Diseñando Colisiones de Satélites en la Guerra Cibernética Encubierta*

Dr. Jan Kallberg, PhD

EL ESPACIO EXTERIOR ha gozado después de la Guerra Fría de dos décadas de un desarrollo bastante pacífico, pero una vez más se hizo más competitivo y disputado con la mayor militarización. Por lo tanto, es importante que EE.UU. mantenga su superioridad espacial para asegurarse de que tenga las capacidades bélicas modernas para tener éxito en las operaciones. La diferencia con los períodos anteriores en el espacio[1] es que no es una carrera armamentística espacial[2] anunciada de forma flagrante sino un reto encubierto para los intereses de EE.UU. en mantener la superioridad, la resistencia y la capacidad. Hay un número finito de naciones que se consideran actores geopolíticos, pero mientras EE.UU. mantiene la superioridad espacial, esos estados deben comportarse según un conjunto de reglas escritas sin su consentimiento y sin ser forzados. Para los regímenes autoritarios, los haberes espaciales de EE.UU. supervisan sus acciones y buscan tener una influencia regional, lo que es muy inquietante. Para ellos, cualquier degradación o limitación de las capacidades espaciales de EE.UU. se consideraría como un resultado satisfactorio. La guerra cibernética de estos actores antagonistas ofrece la oportunidad de destruir directa o indirectamente los haberes espaciales de EE.UU. con un riesgo mínimo debido a una atribución y capacidad de identificación limitadas. El asunto de este artículo es cómo podrían lograr esta tarea. Uno debe empezar examinando la dependencia de Estados Unidos en el espacio antes de concentrarse en la obstrucción espacial y los medios que utilizaría un adversario. Mientras que la protección satelital es un reto, hay varias soluciones que EE.UU. debe tener en cuenta en los años venideros.

Dependencia de EE.UU. del espacio

La guerra concentrada en la red depende de la red de información global para capacidades de combate conjuntas.[3] La capa fundamental crea la capacidad de combate global como la columna vertebral espacial de la red de información donde los haberes espaciales son el elemento decisivo. EE.UU. depende de las capacidades espaciales para su éxito y la seguridad nacional de EE.UU. se basa hoy en día en un número limitado de satélites muy utilizados. Estos satélites son cruciales para la disuasión estratégica, la vigilancia, la recopilación de inteligencia y las comunicaciones militares. Si la disuasión estratégica falla, los satélites forman parte integral de la defensa de misiles balísticos ofensivos y defensivos. Los satélites son fundamentales no solamente para la superioridad espacial de EE.UU., sino también para la superioridad de información—el motor en la maquinaria de combate bélico conjunta de canales múltiples que ha demostrado tener éxito en recientes conflictos. Las fuerzas estadounidenses pueden luchar globalmente debido al acceso al C4ISR apoyado por satélites. Los adversarios potenciales, de todos los tamaños e intenciones, entienden que las fuerzas militares de EE.UU. podrían estar estrechamente relacionadas con los haberes espaciales de EE.UU. Este enlace exclusivo entre los haberes espaciales y la seguridad nacional lo expresa bien el director Finch y el subdirector Steele de la Oficina del Subsecretario de Defensa para Política;

*Fuente: Publicado anteriormente en nuestra revista Strategic Studies Quarterly, Spring 2012

> "Aunque otros estados utilizan cada vez más el espacio para fines económicos y militares, Estados Unidos es el país que mucho más depende de sistemas espaciales debido a sus responsabilidades globales y su método de combate de alta tecnología que aprovecha en gran medida los sistemas espaciales para la comunicación, la navegación, la inteligencia, la vigilancia y el reconocimiento. Esta asimetría crea un desequilibrio; cuanto más confíe una nación en sistemas espaciales, mayor será la tentación de que un posible adversario fije esos sistemas como objetivos".[4]

Desde la caída de la Unión Soviética, la superioridad espacial de EE.UU. no ha sido retada extensivamente y hemos presenciado dos décadas de supremacía espacial de EE.UU. Los ataques contra los satélites de EE.UU. han sido una preocupación desde los años 70[5] con un enfoque en interferencia de señales, rayos láser desde tierra[6] y ataques de misiles directos antisatelitales cinéticos. William J. Lynn, III, anterior Subsecretario de Defensa de EE.UU., afirmó lo siguiente en el verano de 2011;

> "La voluntad de los estados de interferir con satélites en órbita tienen implicaciones serias para nuestra seguridad nacional. Los sistemas espaciales permiten nuestra forma de guerra moderna. Permiten que nuestros combatientes ataquen con precisión, naveguen con exactitud, se comuniquen con certeza y vean el campo de batalla con claridad. Sin ellos, muchas de nuestras ventajas militares más importantes se evaporan".[7]

Los comentarios de Lynn se deben en gran medida a la Estrategia Espacial de Seguridad Nacional de enero de 2011. La estrategia indica que el espacio está congestionándose, disputándose y haciéndose más competitivo. Claramente describe la importancia de proteger las capacidades espaciales de EE.UU.;

> "La Estrategia Espacial de Seguridad Nacional se basa en todos los elementos del poder nacional y requiere un liderazgo activo de EE.UU. en el espacio. Estados Unidos buscará un conjunto de métodos estratégicos interrelacionados para cumplir con nuestros objetivos espaciales de seguridad nacional, a saber: estimular el uso responsable, pacífico y seguro del espacio; mejorar las capacidades espaciales mejoradas de EE.UU.; asociarse con naciones responsables, organizaciones internacionales y firmas comerciales; prevenir y disuadir la agresión contra la infraestructura espacial que respalda la seguridad nacional de EE.UU.; y prepararse para rechazar ataques y operar en un entorno degradado".[8]

Lynn también observó el impacto de la cantidad creciente de residuos espaciales;

> "El espectro de las interferencias no es la única nueva preocupación. La colisión de febrero de 2009 de un satélite de comunicaciones Iridium con un satélite soviético desactivado, y la anterior y deliberada destrucción de un satélite por China, produjeron miles de fragmentos residuales, cada uno de los cuales plantea una amenaza potencialmente catastrófica a la aeronave espacial operacional. En un instante, estos eventos, uno accidental, el otro premeditado, duplicaron la cantidad de residuos espaciales, haciendo que las operaciones espaciales sean más complicadas y peligrosas".[9]

El ataque cinético y la destrucción deliberados de un satélite en desuso por los mismos chinos usando un misil antisatélite atrajo la atención no solamente al hecho de que los chinos probaran el misil antisatélite y el impacto de la política[10], sino también la nube de residuos que produjo la explosión.

Un espacio muy congestionado

La cuestión de residuos espaciales se complica debido a la miríada de problemas que representan no solamente los obstáculos físicos para eliminar residuos sino también los asuntos legales e internacionales.[11] En consecuencia, el espacio se está congestionando más con unos 1.100 y 2.000 satélites inactivos en órbita.[12] Con el tiempo, la cantidad de residuos espaciales ha aumentado constantemente[13] y la cantidad total de residuos rastreados asciende actualmente a 22.000 objetos. Los primeros pasos para crear una estrategia de mitigación de residuos se dieron a finales de

los años 70.[14] Desde entonces, se han lanzado al espacio miles de satélites y la mayoría de éstos están inactivos o son de una generación de tecnología más antigua al final de su vida útil. EE.UU. ha liderado el esfuerzo de reducción de residuos para mitigar los riesgos diseñando activamente vehículos espaciales que podrían desecharse o eliminarse de forma segura por degradación orbital.[15] El problema principal referente a los residuos espaciales es el interés mutuo en limitar los efectos de los residuos espaciales y en hacer un esfuerzo conjunto para disminuir la cantidad de residuos de modo que con el tiempo predominen la degradación orbital y la gravedad.

Para entender la potencia destructora de los residuos espaciales la velocidad tiene importancia. Un proyectil militar estándar de 5,56 mm se desplaza a 940 m/s cuando sale del cañón y puede penetrar fácilmente en un ser humano. Un proyectil de carro de combate de EE.UU. de 120 mm tiene una velocidad inicial de 1.740 m/s[16] y puede atravesar un carro de combate de batalla de tamaño medio. Los residuos espaciales y la basura espacial que se desplazan a una velocidad orbital circular impactarán en un satélite a una velocidad de 3.000 a 7.600 m/s, dependiendo de la altitud. Los residuos, que se desplazan más de ocho veces más rápido que una bala de rifle de alta velocidad, ya sea una llave ajustable perdida hace mucho tiempo, de los años 70, con las letras CCCP estampadas, o una bala de acero dispersada intencionadamente, crea un impacto sin precedentes. La creación de residuos espaciales de forma deliberada e intencionada en órbitas específicas cambiaría radicalmente las probabilidades de impacto, incluso si la mayoría de los residuos se perdieran en otras direcciones o fueran afectados y eliminados por efectos físicos. Una colisión planeada o una nube grande de residuos en una órbita idéntica anularía la opción de sacar el objetivo del área fijada como objetivo. Los satélites son obras maestras frágiles de ingeniería electrónica, cables, conectores, paneles solares, circuitos integrados y antenas de alta frecuencia. Cada centímetro tiene una función especial. Cualquier objeto que se desplace a 7.600 m/s es una amenaza real para el satélite.

El síndrome de Kessler

El antiguo experto de la NASA en residuos espaciales, Donald J. Kessler, predijo la probabilidad de colisiones en el espacio y el riesgo de colisión que produciría una gran cantidad de residuos espaciales después del impacto de una colisión a alta velocidad.[17] Una reacción en cadena, llamada síndrome de Kessler podría ser la consecuencia. El síndrome de Kessler se produce cuando los residuos u otro satélite colisionan con otro satélite (o basura espacial) con hipervelocidad, producen muchos más residuos debido al impacto hiperveloz y si la densidad del satélite (o basura espacial) es suficientemente alta podría surtir un efecto en cadena por el espacio. Kessler predijo el problema pero también indicó claramente, en los años 70, que la cantidad de basura espacial y satélites era demasiado pequeña para producir efectos en cadena en el espacio. Más adelante, ha reconfirmado la posición. La contribución de Kessler era identificar el problema y explicarlo. Desde que Kessler escribió sobre el problema en 1978, ha vuelto al tema para aclarar, ampliar la cuestión o presentar sus cálculos.[18] El trabajo de Kessler se concentró en colisiones inintencionadas, aleatorias y descontroladas. De forma similar el debate sobre los residuos espaciales se concentra en la creación inintencionada de residuos espaciales al arrojar desperdicios desde estaciones espaciales, haciendo estallar propulsores espaciales y colisionando objetos.[19] En términos reales, debido a la probabilidad limitada de una colisión aleatoria, el mayor riesgo se produce con creación intencionada y premeditada de nubes de residuos que se concentran en órbitas de satélites críticas de misiones de EE.UU. Si en vez de esto las colisiones son intencionadas, planificadas y controladas se multiplican los riesgos y se presenta al adversario la oportunidad de destruir equipos satelitales fundamentales de EE.UU. Para alcanzar un umbral en cadena, un adversario puede añadir residuos espaciales a través de acciones controladas e intencionadas. La forma más rápida de añadir residuos espaciales a la órbita es hacer colisionar la masa existente de satélites y los residuos espaciales que orbitan la tierra.

Si la masa que ya está en el espacio puede secuestrarse mediante ciberataques, traspasa la exposición al rastreo y a la atribución.

Tipo y medios de ataque

Para cualquier estado con intención de llevar a cabo operaciones en secreto, los satélites extranjeros son un problema importante. Los satélites llevan a cabo tareas de recopilación de inteligencia, vigilancia y reconocimiento, lo que puede ser muy importuno para estados que carecen de transparencia entre sus compromisos internacionales, su postura pública y lo que están haciendo entre bastidores. Normalmente, un adversario puede elegir entre dos tipos de ataques antisatelitales no cibernéticos: cinético directo y cinético indirecto. Aunque es posible un ataque de misiles antisatelitales cinético directo a un satélite de EE.UU., tendría una atribución directa al atacador que desembocaría en repercusiones. El propulsor y el calor del misil se identificarían y se atribuirían al país o a la aeronave que lanzaron el ataque. Un ataque cinético directo podría ser tentador pero el precio político es alto. Incluso si resultara atractivo atacar satélites, un adversario no podría atacar sin dejar un rastro de evidencia tangible. El uso de un misil antisatelital (ASAT) es un acto de guerra grave y solamente puede usarse razonablemente si el perpetrador anticipa y acepta una respuesta bélica.

Para un adversario potencial puede ser mucho más interesante aumentar la cantidad de residuos que obstruyen las órbitas específicas que resumen así el ataque indirecto. El aumento de residuos puede hacerse añadiendo activamente residuos a órbitas específicamente bien definidas, accidentes de diseño sistemáticos o colisiones en el espacio.

Durante el siglo XVIII, hasta la Segunda Guerra Mundial, las unidades de artillería tenían un proyectil especial si la infantería enemiga se acercaba demasiado a la posición de la batería –la metralla. La batería apuntaba hacia la infantería que se aproximaba y disparaba metralla que dispersaba miles bolas de acero que creaban bajas masivas en las filas de la infantería. No importaba si las bolas de acero impactaban en un brazo, una pierna, el torso o una mano. El asalto de infantería hacia la posición de la batería perdía ímpetu y terminaba. Al aplicar la idea de metralla al espacio observamos una forma simplificada de aumentar radicalmente los residuos usando propulsores espaciales para alcanzar la órbita terrestre inferior (LEO) y después usar la energía cinética para dispersar miles de bolas de acero en una sección del espacio. Como propulsor espacial cualquier misil obsoleto o rudimentario, como el Shahab iraní o el Taepodong norcoreano, podría comportarse como un vehículo para transportar la carga al espacio. Una andanada de veinte propulsores espaciales rudimentarios que suministren una cantidad significativa de metralla prefragmentada o bolas de acero podría aumentar radicalmente la cantidad de residuos que se desplazan a hipervelocidad. La probabilidad de una colisión en el espacio entre un satélite en funcionamiento y los residuos es cuestión de números. Reducido a un ejemplo simplificado, si la presencia de 5.000 unidades residuales a una altura genérica específica genera un riesgo de impacto de satélite cada diez años, sin tener en cuenta los residuos adicionales generados por el impacto, unas 100.000 unidades residuales aumentarían considerablemente el riesgo. Para explicar el principio, veinte propulsores espaciales pueden lanzar 30 toneladas métricas de carga útil a la LEO—unas 400.000 bolas de acero—que se propagarían a hipervelocidad por las órbitas del satélite. El ataque es cinético pero indirecto, ya que los satélites objetivo no están fijados como objetivos individualmente sino que son atacados por un enjambre de residuos hiperveloces que impactan en los satélites deseados por penetración o destruyendo antenas, paneles solares u otros equipos. Este impacto generaría inicialmente más residuos aunque la degradación orbital contrarresta algunos de ellos moviendo residuos a una menor altitud que con el tiempo desaparecerían del espacio.

El ataque cinético directo e indirecto sería un acto de guerra y tendría la atribución necesaria para dar a EE.UU. un casus belli o motivo de guerra aprobado por al menos parte de la comuni-

dad internacional. En primer lugar, tanto el ataque cinético directo como indirecto se atribuiría a una nación que lanzara el ataque y las observaciones de satélites monitores espaciales serían suficientemente exactas para dar a EE.UU. un argumento sólido. En segundo lugar, la creación de cantidades sin precedentes de residuos espaciales no solamente sería peligroso para los satélites de EE.UU. sino también para otras potencias extranjeras. Si la nación inconformista X lanza un ataque cinético indirecto, afectaría a satélites rusos, europeos, chinos, indios, paquistaníes y de otras naciones. Dependiendo de la dispersión de estos objetos residuales, los daños podrían limitarse a pequeñas partes del espacio, pero seguiría siendo un territorio espacial no usado exclusivamente por EE.UU. La nación inconformista X evita tradicionalmente las repercusiones apoyadas por la ONU de la comunidad internacional cuando se hayan perjudicado los intereses de EE.UU. Probablemente Rusia o China, en particular, vetarían las acciones punitivas propuestas por EE.UU. en el Consejo de Seguridad de la ONU.[20] No obstante, en esta situación, la nación inconformista X no puede permitirse el lujo de ese apoyo dañando los haberes espaciales rusos y chinos como daños colaterales en un ataque a satélites de EE.UU. Los haberes espaciales chinos son muy limitados comparados con el inventario ruso y de EE.UU. Un ataque cinético indirecto contra haberes de EE.UU. podría causar daños importantes a intereses chinos, ya que los chinos carecen de elasticidad espacial. Ni los ataques cinéticos directos ni indirectos eran opciones adecuadas o viables para una nación inconformista que trate de dañar los satélites.

Ciberataque en el espacio

La vida útil de un satélite está comprendida entre cinco y treinta años, e incluso después puede seguir orbitando en el espacio con suficiente combustible propulsor para desplazarse por el espacio con comunicaciones funcionales que pueden activarse. El espacio contiene miles de satélites, activos y desactivados, lanzados por numerosas organizaciones y países con más de 5.000 transpondedores espaciales comunicándose con la tierra. Cada transmisión es una entrada potencial de un ciberataque. Los satélites viejos comparten similitudes con la oportunidad de ciberexplotar sistemas industriales para el control y el procesamiento. Los sistemas de control de supervisión y adquisición de datos (SCADA) dentro de nuestras municipalidades, instalaciones, infraestructura y fábricas están diseñados y construidos con tecnología y equipos más viejos, algunas veces diseñados hace décadas, y el software raramente se actualiza. Estos sistemas SCADA se consideran una vulnerabilidad estratégica y han atraído una atención creciente de la comunidad de ciberdefensa de EE.UU. en años recientes. Los satélites pueden basarse en hardware y tecnología de los años 80 por una razón muy sencilla–es poco probable que los satélites se actualicen después de haberse lanzado al espacio.

Los ciberataques terrestres son un "exploit" individual para miles, si no millones de sistemas idénticos y la amenaza se eliminará después en actualizaciones o modernizaciones. La diferencia entre satélites y "exploits" cibernéticos terrestres es que un satélite en muchos casos está hecho a la medida y el diseño de computación está patentado. En vez de eso, los ciberataques espaciales aprovechan un solo sistema, o un grupo limitado de sistemas, dentro de un grupo de satélites más numerosos. Estos haberes espaciales tienen una variedad de sistemas de operación, software integrado y diversos diseños de legados tecnológicos. A medida que más naciones participan en el lanzamiento de satélites con una variedad de refinamiento técnico, aumenta el riesgo de secuestrar y manipular mediante el uso de actividades encubiertas. La computadora abordo (OBC) del satélite puede permitir la reconfiguración y las actualizaciones de software, lo que aumenta la vulnerabilidad de los ciberataques. Un satélite vulnerable que orbite durante los próximos diez años puede prefijarse para el uso no autorizado cuando lo necesite un perpetrador cibernético.

Incluso con las capacidades forenses digitales más avanzadas para rastrear un ciberataque es complicado en sistemas de computadoras terrestres físicamente disponibles. Los sistemas espaciales no permiten el acceso físico y por ello la falta de acceso a un sistema de computadora anula

varias opciones de recopilación de evidencia forense. El único rastro del perpetrador son las transmisiones reales y los intentos inalámbricos para penetrar en el sistema. Si no se capturan estas transmisiones el rastro está perdido.

Además, si el adversario es habilidoso, es más probable de que la investigación de la atribución termine con un conjunto de actores inocentes engañados, cuyas identidades digitales han sido vehículos en el ataque, en vez de la atribución al perpetrador real. Una sospecha fundamentada impactaría las relaciones interestatales pero para crear un caso de represalias se necesita una atribución y un rastreo. La atribución puede graduarse pero depende de lo que se aceptaría como un ataque "atribuido". El liderazgo nacional puede aceptar un menor nivel de una atribución tangible que la comunidad internacional, basándose en informes de inteligencia anteriores y modus operandi adversario pero está limitado para tomar medidas. China ha tenido un interés creciente en adquirir capacidades de guerra cibernética[21] y es una de varias naciones que tendrían un interés sincero en degradar los haberes espaciales de EE.UU. Actualmente, las naciones están limitadas por las repercusiones políticas y económicas de un ataque atribuido. No obstante, la determinación de objetivos de guerra cibernética encubierta que fija como objetivos haberes espaciales de EE.UU. elimina la limitación de la atribución.

Un ciberataque que dé lugar a una colisión carecería de atribución e invitaría a nuestros adversarios encubiertos. Una colisión entre un satélite extranjero de movimiento súbito y un satélite de EE.UU. crítico para la misión no es ni coincidencia ni accidente. Pero sin atribución no importa si es evidente. Otras formas de ataques directos e indirectos corresponden a un atacante que podría tener repercusiones militares, económicas y políticas. En criminología sabemos que la consideración más importante principal de un perpetrador de actos premeditados es el riesgo de ser atrapado. La magnitud de las repercusiones, si se descubre, es secundaria. Si un ciberataque puede destruir o desactivar satélites de EE.UU., sin atribución ni identificación, es probable que sea considerado por aquellos que sean abiertamente nuestros adversarios y ciertamente los que de forma encubierta son nuestros adversarios. Desde una perspectiva de guerra cibernética esto crea una oportunidad para una tercera parte para atacar y secuestrar un satélite con la finalidad expresa de colisionar con un satélite de EE.UU. en misión crítica. El ataque podría ser una colisión directa o un ataque indirecto usando la nube de residuos de otra colisión. El satélite ariete puede proceder de cualquier otro país u organización internacional. La forma más sencilla de perpetuar este ataque sería secuestrar satélites de países menos avanzado técnicamente, sistemas menos protegidos o caídos en desuso.

El impacto en satélites fijados como objetivos

El impacto en satélites fijados como objetivos directa o indirectamente con la intención de destruir el objetivo por colisión con objetos hiperveloces. Según se ha hablado anteriormente, el adversario puede crear un ataque directo impactando satélites de EE.UU. fijados como blancos con vehículos espaciales usando comandos sin autorizar mediante medios cibernéticos. El objetivo del paso inicial en un ataque indirecto podría ser perfectamente otro satélite, parte de un vehículo de suministro, o desechos espaciales que crearían residuos significativos en el impacto. La colisión crearía cientos o miles de residuos espaciales que continuarían en el espacio a alta velocidad. La nube de residuos afectaría a otros satélites en la órbita de colisión e incluso pueden iniciar el síndrome de Kessler causando daños multiplicadores si se alcanza el umbral.

Resolución del reto espacial

Aunque los problemas y las vulnerabilidades en el espacio y los medios para atacar haberes espaciales son significativos, EE.UU. tiene opciones para mitigar los riesgos.

El impacto en satélites fijados como objetivos es más probable que ocurra si hay satélites obsoletos e inactivos abandonados en el espacio que puedan ser secuestrados para la determinación de blancos y la colisión. La eliminación después de la misión (PMD)[22], el esfuerzo de la ONU e internacional de eliminar satélites después de su duración productiva, requeriría eliminar satélites del espacio 25 años[23] después de terminar su misión.[24] Naturalmente, podría ocurrir antes de 25 años pero también podría ser un proceso prolongado, ya que no hay sanciones tangibles por incumplimiento como hoy en día. Si un satélite tiene una duración de 10-20 años, los 25 años adicionales dejarían un número total de años cuando el satélite puede ser controlado remotamente a 35–45 años. Los satélites lanzados en 1977, 1987 y 1997 ya estaban técnicamente pasados de moda y varias generaciones atrasados. El tiempo entre el lanzamiento y el final de la operación para un satélite es la base de su vulnerabilidad cibernética. Es una buena decisión financiera usar un satélite en la máxima medida de su duración. Pero la cuestión se convierte en: ¿merecen la pena los riesgos? Debemos tener en cuenta el progreso técnico conseguido desde los primeros lanzamientos espaciales y qué vulnerabilidades podrían estar integradas cuando el espacio esté poblado por haberes de 25 a 45 años que todavía puedan navegar. Como la tecnología actual se desarrolla tan rápidamente, en realidad, la PMD aumenta el riesgo de un ciberataque por satélites secuestrados porque prolonga el tiempo que un satélite puede ser controlado de forma remota mediante señales de radio usando equipos de comunicación obsoletos y pasados de moda. Estados Unidos debe proponer el acortamiento del período de eliminación PMD e insistir en actualizaciones de comunicaciones para crear un control seguro para todos los haberes espaciales.

Si se pierde el uso pacífico y seguro del espacio, EE.UU. tratará de disuadir y rechazar la agresión contra la infraestructura espacial. El grado de preparación para rechazar ataques y operar en un entorno degradado requiere resistencia—la capacidad de absorber la pérdida de capacidad mientras siga en operación. Se puede usar un solo satélite para recopilar inteligencia, todos los niveles de comunicaciones militares y una plataforma para distintos sensores. Para los adversarios, un tipo o diseño específicos de satélites pueden tener una importancia crítica y un blanco de alto valor que destruir. Si un presupuesto insuficiente fuerza a EE.UU. a utilizar excesivamente los satélites también aumenta la dependencia en cada satélite individual para el combate y la inteligencia.[25] El riesgo evidente en una época de austeridad es que los recortes del presupuesto predominan sobre la dependencia en sistemas espaciales fundamentales.

La Política Espacial Nacional de 2010 requiere:

> "Aumentar la seguridad y la resistencia de funciones esenciales para la misión activadas por aviación comercial, civil, científica y nacional e infraestructura de apoyo contra la alteración, degradación y destrucción, ya sean causas medioambientales, mecánicas, electrónicas u hostiles".[26]

Incluso en una época de austeridad federal será necesario reemplazar una flota envejecida de haberes espaciales de EE.UU., ya que estos haberes son cruciales para el éxito. Eso incluiría un mayor número de satélites incluso si la inversión creara una redundancia significativa. Esta redundancia es una salvaguardia contra la capacidad de operar en un entorno degradado y proporciona una resistencia vital.

Por último, EE.UU. debe adoptar una defensa activa y tantear los límites de la guerra cibernética en el espacio. Un factor limitador del éxito en defender los haberes espaciales contra el ciberataque son las limitaciones reguladoras en las operaciones de información llevadas a cabo por el Departamento de Defensa y agencias relacionadas. Es una decisión de política que requiere que los formuladores de políticas entiendan los fundamentos exclusivos del ciberespacio. El carácter exclusivo de la guerra cibernética requerirá restricciones en la guerra cibernética de prioridad. Si EE.UU. puede determinar qué satélites, activos o inactivos, pueden usarse para colisiones de diseñador debido a debilidades de comunicación y navegación, puede asegurar la

eliminación o retirada segura de estas vulnerabilidades. Al usar defensas activas, EE.UU. aumenta la probabilidad de detección de países extranjeros tratando de enviar ataques de satélites.

La mejor forma de poder determinar si la amenaza es real y si se pueden secuestrar haberes espaciales extranjeros es salir y hacerlo nosotros mismos–aunque sea solamente para determinar posibilidades. La seguridad no se crea esperando a que sus adversarios ejecuten sus opciones y se basan en una respuesta reactiva a un incidente; en vez de seguridad, se requiere mitigar el riesgo y determinar las vulnerabilidades. La única forma de establecer conocimientos sobre vulnerabilidades extranjeras es tantear digitalmente las defensas de los haberes. Adoptar una postura de defensa activa aumenta la oportunidad de atribuir y rastrear ciberataques que aumenta la incertidumbre entre los adversarios potenciales.

Conclusión

El ataque a satélites de EE.UU. puede ser una prioridad principal para cualquier adversario potencial o encubierto y la ventaja geopolítica de ataques encubiertos satisfactorios a haberes espaciales de EE.UU. es alta. Al mismo tiempo, el costo de entrada en la guerra cibernética es bajo, lo que permite a las naciones que no puedan retar la presencia regional de EE.UU. por medios convencionales adaptarse y llevar a cabo ciberataques sin atribuir contra haberes espaciales para degradar la capacidad combate de EE.UU.

Los haberes espaciales son críticos de la forma en que combate hoy EE.UU. y en un futuro previsible es probable que EE.UU. dependa aún más del uso de haberes espaciales para mantener y defender la superioridad de la información. Aun cuando los satélites no han sido atacados ni manipulados ni destruidos por adversarios, no verifican su intención de no hacerlo.

Los ciberataques son tradicionalmente un ataque de una vez porque explotan una vulnerabilidad que puede eliminarse después o corregirse por una tecnología más reciente. La realidad es que, con 3.000 satélites, activos e inactivos, en órbita es probable que los satélites ya estén condicionados para ser secuestrados si es necesario. Un satélite vulnerable que esté en órbita durante los diez años siguientes es una oportunidad que cualquier adversario aprovecharía. Un ciberataque ofrece la opción de dañar satélites de EE.UU. de forma encubierta para un adversario que no esté ya en guerra con EE.UU.

La mejor solución es una defensa activa: recopilar información y tantear las vulnerabilidades de EE.UU. y satélites extranjeros, construir nuevos satélites de EE.UU. para reemplazar los haberes espaciales envejecidos, mantener un espectro de radio militar máximo para asegurar comunicaciones seguras, y aumentar el número de satélites para asegurar la resistencia en un entorno degradado. La renovación y expansión de los haberes espaciales de EE.UU. son críticas para la seguridad nacional en las décadas siguientes. ❑

Notas

1. Renaker, John. Dr. Strangelove and the Hideous Epoch (El Dr. Strangelove y la época horrible). Claremont: Regina Books, 2000.
2. Moltz, James Clay. The Politics of Space Security (La política de la seguridad en el espacio). 2ª edición. Stanford, CA: Stanford University Press, 2011.
3. Alberts, David S., John J. Garstka, Richard E. Hayes y David T. Signori. Understanding Information Age Warfare (Cómo entender la guerra de la era informática). Washington, DC: Command and Control Research Program Publication Series, 2001.
4. Finch, James P. y Shawn Steele. Finding Space in Deterrence Toward a General Framework for Space Deterrence (Cómo encontrar el espacio en la disuasión hacia una estructura general para la disuasión espacial). Strategic Studies Quarterly, Invierno 2011.
5. The Baltimore Sun. Soviet arms could destroy U.S. satellites, Brown says (Las armas soviéticas pueden destruir los satélites de EE.UU., dice Brown), 5 de octubre de 1977.
6. Chicago Tribune. Russian laser 'blinds' U. S. 'spy satellite' (El láser ruso ciega un satélite espía de EE.UU.). 22 de noviembre de 1976.
7. William J. Lynn, III, A Military Strategy for the New Space Environment (Estrategia militar para el nuevo entorno espacial), The Washington Quarterly, 34:3 pág. 7-16.

8. Departamento de Defensa. National Security Space Strategy (Estrategia Espacial de Seguridad Nacional). Resumen sin clasificar. Enero de 2011. http://www.defense.gov/home/features/2011/0111_nsss/docs/NationalSecuritySpaceStrategyUnclassifiedSummary_Jan2011.pdf.

9. Ibid.

10. Stefan A. Kaiser. Viewpoint: Chinese Anti-Satellite Weapons: New Power Geometry and New Legal Policy (Punto de vista: armas antisatelitales chinas: una nueva geometría del poder y una nueva política legal). Astropolitics Tomo 6, Ejemplar 3, 2008.

11. Brearley, Andrew. Faster than a Speeding Bullet: Orbital Debris (Más rápido que una bala veloz: residuos orbitales). Astropolitics Tomo. 3, Ejemplar 1, 2005.

12. NASA. Orbital Debris Quarterly News. Tomo 15, Ejemplar 4. Octubre de 2011.

13. J.-C. Liou y N.L. Johnson, Risks in Space from Orbiting Debris (Riesgos en el espacio de los residuos orbitales), Science, Tomo 311, pág. 340-341, 20 de enero de 2006.

14. Kessler, D.J. Sources of Orbital Debris and the Projected Environment for Future (Fuentes de residuos orbitales y el entorno proyectado para el futuro). Spacecraft (Naves espaciales), Reunión internacional y exposición tecnológica de AIAA, AIAA-80-0855 (1980).

15. Johnson, N.L., The Historical Effectiveness of Space Debris Mitigation Measures (La eficacia histórica de medidas de mitigación de residuos espaciales), International Space Review, Ejemplar 11, pág. 6-9, Diciembre de 2005.

16. American Ordinance. Folleto de ventas KEW / KEWA1 / KEWA2. http://www.aollc.biz/pdf/120mmTankKEW.pdf

17. Donald J. Kessler y Burton G. Cour-Palais. Collision Frequency of Artificial Satellites: The Creation of a Debris Belt (Frecuencia de colisión de satélites artificiales: la creación de un anillo de residuos). Journal of Geophysical Research (1978) 83: 63.

18. Donald J. Kessler, Nicholas L. Johnson, J.-C. Liou y Mark Matney. The Kessler Syndrome: Implications to Future Space operations (El síndrome de Kessler: implicaciones para futuras operaciones espaciales). 33 CONGRESO ANUAL DE GUÍA Y CONTROL DE AAS. 6 - 10 de febrero de 2010. Breckenridge, Colorado.

19. Oficina de las Naciones Unidas para los asuntos del espacio exterior. Space Debris Mitigation Guidelines of the Committee on the peaceful uses of outer Space (Guías de mitigación de residuos espaciales del comité para los usos pacíficos del espacio exterior). http://orbitaldebris.jsc.nasa.gov/library/Space%20Debris%20Mitigation%20Guidelines_COPUOS.pdf.

20. U.N. New Service. Russia and China veto draft Security Council resolution on Syria (Rusia y China vetan el borrador de la resolución del Consejo de Seguridad sobre Siria). 2011. http://www.un.org/apps/news/story.asp?NewsID=39935&Cr=syria&Cr1=.

21. Wired. Hackers Targeted U.S. Government Satellites (Los atacantes fijaron como objetivos satélites del gobierno de EE.UU.). http://www.wired.com/threatlevel/2011/10/hackers-attack-satellites/.

22. P.H. Krisko, N.L. Johnson, J.N. Opiela. EVOLVE 4.0 orbital debris mitigation studies (Estudios de mitigación de residuos orbitales EVOLVE 4.0). Advances in Space Research (Avances en la investigación especial) Tomo 28, Ejemplar 9, 2001, páginas 1385-1390.

23. Johnson, Nicholas L. The Disposal of Spacecraft and Launch Vehicle Stages in Low Earth Orbit (La eliminación de las naves espaciales y fases de lanzamiento de vehículo a la órbita terrestre baja). NASA, 2007, http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20070021588_2007019149.pdf.

24. National Research Council. Committee for the Assessment of NASA's Orbital Debris Programs (Comité para la evaluación de los programas de residuos orbitales de la NASA). Limiting Future Collision Risk to Spacecraft: An Assessment of NASA's Meteoroid and Orbital Debris Programs (Limitación del riesgo de colisión futuro con la nave especial: evaluación de los programas de residuos meteóricos y orbitales de la NSA). Washington D.C.: National Academies Press, 2011.

25. Office of the Under Secretary for Defense, National defense budget estimates for FY 2012 (Estimaciones del presupuesto de defensa nacional para el año fiscal de 2012), http://comptroller.defense.gov/defbudget/fy2012/FY12_Green_Book.pdf (se accedió a la misma el 7 de noviembre de 2011).

26. El Presidente de Estados Unidos. National Space Policy. 2010. http://www.whitehouse.gov/sites/default/files/national_space_policy_6-28-10.pdf.

El Dr. Jan Kallberg, PhD es un abogado, científico político y escritor de opinión estadounidense de origen sueco. Recibió su doctorado en asuntos públicos y MA en ciencias políticas de la Universidad de Texas en Dallas y tiene un título de derecho de la Universidad de Estocolmo. Sus intereses de investigación incluyen asuntos de seguridad nacional como la disuasión estratégica y el campo de batalla de la Internet.