Blandir nuestras espadas aérea, espacial y ciberespacial

Recomendaciones para la disuasión y más

Teniente Coronel Mark Reith, Fuerza Aérea de EE.UU.*

Cortesía de Stacy Burns

Estados Unidos ha llegado a un hito histórico para el espacio y el ciberespacio. Durante décadas, el espacio y el ciberespacio se han considerado como un territorio neutral o parte de un espacio común global, pero el aumento de competidores y la conversión de la tecnología en productos básicos dentro de estos dominios han cambiado drásticamente el cálculo de la disuasión estratégica. Un camino lleva a Estados Unidos a inversiones masivas e intensivas con respecto al tiempo en sistemas de protección reforzada y resistentes sin garantía de que la siguiente generación de tecnología vaya a ser más resistente a los ingeniosos atacantes que la última. Otro camino lleva a Estados Unidos a capacidades ofensivas de dominios múltiples para crear múltiples dilemas que abrumen y pongan en riesgo al adversario, pero la eficacia de este método en una gama de actores es desconocida. No obstante, más allá del horizonte técnico, nos enfrentamos a las implicaciones de ciencia ficción en movimiento a medida que nuevas tecnologías como inteligencia artificial, robótica y laser armados se desarrollan y

*Gracias especiales al Coronel Brad Pyburn, Coronel David Snoddy, Coronel Heather Blackwell, Teniente Coronel Eric Trias, Teniente Coronel Joy Kaczor y Capitán Carlos Rodriguez por sus esclarecedoras contribuciones.

despliegan contra un fondo perturbador de eventos mundiales.[1] Considere el conflicto ciberespacial entre Rusia y Ucrania que está teniendo lugar en la estructura de la sociedad, incluidos servicios públicos, medios de comunicación de masas y finanzas, y todo ello mientras la comunidad internacional no establece líneas rojas de intervención como desbordamiento de malware más allá de las fronteras del conflicto.[2]

La disuasión estratégica en el siglo XXI es mucho mayor que lo que era la disuasión nuclear en el siglo XX. Las FF.AA. de EE.UU. todavía se están "poniendo al día" acerca de esta nueva realidad de disuasión y están debatiendo intensamente lo que significa la disuasión en el entorno de amenazas global actual.

General John Hyten, USAF
Comandante, Mando Estratégico de EE.UU.

Se puede producir un conflicto en cualquier punto del espectro, con varios grados de intensidad, con más de un adversario y en múltiples dominios. En todas las fases . . . nuestra planificación y nuestras operaciones están diseñadas para disuadir y crear "rampas de salida" a fin de desescalar el conflicto. . . mientras disuadimos a nuestros adversarios de que consideren el uso de ataques ciberespaciales, actividades contraespaciales o armas nucleares.

Almirante Cecil D. Haney, USN
Ex-comandante, Mando Estratégico de EE.UU.

Además, piense en la estrategia de compensación de Corea del Norte de poner fuerzas estadounidenses convencionales en riesgo con armas nucleares mientras emplean herramientas asimétricas con la intención y determinación claras de cuestionar la hegemonía de EE.UU.[3] A medida que tratamos de entender este entorno dinámico, nos encontramos al borde de la siguiente revolución en asuntos militares, y nuestras siguientes inversiones influirán en gran medida en nuestras futuras opciones.

Este artículo examina cómo la nación podría prepararse mejor para disuadir una acción agresiva en el espacio y ciberespacio, y si es necesario, prevalecer en caso de que fracase la disuasión. Entre los temas clave de este artículo se incluye una gran necesidad de concienciación situacional en el espacio y el ciberespacio, la necesidad de un marco internacional de atribución y escalada, y una inversión nacional en educación espacial y ciberespacial, junto con una estrategia nacional y una doctrina militar actualizadas. Aunque está relacionado con la disuasión, este artículo se concentra en la disuasión y omite el tema de la coacción ciberespacial.

Suposiciones problemáticas en la estructura de disuasión estratégica

La disuasión impide la acción del adversario mediante la presentación de una amenaza creíble de una acción contraria. Tanto en la paz como en la guerra, las Fuerzas Armadas de EE.UU. ayudan a disuadir a adversario de que usan violencia para conseguir sus objetivos. La disuasión se deriva de la creencia de un adversario de que existe una amenaza creíble de represalia, que la acción contemplada no puede tener éxito o que los costos superan las ventajas percibidas de la acción. Así pues, un agresor potencial decide no actuar por miedo al fracaso, al costo o a las consecuencias.

—Publicación Conjunta 3-0, *Operaciones conjuntas*

El concepto de disuasión tiene una larga historia en la guerra y la doctrina militar refleja un entendimiento profundo de sus elementos más destacados. En la descripción de disuasión de la Publicación Conjunta, el elemento más importante es la creencia del adversario en una represalia, un fracaso o unos costos inaceptables. La descripción hace varias suposiciones que son problemáticas cuando se considera el espacio y el ciberespacio. La primera suposición afirma que Estados Unidos puede atribuir un comportamiento a un adversario de forma rápida y fiable. La segunda suposición es que el adversario puede observar el éxito o el fracaso de sus acciones, por no hablar de las acciones de los demás. Por último, la tercera suposición indica que los costos y las ventajas pueden medirse y justificare. Retar estas suposiciones pueden poner al descubierto oportunidades para explotar situaciones.

Para que la disuasión sea efectiva, se tienen que cumplir varias condiciones:

1. La amenaza debe comunicarse de forma precisa al objetivo.
2. El objetivo debe entender claramente la amenaza.
3. El objetivo debe creer que el costo anticipado de emprender la acción supera las ventajas potenciales.
4. El objetivo debe creer que el "disuasor" efectuará las acciones amenazadas.

—Anexo de Doctrina de la USAF 3-0
Operaciones y planificación

La Fuerza Aérea de EE.UU. profundiza en las condiciones de la disuasión como parte de la doctrina de la USAF. Aquí también observamos suposiciones que son problemáticas en la edad moderna. Primero, las actividades ciberespaciales y espaciales se encuentran ocultas a menudo debido a su naturaleza muy secreta y después de que hayan ocurrido, y a menudo de forma anónima. A diferencia de las pruebas y operaciones nucleares que generalmente son observables por todos los adversarios, las actividades ciberespaciales y espaciales pueden ser detectables o no por parte del objetivo, y normalmente no por parte de terceros. Segundo, la descripción supone que todos los adversarios están prestando atención y entienden la amenaza. Dentro de los dominios espacial y ciberespacial, esto puede requerir herramientas especializadas que detecten perturbaciones en estos dominios, y lo que es más importante, que interpreten correctamente su situación. Por último, la descripción supone que ya se ha logrado el trabajo de preparación que apoya las acciones de amenaza. Por ejemplo, Estados Unidos tiene estrechas relaciones con la comunidad internacional y por lo general se ajusta a un marco ético y legal para mantener la legitimidad de su función de liderazgo en todo el mundo. Un adversario, al sospechar que no existe un marco legal para la represalia en el espacio común global, tal vez no crea que Estados Unidos esté dispuesto a aceptar acciones amenazadoras. Además, es posible que el mismo adversario no crea que Estados Unidos ha puesto a su disposición de antemano armas espaciales y ciberespaciales para represalias. En cualquier caso, la base de las acciones de represalia debe tratarse antes de que la disuasión pueda dar resultado según la doctrina actual.

Retos para disuadir los ciberataques

Resumen de los retos de la disuasión ciberespacial

- Dificultad de atribuir los ciberataques a sus perpetradores
- Facilidad de adquirir armas ciberespaciales y llevar a cabo ciberataques
- Amplia variedad de actores estatales y no estatales que participan en ciberataques por una multitud de razones y contra objetivos estatales y no estatales
- Corta duración de almacenamiento de muchas armas ciberespaciales

- Dificultad de establecer umbrales y líneas rojas de agresión cibernética
- Dificultad de fijar y hacer cumplir normas internacionales en lo que se refiere al comportamiento ciberespacial
- Retos relacionados con evitar la escalada

—Dorothy E. Denning
Profesora Emérita Distinguida
Escuela de Posgraduados de la Armada

Algunos expertos académicos han identificado una serie de retos asociados con la disuasión ciberespacial.[4] La investigadora de seguridad de información Dorothy E. Denning resume muchos de estos retos y compara, como ya lo han hecho muchos, la naturaleza de la disuasión ciberespacial con la disuasión nuclear. Entre las diferencias clave se podrían incluir el grado de dificultad para adquirir armas, la duración de almacenamiento de estas armas, y las motivaciones y la atribución de disparar estas armas por nombrar unas cuantas. Se podría inferir de la comunidad de investigadores que, en vez de comparar la disuasión ciberespacial con la disuasión nuclear, los estrategas y los encargados de formular políticas necesitan reflexionar sobre el marco estratégico de la disuasión y conformar el espacio o el ciberespacio para permitir el modelo de disuasión tradicional para trabajar, o reajustar las expectativas sobre la efectividad de la disuasión en estos dominios. La sección siguiente proporciona algunos puntos de vista sobre cómo lograr ambas.

Aplicación del marco de disuasión al ciberespacio

La disuasión es sobre todo capacidad e intención, y en el ciberespacio, hemos mostrado un poco de ambas públicamente. Pienso en las "pruebas" nucleares que llevamos a cabo en los 50 y 60 para demostrar no solo capacidad, sino también determinación. . . debemos mostrar el amplio espectro de capacidades que podemos aplicar a nuestro potente "motor" de ciberespacio ofensivo. Mostramos "maneras" de cómo el ciberespacio puede impactar en sistemas cinéticos, esto también ayuda a los encargados de tomar decisiones a ordenar debidamente por prioridades seguridad/higiene/defensa ciberespaciales mediante estrategias de inversión apropiadas informadas sobre el riesgo.

—Coronel Brad Pyburn, USAF
Comandante, 67ª Escuadra Ciberespacial

Como tratamos anteriormente, aplicar el marco disuasorio al ciberdominio puede ser difícil y complicado. Este artículo amplía la recomendación de Geist de una "estrategia de tecnología" para implementar un marco de disuasión ciberespacial.[5] Geist describe tres componentes de su estrategia: negación, resistencia y capacidades ofensivas. El artículo examina cada componente, lo representa en un mapa en la doctrina de Operaciones Conjuntas del Departamento de Defensa, describe las carencias y hace recomendaciones para formar un marco disuasorio robusto.

Disuasión por negación (miedo a fracasar)

El primer componente, y generalmente considerado el más efectivo, es la disuasión por negación. Este tipo de disuasión se caracteriza por hacer inefectivas las armas ciberespaciales de modo que un adversario se desanime incluso para tratar de efectuar un ataque. De Operaciones Conjuntas del Departamento de Defensa, esto aprovecha el miedo a fracasar y abre la posibilidad de una atribución potencial. El ejemplo clásico comprende un método de parcheo fuerte de una

vulnerabilidad que convierte en inertes las armas de explotación. La negación da resultado porque los exploits tienden a ser frágiles, ya que es necesario satisfacer algunas condiciones técnicas y situacionales antes de que un exploit sea efectivo. El hecho de que existan algunas condiciones es muy esperanzador como forma de disuasión porque el defensor puede influir a menudo en muchas de estas condiciones. El problema típico incluye un juego de números: multiplique el número de vulnerabilidades potenciales (orden de miles) por el número de sistemas de empresas (orden de cientos de miles) y el número de intentos de explotación (es decir, la Fuerza Aérea bloqueó 1.300 millones de intentos de conexión en 2016) y se obtiene un límite superior de los posibles exploits en un intervalo dado.[6] Se da por sentado que la exposición al riesgo real depende de las relaciones entre sistemas, las vulnerabilidades y los intentos de explotación, pero el tema clave comprende una escala de problema que es difícil de manejar. Otro problema típico incluye algunos sistemas heredados de programadores que nunca se imaginaron que estos sistemas iban a exponerse a intentos de explotación. La infraestructura de los servicios públicos, los vehículos y los sistemas integrados son buenos ejemplos de dicha exposición.

Estados Unidos puede mejorar su disuasión mediante una estrategia de negación de varias formas. Primero, la solución más evidente consiste en implementar las mejores prácticas de ciberseguridad como defensa en profundidad, parcheo, gestión de configuraciones, autenticación fuerte, inspección detallada del tráfico de comunicaciones, y así sucesivamente. La investigación china en criptografía cuántica mediante el uso de satélites es un gran ejemplo de inversión estratégica en su disuasión de negación.[7] Segundo, la educación y el adiestramiento de la fuerza laboral son primordiales, junto con ejercicios, simulacros y responsabilidad por el comportamiento en línea. Tercero, Estados Unidos necesita cambiar las expectativas en lo que respecta a la tecnología. Específicamente, los estrategas y encargados de formular políticas deben dejar de considerar la tecnología de información como un servicio público, y en vez de eso esperar un entorno disputado perpetuamente. Al hacer esto, pueden segmentar las fuerzas en grupos con una exposición muy limitada a las amenazas cibernéticas, aceptando el potencial de una capacidad reducida para el corto período en el que se disputa el terreno ciberespacial.

Disuasión por resistencia (Costo)

El segundo componente es disuasión por resistencia. Este tipo de disuasión se caracteriza por esfuerzos cada vez más costosos de modo que un adversario se desanime a atacar, aunque no se prevenga el ataque necesariamente. De Operaciones conjuntas del Departamento de Defensa, esto aprovecha un recurso de múltiples maneras. Primero, esta estrategia puede consumir las herramientas de explotación del adversario y oportunidades de cero días. Los propietarios del exploit no pueden garantizar una posesión única, y con el tiempo dicha herramienta y dichas oportunidades a menudo se hacen obsoletas. Una vez que se entienda un exploit, y se despliegue un parche, la herramienta puede tener un valor reducido. Esto es particularmente un problema si resultó costoso desarrollar o adquirir la herramienta de explotación. La pérdida de anonimidad es un costo relacionado porque a medida que se usa repetidamente una herramienta o técnica de explotación, el defensor puede figurarse suficiente información para una atribución razonable. Segundo, a medida que aumenta la capacidad del defensor, es posible que el adversario pueda requerir una fuerza mayor para encontrar y explotar vulnerabilidades *que cumplan sus objetivos específicos.* Considere cómo las redundancias pueden disminuir el efecto de los ataques de negación de servicio mientras se aumentan los recursos requeridos del adversario. Tercero, con el tiempo, las redes previamente entendidas pueden cambiar, reduciendo el valor de la información de reconocimiento e instando a su modificación. Por último, incluso después de un *exploit*

con éxito, los defensores activos podrían detectar y expulsar a un adversario, provocando así el costo de encontrar otra manera de entrar en el sistema.

Estados Unidos puede mejorar su disuasión mediante una estrategia de resistencia de varias formas. Primero, el método más directo comprende la inversión en capacidades de defensa activas. Los recursos humanos y la investigación de capacidades de detección e investigación automatizadas ayudan a encontrar, fijar, rastrear, participar y evaluar adversarios en redes de EE.UU. disputadas. Las inversiones en tecnología de mapas de misiones ayudan a los defensores a identificar terrenos ciberespaciales clave y luchar contra la actividad del adversario para asegurar las misiones.[8] Segundo, aproveche la ventaja natural del juego en casa. Como el ciberespacio es maleable y mutable, tiene sentido la conformación del entorno para dar ventaja a los defensores. Despliegue redes definidas por software para cambiar de forma impredecible el entorno e inutilizar un reconocimiento previo del adversario. Domine la fuerza laboral definiendo unas condiciones cibernéticas significativas basándose en el conjunto de misiones en vez de en geografía, y ejerza dichas condiciones de forma rutinaria. Tercero, aproveche la complejidad natural inherente del ciberespacio. Despliegue miles de sistemas de señuelo, y deje que los adversarios den vueltas por el laberinto de espejos mientras los defensores observan y aprenden de sus tácticas. Despliegue sistemas de archivos distribuidos que almacenan fragmentos de archivos en miles de sistemas. Los propietarios podrán encontrarse y reagruparse, mientras que los adversarios se frustrarán y cometerán errores, desembocando al final en una atribución. La implantación de malware en estos señuelos y sistemas de archivos puede aumentar al final de forma considerable el costo del adversario. Además, al revelar la evidencia de un ciberataque a la comunidad internacional, particularmente en el contexto de tratados en vigor, también podría aumentar el costo de un adversario.

Disuasión por castigo (consecuencias)

Finalmente, el tercer componente es disuasión por castigo. Este tipo de disuasión se caracteriza por atacar, o amenazar con atacar, al adversario directamente de modo que se les intimide mucho como para responder. De Operaciones conjuntas del Departamento de Defensa, esto explota un miedo a las consecuencias, pero requiere que una atribución fuerte para ser efectiva. La disuasión por castigo puede ser un tema complejo por varias razones descritas previamente por Denning. Entre ellas es crítica la cuestión de si la disuasión ciberespacial se limita a tipos ciberespaciales de castigo, o ¿se dispone de otros instrumentos de poder? Cuestiones de líneas rojas, escalada, proporcionalidad y capacidad de sobrevivencia son pertinentes a este debate y deben enmarcarse antes de considerar esta dimensión de disuasión.

Estados Unidos podría trabajar hacia una estrategia de disuasión por castigo de varias maneras. Primero, se debería establecer un marco legal internacional y nacional en al menos dos áreas. Un área comprende guías para asociar los castigos ciberespaciales con las violaciones ciberespaciales. La otra área consiste en integrar y relacionar acciones del dominio estratégico (espacio y ciberespacio) con acciones del dominio tradicional (aire, tierra y mar).[9] Aquí Manzo sugiere establecer clases equivalentes acordadas por la comunidad internacional que podrían usarse para interpretar el significado de las acciones en todos los dominios, y podrían evitar una escalada no intencionada. Normalmente, esto ocurre por tradición y costumbre, pero el conflicto en el espacio y el ciberespacio se sigue normalizando. Por ejemplo, si Estados Unidos decide aprovechar su nueva tecnología láser naval como arma espacial potencial, debe establecer un marco que establezca claramente líneas rojas y criterios de empleo.[10] Segundo, Estados Unidos podría promover una carrera de armas ciberespaciales con una demostración completa de herramientas de explotación y una base industrial suficientemente grande para crear nuevas herramientas de explotación con el tiempo. Observe que la disuasión no es cualquier herramienta de explotación particular, sino la base industrial que la forma. Aunque esto puede llevar

a una carrera de armas espaciales y ciberespaciales, el contraargumento podría ser que esto es una eventualidad, y Estados Unidos podría tomar también la iniciativa. La clave para desarrollar una capacidad viable de armas ciberespaciales de tipo construir y descartar incluye reformas significativas o nuevas autoridades en los reglamentos de adquisición federales. Tercero, Estados Unidos podría tomar la iniciativa para colocar de antemano malware en la infraestructura crítica de sus adversarios como medio de poner en riesgo un terreno cibernético. Aunque la evidencia demostrable de que dichas capacidades colocadas de antemano podrían sacrificar el haber, plantar dudas sobre la fiabilidad de sus sistemas puede producir beneficios durante años. Si Estados Unidos resaltara esta exposición a otros adversarios potenciales, el impacto podría tener consecuencia en actores patrocinados por el estado. Habría que tener cuidado para distinguir el malware destinado a crear efectos ciberespaciales en función del malware para facilitar la recopilación de inteligencia.

Cuarto, Estados Unidos podría enmarañar sistemas gubernamentales y militares con sistemas civiles globales para cambiar el cálculo de la disuasión. Este método supone que un ataque al gobierno de EE.UU. sería suficientemente atroz para la población civil y la economía mundial como para obtener apoyo político para opciones del espectro completo. El Sistema de Posicionamiento Global (GPS) comparte esta característica en la medida en que un ataque a este para degradar las operaciones militares también impactaría en las poblaciones civiles de todo el mundo y ayudaría a justificar contramedidas cinéticas.

Disuasión en una serie de actores

Las inversiones en estrategias de disuasión deben tener en cuenta ataques potenciales en una serie de actores adversarios. Mientras que una nación estado podría ser más receptiva a la disuasión por castigo, los actores no estatales podrían poner en riesgo poco y por lo tanto la disuasión por negación o resistencia podría ser más apropiada. Históricamente, las FF.AA. de EE.UU. ha hecho un esfuerzo más desproporcionado hacia la estrategia de negación, con algunos esfuerzos crecientes hacia la resistencia, porque requiere poca coordinación externa. No obstante, los estados nacionales no son disuadidos por estos esfuerzos internos porque, dentro de su cálculo estratégico, la ventaja potencial históricamente ha excedido con mucho el riesgo de atribución y acción de EE.UU. La clave para la disuasión por castigo es poner en riesgo algo que el adversario valore. Para los estados nacionales, tal vez esto se alinee con la teoría de los centros de gravedad del Coronel John A. Warden.[11] Para los actores no estatales, el impacto de las ciberoperaciones ofensivas sigue sin estar claro.[12] La teoría actual sugiere concentrarse en individuos de liderazgo clave y sus objetivos inmediatos.[13]

Recomendaciones

Aumente la concienciación situacional espacial y ciberespacial global

> *Creo que todas las guerras actuales requieren interdependencias, coaliciones y socios. Pero en el ciberespacio, creo que hay un requisito más profundo para tener asociaciones en formas que son diferentes de otros dominios de combate militares.*
>
> —Teniente General J. Kevin McLaughlin, USAF
> Subcomandantes, Mando Ciberespacial de EE.UU.

Entre las muchas preocupaciones referentes a la disuasión espacial y ciberespacial, deben considerarse la atribución y la transparencia si se desea una disuasión significativa. Cada factor debe incluir al menos dos componentes. Primero, el adversario necesita saber que han sido sorprendidos con las manos en la masa y por ello están sujetos a la justicia. Segundo, los adversarios potenciales necesitan observar que los actores maliciosos sean responsables de sus acciones para disuadir más un comportamiento no deseado. En una edad de cifrado y burlas, hacer responsables a los ofensores puede parecer un problema infranqueable, pero uno solo tiene que recordar meramente lo que es el ciberespacio, por definición, un entorno artificial y por lo tanto maleable y mutable.[14] En vez de pasar por defecto a un entorno que permite el paso de forma oculta de tráfico cifrado de un lado a otro a través de sistemas que son propiedad de estados nacionales, requiera que el tráfico sea inspeccionable según las leyes del gobierno central.[15] Esto no quiere decir que se vaya a inspeccionar todo el tráfico, solamente que los gobiernos retienen el derecho de inspeccionar cualquier bien o servicio (en este caso, información) que atraviese sus fronteras, incluso el tráfico temporal. Aunque es posible que algunos países no adopten este modelo, tampoco está el destinatario de dicho tráfico obligado a aceptarlo, ni tampoco el modelo impide el tráfico público. No obstante, este modelo proporciona a los gobiernos colaboradores un medio de detectar y rastrear comportamientos malos, y lo que es más importante, recopilar evidencia para una inspección más estrecha por parte de la comunidad internacional. Además, los gobiernos colaboradores pueden ayudarse entre sí para facilitar ciberataques de una forma similar al permiso de trayectorias de vuelo por un espacio aéreo amigo, creando un marco más natural para la coalición frente a la participación unilateral. Con la evidencia en la mano, se hacen plausibles todos los instrumentos de poder nacional en todos los dominios.

Establecer un marco nacional e internacional

> *Una cosa que los ejercicios han resaltado es la dificultad, a veces, de determinar la respuesta apropiada debido a la falta de reglas de enfrentamiento en el espacio. Si vamos a actuar de forma decisiva en tiempo real, tenemos que tratar estos asuntos de forma legal y operacional.*
>
> —Vicealmirante Charles A. Richard, USN
> Subcomandante, Mando Estratégico de EE.UU.

La necesidad de un marco nacional e internacional, estrechamente relacionada con las inversiones mencionadas antes en la concienciación situacional espacial y ciberespacial global con el fin de gestionar el comportamiento en el espacio común global, es suprema. Entre estas necesidades es clave un requisito para que los gobiernos sean responsables de las actividades espaciales y ciberespaciales que estén sancionadas por su jurisdicción o se originen en ella. Aunque puede parecer ridículo a simple vista promulgar una ley que sea difícil de hacer cumplir, el verdadero objetivo es forzar una decisión en los actores estatales. Hay dos posibilidades, que el originador reconozca que es un combatiente espacial/ciberespacial y que se atenga a las repercusiones, o puede adoptar el papel de víctima o espectador. En los últimos casos, esto permite una oportunidad a las partes dañadas de conformar el resultado requiriendo leyes adicionales, educación de ciberseguridad, limitaciones del tráfico de salida, o en casos extremos aislamiento de redes. La premisa detrás de esta estrategia compara una expectativa de que los estados que permitan el uso de tecnología deben demostrar primero la capacidad de gobernarla debido al potencial de impacto global.

Considere la idea de consolidar la gestión del ciberespacio y asignar a Estados Unidos la administración internacional para el beneficio de la humanidad. Aunque esto parezca increíble al principio, piense en la forma en que Estados Unidos ya juega un papel similar para el espacio

(GPS) y las divisas del mundo (el dólar de EE.UU. es la divisa de reserva del mundo). Estados Unidos ya influye mucho en la infraestructura (es decir, servicios de nombres de dominios) mediante investigación y desarrollo, y compañías de EE.UU. (Google, Intel, Microsoft, y así sucesivamente) están directamente involucradas en elaborar ciberespacio, por lo que quizás el gobierno de EE.UU. podría asumir una función más importante en el empleo de dichas tecnologías. Tal vez parte de esta función podría incluir el registro de dispositivos y personas que tengan permiso para usar internet, estableciendo así un equilibrio entre privacidad y seguridad.

Desarrolle estratégicamente los operadores militares espaciales/ciberespaciales y las milicias ciudadanas

> *Los aerotécnicos ciberespaciales pueden asistir a oportunidades de desarrollo profesional como el Instituto de Tecnología de la Fuerza Aérea, Programa de Desarrollo de Operaciones de Redes Informáticas, o la Escuela de Armas de la Fuerza Aérea, todas las cuales tendrán un impacto positivo en la operacionalización del dominio ciberespacial dentro de la Fuerza Aérea y a su vez, en el futuro de las fuerzas de las misiones ciberespaciales.*General de División Chris P. Weggeman, USAF Comandante, 24ª Fuerza Aérea y Fuerzas Ciberespaciales

Una de las fortalezas clave de Estados Unidos y muchas democracias occidentales es la libertad de innovación e industria. Las inversiones en programas como Cyber Patriot (Patriota ciberespacial) National Collegiate Cyber Defense (Defensa Ciberespacial Universitaria Nacional) y Advanced Cyber Education (Educación Ciberespacial Avanzada) producen generaciones de ciudadanos con agudeza ciberespacial (mostrado en la fig. 1).[16]

Cortesía Stacy Burns

Hannah Kirst (Universidad Texas A&M), David Home (Universidad de Colorado), Matthew Holt (Universidad de Lock Haven, Anh Bui (Universidad de Carolina el Norte en Charlotte) y Albert Bierley (Universidad de California) están entre los estudiantes que se benefician de la Educación Avanzada Ciberespacial en el Instituto de Tecnología de la Fuerza Aérea en julio de 2017.

Mostrar la inversión y las capacidades resultantes se convierte en una herramienta estratégica para la disuasión, ya que no solo las agencias del gobierno, sino también las corporaciones privadas entienden muy bien la ciberseguridad. No obstante, se necesitan mayores inversiones en ciencia informática, ingeniería y operaciones cibernéticas en K-12 para demostrar un compromiso nacional para nuestra seguridad. Esto es mucho más que la educación formal, pero en vez de ser un intercambio cultural donde los modelos de función ciberespacial, la programación de

televisión infantil y las carreras exitosas conforman las actitudes de su juventud. Al formar una reserva nacional de talento ético, Estados Unidos no solamente mejora la resistencia y el ciberespacio dentro de compañías y productos nacionales, sino que también puede recurrir a esta reserva en tiempos de crisis. Mientras que los regímenes totalitarios podrían limitar el desarrollo de dicho talento por temor al derrocamiento de un régimen, Estados Unidos podría adoptar un pirateo informático ético de una manera similar a los derechos y propiedad universales de armas de fuego, dando así a Estados Unidos una ventaja estratégica. De forma similar, la ubicuidad pronosticada de viajes espaciales mediante compañías como Space X podría crear un efecto de disuasión similar donde ningún ataque a viajeros podría producir una respuesta convencional, particularmente si se tratan la atribución y la transparencia.[17]

Actualice la estrategia de seguridad nacional y la doctrina espacial/ciberespacial conjunta de la Fuerza Aérea

> *Diría que debemos considerar el ciberespacio como un elemento de una campaña de disuasión más amplia.*
>
> —Almirante Mike Rogers, USN
> Comandante, Mando Cibernético de EE.UU.

Como se ha mencionado previamente en la doctrina conjunta y de la Fuerza Aérea, la disuasión requiere amenazas claramente creíbles y comunicadas junto a una intención creíble de ejercer esas amenazas. La doctrina especial actual hace énfasis en un comportamiento responsable, asociaciones que animan la limitación, colaboración hacia una atribución rápida y respuestas apropiadas cuando la disuasión no dé resultado.[18] No obstante, la doctrina ciberespacial actual especifica muy poco una estrategia disuasoria.[19] Uno podría estar tentado a adoptar la misma estrategia disuasoria en el espacio y el ciberespacio, no obstante, esto podría no dar resultado por varias razones. Primero, el paisaje ciberespacial cambia más rápidamente que el espacio. Segundo, Estados Unidos dispone de más opciones y actores de disuasión en el ciberespacio. Sin embargo, dada la naturaleza cada vez más disputada de ambos dominios, Estados Unidos debe ser más explícito sobre realizar acciones dentro de dominios y entre dominios. Además, entre las mejoras de la Estrategia de Seguridad Nacional se podría incluir el espectro completo de instrumentos de poder nacional para hacer posible las recomendaciones de este artículo. Una estrategia y doctrina uniformes será clave para salvaguarda la nación.

Conclusión

> *Es lamentable cuando los hombres no pueden, o no quieren, ver el peligro a distancia; o al verlo, están limitados en los medios que son necesarios para evitarlo, o mantenerlo alejado. . . No es menos difícil hacerlos creer, que las operaciones ofensivas, a menudo, son los medios de defensa más seguros, si es que no son los únicos (en algunos casos).*
>
> —Presidente George Washington
> 25 de junio de 1799

En resumen, Estados Unidos ha alcanzado un hito importante a medida que contempla el futuro de la disuasión especial y ciberespacial. Históricamente la disuasión estratégica ha dado resultado, pero aplicar dichas estructuras a los dominios espacial y ciberespacial sigue siendo un

reto sin mejor atribución, leyes internacionales, inversión en capital humano y estrategias y doctrina nacionales actualizadas. Sin estos cambios, el espacio y el ciberespacio seguirán siendo dominios especializados y matizados, susceptibles a ataque y explotación, y en el peor de los casos, el talón de Aquiles de nuestra nación. Como líderes a los que se les ha confiado tomar buenas decisiones de inversión, tenemos la habilidad de conformar no solo el espacio y el ciberespacio, sino posiblemente también nuestro destino nacional. ❑

Notas

1. Junta de Ciencia de Defensa, "Task Force on Cyber Deterrence" (Fuerza de tare sobre disuasión ciberespacial), Informe técnico (Washington, DC: Subsecretaría de Defensa para Adquisición, Tecnología y Logística, 1 de febrero de 2017, http://www.dtic.mil/docs/citations/AD1028516.

2. Andy Greenberg, "How an Entire Nation became Russia's Test Lab for Cyber War" (Cómo toda una nación se convirtió en el laboratorio de pruebas de Rusia para la guerra ciberespacial), *Wired*, 20 de junio de 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/.

3. Teniente General in-bum Chun, Ejército de la República de Corea (retirado), "North Korea's Offset Strategy" (Estrategia de compensación de Corea del Norte), en *Breakthrough on the Peninsula: Third Offset Strategies and the Future Defense of Korea (Avance importante en la península: terceras estrategias de compensación y la futura defensa de Corea)*, editado por el Dr. Patrick M. Cronin (Washington, DC: Centro para la Nueva Seguridad de EE.UU., noviembre de 2016), 39–48, https://www.cnas.org/publications/reports/breakthrough-on-the-peninsula.

4. Martin C. Libicki, Edward Geist, Dorothy E. Denning, Stephen J. Cimbala, Frank J. Cilluffo y otros han identificado los retos asociados con la disuasión ciberespacial.

5 . Edward Geist, "Deterrence: Stability in the Cyber Age" (Disuasión: estabilidad en la edad ciberespacial), *Strategic Studies Quarterly* 9, no. 4 (Invierno de 2015), 44–62, http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-09_Issue-4/Geist.pdf.

6. Datos compilados de la Base de Datos de Vulnerabilidad Nacional, https://nvd.nist.gov; y Asociación de Antiguos Alumnos de Asuntos Públicos de la Fuerza Aérea, *Air Force Communication Waypoints 2017*, http://www.afpaaa.org/PDF/Waypoints0817.pdf, 20.

7. ophia Chen, "Chinese Satellite Relays a Quantum Signal between Cities" (Satélite chico envía una señal cuántica entre ciudades), *Wired*, 15 de junio de 2017, https://www.wired.com/story/chinese-satellite-relays-a-quantum-signal-between-cities/.

8. Jeff Guion y Mark Reith, "Dynamic Cyber Mission Mapping" (Mapeo de misiones ciberespaciales dinámicas), Conferencia Anual del Instituto de Ingenieros Industriales y de Sistemas, 2017.

9. incent Manzo, "Deterrence and Escalation in Cross-domain Operations: Where Do Space and Cyberspace Fit?" (Disuasión y escalada en operaciones entre dominios: ¿dónde encajan el espacio y el ciberespacio?), *Strategic Forum* 272, Instituto de la Universidad de Defensa Nacional para Estudios Estratégicos Nacionales, diciembre de 2011, http://ndupress.ndu.edu/Portals/68/Documents/stratforum/SF-272.pdf.

10 Michael Fabey y Kris Osborn, "Navy to Fire 150Kw Ship Laser Weapon" (La Armada va a disparar un arma láser de barco de 150 Kw), *Scout*, 23 de enero 2017, https://scout.com/military/warrior/Article/Navy-to-Fire-150Kw-Ship-Laser-Weapon-From-Destroyers-Carriers-101455353.

11. Mayor Gary M. Jackson, USAF, "Warden's Five-Ring System Theory: Legitimate Wartime Military Targeting or An Increased Potential to Violate the Law and Norms of Expected Behavior?" (Teoría de los cinco anillos de Warden: ¿selección de objetivos militares legítimos en tiempo de guerra o un aumento del potencial para violar la ley y las normas de un comportamiento esperado?), Informe de investigación (Base de la Fuerza Aérea Maxwell, AL: Air University Press, abril de 2000), www.dtic.mil/get-tr-doc/pdf?AD=ADA425331.

12. Jeff Seldin, "Cyber War Versus Islamic State 'Work in Progress'" (Guerra ciberespacial contra la guerra en curso del Estados Islámico), *Voice of America News*, 18 de mayo de 2016, https://www.voanews.com/a/cyber-war-versus-islamic-state-work-in-progress/3336773.html.

13. Declaración del Dr. Craig Fields, presidente, Junta de Ciencia de Defensa y Dr. Jim Miller, antiguo subsecretario de defensa (política) y miembro, Junta de Ciencia de Defensa, testimonio no secreto sobre "Disuasión ciberespacial" ante el Comité de los Servicios Armados del Senado de EE.UU., 115º Congreso (Washington, DC: 2 de marzo 2017), https://www.armed-services.senate.gov/imo/media/doc/Fields-Miller_03-02-17.pdf.

14 . Mark Reith, Seeley Pentecost, Daniel Celebucki y Robert Kaufman, "Operationalizing Cyberspace: Recommendations for Future Research" (Operacionalización del ciberespacio: recomendación para futuras recomendaciones), Conferencia Internacional sobre Guerra y Seguridad Ciberespacial, marzo de 2017, https://search.proquest.com/openview/0c3e05994e4a362d80ad6374fb1b10e9/1?pq-origsite=gscholar&cbl=396500.

15. Esto se logra descifrando y volviendo a cifrar en cada segmento del viaje de tráfico usando tecnología de infraestructura clave. Esto crearía claramente múltiples preocupaciones de privacidad; no obstante, la historia revela que las sociedades están cambiando continuamente las expectativas de la privacidad frente a la necesidad de seguridad, y el

concepto de privacidad ha aumentado en proporción a la tecnología, autosuficiencia y riqueza. Por lo tanto, el concepto de privacidad no es un derecho absoluto, sino un privilegio determinado por la comunidad.

16. El Instituto de tecnología de la Fuerza Aérea organizad la Educación Ciberespacial Avanzada, https://www.afit.edu/ace/news.cfm.

17 . Don Lincoln, "Elon Musk is Changing the Rules of Space Travel" (Elon Musk está cambiando las reglas de viaje por el espacio), *CNN*, 1 de abril 2017, http://www.cnn.com/2017/04/01/opinions/elon-musk-change-rules-of-space-travel-lincoln/index.html.

18. Publicación Conjunta (JP) 3-14, *Operaciones espaciales*, 29 de mayo de 2013, http://www.dtic.mil/doctrine/new_pubs/jp3_14.pdf.

19. JP 3-12, *Operaciones ciberespaciales*, 5 de febrero de 2013, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

Teniente Coronel Mark Reith (PhD, Universidad de Texas en San Antonio) sirvió de antemano como subcomandante del 26º Grupo de Operaciones Ciberespaciales y comandante del 690º Escuadrón de Soporte de Redes, liderando las fuerzas de defensa ciberespacial de empresa y de la Red de Información del Departamento de Defensa respectivamente. Actualmente sirve como director del Centro de Investigación Ciberespacial y profesor asistente de Ciencia Informática de Instituto de Tecnología de la Fuerza Aérea.