la guerra cibernética solo son parte de la amenaza: "La dependencia de tecnologías cibernéticas crean la oportunidad de comunicaciones interrumpidas, transacciones falsas o engañosas, fraude o incumplimiento de contratos y puede resultar en pérdida del servicio, pérdida de confianza de los interesados o el fracaso de la misma empresa.[32]

Del mismo modo, el anonimato de la guerra cibernética[33] permite el coordinado ataque tipo "submarino" contra los aspectos físicos y cibernéticos de la cadena de suministro de petróleo estadounidense. La proliferación de grupos armados a lo largo de las rutas de transporte marítimo mundial, podría permitir que un actor anónimo coordine una campaña equivalente a la de submarinos contra los vínculos físicos de la cadena de suministro global de petróleo. Esta campaña de interrupción de recurso podría ser ayudada por directos ataques cibernéticos contra los sistemas *SCADA* que ejecutan la logística de los centros de petróleo en Estados Unidos.

Los centros logísticos sirven como puertas de enlace para el abastecimiento regional. Se caracterizan por las interconexiones entre muchos de los oleoductos y, a menudo, otros modos de transporte —tales como los tanqueros y barcazas que transportan petróleo, a veces el ferrocarril y, por lo regular y especialmente, los que se usan en el transporte local— permitiendo que el abastecimiento se mueva de un sistema a otro a través de condados, Estados y regiones de centro a centro.[34]

Al examinar el diseño de la infraestructura de petróleo estadounidense, la concentración de oleoductos administrados por los sistemas *SCADA* en centros logísticos son evidentes cuellos de botella internos. Hay seis centros principales en Estados Unidos. Estos centros son vulnerables al sabotaje cibernético dirigido a los sistemas *SCADA* o a la red de energía que apoyan los centros, según quedó demostrado en 2007 cuando una "tormenta de hielo dejó sin energía al centro de Cushing, estado de Oklahoma, desactivando cuatro oleoductos de petróleo crudo y deteniendo el transporte de unos 770.000 barriles de petróleo por día".[35]

…el anonimato de la guerra cibernética permite el coordinado ataque tipo "submarino" contra los aspectos físicos y cibernéticos de la cadena de suministro de petróleo estadounidense.

Aunque todavía es poco conocido, el ataque cibernético de Estados Unidos de 1982 al oleoducto Transiberiano utilizó un programa *Trojan* que ocasionó una explosión dentro de los oleoductos equivalentes a un arma de 3 kilotones; "Estados Unidos se las arregló para interrumpir el abastecimiento de gas y, consecuentemente, los ingresos de la Unión Soviética por más de un año".[36] Si bien, este ejemplo demuestra que los efectos cinéticos de la guerra cibernética pueden ser temibles, no son necesarios para ocasionar un catastrófico daño económico.

¿Miedo al miedo?

Ataques deliberados por un Estado-Nación, que utiliza una combinación de armas cibernéticas y

(Fuerza Aérea de EUA, Lou Hernandez)

Refinería de Petróleo Anacortes, en las faldas de la montaña Baker, estado de Washington.

tradicionales, ya han sido dirigidos a objetivos económicos. La adición de medios cibernéticos y objetivos económicos al estilo de la guerra, ya fue demostrada por los rusos:

> Cuando Rusia invadió Georgia, gran parte de sus operaciones militares no se centraron en la protección de las zonas habitadas por los rusos étnicos, sino en los puertos e instalaciones georgianas para el manejo de petróleo y gas. Las condiciones inestables en el terreno, aumentadas por ataques cibernéticos, pronto hicieron que todos los oleoductos georgianos parecieran poco confiables. Mientras tanto, dos días después de la invasión, la sección turca del oleoducto Bakú-Tbilisi-Ceyhan fue atacada por militantes locales, supuestamente, por su propia iniciativa. Uno de los resultados de estos acontecimientos fue que BP [British Petroleum]Azerbaiyán cambiara su transporte de petróleo al oleoducto de Baku-Novorossiisk rusa, a pesar de que los costos eran el doble que los de los oleoductos georgianos.[37]

La guerra cibernética fue empleada para atacar un blanco que era puramente económico. BP cambió sus contratos petroleros, basado en la percepción; el compromiso físico del oleoducto georgiano no era necesario. Debido a la influencia que ejerce la percepción, Georgia experimentó serios daños económicos sin sufrir ninguna destrucción física en cuanto a su infraestructura.

Dada la facilidad con que pueden infligirse daños económicos en un solo blanco de este tipo (en este caso, un oleoducto) se puede ver cómo el sistema mundial del cual depende Estados Unidos está en peligro. Además, la proliferación de actores independientes haría fácil que una potencia los use para coordinar ataques contra las rutas marítimas

y terrestres de centros logísticos utilizados para el transporte de petróleo. Sólo unos pocos de estos ataques tendrían que tener éxito para socavar la base del sistema internacional de energía y transporte confiable:

> En 2007, la producción mundial total de petróleo era casi 65 millones de barriles por día (bbl/d) y aproximadamente la mitad o más de 43 millones bbl /d, era transportado por los petroleros a través de rutas marítimas fijas. El mercado internacional de energía depende del transporte confiable. El bloqueo de un punto de distribución, aunque sea temporalmente, puede llevar a un aumento sustancial en los costos de la energía total. Además, los puntos de distribución quedan vulnerables al robo de piratas, ataques terroristas y disturbios políticos en forma de guerras u hostilidades, así como accidentes de los transportadores petroleros.[38]

Un comentarista indicó que los ataques cibernéticos también buscan "cuellos de botella digitales", tales como la red eléctrica. Según explica, "El ciberespacio es un terreno complejo, pero en el subyace la misma idea: estrangular una garganta vulnerable".[39] La guerra cibernética, como la guerra submarina, es ideal para cerrar los cuellos de botella. Este enfoque fue empleado con éxito por Estados Unidos contra los japoneses; los planificadores deben anticipar un ataque similar contra la cadena de suministro de petróleo estadounidense, aunque solo sea por la posibilidad de daños catastróficos. Un incidente que cierre el estrecho de Malaca, incluso temporalmente, redirigiría el 50 por ciento del transporte marítimo mundial y ocasionaría más duda sobre la confiabilidad del transporte de energía. El potencial daño económico de una campaña cibernética coordinada, ejecutada contra los cuellos de botella de petroleo mundiales por una gran potencia —o en cuellos de botella internos— es incalculable.[40]

Marionetas fantasmas

Existen armas cibernéticas, potenciales poderes y vulnerabilidades en las cadenas de suministro. Lo que queda por examinar es lo que podría motivar a un actor para coordinar esa campaña. Sun Tzu y Carl von Clausewitz indican lo que podría ocasionar tal campaña contra el suministro de petróleo estadounidense. En primer lugar, considere la aseveración de Clausewitz de que "Las fortificaciones sólidas obligan al enemigo a buscar en otros lugares". Incluso, en la desaceleración económica, el Ejército de EUA ha demostrado su capacidad para combatir en tres conflictos al otro lado del mundo.[41] Esta fuerza militar obliga a potenciales oponentes a encontrar un ángulo de ataque más eficaz, como líneas de suministro vulnerables que proporciona un recurso vital estratégico. En segundo lugar, el uso cibernético contra recursos estratégicos es, según la máxima de Sun Tzu, "vencer al enemigo sin luchar y, de ser necesario, ganar en primer lugar y después pelear". Estos dos conceptos respaldan la idea de eliminar un recurso estratégico a través de medios asimétricos y anónimos. El ejemplo de la guerra submarina en la Segunda Guerra Mundial, que negó los recursos estratégicos, aunque no era anónima, demostró la capacidad de localizar y apuntar a objetivos económicos por parte de un oponente invisible, para poner de rodillas a una gran potencia.

Sin embargo, la guerra cibernética anunciada por Stuxnet y prevista en este artículo, requeriría recursos en cantidades solo disponibles por los actores estatales.[42] Por otra parte, tal enfoque indirecto, es claramente contrario a la típica estrategia occidental.[43] ¿De quién debe esperar Estados Unidos una guerra cibernética contra sus intereses? Es lógico que la nación con el motivo e intención más clara, sea la que más probablemente desafíe a la superpotencia.

La idea de usar la guerra cibernética para atacar a un blanco imprevisto, tales como los recursos estratégicos, está perfectamente en línea con el concepto chino de la guerra, conocido como *shashoujian*:[44] "Una vez identificados y evaluados los puntos fuertes y débiles, se pueden evitar los puntos fuertes y los débiles pueden ser objeto de ataque con el shashoujian".[45]

Desde 2004, China ha llevado a cabo por lo menos 14 significativos ataques, incluyendo la

Titan Rain y el GhostNet, en blancos que van desde ExxonMobile, pasando por el Canciller alemán en India, hasta las redes militares del DoD.[46] Se han observado señales de desarrollo de armas y el llamado al armamentismo económico por parte de los expertos chinos, se ha hecho evidente: "solo es necesario romper con nuestro hábito mental de tratar las generaciones de armas, usuarios y combinaciones como elementos establecidos para poder convertir algo podrido en algo milagroso".[47] Más adelante, los autores dan un ejemplo de lo que podría lograrse con tal planteamiento:

> El 19 de octubre de 1987, buques de la Armada de EUA atacaron una plataforma de perforación de petróleo iraní en el Golfo Pérsico. Estas noticias alcanzaron la bolsa de valores de Nueva York e, inmediatamente, comenzó la peor caída del mercado de valores en la historia de Wall Street. Este suceso, que llegó a conocerse como el lunes negro, ocasionó la pérdida de US $560 mil millones en valor contable para la bolsa de valores estadounidense.

Si bien esta es una afirmación inexacta, la validez de la declaración es irrelevante en la medida que los chinos crean que es verdadera.

…la defensa activa para los sistemas de infraestructura tomaría años de evolución, antes de que se pueda confiar en ellas y estén a la par con las modernas armas ofensivas.

Es cierto que un ataque por parte de los chinos contra los vínculos internacionales de la cadena de suministro de petróleo estadounidense podría perjudicar su propia economía.[49] Por esta razón, parece poco probable que ataquen los vínculos internacionales salvo como un preludio a la guerra con Estados Unidos de escala total.[50] Sin embargo, la teoría de la interdependencia económica no debería utilizarse como escudo para descartar la posibilidad de un ataque cibernético económico. Antes de la Primera Guerra Mundial, circuló la teoría de que las naciones no entrarían en guerra ya que la devastación económica sería demasiado grande, no obstante, probó ser incorrecta.

La guerra fantasma

El potencial destructivo que posee la guerra cibernética en las esferas económicas, sociales y físicas, exige que se conceda el mismo nivel de respeto y estudio que los estrategas le otorgan a las armas nucleares. La defensa contra los ataques cibernéticos es como la defensa contra las armas nucleares: los ataques pueden tomar casi cualquier forma y provenir de cualquier lugar; las defensas estáticas pueden ser saturadas por una ofensiva masiva o no convencional. A diferencia de las armas nucleares, el carácter anónimo y difuso de la guerra cibernética, puede hacer imposible la disuasión.

Lo que complica aún más una defensa exitosa es la proliferación de potenciales actores anónimos que podrían ser manipulados, cibernéticamente, de forma invisible. Si esto se combina con el éxito repetido de infiltración enemiga (Titan Rain), el alcance global de infiltraciones (GhostNet) y los efectos cinéticos (Stuxnet), no puede esperarse que ninguna defensa resista un ataque coordinado cibernético. La guerra cibernética está bien desarrollada y la defensa activa para los sistemas de infraestructura tomaría años de evolución, antes de que se pueda confiar en ellas y estén a la par con las modernas armas ofensivas. La defensa activa no debe ser el enfoque principal. En cambio, participar en la defensa pasiva, evaluar las vulnerabilidades, crear sistemas de respaldo, determinar las capacidades cibernéticas del oponente y resolver el problema de atribución, deben tomar prioridad.

El problema de la jurisdicción sobre la defensa cibernética y el que enfrenta el DoD en la forma de un mandato para la defensa nacional y una prohibición de las operaciones internas, no son cuestiones que pueden ser resueltas por los estrategas. Puesto que las complicaciones fueron creadas por la ley nacional, sólo pueden resolverse mediante ley nacional. Sin embargo,

esta incapacidad de resolver inmediatamente un problema no debe disuadir a los estrategas para tomar en consideración las incómodas implicaciones de una infraestructura que es indefendible contra las armas modernas cibernéticas y podría no ser confiable en caso de un conflicto limitado o de espectro total.

Debemos darnos cuenta de que, si bien hay significativas vulnerabilidades entre los eslabones de la cadena de suministro de petróleo estadounidense, no dejan de ser solo síntomas de un problema mayor. Las advertencias sobre la guerra cibernética han estado presentes durante años y nos recuerdan otro prominente fracaso de la defensa antes del 11-S; las medidas adoptadas siguen siendo insuficientes. En virtud de estos hechos, nos enfrentamos a la inquietante verdad de que China, así como otras naciones, posee un arma y nuestra mejor defensa contra la misma, es boxear con un contrincante imaginario.***MR***

REFERENCIAS BIBLIOGRÁFICAS

1. Roberts, Paul, "Many Stuxnet Vulnerabilities Still Unpatched," *Threatpost.com* Kaspersky Lab Security News Service, 8 de junio de 2011.

2. Biddle, Stephen D., *American Grand Strategy after 9/11: An Assessment* (Carlisle, PA: U.S. Army War College Strategic Studies Institute, 2003), p. 25.

3. Libicki, Martin C., "Cyberwar as a Confidence Game," *Strategic Studies Quarterly 5*, núm. 1 (Primavera de 2001), p. 134.

4. Cyberspace Policy Review (Washington, DC: The White House, mayo de 2009), p. 3, disponible en www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

5. Krepinevich, Andrew F., hijo, *The Military Technical Revolution*: A Preliminary Assessesment (Washington, DC: Center for Strategic and Budgetary Assessments, 2002, from Office of Net Assessment, 1992), p. 3, disponible en www.csbaonline.org/wp-content/uploads/2011/03/2002.10.02-Military-Technical-Revolution.pdf

6. Griffith, Paddy, Battle Tactics of the Civil War (New Haven, CT: Yale University Press, 1989), p. 20.

7. Waelde, Rainer, *The Experience of the Japanese-Chinese War and of the Spanish Civil War for the Development of the German "Blitzkrieg Doctrine" and Its Lessons for the Transformation Process* (Fuerte Leavenworth, estado de Kansas: U.S. Army Command and General Staff College, 203), p. 25, disponible en www.dtic.mil/cgi-bin/GetRRDoc?AD=ADA419865&Location=U2&doc=GetTRDoc.pdf

8. Baxter, Steven, "Arab-Israeli War October 1973: Lessons Remembered, Lessons Forgotten" (Master's thesis, Naval War College, 1994), disponible en www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA279557&Location=U2&doc=GetTRDoc.pdf

9. National Research Council, Computers at Risk: Safe Computing in the Information Age (Washington, DC: National Academies Press, 1991), págs. 2-3

10. President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (Washington, DC: The White House, October 1997), p. 78, disponible en www.fas.org/sgp/library/pccip.pdf

11. Professional for Cyber Defense, letter to President George W. Bush, 27 de febrero de 2002, disponible en www.uspcd.org/letter.html

12. General Accounting Office, Critical Infrastructure Protection; Significant Challenges for Developing National Capabilities, report to the Subcommittee on Technology, Terrorism, and Government Information, Committee on the Judiciary, U.S. Senate, abril de 2001, disponible en www.gao.gov/new.items/d01323.pdf

13. Government Accountability Office, *Defense Department Cyber Efforts: DOD Faces Challenges in Its Cyber Activities*, report to Congressional Requesters, Julio de 2011, disponible en www.gao.gov/new.items/d1175.pdf

14. Guarding Cyber Pentagon, "*CNN.com*, disponible en http://articles.cnn.com/1999-03-05/tech/9903_05_pentagon.hackers_1_pentagon-computers-computer-attacks-computer-hackers?_s=PM:TECH

15. Vatis, Michael, *Cyber Attacks During the War on Terrorism: A Predictive Analysis* (Dart-mouth, NH: Institute for Security Technology Studies, 24 de septiembre de 2001), disponible en www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA395300

16. Norton-Taylor, Richard, "Titan Rain: How Chinese Hackers Targeted Whitehall," *The Guardian*, 4 de septiembre de 2007, disponible en www.guardian, September 4, 2007, disponible en www.guardian.co.uk/technology/2007/sep/04/news.internet

17. President's Information Technology Advisory Committee, *Cyber Security: A Crisis of Prioritization* (Arlington, VA: National Coordination Office for Information Technology Research and Development, febrero de 2005), p. 17, disponible en www.nitrd.org/pitac/reports/20050301_cybersecurity/cybersecurity.pdf

18. Maidment, Paul, "GhostNet in the Machine," *Forbes.com*, 29 de marzo de 2009, disponible en www.forbes.com/2009/03/29/ghostnet.computer-security-internet-technology-ghostnet.html

19. Broad, William J., Markoff, John y Sanger, David, E., "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *The New York Times*, 15 de enero de 2011.

20. Tzu, Sun, *The Art of War*, traducido por Samuel B. Griffith (Oxford: Oxford University Press, 1973). Págs. 77-78

21. Yergin, Daniel, "Ensuring Energy Security," *Foreign Affairs* 85, núm. 2 (marzo-abril 2006), p. 82.

22. Mead, Russell Walter, "The Serpent and the Dove," in *Special Providence*: *American Foreign Policy and How It Changed the World* (New York: Routledge, 2002), p. 110.

23. U.S. Energy Information Administration, "How Dependent Are We on Foreign Oil? *Energy in Brief* (Washington, DC: Department of Energy, 24 de junio de 2011), disponible en http://www.eia.gov/energy_in_brief/article/foreign_oil_dependence.cfm

24. Lindqvist, Ulf, "Security Control Systems in the Oil and Gas Infrastructure," *Oil Gas Processing Review* (London: Touch Briefing, 2005), disponible en www.touchbriefings.com/pdf/1713/ACFIA57.pdf

25. Roberts.

26. Navy Department, Section III: *Japanese Anti-Submarine Warfare and Weapons*, War Damage Report, núm. 58 (Washington, DC: U.S. Hydrographic Office, 1 enero de 1949), p. 8. Disponible en www.ibiblio.org/hyperwar/USN/rep/WDR/WDR58/WDR58-3.html.

27. Holmes, W.J., Undersea Victory: *The Influence of Submarine Operations on the War in the Pacific* (Garden City, NY: Doubleday, 1966), p. 425.

28. Poirier, Michel, T., "Results of the American Pacific Submarine Campaign of World War II," U.S. Navy, 30 de diciembre de 1999, disponible

en www.navy.mil/navydata/cno/n87/history/pac-campaign.html N_19

29. Hollis, David, "Cyberwar Case Study: Georgia 2008, "*Small Wars Journal*, 6 de enero de 2011, p. 2, disponible en http://smallwarshournal.com/blog/journal/docs-temp/639-hollis.pdf.

30. Forest, James J.F., *Homeland Security*: *Protecting America's Targets*, Vol. III: *Critical Infrastructure* (Westport, CT: Greenwood Publishing Group, 2006), p. 136.

31. Tremlett, Giles, "This is London—The Capital of Somali Pirate's Secret Intelligence Operations," The Guardian, 11 de mayo de 2009, disponible en www.guardian.co.uk/world/2009/may/11/somalia-pirates-network.

32. National Petroleum Council, *Securing Oil and Natural Gas Infrastructures in the New Economy* (Washington, DC: Department of Energy, junio de 2001).

33. U.S. Naval Institute and CACI International, Inc., "Cyber Threats to National Security: Symposium I—Countering Challenges to the Global Supply Chain," 2 de marzo de 2010, disponible en http://asymmetricthreat.net/docs/asymmetric_threat_4_paper.pdf.

34. Allegro Energy Group, "How Pipelines Make the Oil Market Work: Their Networks, Operation and Regulation," a memorandum for the Association of Oil Pipelines and American Petroleum Institute's Pipelines Committee, 1 de diciembre de 2001, p. 7.

35. Ice Storm Trips Power, Paralyzes Key U.S. Oil Hub," Reuters, 11 de diciembre de 2007, disponible en www.cnbc.com/id/22200736/Ice_Storm_Trips_Power_Paralyzes_Key_US_Oil_Hubs

36. Byres, Eric J., "Cyber Security and the Pipeline Control System," Pipeline Gas Journal 236, núm. 2 (febrero de 2009), disponible en http://pipelineandgasjournal.com/cyber-security-and-pipeline-control-system.

37. U.S. Cyber Consequences Unit (US-CCU), special report, *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008*, disponible en www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf

38. Energy Information Agency, *World Oil Transit Chokepoints* (1 de enero de 2008), p. 1, disponible en www.eia.gov/cabs/world_oil_transit_chokepoints/Full.html

39. Bay, Austin, "Grab the Planet By the Throat," *RealClearPolitics* (22 de abril de 2009), p. 8, disponible en www.realclearpolitics.com/articles/2009/04/22/grab_the_planet_by_the_throat_96106.html

40. Energy Information Agency, p. 4.

41. Con referencia a Irak, Afganistán y Libia.

42. Stark, Holger, "Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War," *Der Spiegel Online*, 8 de agosto de 2011, disponible en www.spiegel Online, 8 de agosto de 2011, disponible en www.spiegel.de/international/world/0,1518,778912-2,00.html

43. Murawiec, Laurent, "China's Grand Strategy Is to Make War While Avoiding a Battle," *Armed Forces Journal* 143 (noviembre de 2005), disponible en www.armedforcesjournal.com/2005/11/1164221/

44. Comúnmente traducido como "Assassin's Mace," dice relación con la investigación que realizan los chinos, para obtener armas indetectables antes de usar y que ocasionen tanto daño que hagan imposible la reacción de la víctima.

45. Bruzdzinski, Jason E., "Demystifying Shashoujian," *in Civil-Military Change in China: Elites, Institutes, and Ideas after the 16th Party* Congress, ed., Larry Wortzel and Andrew Scobell (Carlisle, PA:U.S. Army War College, Strategic Studies Institute, 2004), disponible en www.mitre.org/work/best_papers/04/bruzdzinski_demystify/bruzdzinski_demystify.pdf.

46. Stiennon, Richard, "A Brief History of Chinese Cyberspying," Forbes.com, 2 de febrero de 2011, disponible en www.forbes.com/sites/firewall/2011/02/11/a-brief-history-of-chinese-cyberspying/

47. Liang, Qiao y Xiansui Wang, *Unrestricted Warfare: China's Master Plan to Destroy America* (Beijing: PLA Literature and Arts Publishing House, febrero de 1999, p. 20

48. *Ibíd*., p. 190.

49. A menos que el ataque solo afecte la red de distribución de petróleo de EUA.

50. Las Naciones que exportan petróleo o tienen poco interés en el sistema internacional (Irán, Venezuela, Rusia y Corea del Norte) podrían ejecutar campañas contra todos los eslabones de la cadena de suministro sufriendo poco daño ellos mismos; de hecho, la inestabilidad del mercado de petróleo resultante podría ser económicamente ventajosa para estos actores.