Mesa	#	Pregunta	Respuesta
1	1	La implementación de una nube táctica de combate dependerá de haber alcanzado la superioridad en el espectro Electromagnético. Ante la existencia de competidores con altas capacidades CEMA, se puede pensar en alcanzar dicha nube táctica, base de las operaciones multidominio?	Al igual que existe el concepto de superioridad y supremacía aérea, debemos entender también la superioridad en el uso del EEM. Ésta no será alcanzable de forma total, pero se debe lograr suficientemente para el cumplimiento de la misión. Conscientes de la actuación en entornos degradaos y limitados la complementariedad de medios, las EPM y la distribución de la información deben presidir nuestra actuación.
1	2	¿es el concepto Zero trust buena solución para la seguridad en el dominio Ciberespacial?	Si porque Zero Trust es un enfoque proactivo e integrado de la seguridad en todas las capas del estado digital, que verifica de forma explícita y continua cada transacción, comprobando los privilegios mínimos y haciendo uso de la inteligencia artificial, la detección avanzada y la respuesta en tiempo real ante amenazas. Los beneficios que se desprenden de su implementación incluyen una mejor resiliencia frente a ciberamenazas a través de una política de seguridad consistente que se gestiona de forma centralizada y se aplica localmente, proporcionando un marco de actuación más flexible y adaptable a la situación.
1	3	Ha mencionado usted que un tema relevante es conseguir espectro para desarrollar 5G (future G) en el ámbito militar. ¿Qué significa eso? Pues, el 5G no está ya implementado en algunos ejércitos?	Existen diferentes prototipos de Redes 5G en los Ejércitos, Armada y UME, pero los mismos aún no tienen en general asignadas bandas de frecuencias de forma permanente por ser este tipo de espectro un recurso crítico. Se está trabajando con SETELECO y los operadores para poder disponer de mayor espectro para el empleo 5G militar.
1	4	En cuanto a la interoperabilidad entre fuerzas terrestres de diferentes naciones, da la impresión que no es fácil de conseguir. Qué piensa al respecto?	Nunca es fácil. Sin embargo, los foros de interoperabilidad, donde se establecen acuerdos técnicos en forma de STANAG, y los múltiples ejercicios OTAN buscan precisamente su mejora. Como ejemplos la iniciativa FMN y ejercicios como son el CWIX
1	5	En cuanto a los sistemas de identificación, ¿son realmente resistentes al spoofing? Es decir, hasta qué punto se puede confiar en ellos con los continuos avances en cuanto a la amenaza cyber.	No se puede asegurar que los sistemas de identificación sean totalmente resistentes al Spoofing. Se están tomando medidas, al igual que con los sistemas PNT, para intentar que lo sean en la mayor medida posible. El sistema RBCI comentado, de identificación basado en señal radio, no se ha implementado aún ni nacionalmente ni en OTAN. Se quiere superponer la funcionalidad RBCI sobre algunas formas de onda de comunicaciones, pero esto no va a ser inmediato.
1	6	¿Cree que, con el estado actual de las cosas, la Alianza está preparada en 2030 para conducir operaciones Multidominio?	El esfuerzo es enorme pero no en el ámbito tecnológico sino en el del cambio de cultura de la organización muy centrada en nichos de capacidades.
1	7	Nos podría resumir, por favor, ¿Cuáles son las variables que componen a la ecuación del ciberespacio?	A pesar de ser el título de la ponencia esta ecuación no está definida y existen diferentes aproximaciones. Lo que está claro es que en ella intervienen los elementos siguientes: (1) infraestructura CIS/TIC, (2) las interconexiones y (3) la información que manejan. Además, autores más audaces como es Paul Kuehl afirman que el conocimiento también forma parte de la ecuación. Personalmente creo que no es así y en este punto estoy de acuerdo con lo dispuesto en el AJP 3,20

1	8	Para alcanzar la capacitación en Operaciones Multidominio, es necesario un cambio de mentalidad. La resistencia al cambio es siempre una barrera difícil de superar. No cree q se está pidiendo un esfuerzo a realizar en poco tiempo en un aspecto que normalmente lleva muchos años cambiar?	Efectivamente, pero en entorno tan demandantes como son los entornos VUCA la agilidad debe priorizarse. El ejemplo de la guerra de Ucrania es evidente en este sentido.
1	9	¿No cree que esa Interoperabilidad que menciona, integrado todas las capacidades, organismos y organizaciones, tanto el contexto nacional como multinacional, no es de momento un puente demasiado lejano?	Es lejano, pero es el único modo de lograr el fin. Esperemos que no tengamos que acelerarlo por motivos exógenos y que seamos capaces de prepararnos a tiempo.
1	10	Han mencionado muchos tipos de ataques o estrategias para hacer daño, pero previamente han mencionado que estamos en una época muy prematura de esta generación ciberespacial, ¿Qué tipo de medidas piensan adoptar para ser capaces de protegerse a futuras técnicas?	Se está desarrollando el SCOMCE - Sistema de COMbate CiberEspacial que pretende ser un sistema integral para acciones de Monitorización, Inteligencia, Defensa, Explotación y Respuesta frente a las Ciberamenazas, con el que se dará un salto cualitativo importante para afrontar las mismas
1	11	¿Las operaciones multidominio se dan también a nivel táctico?	Las MDO suponen una nueva forma de operar que persigue generar efectos en todos los niveles de actuación, incluido el táctico. En el caso de las fuerzas terrestres, la mayor parte de las capacidades multidominio estarán en su escalón más alto ya sea Mando Componente Terrestre o Cuerpo de Ejército, aunque todos los escalones se verán afectados y deberán entender las implicaciones que suponen a su nivel.
1	12	¿No cree usted que los requisitos que configuran las operaciones multidimensionales (hiperconectividad, mando y control e interoperabilidad) están siendo puestos en operación con la I3D, el SC2N y la plataforma ARGO?	En estas operaciones serán prioritarias la conectividad, la interoperabilidad, la libre circulación de la información y la transferencia de datos entre plataformas terrestres y Sistema de Mando y Control Terrestre, además de hacia otros mandos componentes, lo que incrementará la capacidad de decisión a todos los niveles y las opciones tácticas de empleo de armas y sensores. Como no podría ser de otra manera los nuevos desarrollos para facilitar estas operaciones deben estar orientados a obtener estas capacidades y los mencionados en la pregunta constituyen una parte importante de este esfuerzo.
1	13	¿Cómo se va a implementar concepto de guerra multidominio en una fuerza dotada con materiales de principios de los 2000?	Totalmente de acuerdo de ahí el esfuerzo de las FAS, con lo recursos limitados existentes para lograr esta modernización. Programas como el ZEUS C2, MC3 o el SCRT son imprescindibles para lograr establecer una nube táctica de combate; que como dijimos son habilitadores en su construcción. Sin conectividad no hay MDO.

1	14	¿Qué opinión le merece la estrategia de inteligencia artificial del ministerio de defensa?	Para la implementación de la Inteligencia Artificial en el MINISDEF es necesario partir de un documento de alto nivel como es esta Estrategia IA que marque las líneas maestras a seguir para su posterior implementación. Esta IA, tecnología Emergente y Disruptiva, puede ser de gran utilidad para las Fuerzas Armadas para por ejemplo poder realizar un manejo más eficiente de la enorme cantidad de datos que los actuales sistemas proporcionan y que él, a veces, escaso recurso humano no puede asimilar.
1	15	Pese a todos los ciberataques serios entre Estados desde el ciberataque a Estonia no ha habido postura internacional definida. ¿Es por la dificultad de categorizar un ciberataque como "agresión armada" o más un problema de atribución?	Entre otros factores, la incertidumbre jurídica parece haber jugado un papel fundamental en la reticencia para adoptar una clara postura frente a los ciberataques, dada la necesidad de que el Estado agredido identifique la concreta norma de Derecho Internacional pretendidamente vulnerada para poder adoptar legítimamente contramedidas frente al agresor, incluyendo en su caso el ejercicio del derecho de auto-defensa (art. 51 de la Carga de Naciones Unidas) Y, ciertamente, el Derecho Internacional plantea numerosos problemas interpretativos cuando se trata de aplicarlo al ciberespacio. Nótese por lo demás que los principales documentos que tratan de aclarar su alcance -pese a su indiscutible autoridad técnica- no son jurídicamente vinculantes, como sucede con los Manuales Tallin, que, además, en determinados aspectos ponen de manifiesto las divergencias existentes entre los propios expertos. Esos problemas interpretativos se proyectan especialmente en la determinación de categorías básicas, tales como aclarar cuándo una operación cibernética puede catalogarse como “uso de la fuerza” (art. 2.4 Carta de Naciones) o “agresión armada” en el sentido del art. 51 de la Carta. La principal controversia al respecto estriba en determinar si únicamente puede considerarse que conculca la prohibición del uso de la fuerza el ciberataque que genera daños o perjuicios físicos, o si por el contrario también merecen tal valoración los que no alcanzan tal umbral. Esta última es la posición mayoritariamente sostenida por los expertos en el Manual Tallin 2.0, que incluyen en la categoría a las operaciones que impiden el funcionamiento de determinadas infraestructuras de forma permanente. E, incluso, algunos Estados extienden el ámbito a aquellas operaciones que generen importantes daños económicos (por ejemplo, Francia o Italia). Y en lo concerniente al interrogante de precisar cuándo una operación cibernética puede constituir una “agresión armada” a los efectos del artículo 51 de la Carta, diversos países consideran que tal sería el caso si el ciberataque alcanza una escala y severidad comparables a la resultante del uso de la fuerza física mediante el empleo de los medios cinéticos convencionales. A estas incertidumbres interpretativas cabría añadir los problemas de atribución de la responsabilidad del ciberataque, pues, por obvias razones técnicas, se plantean mayores dificultades de identificación del Estado responsable en la esfera cibernética. Dificultades que naturalmente se acrecientan en los muy frecuentes casos en que los ciberataques los realizan materialmente actores no estatales. Como es sabido, los supuestos en los que un Estado se considera internacionalmente responsable de un acto ilícito se encuentran regulados en las normas acuñadas por la Comisión de Derecho Internacional [Responsabilidad del Estado por hechos internacionalmente ilícitos (AG756/83) (2001)], que resultan también de aplicación en el contexto cibernético. Pues bien, de acuerdo con su art. 8, un Estado es responsable por ataques perpetrados por actores no estatales únicamente si actúan de facto siguiendo sus instrucciones o bajo la dirección o el control del mismo. Nos hallamos de nuevo ante unos conceptos jurídicos poco precisos –“instrucciones, “dirección”, “control”- que dificultan notablemente la formulación de una acusación formal dirigida al Estado pretendidamente promotor del ciberataque.

1	16	Han mencionado que no creen de momento necesitar como bien ha dicho el moderador un ejército del ciberespacio, pero ahí países como Alemania que ya lo tienen... No consideran esa decisión un punto de inflexión para tomar la iniciativa a la hora de tratar de protegerse ante futuras amenazas.	Considero que es prematuro aún. A nuestro nivel debemos iniciar un proceso de convergencia de las capacidades ciberespaciales del ET. Un ejemplo a seguir sería el del UK Army que ha puesto bajo el CEMA Effects Group en Andovesus tres Signal Regiment de EW: 13th (especializado en ciber), el 14 th (especializado en EW) y el 15 th (especializado en SIGINT).
1	17	¿Tienen otros estados como Rusia, China o los EE.UU. la misma aproximación que la UE en la regulación del marco jurídico del ciberespacio?	En absoluto, tampoco su cultura y sus valores son idénticos. Con carácter genérico podríamos definirlos como: abierto empresarial en EE. UU., regulado en la UE, estatal patriarcal en la RPCh y agresivo en Rusia. La aplicabilidad del Derecho Internacional, y particularmente la Carta de Naciones Unidas, al ciberespacio es una posición asumida generalizadamente por los Estados. Así lo ponen de manifiesto los diversos informes de los Grupos de Expertos Gubernamentales impulsados por la ONU, en los que se hallaban representados China, Rusia y los Estados Unidos. Pero como se reconoce también en estos informes de forma explícita, es preciso avanzar en un entendimiento común y un consenso entre los Estados sobre el modo en que debe aplicarse ese Derecho Internacional en este nuevo entorno. Pues, en efecto, hay diversos enfoques entre los diferentes Estados sobre el alcance y sentido de dicha regulación. Empezando por el propio concepto de "soberanía cibernética", que es utilizado en China y Rusia para justificar restricciones al acceso a internet en su territorio, lo que desde la óptica occidental sería palmariamente contrario a la libertad de expresión e información de los ciudadanos. Y en consecuencia estos países también conciben la noción de "guerra cibernética" en un sentido muy amplio, pues, desde el año 2008, la Organización de Cooperación de Shanghái incluye en tal definición, no sólo la "guerra cibernética" propiamente dicha, sino también la "guerra de la información" y la "guerra psicológica". También hay diversidad de pareceres en lo concerniente a la atribución de la responsabilidad de los Estados, que puede ser especialmente difícil de identificar cuando los ciberataques son perpetrados por agentes no estatales. Así, mientras que Rusia, China y otros países vienen constantemente sosteniendo que las acusaciones deben ser probadas, los Estados Unidos y el Reino Unido -entre otros- sostienen que el Derecho Internacional no exige que se revelen las pruebas que apoyan la acusación. Y, en fin, cabe apreciar asimismo alguna divergencia en la posible aplicabilidad del Derecho Internacional Humanitario al ciberespacio, puesto que China se ha mostrado sistemáticamente reacia a incorporarlo expresamente en los diversos informes elaborados por los Grupos de Expertos de la ONU.
1	18	¿Cómo actuaría el ejército para garantizar la seguridad de los ciberataques a la sociedad civil en una guerra más allá de garantizar la seguridad de los sistemas del ejército?	La responsabilidad del MCCE en Ciberdefensa es sobre las Redes Militares. No obstante, tenemos una estrecha y permanente colaboración con el INCIBE, el CNI y las FCSE en esta materia. En caso de guerra se arbitrarían los procedimientos nacionales para que esta coordinación fuera aún mucho más fluida. Es posible que en caso de conflicto el MCCE asumiera mayores cometidos que los actuales en lo que a Ciberdefensa se refiere.

1	19	Entiendo cómo puede influir los sistemas inteligentes de toma de decisiones en empresas privadas, sobre todo para la gestión de recursos, pero no en el ámbito de la seguridad y el ejército. ¿También se encarga de la gestión de recursos? ¿Toma decisiones tácticas de ataque y defensa? ¿Cómo se regula?	La Inteligencia Artificial acelerará el ritmo de numerosos procesos en el nivel táctico como pueden ser en el empleo de sistemas autónomos, de defensa cibernética, de mando y control y apoyo a la decisión, de gestión y explotación de los datos o de simuladores de combate. Sin embargo, en el proceso de toma de decisiones el control humano deberá continuar estando presente en aspectos como la rendición de cuentas o la responsabilidad moral.
2	1	Se ha mencionado el ransomware, como uno de los mayores problemas para garantizar la disponibilidad de la información, ¿no cree que además de los antivirus y backups, la concienciación es nuestra mayor baza?	Sí, es cierto, dado que el phising ha sido hasta la fecha la principal táctica de entrada de este tipo de ataque. Pero hay que tener en cuenta que se está observando una nueva táctica aprovechando vulnerabilidades de los sistemas. Mantenerlos actualizados, securizados y monitorizados forma también parte de la solución. La concienciación siempre es la mejor baza. Los antivirus solo dan una protección limitada, y a veces, en ataques avanzados, se han logrado comprometer hasta los backups. La seguridad es un proceso de vigilancia constante, por eso es necesaria la formación y la concienciación para poder detectar posibles anomalías antes de que sea tarde.
2	2	Es un hecho el empleo de la IA en la generación de información falsa indistinguible de la realidad ¿cómo lo combatimos con más IA? ¿No estamos entrando en una dinámica muy peligrosa?	En mi opinión y a día de hoy, la IA debe ser siempre una HERRAMIENTA que FACILITE el trabajo de los analistas, y no que los SUSTITUYA. También considero que actualmente no podemos desarrollar ni confiar en sistemas de IA completamente autónomos. El trabajo del analista humano es insustituible a CORTO Y MEDIO PLAZO. Sí. La dinámica es peligrosa e imprevisible, ya que la IA está empezando a alimentarse de los resultados de otras IAs, generando un círculo que puede ser tanto virtuoso como vicioso (más probable, en mi opinión).
2	3	Teniendo en cuenta la importancia creciente de los sistemas autónomos y de que éstos precisan del IoT para su efectividad ¿somos capaces de garantizar su conectividad en el campo de batalla? ¿es el concepto CEMA la solución?	La solución pasa por conseguir una capa de comunicaciones con buen ancho de banda. El uso de tecnología 5G en la arquitectura táctica es una solución que estamos experimentando.
2	4	Siendo su opinión que cito textualmente "deberíamos darle pocas oportunidades a un posible adversario de adiestrarse con una ocupación del espectro por fuerzas propias", le pregunto ¿cómo hacer para "nadar y guardar la ropa"?	No estoy seguro de haber comprendido la pregunta. Si se trata de evitar que el adversario aproveche nuestras emisiones en tiempo de paz para adiestrarse y conocer nuestro modus operandi, no debemos emplear modos reservados o de guerra en tiempo de paz.
2	5	Considera viable y posible (desde el punto vista seguridad) una solución para permitir el acceso seguro desde dispositivos móviles personales a las aplicaciones y redes internas del Ministerio de Defensa, (para unos 120.000 usuarios)?	Esta responsabilidad recae sobre el CESTIC (Centro de Sistemas y Tecnologías de la Información y las Comunicaciones. En cualquier caso, será preciso buscar un equilibrio entre el nivel de ambición (que aumenta la superficie de exposición) y los riesgos asumidos. Siempre debe primar la SEGURIDAD.

2	6	Si las transmisiones del tipo que sean dependen del espectro electromagnético, que es un recurso finito, cada vez más escaso, en el que la demanda aumenta sin cesar. No se antoja prioritario dominar EMS que es el soporte para el resto de operaciones?	Efectivamente, si perdemos el control del EMS, perdemos no solo la capacidad de mando y control. Todas las actividades en el entorno táctico se verían afectadas: Inteligencia, fuegos, logística… Quedaríamos "ciegos y mudos", al no poder recibir información ni emitir órdenes. En mi opinión, tan importante es ocupar y controlar el terreno o el espacio aéreo como el EMS. La superioridad en el enfrentamiento, también se libra en el dominio ciberespacial, al igual que ocurre en el resto. Las medidas de coordinación y el uso de tecnología cada vez más avanzada, permite obtener un mayor rendimiento del espectro.
2	7	¿el ejército español usa redes MANET creadas específicamente para España o la OTAN, o se basa en soluciones comerciales tipo TRIAD o DTC?	Nuestro modelo pasa por sistemas MANET y FANET, con estándares militares.
2	8	Las fuerzas rusas en Ucrania sufren las perturbaciones propias limitando sus acciones. ¿Es esto extrapolable a los ejércitos occidentales? ¿La guerra electrónica propia podría condicionar las operaciones terrestres?	Buena pregunta. La clave está en realizar una perfecta GESTION DEL ESPECTRO, centralizada, completa y apoyada por buenas herramientas. La aparición del concepto de Operaciones Electromagnéticas (EMO) viene en parte a buscar una solución a este problema, al coordinar EW, SIGINT y Gestión del Espectro. Hay que evitar el "fuego fratricida electromagnético", si se me permite la expresión. Una mala gestión del uso del espectro, indudablemente afecta. Al igual que hay que adoptar medidas para evitar daños por fuego propio, en el espectro sucede algo parecido.
2	9	Con 12 naciones participantes en el cuartel general de la OTAN de Valencia, ¿cómo se asegura la interoperabilidad técnica?	Las 12 naciones aportan personal al Cuartel General de forma permanente. En el trabajo diario la interoperabilidad se consigue porque se usan los medios que proporciona España como país "marco". Esto supone que los oficiales multinacionales deben familiarizarse con los CIS que proporciona España, siendo el caso más importante el de nuestro sistema de conciencia situacional: SIMACET-Antares en su día, hoy Prometeo. Esto se soluciona con instrucción en el día a día y adiestramiento en los ejercicio. Respecto a operaciones, se está imponiendo el estándar FMN que mencioné en una de las trasparencias. Cada nación aporta su red, que debe cumplir los criterios FMN y que debe pasar una "certificación" en algún ejercicio de interoperabilidad, como por ejemplo el ejercicio STEADFAST COBALT 2024. Por último, el escalón superior debe proporcionar al inferior unos elementos mínimos de su propia red (Minimum Military Requirements, MMR) para asegurar la comunicación. La necesidad de disponer de estos elementos es la que determina el volumen de medios y personal del MATRANS, quien debe asegurar no sólo las necesidades de enlace internas del NRDC-ESP, sino el enlace con los subordinados.
2	10	En el nuevo concepto de puestos de mando que has mencionado no has mencionado el uso de instalaciones fijas dentro de la zona de operaciones ¿no lo contempláis?	Sí se contempla. Tradicionalmente hemos utilizado tiendas porque debíamos ser completamente autónomos y porque los ambientes eran permisivos o degradados, no de alta intensidad. Las instalaciones fijas proporcionan disponibilidad, ocultación y/o enmascaramiento y cierto grado de protección física, que son más apropiados en el escenario convencional. De hecho, en el ejercicio VALIANT LYNX, los diferentes módulos se establecieron en tiendas, en edificios y en tiendas ocultas bajo estructuras fijas, precisamente para probar la versatilidad. Por último añadir que la búsqueda de tecnologías inalámbricas también es pensando en reducir los tiempos de cableado de infraestructuras fijas con paredes, puertas y escaleras (por ejemplo) que no se van a conocer con mucha antelación, no como sucede con las tiendas que son módulos perfectamente conocidos con soluciones ya desarrolladas para tender los cables.

2	11	Si ya en 2021 el concepto CEMA se aplicaba en el NRDC-ESP, si fue uno de los requisitos para la certificación como WFC, otros estados miembros ven la necesidad y lo implementan a su nivel, No es difícilmente entendible que la OTAN no lo aplique oficialmente?	La OTAN como organización es muy grande y tiene mucha inercia. Del mismo modo que hay partidarios del concepto CEMA, hay corrientes de opinión que distinguen claramente las actividades cibernéticas de las electromagnéticas. Eventos como el de Jaén ayudan a difundir las ideas. La formación de doctrina es "jerárquica" y normalmente va de arriba hacia abajo. El concepto CEMA es mucho más fácil de entender o asimilar en el nivel táctico y terrestre en particular que en otros y por tanto se está abriendo camino de abajo hacia arriba. La A de la OTAN es de Atlántico, que es un mar y el peso de lo marítimo y lo Aéreo en OTAN es muy importante. Por último la OTAN está compuesta por 32 naciones con sensibilidades y capacidades muy distintas, aunque sean dos pesos pesados como EEUU y Reino Unido los principales abogados del CEMA, todavía son pocos.
2	12	¿Cómo se protegen las fuerzas propias si cada soldado tiene un móvil, aplicaciones, redes sociales, etc.?	Primeramente, con concienciación sobre su uso. Este aspecto se trata en nuestras sesiones de concienciación. También será preciso llegar a limitar o prohibir su uso en determinadas circunstancias, como se hace para acceder a áreas de información clasificada. Tal vez cuando uno sabe que su móvil puede ser un objetivo del fuego enemigo, y también el de sus compañeros, su actitud y comportamiento sea diferentes. Esto es una realidad y está pasando en Ucrania. Puede ver este link. https://www.rfi.fr/es/europa/20230104-ucrania-mosc%C3%BA-reconoce-la-muerte-de-decenas-de-soldados-rusos-localizados-por-sus-celulares.
2	13	¿Hasta qué punto la inteligencia artificial es un activo en las operaciones de su regimiento y qué técnicas son las más empleadas dentro del aprendizaje automático?	Sin ser un experto en I/A y las técnicas más adecuadas (eso no lo puedo contestar), debemos pensar que esa necesidad extensiva e intensiva del uso del espectro, supone una ventana de oportunidad para los combatientes del dominio ciberespacial, que implícitamente impone a las unidades de EW la necesidad de tener que absorber una cantidad de información muy superior a la que es posible gobernar sin automatizaciones y el empleo de herramientas y algoritmos que permitan la vigilancia del espectro y, más importante, su explotación en tiempo útil. Medidas de traducción y transcripción de emisiones, identificación de indicativos, vocablos típicos, punto del terreno, reconocimiento de voces, etc. También identificar medidas de decepción y engaño electrónico y eliminarlas. Si hablamos de perturbación, podemos, con esa información de la situación del campo de batalla, perturbar en el momento más adecuado, las bandas de frecuencia idóneas, con la potencia precisa y por el tiempo justo, para no incidir en comunicaciones propias. También debemos pensar que puede contribuir a la decepción del adversario, emitiendo desde ubicaciones falsas, haciendo creer así que hay un puesto de mando donde no lo hay, también mediante la reemisión de conversaciones desde otras ubicaciones, para dificultar que localización adquirida en la correcta, etc., sin intervención humana. Todo con el objetivo de no dar un dato único al adversario y que este precise de comprobaciones adicionales por otros medios, que en definitiva supongan una ralentización en su proceso de obtención y elaboración de información; y por consiguiente afectar a su ciclo de decisión. También es importante la contribución de la I/A a la gestión propia del uso del espectro electromagnético.

3	1	¿Cómo puede “ayudar” la tecnología cuántica en la ciberseguridad? Y, ¿qué riesgos principales se considera que puede presentar?	La tecnología cuántica tiene un impacto significativo en la ciberseguridad, tanto a favor, "ayudando", como en contra. Por una parte, la criptografía cuántica se está comenzando a utilizar en redes de comunicación para proteger información clasificada militar, gubernamental o transacciones financieras. Sin embargo, actualmente el foco principal en la criptografía está en los algoritmos denominados postcuánticos, que sirven para hacer frente, en el corto o medio plazo, a la amenaza de la aparición de computadores cuánticos cristológicamente relevantes que podrán romper los sistemas de criptografía asimétrica y debilitar los de criptografía simétrica y firmas hash. Por otra parte, la computación cuántica proporciona velocidad de cálculo y permite resolver problemas matemáticos complejos más rápido incluso que los superordenadores convencionales, lo cual permite la aplicación de algoritmos más avanzados para proporcionar capacidades de ciberseguridad más robustas. Además, las aplicaciones de la tecnología cuántica permiten mejorar la seguridad de las comunicaciones. En particular se está avanzando en el intercambio seguro de claves sobre redes de fibra óptica y satélite para conocer con un altísimo grado de seguridad si las claves intercambiadas entre dos interlocutores han sido interceptadas (y desecharlas en ese caso), si bien todavía se encuentra en un grado de madurez de la implementación principalmente experimental, aunque empiezan a aparecer soluciones prácticas. En el extremo opuesto, la tecnología cuántica también plantea riesgos para la ciberseguridad. Los algoritmos de criptoanálisis cuántico ejecutados sobre ordenadores cuánticos cristológicamente relevantes son capaces teóricamente de romper sistemas criptográficos actuales, como los mecanismos de cifrado RSA y de curvas elípticas ECC, amenazando gravemente la confidencialidad de los datos. En segundo lugar, el intercambio de claves cuánticas puede ser objeto de interceptación, por lo que sin un algoritmo suficientemente seguro para hacerlo, como podría ser el BB84, adaptado a las particularidades de la tecnología cuántica, la seguridad de las comunicaciones podría verse comprometida. Existen otros riesgos más generales como el espionaje cuántico aprovechando el fenómeno de la teleportación cuántica, que teóricamente podría permitir espiar comunicaciones sin posibilidad de ser detectados, o el ataque a los sistemas de cadenas de bloques como Blockchain, que podría verse comprometido al romperse en un tiempo manejable la criptografía que permite garantizar la integridad de las cadenas de bloques, por poner algunos ejemplos.
3	2	En caso de caída de los satélites, ¿qué sistema podría emplear para mantener la navegación y localización?	Es muy difícil, incluso en caso de conflicto, la caída de todos los satélites pues cada constelación consta de más de 20 o incluso 30 satélites y hay varias constelaciones que hoy en día gran parte de los receptores las utilizan simultáneamente (GPS, Galileo, Glonass, etc.). En un futuro estas constelaciones también estarán aumentadas con lo que se denomina LEO PNT, que son otras constelaciones con satélites de baja órbita (satélites a unos cientos de kilómetros sobre la superficie terrestre). Esto se complementa además con señales terrestres, por ejemplo, 5G/6G e hibridación con otros sensores (inerciales, odómetros en vehículos, etc.). La combinación de todas estas funcionalidades que aseguran la disponibilidad en cualquier circunstancia de posición, navegación y tiempo es lo que se denomina PNT robusto o PNT resiliente.