El Mundo se ha Vuelto "Ciberloco"

Cómo el "Debilitamiento Mutuamente Asegurado" es la mayor Esperanza para la Disuasión Cibernética

Dr. Matthew D. Crosston

En las extensiones invisibles del ciberespacio, nuestros enemigos están llevando a un nuevo nivel, sin hacer mucho ruido, la forma posmoderna de la guerra de la que fuimos testigos el 11 de septiembre: ya no son simplemente transnacionales—son nonacionales, que ocultan y atacan en un mundo donde no hay fronteras. Ya no son del tipo sin estado—son sin ubicación. Tampoco son virtualmente invisibles—son, bien, virtuales.

—Alan W. Dowd, Fraser Forum (2008)

MUCHOS EXPERTOS cibernéticos dicen que Estados Unidos está muy mal preparado para un ciberataque refinado y que cada día que pasa lo acerca un paso más a un Apocalipsis potencial virtual. Mientras que los problemas que obstaculizan el desarrollo de una política de disuasión cibernética efectiva y completa son claros (medición de la amenaza, atribución, reparto de información, desarrollo de códigos legales y mala infraestructura, entre otros), este artículo se concentra en un aspecto del debate que de ahora en adelante se ha omitido relativamente: que la futilidad de la innovación gubernamental en términos de eficacia defensiva es una debilidad relativamente constante y compartida por todas las grandes potencias modernas, ya sea Estados Unidos, China, Rusia u otras. En otras palabras, todos los estados preocupados con el reino cibernético desde una perspectiva de seguridad global son igualmente deficientes y vulnerables al ataque ofensivo; por lo tanto, es probable que los cibersistemas defensivos sean relativamente impotentes en general.

Estados Unidos tiende a ver este problema como si tuviera una carga exclusiva que llevar. Aunque los estados más pequeños que no consideren prever una función global para ellos temen un ciberataque masivo mucho menos que Estados Unidos, esto no es necesariamente cierto para los estados mencionados anteriormente y otros que desean ser protagonista globales importantes. Como consecuencia, el objetivo para las potencias importantes no debe ser la esperanza inútil de desarrollar un sistema defensivo perfecto de disuasión cibernética, sino la capacidad de inculcar la disuasión basada en un temor mutuamente compartido de una amenaza ofensiva. Estados Unidos está mejor ubicado pasando a una política abierta transparente que trata de disuadir de la eficacia de sus capacidades cibernéticas ofensivas. Esta estrategia tiene mayor proba-

bilidad de estar por delante de los sistemas de disuasión rivales y establecer la percepción entre rivales que Estados Unidos tendría ciertamente las capacidades eficaces de realizar un segundo ataque si es atacado. Es verdad que el objetivo de cualquier potencia importante sería lograr el dominio sobre dichas capacidades (es la forma de las grandes potencias), pero esto también resultaría en el problema de la ciberseguridad transformándose en un juego de suma cero donde el dominio de un estado aumenta la inseguridad de los demás. Por esta razón es lógicamente más estable y potencialmente pacífico tener un sistema de disuasión estructurado mutuamente entre potencias importantes, sin dar a ningún estado la capacidad de alterar el equilibrio cibernético.

Si se adopta, este cambio de política podría tener el mismo potencial que la destrucción nuclear mutuamente asegurada tan eficaz durante tanto tiempo sin ser retado físicamente durante la guerra global. La disuasión nuclear, se basó al principio en la capacidad esperada de un segundo ataque después de sobrevivir un ataque inicial durante un tiempo suficientemente largo para lanzar un contraataque igualmente devastador. Pero con el tiempo—a medida que las grandes potencias nucleares siguieron acumulando arsenales enormes—la eficacia de hecho de la disuasión nuclear no estaba basada tanto en la probabilidad de la capacidad de un segundo ataque como en la aceptación por parte de todos los protagonistas que participan en el juego nuclear que inevitablemente devastarían todo. Una lógica de disuasión emergió de admitir que no tenían defensas.

Quizá podría ser así con esta nueva destrucción cibernética mutuamente asegurada—en un sistema ofensivo abierto y transparente de amenazas cibernéticas, cada protagonista importante en el sistema global llegaría a temer el debilitamiento por igual y por lo tanto no se arriesgaría a iniciar el primer ataque. Aprovechándose de esta vulnerabilidad compartida para atacar y hacer propaganda sobre la acumulación abierta de capacidades ofensivas, habrá discutiblemente un mayor sistema de disuasión cibernética manteniendo seguro el espacio común virtual. Aunque parezca un oxímoron, la defensa más eficaz en este nuevo mundo de peligro virtual es una capacidad ofensiva ciberletal de enormes proporciones; no tanto para usarla realmente, sino para infundir el temor de que pueda usarse. Aunque el caos anárquico y la libertad de Internet será siempre un refugio para actores no estatales que traten de dañar sistemas estatales, una política de destrucción cibernética mutuamente asegurada abierta y transparente daría sistemáticamente a las potencias principales la capacidad de llevar a cabo un segundo ataque para influir potencialmente y disuadir también a estos actores no estatales. En la actualidad, los sistemas de disuasión cibernética defensiva básicamente dan total libertad a estos actores.

Resulta interesante que algunos estados están respetando ya claramente esta estrategia, al menos en el sentido informal aunque no tengan una posición política explícita—el apoyo ferviente de China a los "honkers" [piratas patrióticos] y la dependencia frecuente de la Federación Rusa de los "piratas patrióticos" se nos vienen a la mente inmediatamente. Estados Unidos ciertamente tiene la capacidad tecnológica de igualar a China y Rusia en letalidad virtual. Se podría decir que la carencia formal de una política abierta indica las dudas de parte de Estados Unidos para desarrollar un "espacio común virtual armado". En vez de una indicación de inviabilidad, esta renuencia parece ser una aprobación a consideraciones de inteligencia, lo que significa que Estados Unidos está discutiblemente más satisfecho desarrollando sus capacidades ofensivas en secreto como parte de operaciones más encubiertas que como parte de una política manifiesta. Este artículo indica que el énfasis en una capacidad ofensiva encubierta en vez de manifiesta es un error que pone en peligro la eficacia de la seguridad cibernética de Estados Unidos.

La necesidad de una nueva doctrina, nuevas preguntas y nuevas respuestas

La inercia institucional y la rigidez doctrinal son a menudo obstáculos importantes que bloquean la reforma de la política y pueden incluso obstaculizar la aparición de nuevas ideas de política. No obstante, en el reino cibernético, estos bloqueos no están casi tan arraigados como otros problemas/principios de seguridad. Durante los últimos 10 años la ciberseguridad se ha

convertido en un área cada vez más importante de interés nacional, no obstante el contexto de la ciberseguridad es una era completamente nueva de pensar y de peligros. No fue hasta finales del segundo período del Presidente George W. Bush que se hicieron esfuerzos más definitivos entre agencias para desarrollar explícitamente algo similar a la ciberdoctrina nacional (lo más claro de esta novedad gubernamental fue la creación en 2009 del Cibercomando de EE.UU.). Como analista Mark Young dijo recientemente,

> Es necesaria una ciberdoctrina nacional. Es el enlace entre estrategia y la ejecución de las misiones del sector de seguridad nacional. La doctrina puede ser tradicionalmente una noción militar, pero las agencias reconocen la sabiduría de establecer principios de guía. Una ciberdoctrina nacional puede ser un vehículo usado para definir las funciones de los departamentos y las agencias para todo el gobierno de EE.UU. Al contrario que una orden ejecutiva presidencial o una directiva del Consejo de Seguridad Nacional, una doctrina se desarrolla de una forma abiertamente en colaboración.[1]

Esta evidencia afirma la ausencia de una política abierta, manifiesta y bien definida que guía los intereses de Estados Unidos a largo plazo en lo que se refiere a la seguridad cibernética. Young tiene razón en reconocer que una política cibernética explícita y bien definida es esencial para desarrollar un sistema de ciberseguridad completo y eficaz, en su mayor parte debido a la intensa complejidad inherente a los ciberataques y a la disuasión cibernética. Sigue,

> La naturaleza de los ataques de la red resalta en particular la importancia de una ciberdoctrina bien revisada, ya que los líderes de la seguridad nacional tendrán poco tiempo para consultar con el Consejo de Seguridad Nacional o con el Comandante en Jefe cuando se vean ante un ataque que podría devastar la economía nacional, corromper el flujo del comercio o alterar las cadenas de suministro militares. Debido a los retos técnicos, los contraataques siguen siendo una proposición que lleva mucho tiempo. La alteración de un ciberataque se logra con más facilidad pero tal vez no se logre con tiempo para proteger datos críticos o sistemas de seguridad nacionales.[2]

El problema principal tratado por este artículo es que el debate para crear una ciberdoctrina unificada, explícita y verdaderamente nacional no reconoce abiertamente el axioma más básico del dominio cibernético: la ofensa siempre prevalecerá frente a la defensa lo que, por lo tanto, no incluirá todas las opciones y estrategias potenciales.

Es decir, el lenguaje que utilizan los analistas y especialistas cibernéticos es inherentemente defensivo—es siempre sobre la naturaleza problemática de los contraataques, los retos técnicos para alterar un ataque en curso, y lamentar la ventaja ofensiva que tienen los adversarios sobre los especialistas defensivos. Estos lamentos son reales, pero inexplicablemente no conducen a Estados Unidos a reconocer lo obvio: la doctrina cibernética nacional de Estados Unidos no debe basarse en medidas defensivas que van a estar siempre por detrás de las medidas ofensivas, sino en capacidades ofensivas que den la percepción explícita a los adversarios potenciales que cualquier maniobra agresiva provocará ataques de represalia debilitadores más severos que cualquier agresión inicial—una verdadera política de destrucción cibernética mutuamente asegurada, consagrando inicialmente la capacidad de un segundo ataque y, es de esperar, institucionalizando la admisión disuasoria de la futilidad de un primer ataque.

Ya se está haciendo algún trabajo excelente en los tipos de preguntas que se necesitan al considerar las opciones de seguridad cibernética. Aunque la mayoría de estas preguntas tratan en la actualidad de la disuasión cibernética desde una postura puramente defensiva, las más importantes siguen siendo aún pertinentes para una política de destrucción cibernética mutuamente asegurada:

- ¿Debe el objetivo revelar el ataque cibernético?
- ¿Cuándo debe anunciarse la atribución?
- ¿Deben ser evidentes las represalias cibernéticas?

- ¿Más valen las represalias tarde que nunca?
- ¿Puede haber una confrontación sin represalias?[3]

Todas estas preguntas son increíblemente importantes pero indiscutiblemente tienen respuestas diferentes, dependiendo del tipo de sistema de ciberseguridad que se esté construyendo. Un sistema puramente defensivo basado en el carácter secreto de la inteligencia produce respuestas ineficaces que dejan lagunas en la infraestructura de la seguridad nacional. Las respuestas proporcionadas por una política de destrucción cibernética mutuamente asegurada abierta, transparente y ofensiva sería agresiva y suficientemente explícita para rellenar estas lagunas aprovechándose de la lógica y la eficacia de la disuasión nuclear. El carácter abierto y la transparencia terminan con el "dilema" de revelar objetivos y problemas de atribución, mientras que una concentración en la capacidad ofensiva no solo justifica más las represalias sino que también crea la posibilidad de una confrontación efectiva sin represalias y, por último, evitar una confrontación directa. Este fue posiblemente el verdadero legado de paz dejado por la disuasión nuclear. ¿No podría una política de destrucción cibernética mutuamente asegurada producir la misma esperanza?

Un argumento en contra respondería no a esa pregunta: sigue siendo poco práctico y poco realista pensar que un sistema cibernético de destrucción mutuamente asegurada pueda desarrollarse de forma efectiva. Simplemente hay demasiados problemas para desarrollar y garantizar que se pueda lograr ese "debilitamiento mutuamente asegurado" e, incluso si se logra, garantizarlo podría causar la disuasión de amenaza necesaria para prevenir o limitar los ciberataques. En este caso, los expertos de doctrina deben evitar convertirse en puramente académicos y en simples cascarrabias de política—afirmando que el dominio cibernético es un campo ofensivo sin esperanza donde la disuasión basada en técnicas defensivas no puede ser efectiva, mientras que también indica que un sistema de disuasión cibernética basado en tecnologías ofensivas es igualmente poco práctico e ineficaz. En otras palabras, existe una tendencia a declarar que la defensa no funciona y que la ofensa no da resultado simultáneamente. Esto crea un callejón sin salida erudito y de política, atacando sin esperanza molinos de viento intelectuales y yendo a ninguna parte.

Rumores rusos

El casi apagón virtual de Estonia en 2007 coincidió con la decisión del gobierno de Estonia de trasladar un monumento de la guerra de la era soviética. En esencia, toda la estructura virtual dentro de Estonia se vio inundada y abrumada con "basura" durante un período de tres semanas. Eso puso en peligro fundamentalmente si es que no paralizó temporalmente la red de comunicaciones estonia, ya que periódicos, teléfonos móviles, sistemas de respuesta de emergencia y el banco más grande del estado fueron objetivos de los ataques. Además, un esfuerzo de ataque concentrado se apuntó a las oficinas del presidente, del primer ministro, del parlamento y del ministerio de asuntos exteriores.[4]

No obstante, la importancia de este ataque resalta algunos de los problemas para desarrollar un sistema de disuasión cibernética eficaz: aun cuando Estonia dio a entender que pudo identificar algunos ataques a oficinas del gobierno ruso, no estableció de hecho ningún enlace gubernamental directo. Rusia mantuvo siempre que los ataques vinieron de cibernacionalistas renegados, que actuaban de acuerdo a su propio sentido de patriotismo deformado pero no por órdenes de ninguna oficina o agencia gubernamental oficial. Es más un testimonio de estado de percepción pública global que nadie hoy en día cree la versión rusa de los ataques y da por sentada la versión estonia—nunca hubo una prueba irrefutable que demostrara que la política gubernamental formal rusa fuera la culpable principal de los ataques estonios.

Se trata de un ejemplo perfecto del mundo real del problema de atribución a menudo explicado por la teoría de especialistas cibernéticos: con frecuencia es demasiado difícil identificar

con precisión el origen de un ciberataque. Y lo que es aún peor, en casos en que el punto de origen pueda al menos ser discutido de forma apremiante, aún no existe una forma definitiva de demostrar simplemente quién apretó el "gatillo" y lanzó el ataque. La resolución de ambos problemas sería esencial para el desarrollo de un sistema de disuasión cibernética verdaderamente eficaz. La incapacidad de demostrar la culpabilidad obstaculiza considerablemente cualquier esfuerzo para tomar medidas defensivas. Realmente es tan sencillo como "¿cómo se sabe contra quién tomar represalias si no se está seguro de quién dio el puñetazo virtual?" No se puede, y como consecuencia cualquier esfuerzo para construir un sistema de disuasión cibernética efectivo aparece ya muy quebrantado.

Realidad china

Tal vez el único otro estado asociado en la actualidad con los ataques cibernéticos y el ciberespionaje tanto como la Federación Rusa es China. Ya a finales de la década de los 90, Estados Unidos acusó a China de atacar a varias agencias gubernamentales y trató de infiltrar las instalaciones nucleares de Estados Unidos. En el momento en que Estonia estaba siendo atacada y acusando a Rusia, Alemania sufrió varias infiltraciones en sus agencias gubernamentales y culpó a China. Al igual que con el caso estonio, tanto Estados Unidos como Alemania, a pesar de su convicción inflexible de saber a quién culpar, no tenían de hecho ninguna evidencia real que relacionara al gobierno chino con las incursiones detectadas.[5]

Esto no es un problema pequeño y no es un asunto de semántica de culpabilidad. La respuesta de la comunidad internacional a la evidencia de una implicación directa del gobierno en un ataque cibernético contra otro estado podría considerarse muy fácilmente como una acción bélica, incluso si por el momento es una guerra de menor grado. Por lo tanto, la atribución directa es de la máxima importancia, ya que podría conducir al compromiso de las fuerzas militares y a exponer a un estado a las más serias consecuencias—baja en un campo de batalla. Por lo tanto, cualquier sistema de disuasión cibernética debe poder superar el problema de atribución para que sea pertinente en el asunto más importante de todos—la seguridad del estado. Está claro que el mundo, no simplemente Estados Unidos, es incapaz actualmente de idear un sistema que pueda superar este problema.

A diferencia de Rusia, que siempre ha sido muy reservada sobre sus actividades cibernéticas y férrea en su negativa de participar en cualquier ataque cibernético patrocinado por cualquier estado, China ha sido sorprendentemente abierta sobre su creencia en la necesidad e idoneidad de establecer un ejército de ciberguerreros. China recluta activamente y facilita el apoyo de algunos de los piratas más brillantes desarrollados localmente, llamados "honkers." Los "honkers", en su descarado patriotismo virtual, creen en la filosofía de que la "mejor defensa es una ofensa capaz". No se consideran ellos mismos empleados necesarios del gobierno ni miembros de la comunidad de inteligencia china; simplemente creen que China necesita protegerse de sus adversarios. Si se hace llegar a su atención que otro estado o corporación está iniciando maniobras dañinas contra su país, entonces su obligación es responder del mismo modo. Observe que responder del mismo modo no es sencillamente detener un ciberataque sino formular un ataque cibernético de represalia que de hecho es más intenso y más completo que el ataque inicial.

De algunas formas esta realidad da argumento a la posibilidad de una guerra cibernética que existe más allá de la guerra convencional; no porque la guerra convencional se vaya a volver obsoleta alguna vez o porque sea la forma de seguridad más suprema, sino porque la ciberguerra puede ser considerada por muchos estados como menos conflictiva y una maniobra más orientada a resultados. La piratería informática efectiva y los ataques ciberestratégicos en el momento siguen dando muchas más oportunidades para ocultar la participación mientras se obtienen con éxito secretos económicos, políticos, diplomáticos y militares. Haciendo un cálculo sencillo de costos-beneficios, la ciberguerra es mucho más económica que la guerra convencional, por lo que es discutible que su popularidad crezca exponencialmente con el tiempo. Al considerar la

impotencia de los sistemas defensivos cuya tarea es detener tales esfuerzos, la ciberguerra es un concepto fundamentalmente complejo, complicado y difuso por diseño. Estas características serían retadas al menos por un sistema de destrucción cibernética mutuamente asegurada abierto y transparente en formas en que los métodos de disuasión cibernética actuales no lo son.

Por el momento es justo suponer que los "honkers" chinos no están tratando explícitamente de crear una versión cibernética de la teoría de destrucción nuclear mutuamente asegurada, pero esto no significa que no hayan creado dicha política en sus acciones de hecho. Lo que parece indiscutible es que China ha decidido que no hay consideraciones éticas en el dominio cibernético. De hecho, es fácil ver cómo un estado podría hacer uso del argumento contrario—si la ciberguerra no quiere decir necesariamente derramamiento de sangre inmediato y directo debido a ciberataques, entonces se podrían retirar libremente las esposas éticas de las consideraciones estatales. Y lo que es más importante, China ha dado al resto del mundo un esquema teórico justificando esa política—la filosofía ofensiva de los "honkers" no se basa en ningún sentido vengativo de derramamiento de sangre, sino en un cálculo cuidadoso de lo que es realmente eficaz en el reino cibernético: las capacidades defensivas están comprometidas de forma irremediable; por lo tanto, solamente las amenazas ofensivas tienen el potencial de disuadir iniciativas enemigas.

En algunas maneras este proceso de pensamiento ya ha sido apoyado nada menos que por el vicepresidente del Estado Mayor Conjunto actual, el General James Cartwright, que dijo en 2007 ante el Subcomité de las Fuerzas Estratégicas del Comité de las Fuerzas Armadas del Senado que era "hora de aplicar los principios bélicos al dominio cibernético . . . y la defensa de la nación se hace mejor usando capacidades que nos permitan luchar contra nuestros adversarios cuando sea necesario disuadir acciones negativas para nuestros intereses".[6] La disuasión cibernética tal como se cree actualmente no tiene esta capacidad y no permite a Estados Unidos luchar contra sus adversarios. No se trata de insistir continuamente en algo que ya se ha tratado, sino en hacer el énfasis necesario sobre cómo Estados Unidos se aferra a la defensa. El país está determinado en ser diferente, incluso si va en contra de su propia seguridad. Aunque pueda ser políticamente incómodo modelar algo importante para la seguridad nacional de EE.UU. imitando a los piratas chinos, está claro que por el momento los "honkers" están aplicando de forma más abierta y con mayor éxito los principios bélicos al dominio cibernético. Entretanto, Estados Unidos, se niega a considerar y desarrollar de forma transparente sus propias posibilidades y capacidades y por lo tanto sigue siendo el objetivo cibernético más vulnerable.

Contraciberespacio

Un desarrollo fascinante, inspirado tal vez por la amonestación del General Cartwright, viene con el concepto de contraciberespacio, definido como "una función que consiste en operaciones para lograr y mantener un grado deseado de superioridad ciberespacial debido a la destrucción, degradación o alteración de las capacidades de un enemigo de usar el ciberespacio".[7] Este trabajo procede de una nueva conceptuación de la doctrina básica de la Fuerza Aérea y es una admisión de la necesidad de producir nuevas ideas (aunque discutiblemente mediante la aplicación de ideas bélicas viejas ya demostradas) en el dominio del ciberespacio y su defensa. El asunto a mano es por supuesto tratar de establecer una "superioridad ciberespacial", cuyo documento de doctrina AF 2-11, "Operaciones ciberespaciales", borrador de versión definida como "el grado de ventaja poseído por una fuerza sobre otra que permite llevar a cabo operaciones en el ciberespacio en un momento y en un lugar dados sin interferencias prohibitivas de la fuerza contraria".[8] Al tomar en consideración estos conceptos y definiciones, se pone claramente de manifiesto lo ineficaz que será siempre la disuasión cibernética mientras sea un sistema construido a partir de prioridades defensivas. En el dominio cibernético, un sistema defensivo, por definición, pone a un estado en desventaja y no dispone del potencial de llevar a cabo operacio-

nes sin una interferencia prohibitiva. La doctrina cibernética de Estados Unidos debe lograr esta capacidad.

En mayo de 2007, el Presidente Bush ordenó a la Agencia de Seguridad Nacional (NSA) llevar a cabo un ciberataque contra redes de teléfonos móviles y computadoras que los insurgentes iraquíes habían usado o tratado de usar en la colocación de bombas en carreteras. La NSA cumplió, y su éxito subsiguiente esencialmente destruyó lo que hasta ese momento era para ellos una red de comunicaciones insurgente eficaz. Muchos analistas militares indican que ese esfuerzo fue primordial para cambiar el curso de la guerra.[9] Es cierto que una destrucción cibernética mutuamente asegurada no puede ser exactamente igual a una nuclear. No se trata de semántica cuando destrucción se reemplaza por debilitamiento. Así pues, mientras que la analogía tal vez no se adapte perfectamente, funciona de forma eficaz, basada en el hecho de que se puede decir que la guerra en el siglo XXI se ha alejado de ser global y apocalíptica y ha pasado a ser algo más regional y temporalmente dañino. Como tal, las armas en una política de destrucción cibernética mutuamente asegurada no destruye estados convirtiéndolos en arena y vidrio sino simplemente los paraliza e incapacita en dominios tan cruciales para su funcionamiento y gobierno eficaces. Dichos daños no son insignificantes.

Claramente, Estados Unidos tiene la capacidad técnica y la agresividad estratégica de llevar a cabo dichas operaciones. Ahora debe conceptuar una mente ofensiva para empezar a defender el ciberespacio. El problema hasta este momento ha sido su esfera de utilización relativamente limitada—el ejemplo de Irak fue un caso de guerra abierta y explícita dirigido a un objetivo que estaba atacando de forma activa y agresiva el personal militar estadounidense. Por supuesto, esto tal vez no sea tan políticamente limpio, pero puede ser dramáticamente más efectivo para limitar a los adversarios que están motivados para atacar a Estados Unidos u otros países en el espacio virtual común. Tenga en mente que en el siglo XXI, el ciberespacio no es menos espacio que proteger. Es cierto que los medios de comunicación no podrán mostrar los cuerpos o campos de batalla sangrientos cuando un país es víctima de un ciberataque masivo, pero la devastación y la destrucción de dicho ataque es de muchas maneras más completo y de mayor alcance.

Carencia de infraestructura

Los argumentos lógicos para una política de destrucción cibernética mutuamente asegurada se hacen aún más apremiantes cuando se examinan por completo los obstáculos técnicos que hacen frente a una verdadera disuasión cibernética defensiva. Durante los últimos 10 años, Estados Unidos ha invertido mucho en tecnologías de ciberseguridad. A pesar de este compromiso e inversión, quedan problemas importantes en las áreas más fundamentales. Aún sigue sin producirse un despliegue a gran escala de tecnología de seguridad capaz de proteger completamente la infraestructura estadounidense vital.[10] La necesidad de nuevas tecnologías de seguridad es esencial, pero hasta la fecha los mejores desarrollos solamente han sido en las instalaciones de investigación privadas de escala pequeña a intermedia. Lo que se requeriría para hacer avances rápidos a gran escala en nuevos mecanismos de seguridad de redes es de enormes proporciones:

- desarrollo de plataformas de pruebas de seguridad a gran escala, combinado con nuevas estructuras y normas para pruebas y referencias;
- superar deficiencias e impedimentos actuales para evaluar mecanismos de seguridad de redes, que hasta la fecha sufren de una carencia de rigor;
- datos de redes pertinentes y representativos;
- modelos de mecanismos de defensa adecuados; y
- modelos adecuados de la red y para datos de tráfico básicos y de ataque.

La mayoría de estos asuntos son problemáticos debido a la gran complejidad de las interacciones entre el tráfico, la topología y los protocolos.[11] En pocas palabras, es simplemente más sencillo atacar que defender en el dominio cibernético, y las complejidades innatas de preparación de la infraestructura hacen que probablemente no se trate simplemente de una estimación de asuntos actuales sino de un axioma que perdurará durante eras. Los piratas prevalecerán siempre ante los defensores. Estados Unidos no debe desperdiciar el tiempo atacando molinos de viento virtuales cuando ya tiene la tecnología, el talento y la capacidad de crear una ruta de políticas diferentes.

Un argumento contrario a estos rechazos es que el dominio cibernético seguirá dominado inherentemente por capacidades ofensivas. Las medidas defensivas alabadas más a menudo que presuntamente están alcanzando a las amenazas ofensivas (IPV-6 y tecnologías de portal) son desgraciadamente un poco exageradas, ya que el dominio cibernético no es nunca estático—sean cuales sean las contramedidas defensivas que se desarrollen, uno puede estar seguro de que habrá respuestas a esas medidas. Y las respuestas ofensivas hasta ahora han ido por delante de las "mejoras" defensivas. No hay nada en el futuro previsible que parezca retar ciertamente esta realidad básica. Estados Unidos debe continuar de veras desarrollando, mejorando y refinando sus tecnologías defensivas. Pero no debe ser uno tan ingenuo como para pensar que ser capaz de desarrollar una disuasión defensiva se podrá superar continuamente y de forma rutinaria en trabajo y maniobra las amenazas ofensivas. Simplemente no parece que la estructura del dominio cibernético permita emerger esta realidad.

La naturaleza asimétrica de la ciberguerra

El fracaso de Estados Unidos de participar ofensivamente en la ciberguerra, como reflexión de una política abierta y transparente (o incluso crear la percepción de voluntad para enfrentarse ofensivamente), solamente ha exacerbado la naturaleza asimétrica de los ciberataques. La comercialización, la normalización y el bajo costo de la alta tecnología alrededor del globo hacen que librar campañas cibernéticas sea dramáticamente más sencillo que defenderse de ellas. Literalmente una docena de programadores determinados es capaz de amenazar la red logística de EE.UU., robando planes de operaciones, cegando capacidades de inteligencia u obstaculizando la capacidad de suministrar armas conforme a los objetivos.[12] Eso nunca fue más evidente que en 2008, cuando el Departamento de Defensa sufrió una intrusión significativa en sus redes militares supuestamente seguras. Se introdujo una unidad flash infectada en una computadora portátil militar en Oriente Próximo. Puesta allí por una agencia de inteligencia extranjera, la unidad tuvo éxito en enviar código informático malicioso que pudo propagarse a gran distancia y en gran medida en información clasificada y sin clasificar de modo que se consideró similar a establecer una "cabeza de playa digital".[13]

Estos ejemplos explican perfectamente el carácter malicioso y la futilidad potenciales de luchar contra la asimetría. Es un problema estructural innato que no puede superarse, debido a la naturaleza de la tecnología y al mercado libre. Internet se diseñó para ser abierta y accesible, no solamente para facilitar el uso entre los consumidores más básicos sino también para animar y estimular bajas barreras para la innovación. Como consecuencia, la ofensa tendrá siempre la ventaja.[14] Pero en vez de dejar que la lógica de esta realidad condujera a Estados Unidos a una nueva conceptuación de "defensa ofensiva", el pensamiento de Estados Unidos está aferrado a una mentalidad defensiva que solamente puede resultar en un sistema de disuasión arriesgado.

Aunque la asimetría hace que estar adelantado a los adversarios atacantes sea muy dudoso, Lynn dice que esto solamente enfatiza a necesidad de que Estados Unidos sea más adaptable para ajustarse constantemente y mejorar su defensas. Incluso dice que las tradiciones antiguas de disuasión de la Guerra Fría (modelos de represalias aseguradas) no darán resultado en el ciberespacio debido al problema de atribuciones mencionado arriba, imposibilitando casi saber justo contra quien tomar represalias. Por lo tanto, se supone que la disuasión tenga tanto éxito

en negar las ventajas a un atacante, en vez de tratar de imponer costos a través de represalias agresivas.[15]

Aunque este artículo evidencia el problema de la atribución, esto no conduce a un argumento para alejarse de los antiguos modelos de disuasión de represalias sino que en realidad es lo contrario: un modelo cibernético de represalias no sería sobre a quién lanzar misiles, sino en forzar la percepción de un debilitamiento tecnológico/infraestructural masivo incluso si se determina y atribuye la sospecha de un ataque. La destrucción nuclear mutuamente asegurada tuvo éxito no porque diversos estados lanzaran realmente armas nucleares; tuvo éxito gracias a la convicción entre todas las partes de que un ataque de esta naturaleza sería tan universalmente destructor que el costo superaba con mucho las posibles ventajas potenciales. Un modelo de destrucción cibernética mutuamente asegurada tiene que operar con este mismo principio, solamente con armas virtuales en vez de armas cinéticas. Si se hace bien, armando esencialmente la doctrina cibernética de Estados Unidos, entonces es prohibitivamente caro para un adversario que se arriesgue a atacar.

No se trata de hecho de discutir sobre la creación de cierta variante cibernética de una máquina del fin del mundo del Dr. Strangelove, cuyas repercusiones resuelvan el problema de atribución. Extrapolando al máximo, una política de destrucción cibernética mutuamente asegurada disuade una destrucción nuclear mutuamente asegurada—la percepción de devastación virtual realista mediante ataques de represalia provoca temor de acción, haciendo así que el sistema global sea seguro mediante un equilibrio peligroso, pero estable. Lo mismo que con las armas nucleares, la capacidad de destruir universalmente el espacio común virtual no puede ser la última esperanza de paz en el sistema. Este no es un argumento para dar al presidente una opción entre rendirse o piratear el mundo moderno hasta hacerlo volver a la Edad Media. En vez de eso, una política de destrucción cibernética mutuamente asegurada—al ser abierta, transparente, mutua y ofensiva—tendría suficientes nuevos controles disuasorios integrados en ella estructuralmente para no solamente proporcionar más opciones sino también para hacer vacilar a los malhechores de un comportamiento que podría poner a prueba sus límites.

Recuerde que la mutualidad no solo aumenta el temor sino que ese mismo temor permite la posibilidad de aumentar la confianza mediante un enfrentamiento repetido. Hasta ahora la naturaleza dinámica del dominio cibernético favorecía demasiado a los que lo dañarían. La destrucción cibernética mutuamente asegurada pondría finalmente parte de ese dinamismo en manos de potencias importantes con un interés mutuo en reglas, regulaciones y estabilidad.

Ciberguerra, disuasión cibernética y complejidad política

Tratar de estudiar las consecuencias del impacto del dominio cibernético sobre la guerra y el conflicto es un avispero de complicaciones políticas. Incluso al tratar de desarrollar un sistema de protección puramente defensivo no atacante, existe una preponderancia de consideraciones complejas. ¿Cómo puede estar uno seguro del atacante? ¿Pueden arriesgarse los haberes cuando se sospeche de un ciberataque? ¿Envían las represalias el mensaje correcto al lado defensivo? ¿Debe haber un umbral de respuesta? ¿Cómo se evita la escalada?[16] Todas estas preguntas plantean problemas no solo porque son complicadas sino porque la naturaleza de un sistema cibernético defensivo exacerba los defectos dentro de esa política en vez de eliminarlos, y sin embargo otras preguntas discutiblemente aparecen solamente debido a estos defectos inherentes en una mentalidad defensiva.

La complejidad se reduce al considerar el desarrollo de una política de destrucción cibernética mutuamente asegurada, pero admitimos que puede poner a Estados Unidos en una posición política incómoda al principio. Considere simplemente la teoría de la guerra. En el primer ejemplo, derecho a la guerra, cuando los estados pueden legalmente considerar pasar de la paz a la guerra, hay al menos tres criterios inmediatos que la mayoría de los estados preferirían tener a su favor: finalidad adecuada, autoridad debidamente constituida y último recurso.[17] Una política

de destrucción cibernética mutuamente asegurada sería especialmente dura en cada criterio: la política no opera solamente yendo a la guerra en defensa propia, ya que la naturaleza de la seguridad cibernética excluye cualquier noción real de poder defenderse eficazmente contra un ciberataque masivo; también existe el riesgo de que la destrucción cibernética mutuamente asegurada eluda la notificación gubernamental apropiada debido a que el debilitamiento total dependería en gran parte del elemento de sorpresa, que funciona contra la transparencia y el carácter abierto premeditados; y por último, la destrucción cibernética mutuamente asegurada por naturaleza propia es la antítesis del último recurso—la eficacia de la posición procede de no ser puramente de represalia sino potencialmente prioritaria, indicando la voluntad de usar armas virtuales en circunstancias no solamente desesperadas.

Muchos argumentarían que desde una perspectiva puramente política/diplomática, estas posiciones parecen algo insostenibles. Esto sería cierto si la destrucción cibernética mutuamente asegurada se configurara estructuralmente, de modo que Estados Unidos domine esas capacidades ofensivas solo y de hecho, convirtiéndose en un tirano virtual cara a cara con otras grandes potencias. Pero según se trató antes, la estructura inherente del dominio cibernético hace que dicho objetivo, incluso si es lógico para una gran potencia, es muy poco probable y casi imposible. Por lo tanto, todos los estados que se afanen en una destrucción cibernética mutuamente asegurada harían esfuerzos relativamente iguales en armarse. Esto permite la posibilidad con el tiempo de una percepción de igual debilitamiento para surtir efecto y discutiblemente crear estímulos de disuasión similares a la destrucción nuclear mutuamente asegurada.

La incomodidad política y diplomática inicial relacionada con la destrucción cibernética mutuamente asegurada no mejora cuando se considera el derecho a la guerra, o el deseo de que los estados mantengan los principios de justicia en guerra. Nuevamente, se pueden resaltar tres criterios principales: inmunidad para los no combatientes, proporcionalidad y más bien que mal.[18] Una política de destrucción cibernética mutuamente asegurada seguiría teniendo la ventaja principal de cualquier sistema de defensa cibernético: que es relativamente incruento. No obstante, la ventaja empieza a ser más ambigua según la destrucción cibernética mutuamente asegurada; un ataque masivo contra la infraestructura de un estado, el debilitamiento de los mecanismos y funciones sociales importantes, resultaría casi ciertamente en sufrimiento para los no combatientes y por lo tanto no garantizaría inmunidad en el sentido más formal. La proporcionalidad claramente no puede cumplirse simplemente porque el punto de una política de destrucción cibernética mutuamente asegurada sería asegurar la defensa mediante un segundo ataque de represalia no proporcional. Sería la garantía de la respuesta/ataque no proporcional la que causaría el impulso disuasorio. Por último, el criterio de más bien que mal según la destrucción cibernética mutuamente asegurada sería realmente, al final, una interpretación completamente arbitraria basada en qué lado y qué objetivos de seguridad se están considerando.

Se ha hecho poco trabajo hasta la fecha en una conceptuación explícita de una ciberestrategia ofensiva y transparente para aumentar la seguridad nacional. Lo que se ha hecho es lograr un consenso general de que hay tres formas evidentes en que un estado podría crear la capacidad de infringir daños a otro adversario tipo estado o no estado mediante un ciberataque. La primera opción es simplemente crear la capacidad de nuestras propias fuerzas y tecnologías. La segunda opción es cultivar una fuerza de voluntarios que pueda guiarse para atacar objetivos designados con poca o ninguna atribución del gobierno que los apoya. La tercera opción es subcontratar al menos partes del problema a otros gobiernos, entidades comerciales u organizaciones clandestinas criminales siguiendo un modelo prácticamente mercenario.[19] Cada opción tiene claramente sus propios errores.

Tanto China como Rusia formal e informalmente juegan con la idea de utilizar las opciones una y dos. Estados como Irán, Corea del Norte y Nigeria han estado al menos curiosamente relacionados con la opción tres. Tal vez esta es la mayor dificultad que impacta la formulación de políticas de Estados Unidos—parece plausible que Estados Unidos simplemente no quiera con-

siderar un cambio de política que se asocie tan claramente con este grupo de países, fueran cuales fueran las ventajas. De las tres opciones, la primera opción tiene la mayor posibilidad de ser considerada por parte de Estados Unidos, ya que esta política de creación propia sería al menos discutiblemente controlable y podría ser definida explícitamente por instituciones democráticas estadounidenses con sus controles inherentes informados por principios de transparencia y responsabilidad.

Estados Unidos tiene ciertamente la capacidad de desarrollar cuadros orgánicos asignados a la tarea de desarrollar un dominio cibernético armado. Pero donde se ha hecho esto hasta ahora ha sido en pequeña escala y en áreas muy secretas. Estas características hacen que sea una capacidad de ataque evidente estructurada más eficazmente para usar en el contexto de una agresión abierta y guerra en vez de según se necesita en última instancia—como una capacidad disuasoria diseñada para prevenir que dicha agresión se produzca en épocas de paz. Nuevamente, la máxima ventaja de la destrucción cibernética mutuamente asegurada no radica en lograr verdaderamente una capacidad de segundo ataque útil sino en crear con el tiempo la credibilidad en dichas represalias de modo que no sea necesario nunca el segundo ataque.

Las otras dos opciones no permiten dicha oportunidad de una política realmente gobernable y responsable y no es probable que sea considerada por Estados Unidos. Este artículo no reta la premisa que inicialmente una política de destrucción cibernética mutuamente asegurada pondría a Estados Unidos en algunas posiciones políticas bastante extrañas. En vez de eso, adopta la posición más fundamentalmente maquiavélica de que la seguridad nacional se administra mejor mediante eficacia y control, incluso a expensas de la imagen diplomática y las percepciones públicas de rectitud.

Conclusión

La mayoría de los analistas, especialistas militares y oficiales del gobierno admiten que la vida en el siglo XXI incluirá ciberataques. No existe una visión de un mundo libre sin tales ataques. Esta simple admisión socava la eficacia de un sistema de disuasión cibernética cuya razón de ser es la prevención de dichos ataques. Este artículo no lleva tanto la contraria como para discutir anárquicamente el abandono del esfuerzo a fin de lograr una seguridad cibernética real. En vez de eso, pide que finalmente se dé a ciertas realidades estructurales un espacio intelectual en la mesa de debates y que se permita ese espacio para considerar nuevas opciones y posibilidades. Hay dos realidades estructurales en particular en las que se debe hacer hincapié. Primero, en el dominio cibernético la ofensa domina siempre y siempre lo hará. Es estructural y axiomático. Segundo, las capacidades, la tecnología y el talento existen para instituir este sistema en Estados Unidos. Lo que se necesita es un cambio de mentalidad y estimular nuevas ideas y políticas—de modo transparente. No es fácil en absoluto, pero se puede lograr.

La imposición de una política de destrucción cibernética mutuamente asegurada podría demostrar ser más efectiva, aun cuando pueda incomodar más a Estados Unidos política y diplomáticamente. El debate continúa y el argumento sigue: se puede conseguir una mayor seguridad cibernética mediante un debilitamiento mutuamente asegurado para todos. ❑

Notas

1. Mark Young, "National Cyber Doctrine: The Missing Link in the Application of American Cyber Power" (Doctrina cibernética nacional: el eslabón perdido en la aplicación del poder cibernético de EE.UU.), Journal of National Security Law and Policy 4, no. 1 (2010): 173–96.

2. Ibid.

3. Martin C. Libicki, Cyberdeterrence and Cyberwar (La disuasión y la guerra cibernéticas), (Santa Monica, CA: RAND, 2009).

4. Arthur Bright, "Estonia Accuses Russia of Cyberattack" (Estonia acusa a Rusia de un ataque cibernético), Christian Science Monitor, 17 mayo de 2007, http://www.csmonitor.com/2007/0517/p99s01-duts.html.

5. Alan W. Dowd, "Are We Ready for WWI?" (¿Estamos listos para la Primera Guerra Mundial?), Fraser Forum, septiembre de 2009, 12–14.
6. James Cartwright, "Afirmación ante el Subcomité de Fuerzas Estratégicas del Comité de Servicios Armados del Senado", 28 de marzo de 2007.
7. Eric D. Trias y Bryan M Bell, "Cyber This, Cyber That . . . So What?" (Ciberesto, cibereso ... ¿y qué?) Air and Space Power Journal 24, no. 1 (Verano de 2010): 90–100.
8. Ibid.
9. Ibid.
10. Ruzena Bajcsy y otros, "Cyber Defense Technology Networking and Evaluation" (Redes y evaluación de la tecnología de defensa cibernética), Communications of the Association of Computing Machinery 47, no. 3 (marzo de 2004): 58–61.
11. Ibid.
12. William J. Lynn, "Defending a New Domain" (Defensa de un nuevo dominio), Foreign Affairs 89, no. 5 (septiembre/octubre de 2010).
13. Ibid.
14. Ibid.
15. Ibid.
16. Libicki, Cyberdeterrence and Cyberwar (Disuasión y guerra cibernéticas).
17. Andrew Liaropoulos, "War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory" (La guerra y la ética en el ciberespacio: conflicto cibernético y teoría de la guerra justa), Minutas del 9º Congreso Europeo sobre guerra y seguridad de información (Reading, Reino Unido: Academic Publishing, Ltd., 2010), 177–82.
18. Ibid.
19. Rain Ottis, "Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability" (El modelo teórico para crear una capacidad cibernética ofensiva a nivel de nación-estado), Minutas del 8º Congreso Europeo sobre guerra y seguridad de información, (Reading, Reino Unido: Academic Publishing, Ltd., 2009), 177–82.

El Dr. Matthew Crosston es presidente de Seguridad Industrial e Internacional de la Fundación Miller y Director del Programa de Estudios Internacionales de Seguridad e Inteligencia (ISIS, por sus siglas en inglés) en la Universidad Bellevue, Nebraska. Es autor de dos libros bien reconocidos y diez artículos revisados por homólogos sobre temas que abarcan contraterrorismo, corrupción, democratización, Islam radical y disuasión cibernética. Su agenda de investigación continúa en esos campos a la vez que se enfoca en conceptos nuevos de conflictos futuros. Crosston ha hecho presentaciones y ha hablado por todo el mundo para fomentar la interacción transnacional entre las agencias de inteligencia que comparten intereses comunes pero que carecen de canales de conectividad. El Dr. Crosston ostenta una licenciatura en arte de la Universidad Colgate, New York; una maestría de la Universidad de Londres, y un doctorado de la Universidad Brown, Rhode Island (2003). Después de terminar sus estudios de posdoctorado en la Universidad de Toronto, Crosston pasó a formar parte del cuerpo docente en Relaciones Internacionales y Política Comparativa en la Universidad Clemson, South Carolina, antes de trasladarse al Instituto Militar de Virginia para enfocarse en la Seguridad Nacional y Estudios Internacionales. En el 2010 llegó a la Universidad Bellevue para desarrollar el programa ISIS, una iniciativa que fue comenzada bajo los auspicios del programa ISIS, una iniciativa que fue comenzada bajo los auspicios del USSTRATCOM. Dos características destacadas del programa ISIS son la relación proactiva con miembros militares actuales y antiguos que buscan continuar su educación y el uso emprendedor de la tecnología de punta con métodos de entrega en línea a la vez que no se sacrifican ni el rigor intelectual ni el aprendizaje activo.

Fuente: Publicado anteriormente en nuestra revista Strategic Studies Quarterly, Spring 2011