Ciberespacio Espacial: El Talón de Aquiles de la Seguridad y Defensa

Enrique Cubeiro Cabello
Capitán de Navío (reserva)

Director de Ciberseguridad de Ghenova

SÍNTESIS

Espacio y Ciberespacio son los ámbitos más nuevos en los que operan las fuerzas militares. Ambos reúnen una serie de peculiaridades que los diferencian notablemente de los ámbitos "tradicionales": terrestre, naval y aéreo. Una de ellas es su transversalidad, que da lugar a amplias intersecciones con los otros ámbitos operativos. La defensa de los ámbitos espacial y ciberespacial supone un complejo reto para los Estados, complejidad que alcanza su máxima expresión, precisamente, en esa intersección entre ambos que expone el ámbito espacial a la acción de las ciberamenazas. Los sistemas espaciales son de naturaleza frágil y operan en entornos en los que resulta muy complicada su protección física, pero es su enorme dependencia del ciberespacio y, por tanto, su gran exposición a las ciberamenazas, lo que propicia el cóctel perfecto.

Palabras clave: Espacio, Ciberespacio, ciberamenaza, ciberataque, satcom, PNT, SSA/SST, GNSS, SEOT, new space.

Introducción

Una de las principales peculiaridades del ciberespacio como ámbito de las operaciones militares es su transversalidad. Ello implica que existe una zona de intersección entre el ciberespacio y cualquiera de los otros ámbitos operacionales: terrestre, naval, aéreo y espacial.

Este artículo trata de una de esas intersecciones, que considero que reúne unas características únicas por las que debe ser objeto de especial atención. He tardado algún tiempo en decidir si el título de este artículo debería ser «ciberespacio espacial» o «espacio

ciberespacial» y, sin estar completamente seguro, creo que lo primero define más correctamente esa parte del ámbito espacial que puede llegar a ser vulnerable a las ciberamenazas. Y he añadido la coletilla de «El Talón de Aquiles para la Seguridad y Defensa» por motivos que irán aclarándose en las páginas siguientes.

Llevamos escuchando desde hace ya bastantes años que la siguiente gran guerra comenzará con un clic. Hoy, podemos ir algo más lejos y afirmar, con gran probabilidad de acierto, que ese clic que algún cibersoldado ejecutará como inicio de esa gran guerra futura tendrá como finalidad actuar contra alguna capacidad espacial de su adversario.

En las siguientes páginas pretendo exponer cómo confluyen espacio y ciberespacio y de qué forma pueden afectar las ciberamenazas a las capacidades militares espaciales en o a través de esa inevitable intersección de los sistemas espaciales con el ciberespacio.

Un ámbito recién nacido y otro que aún va a la guardería

En cada momento de la historia, el ser humano ha combatido con las armas y en los ámbitos que la tecnología disponible le ha permitido. Ello ha dado lugar a que el conjunto formado por los cinco ámbitos en

los que se hoy desarrollan las operaciones militares englobe dos que son tan viejos como el ser humano (terrestre y naval), otro centenario (el aéreo) y dos de muy corta edad (espacial y ciberespacial)[1].

Y mientras que existe una amplísima experiencia en los tres primeros, resulta aún muy escasa en los dos últimos: apenas hemos vivido conflictos en los que se haya combatido de forma intensa en espacio y ciberespacio o en los que estos ámbitos hayan jugado un papel crucial en el transcurso de la contienda. Y creo que «apenas» no es el adverbio apropiado y quizás «nunca» se ajuste más a la realidad. Incluso el conflicto sobre el que existía más amplio consenso en cuanto a que el ciberespacio iba a jugar un papel absolutamente determinante, la guerra de Ucrania está resultando muchísimo más parecido a la I Guerra Mundial que a esa ciberguerra cuyo imaginario procede casi por completo de la literatura y el cine.

Y, dado que el ser humano estratega militar tiene la mala costumbre de aplicar las lecciones aprendidas en la guerra N para tratar de ganar la N+1, es posible que obtengamos del conflicto de Ucrania la enseñanza errónea de que espacio y ciberespacio son todavía dominios de importancia residual en los conflictos armados y que así va a seguir siendo. A mi juicio, está claro que no va a ser así y que, aunque pueda no resultar cierto en algún caso aislado, el peso promedio de la dimensión especial y ciberespacial en el devenir de los conflictos irá siendo cada vez mayor por la simple y poderosa razón de que la dependencia de las operaciones militares en las capacidades que emplean y explotan los ámbitos espacial y ciberespacial no hace otra cosa que crecer.

Comencemos por analizar el ámbito espacial.

El ámbito espacial

Desde el punto de vista de la Defensa, las capacidades espaciales se pueden categorizar hoy en día en cuatro grandes grupos:

- Comunicaciones por satélite (SATCOM):
- Posicionamiento, Navegación y Sincronización por satélite (PNT).
- Observación de la Tierra desde el Espacio (SEOT).

(1) La OTAN reconoce antes al Ciberespacio (julio de 2016, Cumbre de Varsovia) que al Espacio (diciembre de 2019) como dominio operacional. Sin embargo, a mi entender, el reconocimiento tácito y generalizado del espacio como tal es muy anterior a ambas fechas.

- Conocimiento de la situación espacial y Vigilancia y seguimiento espacial (SSA /SST).

Los satélites de comunicaciones se utilizan para aplicaciones de telefonía, televisión, radio, Internet, permitiendo comunicar puntos muy apartados de la Tierra. Hoy en día existen alrededor de 2.300 satélites de comunicaciones en órbita terrestre; la mayoría, en órbitas geoestacionarias (a unos 36.000 km de altura sobre el ecuador), manteniendo la posición relativa con la Tierra, lo que permite el apuntamiento fijo de las antenas terrestres y obtener con un solo satélite una amplia cobertura de alrededor del 35% de la superficie terrestre. El progresivo incremento de las frecuencias empleadas ha permitido ampliar los anchos de banda y, en consecuencia, las velocidades de transmisión. Al mismo tiempo, las antenas de última generación permiten conformar haces direccionales con el fin de optimizar la señal en las zonas geográficas de interés, con muy alta protección frente a las interferencias. La actual capacidad SATCOM que emplean nuestras Fuerzas Armadas se sustenta en los satélites SPAINSAT y XTAR-EUR, cuya vida útil está muy próxima a finalizar. Su relevo está garantizado por el programa SPAINSAT NG, que comenzará a proporcionar servicio en torno a 2024.

Las capacidades PNT descansan sobre los sistemas globales de navegación por satélite (*Global Navigation Satellite System,* GNSS), que emplean constelaciones de cobertura global y proporcionan a los usuarios información muy precisa sobre posición (coordenadas y altura), navegación (rumbo, velocidad) y tiempo (hora y sincronización), en cualquier parte del mundo y de forma permanente. Los usos de estos servicios son muy amplios: navegación, transporte, geodésicos, hidrográficos, agrícolas, … La entrada en servicio del sistema Galileo ha permitido a la UE la autonomía frente a terceros, fundamentalmente del GPS de los EE.UU. Nuestro Ministerio de Defensa trabaja desde hace algún tiempo en la obtención de equipos para las diferentes plataformas que permitan explotar con las máximas garantías todas las capacidades que permitirá el servicio público regulado de Galileo (Galileo PRS) y beneficiarse del efecto multiplicador que ello supone.

La capacidad de observación de la Tierra (SEOT) resulta fundamental para aspectos tan diversos como los medioambientales, logísticos, seguimiento de catástrofes y, por supuesto, para la obtención de inteligencia y el seguimiento de las operaciones militares. Se obtiene mediante satélites en órbitas de alturas muy diversas en los que se instalan cámaras ópticas (espectros visual e IR) o radares. Las necesidades de imágenes ópticas de nuestras Fuerzas Armadas han sido cubiertas durante años mediante la participación en el programa

francés Helios II, que finalizó el 31 de diciembre de 2021, y actualmente por su relevo, el programa francés de observación de la Tierra CSO (Comoposante Spatiale Optique), con un horizonte de 5 años (2023-28). La capacidad SEOT radar está cubierta, como mínimo, hasta 2023 por el satélite PAZ. Para la renovación de ambas capacidades existen diferentes alternativas de obtención, que incluyen el desarrollo de sistemas nacionales.

La vigilancia y el conocimiento de la situación espacial (Space Search and Tracking – SST; Space Situational Awareness - SSA) resulta fundamental para anticipar y evitar amenazas a los activos espaciales (basura espacial, meteoritos, otros satélites, etc.) o que procedan del espacio, y se obtiene fundamentalmente de la información de radares y telescopios especialmente diseñados para tal fin. La actual capacidad SST/SSA de España descansa principalmente en el Centro Operaciones de Vigilancia Espacial (COVE), ubicado en la base aérea de Torrejón (Madrid), el radar de vigilancia espacial (S3TSR), en la base aérea de Morón (Sevilla), y el telescopio y láser del Real Observatorio de la Armada, en San Fernando (Cádiz). Todos ellos están siendo objeto de diferentes procesos para su potenciación y mejora.

Una peculiaridad de todas estas capacidades espaciales es que, por lo general, soportan tanto servicios del ámbito civil como del militar y se han convertido en activos vitales para la seguridad pública, el bienestar económico y la seguridad nacional de todos los países avanzados, al apoyar todo el espectro de actividades de la población, empresas y organismos de los Estados. En el primer mundo, no hay una sola actividad de importancia que no dependa en mayor o menor medida del espacio: comunicaciones, finanzas, logística, ocio, transporte, movilidad, vigilancia, seguridad, investigación científica ...

En cualquier caso, todos ellas resultan de vital importancia para las Fuerzas Armadas, en tanto sustentan las capacidades de inteligencia, de comunicaciones, de mando y control, de navegación, de posicionamiento y de sincronismo o de alerta previa, todas esenciales en cualquier operación militar, hasta el punto de que la carencia de cualquiera de ellas abocaría de forma ineludible al fracaso.

En las últimas décadas, los avances tecnológicos han propiciado que las capacidades espaciales, antes restringidas a las superpotencias, sean cada vez más asequibles y no se limiten al ámbito gubernamental. Hoy, instituciones académicas, empresas pequeñas y hasta particulares tienen a su alcance la fabricación, lanzamiento, operación y explotación de sistemas satelitales. Esto lleva a una comercialización cada vez mayor de las actividades frente al dominio gubernamental-militar propio del siglo XX.

Impensable hace unos años, nos encontramos hoy con que varias de las principales constelaciones satelitales pertenecen al sector privado y asistimos asombrados a una carrera espacial que ya no se juega entre superpotencias sino entre multimillonarios.

Este nuevo paradigma, conocido como *New Space*, crea cada día nuevas oportunidades comerciales, y abre nuevos mercados en todo el mundo. Pero, lo más importante, está haciendo depender cada vez más las operaciones militares de los operadores civiles propietarios de los sistemas y proveedores de servicios espaciales. Quizás el ejemplo más claro sea la fuerte irrupción de compañías civiles en el mercado de las imágenes de la Tierra desde el espacio, propiciado tanto por el abaratamiento de los satélites de órbita baja como por la progresiva miniaturización de las cámaras que equipan estos ingenios, que permiten obtener fotografías de buena resolución con satélites de un tamaño parecido al de una caja de zapatos. Resolución aún no suficiente para los requerimientos de la inteligencia militar, pero cuya progresión anima a vaticinar que será algo que se conseguirá en pocos años.

A pesar de la «democratización» del sector espacial llegada de la mano del *New Space*, el coste de obtención y operación de algunos de estos sistemas espaciales puede ser todavía lo suficientemente elevado como para resultar inalcanzable para la empresa privada, o no resultar para ésta lo suficientemente atractiva por la dificultad de monetizar los servicios ofrecidos; por ello no es raro que algunas de estas capacidades queden restringidas al ámbito gubernamental y que su obtención deba abordarse mediante acuerdos interministeriales, a través de desarrollos duales, o entre Estados.

El ejemplo más claro de esto es PNT. Hoy en día son todavía muy pocos los sistemas que proveen señales de posicionamiento y sincronismo y no es de extrañar que, a pesar de su enorme coste, las grandes potencias hayan procurado por todos los medios ser completamente autónomas en la producción y obtención de los medios para ello. La autonomía en la capacidad PNT es, hoy en día, una de las mejores pruebas del poder de un Estado.

Así, EEUU cuenta con GPS, Rusia con GLONASS, China con Beidou y la UE con Galileo. Todos ellos proveen de ciertos servicios universales, pero, llegado el caso, pueden restringir su uso por parte de terceros y se reservan para su exclusivo empleo los más resilientes, seguros y precisos; es decir, aquellos que apoyan a servicios gubernamentales críticos o a capacidades militares.

Pero hay otra capacidad que permite calibrar aún mejor el poder de una nación: la de anular o destruir las capacidades espaciales de otros Estados.

Las amenazas a los sistemas espaciales

Hace algunas décadas, la única forma de atentar contra un sistema espacial del adversario era mediante la destrucción física de las estaciones terrestres o mediante técnicas de guerra electrónica (EW), como el *jamming* o el *spoofing*.

Pero hoy en día la profusión de ingenios en órbitas bajas, así como la entrada en juego de desarrollos armamentísticos de alta precisión y alcance, especializados precisamente en la destrucción de activos en órbita, ha supuesto un cambio muy notable en la situación.

Desde hace años, Rusia y China están desarrollando armamento espacial, con un espectro de actuación que abarca tanto ataques a la infraestructura terrestre como contra los activos en órbita. Por supuesto, EE.UU. cuenta desde mucho antes con tales capacidades. En marzo de 2019, India probó con éxito su primer misil antisatélite, convirtiéndose así en el cuarto miembro del club. La militarización del espacio ultraterrestre es ya una realidad y, por ello, la Defensa del Espacio (*Space Defence, Defence in Space*) ha pasado casi de repente a ser asunto crucial en la agenda estratégica de los grandes Estados, y con tal peso y relevancia es abordado por la Brújula Estratégica de la Unión Europea.

Los satélites son artefactos ligeros, que se desplazan a gran velocidad por trayectorias predecibles; son, por ello, de naturaleza física frágil y altamente vulnerables, hasta el punto que un pequeño proyectil o un fragmento minúsculo de basura espacial puede destruirlos. Esto puede llevar a suponer (spoiler: erróneamente) que su principal amenaza la constituye ese armamento cinético de gran alcance y precisión antes mencionado (detonaciones de ojivas en las inmediaciones del satélite o misiles balísticos de ascenso directo) u otros ingenios, también de naturaleza física, diseñados para ataques coorbitales: artefactos capaces de aproximarse al objetivo en órbita y destruirlo por medio de armamento cinético instalado en la propia plataforma o incluso mediante brazos robóticos capaces de agarrar, desplazar o destrozar a su víctima. El problema de este tipo de ingenios es que sus ataques son muy fácilmente detectables y evidenciables y, por lo tanto, atribuibles con un alto grado de certeza.

Por todo ello, la mayor y más probable amenaza al dominio espacial, tanto para los activos orbitales como para las estaciones terrestres, está en el plano no cinético: acciones ofensivas ejecutadas sin contacto o proximidad física, no observables, rápidas y sigilosas y, lo más importante, muy difíciles de atribuir, lo que engloba a su vez diversas posibilidades: armas de energía dirigida capaces de dañar componentes y sensores, ataques de jamming o spoofing contra las

señales de radiofrecuencia, pero, sobre todo, ciberataques dirigidos contra los flujos de datos, los activos de la red, las unidades de procesamiento y, en definitiva, contra cualquier elemento potencialmente cibervulnerable del sistema objetivo.

Las peculiaridades del Ciberespacio

Como se mencionaba en la introducción, Espacio y Ciberespacio comparten una característica muy particular: su transversalidad. En su calidad de ámbitos operacionales, eso significa que lo que en ellos ocurre tiene enorme repercusión en los otros. Es fácilmente entendible que la destrucción de un satélite geoestacionario de comunicaciones, la pérdida de operatividad de parte de una constelación GNSS o que un virus deje inoperativo un sistema de mando y control son hechos que pueden tener profundas y graves repercusiones en una operación terrestre o aeronaval. Sin embargo, no parece tan probable que la destrucción de una base o la pérdida de un buque o aeronave provoquen unos trastornos equivalentes en los ámbitos espacial o ciberespacial.

Decíamos unas páginas atrás que no hay ningún sector de actividad relevante que no dependa en mayor o menor medida del espacio: comunicaciones, finanzas, logística, ocio, transporte, movilidad, vigilancia, seguridad, investigación científica ... Sustitúyase espacio por ciberespacio y se verá que sigue siendo completamente cierto.

El ciberespacio es un ámbito de naturaleza artificial, construido por el hombre y, como tal, muy imperfecto y frágil. Los elementos que lo componen y su empleo están sujetos a infinidad de vulnerabilidades explotables que abarcan los planos físico, lógico y humano: fallos de fabricación, de configuración, de arquitectura, de programación, emanaciones no deseadas, puertas traseras, funcionalidades de doble uso, interconexiones inadecuadas, accesos mal protegidos, desconocimiento, falta de concienciación, malicia, …

Sobre este descomunal y creciente conglomerado de hardware y software, empleado por seres imperfectos y cada vez más interconectado, descansa gran parte de la actividad humana. Y, por supuesto, la militar. Cazabombarderos o fragatas no son ya más que conjuntos de hardware y software que vuelan o navegan. Como los satélites, sustituyendo la forma verbal por "orbitan". Y a todos ellos resulta aplicable ese principio casi universal de que cualquier requisito de ciberseguridad en el desarrollo e implantación de todo elemento, componente, subsistema o protocolo estará supeditado a los de funcionalidad u operación. Por todo ello, no es descabellado afirmar

que, hoy en día, un troyano constituye para una fragata una amenaza tan real (o quizás más) que un torpedo o un misil.

Hay otras muchas peculiaridades del ciberespacio que tienen enorme importancia desde el punto de vista de la Seguridad y Defensa de los Estados. Esbocemos las más importantes.

El ciberespacio está en constante crecimiento: crece el número de los dispositivos que lo conforman, y las redes, los sistemas, y las interconexiones entre ellos, y, por supuesto, los datos, … Y todos ellos de forma exponencial: así, por ejemplo, los dispositivos conectados a Internet (unos 40.000 millones a finales de 2022) se multiplican por 3 cada 5 años, y los datos procesados se duplican cada dos años, dato este que impresiona puesto que significa que cada 24 meses se origina, procesa y almacena tanta información como en toda la Historia precedente de la humanidad.

Todo esto implica que el territorio a defender crece en consonancia (exponencialmente), en tanto que el de los medios para su defensa lo hacen de forma casi lineal. Es decir, cada día se agrava (exponencialmente) la brecha existente entre lo que nos pueden atacar y lo que somos capaces de defender. Algo parecido pasa con el espacio ultraterrestre, aunque en mucha menor medida, en tanto cada vez es mayor el número de ingenios y sistemas que lo ocupan. En contraste, las dimensiones de los ámbitos terrestre, naval y aéreo permanecen prácticamente inmutables en el tiempo.

Otra peculiaridad: mientras en los ámbitos terrestre, naval y aéreo resulta impensable que un actor no estatal tenga alguna significancia, en el ciberespacio no es así. Existen infinidad de actores no estatales con amplias capacidades, recursos y potencialidad para provocar graves y extensos daños. Actores que, además, responden a motivaciones muy variadas: económicas, ideológicas, de poder, … En esto, se parece también al espacio, en el que como hemos visto los actores no estatales van ganado peso. Sin embargo, parece muy difícil que actores no estatales lleguen a poseer capacidades espaciales enfocadas a la destrucción. Eso queda, de momento, para las películas de James Bond.

Muy relacionado con lo anterior está el aspecto armamentístico. Mientras que en el resto de ámbitos el armamento pesado está casi en exclusividad en poder de los Estados, las «ciberarmas» están repartidas entre infinidad de actores, entre los que se encuentran tanto organizaciones criminales y grupos *hackivistas* como agencias de inteligencia o unidades militares. Con el agravante de que ese control armamentístico, que es razonablemente posible en los otros ámbitos, resulta inabordable en el ciberespacial, en tanto la naturaleza de las

«*ciberarmas*» (código + dispositivo de almacenamiento minúsculo) las hace invisibles a cualquier intento de control.

El ciberespacio es opaco por naturaleza. Es muy difícil ver lo que en él ocurre. Y, más aún, interpretarlo correctamente. Desde el punto de vista militar, ello implica desconocer las capacidades e intenciones del adversario, carecer de alerta previa, tener que tomar decisiones sobre un dibujo operacional incompleto y distorsionado y correr el riesgo de malinterpretar o de atribuir erróneamente las acciones. Este último aspecto es tremendamente importante: el ciberespacio concede enormes facilidades para la suplantación, el anonimato o el uso de infraestructuras de terceros. Lograr una atribución sobre una acción que esté sólidamente respaldada en evidencias probatorias resulta prácticamente imposible. Y si no hay atribución, no existe posibilidad de represalia, principal sustento de un modelo de disuasión. Este único argumento sirve por sí solo para explicar por qué el ciberespacio es el ámbito preferido de actuación para la guerra híbrida y por qué el cibercrimen es desde hace años la modalidad delictiva que más dinero mueve en el mundo.

Si a esta ausencia de riesgo (impunidad) añadimos el elevado impacto potencial y lo relativamente barato y sencillo de las acciones (rentabilidad), es fácilmente entendible esa intensa, permanente y creciente actividad hostil que se desarrolla en el ciberespacio, con independencia de si el mundo «real» se encuentra en paz, crisis o conflicto.

El talón de Aquiles de la Seguridad y Defensa

Son varias las versiones sobre el origen del «talón de Aquiles». En cualquier caso, todas ellas hacen referencia a que, a diferencia del resto de su cuerpo, el talón derecho del héroe mitológico griego era vulnerable, lo que permitió a París matarlo durante el asedio de Troya clavándole una flecha envenenada en ese preciso punto.

Podemos decir que el Ciberespacio Espacial es el talón de Aquiles de la Seguridad y Defensa de los Estados y de las grandes Organizaciones a ellas enfocadas. Obviando el hecho de que no podemos atribuir la invulnerabilidad completa a ninguna dimensión de los Estados, sí que parece lógico inferir que será precisamente la intersección de las dos más potencialmente vulnerables la que plantee mayores dificultades para su protección y, por tanto, donde se concentre la más acusada vulnerabilidad. Y, además, que, siendo las dos más transversales, cualquier acción que afecte a su intersección tendrá unos efectos amplificados sobre el resto.

Como antes he mencionado, carecemos de experiencia suficiente sobre el papel que espacio y ciberespacio pueden jugar en los conflictos armados. En la mayoría de los conflictos recientes, el ciberespacio ha servido más como campo de batalla de la desinformación y la propaganda que como medio para contrarrestar o atacar las capacidades militares adversarias.

En la guerra de Ucrania, el «apagón» del ciberespacio ucraniano que algunos vaticinaban (y aquí me incluyo) no ha ocurrido y Rusia no alcanzado en ningún momento esa supremacía ciberespacial que se suponía que conseguiría casi de inmediato. En el ámbito espacial, tampoco han ocurrido grandes cosas. La más notoria, alcanzada precisamente mediante un ciberataque, la sufría a finales de febrero de 2022, recién iniciada la invasión rusa, la compañía VIASAT que, según el comunicado entonces emitido, informaba de que procedía a investigar un ciberataque que había provocado una interrupción parcial de sus servicios de banda ancha en Ucrania y en toda Europa. Al parecer, se trató de un ataque DDoS[2], modalidad de la que los rusos hicieron amplio uso en las primeras etapas del conflicto.

Son muchos los posibles motivos a los que se puede achacar el escaso peso de espacio y ciberespacio en el conflicto de Ucrania. A mi juicio, ninguno tan poderoso como el enorme apoyo que EE.UU. ha prestado a Ucrania en la protección y defensa de su ciberespacio, y muy especialmente del de sus infraestructuras críticas y sistemas que apoyaban servicios esenciales (especialmente Internet y telefonía móvil). Apoyo en medios y capacidades que, en cuestión de meses, incrementó enormemente tanto su protección frente a las ciberamenazas como su capacidad para seguir operando en ambientes muy hostiles. Con ello, se consiguió algo parecido a la desactivación de la capacidad ofensiva rusa, firmándose una especie de tablas. En definitiva, que si en el espacio y ciberespacio apenas han pasado cosas relevantes en esta guerra no ha sido porque no se haya intentado.

Debemos inferir, por tanto, que en cualquier conflicto venidero entre Estados avanzados tecnológicamente (y, por tanto, espacio y ciberespacio dependientes) ambas partes tratarán de atacar prioritariamente los activos adversarios en estos dominios, empleando para

---

(2) Denegación Distribuida de Servicio *(Distributted Denyal of Services*) Ataque a un sistema, aplicación o dispositivo para dejarlo fuera de servicio mediante una saturación de peticiones que se realizan desde diversos orígenes, haciéndolo más efectivo, y más complicado de detener y de determinar su origen. Fuente: *INCIBE.* **Glosario de términos de Ciberseguridad.** *(2022).*
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

ello todos los recursos de los que dispongan: satélites asesinos, misiles antisatélite, ciberataques, *jamming,* ...

Sin embargo, la amenaza a los activos espaciales (y, en general, a cualquier activo relevante de un Estado) no queda restringida a las épocas de conflicto. Es lo que trae consigo la dificultad de atribución de los ciberataques. Y, sea tiempo de paz, crisis o conflicto, son tantas y tan críticas las capacidades de un Estado que descansan sobre sus sistemas espaciales que van a ser siempre objetivo prioritario de sus potenciales adversarios. Por lo tanto, hay que considerarla una amenaza especialmente seria, tanto por su carácter permanente como su elevada probabilidad de ocurrencia.

Pero, y aquí viene quizás lo más grave, la amenaza a los activos espaciales no se limita a la de los Estados rivales. Ya hemos dicho que el ecosistema de las ciberamenazas incluye un sinfín de perfiles no estatales, con capacidades y motivaciones muy diversas. Un ataque de *ransomware* exitoso a un sistema espacial puede suponer tanto un fantástico botín para un grupo de ciberdelincuentes como una acción de enorme visibilidad para un grupo *hackivista*. Tenemos, pues, que pensar que ahora mismo existen múltiples actores explorando esa posibilidad contra cualquiera del enorme y heterogéneo conjunto de activos que hoy conforman el ámbito espacial.

Resumiendo: tenemos un ámbito sobre el que descansan gran parte de las actividades humanas, especialmente las más críticas y esenciales, que es un objetivo tan altamente vulnerable como apetecible para infinidad de actores; actores entre los que debemos considerar a las ciberamenazas como los más numerosos y potencialmente peligrosos.

Panorama nada tranquilizador.

Epílogo

Hace unos años recayó sobre mí la responsabilidad de liderar un Grupo de Trabajo interministerial con la misión de desarrollar una de las líneas de acción de la Estrategia de Seguridad Marítima del año 2013: Mejora de la ciberseguridad en el ámbito marítimo. En aquel momento, una búsqueda en Google de la expresión "*maritime cybersecurity*" arrojaba el saldo desolador de media docena de resultados. Lo sé, porque fue lo primero que hice al recibir el encargo del Almirante General García Sánchez. Acabo de repetir la prueba y el resultado supera los 17 millones.

Algo parecido pasó, con unos pocos años de adelanto, con el ámbito espacial y la ciberseguridad. Y es que desde hace ya unos cuantos

años existe una seria preocupación en el sector por este aspecto. Hoy en día es fácilmente constatable que los sistemas se diseñan, construyen y operan con requisitos de ciberseguridad cada vez más exigentes, frente a los prácticamente inexistentes o muy ligeros de hace apenas una década. Requisitos que aplican tanto a los ingenios espaciales como a las estaciones terrestres y a todos los sistemas y subsistemas que los componen y a todos aquellos con los que se interconectan y que participan de alguna forma en cualquiera de los aspectos de su control y operación.

La ciberseguridad ha de abarcar un sinfín de aspectos, que se articulan en varios grandes apartados: arquitecturas, configuraciones, equipamiento, políticas, procedimientos. Proteger un sistema tiene tanto que ver con dotarlo de *firewalls* y antivirus como con concienciar convenientemente a sus operadores frente a las ciberamenazas o con establecer unas buenas políticas de contraseñas o procedimientos de *back-up*. Ello implica abarcar tanto la ciberseguridad corporativa, incluyendo la de los proveedores, como la de los elementos del sistema, abarcando también la cadena de suministro.

Se trata, pues, de un problema que hay que abordar con una amplia perspectiva y recursos suficientes. Y si hace unos años apenas había consciencia del riesgo, lo que derivaba en ausencia de interés y voluntad para mitigarlo, parece que las cosas están cambiando. Y en el sector espacial, como ocurrió bastante antes en la banca, la ciberseguridad ha dejado ser un aspecto puramente tecnológico para convertirse en un asunto fundamental de la gestión de riesgos que involucra a la alta dirección y al nivel estratégico.

Valgan como pruebas de esta concienciación creciente la ya referida importancia que se concede a este asunto en la Brújula Estratégica de la UE o en recientes directivas de la UE (Directiva NIS, *EU Cyberresillience Act*), el que la Oficina Federal para la Seguridad de la Información (BSI[3]) acabe de publicar un modelo de estándares de ciberseguridad para la industria espacial[4], que haya Estados que ya hayan publicado estrategias nacionales específicas para la ciberseguridad espacial, el que la Agencia Espacial Europea (ESA) cuente con un grupo específico para este asunto[5], el que en

(3) BSI: *Bundesamt für Sicherheit in der Informationstechnik.*

(4) https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/IT-Sicherheit-in-Luft-und-Raumfahrt/it-sicherheit-in-luft-und-raumfahrt.html

(5) https://www.esa.int/Space_Safety/ESA_practices_cybersecurity

la DGAM[6] los programas de sistemas espaciales y de ciberdefensa compartan la misma Jefatura, o el que la búsqueda en Google de «*space cybersecurity*» devuelva más de 320 millones de resultados.

El problema: que aún permanecen ahí arriba ingenios longevos, creados en una etapa en la que las ciberamenazas no eran tenidas en cuenta en forma alguna en su diseño, y que sustentan servicios esenciales o cuya carencia puede suponer un grave impacto. Y tampoco podemos asegurar que todos los sistemas puestos en operación en estos últimos años reúnan unos estándares de ciberseguridad suficientes, que probablemente sea el caso y en un porcentaje mayor de los que a priori se pueda suponer en un ámbito tan crítico y tecnológicamente demandante. En este sentido, preocupa mucho lo que para los sistemas ya en servicio y cuya esperanza de vida es todavía amplia (de 10 años o más) pueda suponer la ciberamenaza con capacidad computacional postcuántica, que se estima llegará antes de que haya finalizado la vida operativa de estos sistemas.

En estos días se ha puesto de moda en el ámbito futbolístico la expresión «defensa pesimista», término que Carlo Ancelotti, entrenador del Real Madrid, aplicó al futbolista Nacho como alabanza. Se refería a la especial capacidad del canterano merengue para imaginar posibles fallos del equipo propio para así anticiparse defensivamente a la acción del rival.

Pues en esto de la defensa del ciberespacio espacial no cabe una aproximación más apropiada; Estados, organizaciones, agencias y empresas tienen que ser como Nacho: defensores pesimistas.

(6) DGAM: Dirección General de Armamento y Material del Ministerio de Defensa.

Bibliografía

- CUBEIRO CABELLO, Enrique. *El ciberespacio en la guerra de Ucrania.* (2022). Documento de Opinión IEEE 32/2022. https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO32_2022_ENRCUB_Ucrania.pdf
- Departamento de Seguridad Nacional (DSN): *Estrategia Nacional de Seguridad Espacial.* (2019). https://www.dsn.gob.es/sites/dsn/files/Estrategia%20Aeroespacial%202019%20Interactiva.pdf
- Departamento de Seguridad Nacional (DSN): *Estrategia Nacional de Ciberseguridad.* (2019). https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019
- Dirección General de Armamento y Material (DGAM). *Plan Director de Capacidades Espaciales.* (2015). https://www.defensa.gob.es/Galerias/dgamdocs/plan-director-sistemas-espaciales.pdf
- Eurpean Space Agency (ESA). *ESA practices cybersecurity.* (2019). https://www.esa.int/Space_Safety/ESA_practices_cybersecurity
- GANUZA, Néstor. *Guía de Ciberdefensa. Orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar.* Junta Interamericana de Defensa. (2020).
- INCIBE. *Glosario de términos de Ciberseguridad.* (2022). https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf
- LIBICKI, Martin C. *Cyberdeterrence and cyberwar.* (2009).
- SCHMITT, Michael N. *Grey Zones in the International Law of Cyberspace.* (2017).
- White House. *National Cyber Strategy of the United States of America.* (2018). https://digital.library.unt.edu/ark:/67531/metadc1259394/m2/1/high_res_d/National-Cyber-Strategy.pdf