Ciberseguridad espacial: la conexión insondable entre dos dominios omnipresentes

Sofía Vega Buono[9]

En la actualidad se da por sentada la tecnología espacial en la vida cotidiana de los ciudadanos del mundo. Los satélites en órbita apoyan las comunicaciones globales, sin mencionar la actividad económica, comercial, gubernamental y militar diaria. La dependencia de la tecnología espacial para la vida en la Tierra genera riesgos profundos que, de no ser abordados correctamente, podrían poner en peligro la vida de millones de personas, pues los activos espaciales son cruciales para el arte de gobernar moderno. Si se tiene en consideración que los satélites almacenan información confidencial de los Estados —imágenes de instalaciones militares sensibles o infraestructura crítica—, no sorprende que el espacio ultraterrestre sea percibido como un objetivo atractivo para los ataques cibernéticos. En este sentido, el espacio no solo es un medio, sino también un fin.

Democratización del espacio

Durante el siglo pasado, el espacio exterior parecía ser un campo exclusivo de las películas de ciencia ficción y de las superpotencias. El advenimiento de un nuevo siglo globalizado y la privatización del espacio ultraterrestre han permitido el ingreso de numerosos y nuevos tipos de actores en él. En rigor, la democratización del acceso al espacio ha profundizado la dependencia de la vida en la Tierra a las herramientas espaciales. Naturalmente, la mayor utilidad, supeditación y actores involucrados en la dinámica espacial se traduce en mayores niveles de vulnerabilidad del ciberespacio y las infraestructuras espaciales frente a agresiones de tipo cibernético.

La ciberseguridad y la seguridad espacial son dos dominios interconectados, y la variedad de amenazas que presenta la unión entre ambos requiere un llamado de atención para la comunidad internacional. Las misiones espaciales exigen estructuras organizativas propias e infraestructuras TIC y centros de control particulares, especialmente en la Tierra, que deben gestionar los riesgos suscitados por la sofisticación y exposición de los datos espaciales recolectados (Al-Rodhan, 2020).

Las amenazas en el nexo entre el espacio ultraterrestre y la seguridad cibernética son diversas, pasando de las de tipo cinético física hasta las electrónicas y cibernéticas. Las amenazas cinéticas físicas comprenden ataques directos contra la infraestructura tangible espacial, ya sea a través de otro satélite o de los sistemas antisatélite (ASAT). Con el auge de la era digital, las amenazas electrónicas y cibernéticas proliferan en el campo de la seguridad espacial. Las amenazas electrónicas pretenden dañar la transmisión de datos (*jamming*), e incluso ejecutar la transmisión de datos falsos (*spoofing*). En este último, los piratas informáticos interceptan los canales de comunicación por aire, inyectan datos falsos y monitorean, sin autorización, las actividades espaciales de otros actores (Al-Rodhan, 2020). Más aún, la inteligencia electrónica (ELINT) satelital es una de las herramientas empleadas por los servicios militares y de seguridad de numerosos países a fin de intervenir la información transmitida por sus adversarios.

Se pueden identificar varios flujos de datos entre la Tierra y los activos espaciales. Primero, la información se envía desde la Tierra a los satélites y otros activos espaciales (interacciones Tierra-espacio). En segundo lugar, la información se envía a la Tierra desde satélites y otros activos espaciales (interacciones espacio-Tierra). Los satélites son susceptibles a las violaciones cibernéticas (Eddy, 2019), ya que algunos de estos enlaces críticos ni siquiera están cifrados. La seguridad de la infraestructura depende de la seguridad de las interacciones Tierra-espacio, y la seguridad de los sistemas de datos espaciales depende de la seguridad de las interacciones espacio-Tierra. Las antenas satelitales y estaciones terrestres o las líneas fijas que conectan estaciones terrestres con redes terrestres y usuarios terminales que se conectan a satélites son los nuevos campos a conquistar. Amén de ello, el eslabón más débil de la ciberseguridad espacial son las personas, pues la ingeniería social funciona como una herramienta para el adversario.

9 Estudiante avanzada de la Licenciatura en Relaciones Internacionales, miembro del Grupo de Jóvenes Investigadores del Instituto de Relaciones Internacionales (Universidad Nacional de La Plata)

La guerra cibernética en el espacio exterior

Según la Doctrina de la Fuerza Aérea de Estados Unidos, las capacidades militares contra-espaciales pretenden evitar que cierto adversario explote el espacio ultraterrestre en ventaja propia, permitiendo que una potencia espacial mantenga un alto grado de superioridad, a través de la neutralización de los activos espaciales (o terrestres vinculados al espacio) de las fuerzas enemigas. Aunque en el pasado han existido acciones contra-espaciales, las condiciones globales actuales despiertan la voluntad de los Estados para desarrollar y utilizar dichas capacidades (Rajalopagan, 2019).

La creciente armamentización y militarización del espacio ultraterrestre podría incrementar la probabilidad de confrontación y, por tanto, el número de ataques cibernéticos. Asimismo, el acceso económico a las tecnologías informáticas y la proliferación de piratas informáticos autónomos o apoyados por Estados aumentan el riesgo de interrupción de las interacciones Tierra-espacio y espacio-Tierra. Los ataques electrónicos y cibernéticos son difícilmente detectables, obstruyendo la atribución de responsabilidades (Rajalopagan, 2019).

La guerra cibernética ya se ha extendido a los dominios del espacio exterior. Por ejemplo, en 2014, la red de la Administración Nacional Oceánica y Atmosférica (NOAA) de Estados Unidos reportó haber sido hackeada por piratas cibernéticos de origen chino. En 2018, funcionarios militares noruegos confirmaron que Rusia había interrumpido el ejercicio *Trident Juncture* de la OTAN, en la región del Alto Norte de Europa, al bloquear sistemáticamente las señales de GPS.

Las operaciones militares dependen de activos espaciales para el suministro de datos que incrementen las capacidades instrumento militar, como su posicionamiento, navegación y cronometraje (PNT), inteligencia, vigilancia y reconocimiento (ISR), defensa antimisiles, comunicaciones, conocimiento de la situación espacial (SSA) y monitoreo ambiental. En efecto, la tecnología satelital recolecta datos sensibles para la seguridad nacional, lo cual la convierte en un blanco atractivo para los atacantes cibernéticos, patrocinados por Estados o por actores no estatales.

En este contexto, varias naciones han desarrollado sistemas ASAT sofisticados, e inclusive se plantean la posibilidad de secuestrar sistemas espaciales enteros. Tal es así que, bajo el nombre de *Hack-a-Sat*, la Fuerza Aérea de Estados Unidos ha convocado un concurso para poner a prueba sus propios sistemas de seguridad en el espacio exterior. En la Defcon de este año, diversos equipos de informáticos e ingenieros competirán por lograr hackear un satélite en órbita, a efectos de comprobar y subsanar sus vulnerabilidades cibernéticas.

¿Cooperación o competencia?

Como los activos espaciales están vinculados a las actividades más sensibles y valiosas de los Estados, impera la lógica de la supervivencia. La reticencia a compartir información, la transparencia selectiva y la falta de mecanismos vinculantes configuran un marco jurídico y operativo internacional deficitario. El Tratado del Espacio Ultraterrestre de 1967 únicamente prohíbe las armas nucleares y las de destrucción masiva en el espacio, mas no existe ninguna limitación respecto a la instalación de armas convencionales en los satélites espaciales, ni la utilización de los mismos para funciones militares. Esto deja el camino llano para aquellos Estados que fomentan el armamento espacial y el espacio exterior como una nueva frontera de conflicto, tensiones y guerra (Vega Buono, 2020). Los sistemas ASAT y la interferencia cibernética de los sistemas espaciales no están explícitamente regulados, mucho menos prohibidos.

Lo cierto es que, si el espacio no es seguro para uno, no será seguro para nadie. Por tanto, la ciberseguridad de los activos espaciales es un desafío colectivo. Los procesos y dinámicas en el espacio ultraterrestre repercuten en las diversas dimensiones del arte de gobernar. La telemedicina demostró ser una herramienta importante para abordar las epidemias y pandemias, como se ha evidenciado durante la crisis sanitaria actual por COVID-19. Las tecnologías espaciales también son fundamentales para la economía, pues proporcionan capacidades de navegación global y servicios de comunicación que fomentan, por ejemplo, la agricultura. Igualmente, son herramientas vitales para rastrear los patrones climáticos en la Tierra, monitoreando el cambio climático y pronosticando la degradación ambiental (Al-Rodhan, 2018).

Ignorar la sinergia entre la seguridad espacial y la seguridad humana pone en peligro la paz internacional y la seguridad de millones de vidas. Al dedicar esfuerzos a la ciberseguridad espacial, los gobiernos estarán invirtiendo en sistemas de salud, económicos, de medio ambiente e innovación más seguros y eficaces, defendiendo no solo la supervivencia del Estado, sino también la calidad de vida de sus ciudadanos.

En espera de un nuevo ethos

La crisis del multilateralismo liberal no es un fenómeno que pasa desapercibido para la seguridad espacial. De cara a una nueva configuración de un sistema de cooperación internacional más realista y justo, poner como prioridad la seguridad espacial y la ciberseguridad de los activos espaciales en la agenda es sustancial. Mientras tanto los gobiernos nacionales con capacidades espaciales deberán tomar medidas para reducir la vulnerabilidad de las interacciones Tierra-espacio y espacio-Tierra, empezando por una evaluación de correcciones de primer nivel. Una posible solución, aunque parcial, es aplicar criptografía —cifrado secreto— a efectos de asegurar la confidencialidad de la información recolectada.

Ciertamente, es imperativo que los Estados consideren aumentar sus esfuerzos y coordinación en la materia. Sin embargo, en un mundo donde reina el instinto de supervivencia y las ansias por conquistar una nueva frontera de dominación estratégica como el espacio exterior, la cooperación parece ser más una quimera idealista que un objetivo factible. Aún está en manos de los Estados desbloquear el potencial de los foros internacionales a su disposición y construir nuevos polos de coincidencia. Solo así, la seguridad en todos sus órdenes estará garantizada.

Referencias bibliográficas

Al-Rodhan, N. (2018) “The interplay between outer space security and terrestrial global security”. Oxpol, 6 de julio de 2018. https://blog.politics.ox.ac.uk/the-interplay-between-outer-space-security-and-terrestrial-global-security/

Al-Rodhan, N. (2020) “Cyber security and space security”. The Space Review, 26 de mayo de 2020. https://www.thespacereview.com/article/3950/1

Eddy, M. (2019) “Want to Hack a Satellite? It Might Be Easier Than You Think”. PCMag. 07 de mayo de 2019. https://uk.pcmag.com/news/119996/want-to-hack-a-satellite-it-might-be-easier-than-you-think

Rajagopalan, R. (2019). “Electronic and Cyber Warfare in Outer Space”. United Nations Institute for Disarmament Research

Vega Buono, S. (2020) “Al infinito y más allá: militarización y armamentización del espacio ultraterrestre”. Visión Global. 22 de octubre de 2020. https://visionglobal.com.uy/new/militarizacion-y-armamentizacion-espacio-ultraterrestre/