Capítulo octavo

Las nuevas capacidades ISR de la OTAN

José Luis Fernández Martín

Resumen

El presente artículo tiene por objeto analizar y conocer las novedosas capacidades ISR que aporta el sistema UAV HALE *Global Hawk,* adquirido recientemente por la OTAN mediante financiación común, conocido como RQ-4D e identificado en la Alianza como *Alliance Ground Surveillance System* o Sistema de Vigilancia Terrestre de la Alianza (AGS).

El objeto de estudio es conocer las condiciones necesarias para que el AGS pueda cumplir su misión en función del nivel de amenaza en el escenario donde tenga que desarrollar su misión. Para ello, la frontera este de Europa con la Federación de Rusia es el mejor escenario para el estudio de la cuestión.

Consecuentemente, en este trabajo de divulgación se pretende ahondar en el conocimiento del Global Hawk RQ-4D y de las capacidades defensivas rusas a las que se debe enfrentar. Adicionalmente, el estudio y análisis pretende discernir acerca de las posibles aproximaciones que la OTAN podría seguir para contraponerse al sistema defensivo ruso.

Palabras clave

Antiacceso y denegación de área (A2/AD), Sistema de vigilancia terrestre de la Alianza (AGS), Global Hawk, ISR conjunto (JISR), Fuerza Aeroespacial rusa (Vozdushno-Kosmicheskiye Sily-VKS).

NATO'S new ISR capabilities

Abstract

The purpose of this article is to analyze and learn about the new ISR capabilities provided by the HALE Global Hawk UAV system, recently acquired by NATO through joint funding, known as RQ-4D and identified in the Alliance as Alliance Ground Surveillance System (AGS).

The aim of the study is to understand conditions necessary for the AGS to fulfill its mission based on the level of threat in the scenario where it has to carry out its mission. For this purpose, the eastern border of Europe with the Russian Federation is the best scenario for studying the problem.

Consequently, this work aims to deepen the knowledge of the Global Hawk RQ-4D and the Russian defensive capabilities that has to face. In addition, the study aims to identify the possible approaches that NATO could take to oppose the Russian defensive system.

Key words

Anti-access/Area Denial (A2/AD), Alliance Ground Surveillance (AGS), Global Hawk, Joint Intelligence, Surveillance and Reconnaissance (JISR), Russian Air Force (Vozdushno-Kosmicheskiye Sily - VKS).

1. Introducción

Desde la crisis de Crimea en 2014, las tensiones entre los países miembros de la OTAN[1] y la Federación de Rusia –en adelante FdR– se han incrementado notablemente. Submarinos rusos en aguas de soberanía nacional sueca; bombarderos Tu-160 sobre territorio europeo, cruce ilegal de migrantes por la frontera de Polonia y ciberataques contra instituciones de la UE[2] son solo algunos ejemplos de las actividades de «Guerra Híbrida» en espacios de soberanía europeos que Rusia ha venido intensificando desde la invasión de Ucrania en 2014.

> La agresión de 2014 fue el detonante que produjo el cambio de visión geoestratégica de EE. UU. y Europa respecto a la FdR. Además, antes de este nuevo paradigma, las relaciones políticas y comerciales entre Europa y la Federación de Rusia eran positivas y vislumbraban un futuro de estabilidad. Lamentablemente, después del 2014, la OTAN convino revisar su modelo estratégico en la frontera este de Europa en previsión de lo que en febrero de 2022 pasaría.
>
> Esta situación de inestabilidad en Ucrania provocó que el secretario general de la OTAN instara al presidente de Rusia a dar una prueba de transparencia sobre sus actividades militares y advirtiera en rueda de prensa el 15 de noviembre de 2021 que: «Toda nueva provocación o acción agresiva por parte de Rusia sería muy preocupante (Stoltenberg, 2021).

Las advertencias a la FdR por parte de la comunidad internacional no evitaron que el presidente Putin ordenara la invasión de toda Ucrania el 24 de febrero de 2022. Nuevamente, el secretario general de la OTAN, en una declaración sobre el ataque de Rusia contra Ucrania, manifestó:

> Condeno enérgicamente el ataque temerario y no provocado de Rusia contra Ucrania. Un ataque que pone en peligro innumerables vidas civiles. Una vez más, a pesar de nuestras reiteradas advertencias y de nuestros incansables esfuerzos por ejercer la diplomacia, Rusia ha elegido el camino de la agresión contra un país soberano e independiente. Esta es una grave violación del derecho internacional y una grave amenaza para la seguridad euroatlántica. Hago un llamado a Rusia para que

[1] Organización del Tratado del Atlántico Norte.
[2] Unión Europea.

> cese su acción militar de inmediato y respete la soberanía y la integridad territorial de Ucrania. Los aliados de la OTAN se reunirán para abordar las consecuencias de las acciones agresivas de Rusia. Apoyamos al pueblo de Ucrania en este terrible momento. La OTAN hará todo lo necesario para proteger y defender a todos los Aliados (Stoltenberg, 2022).

En este nuevo panorama geoestratégico, más que nunca, los servicios de información e inteligencia tiene un papel muy relevante en la toma de decisiones del poder político, pues alertan sobre situaciones que puedan provocar una crisis. De forma particular para la Alianza, los medios JISR[3] como el AGS (Alliance Ground Surveillance) permiten satisfacer en tiempo casi real aquellas necesidades de inteligencia que puedan surgir en una hipotética guerra en la zona euroatlántica.

Por consiguiente, la información y la inteligencia tienen una importancia capital en un mundo globalizado y conectado en tiempo real. La decisión política tiene que estar basada en información creíble, relevante, contrastada, oportuna y sobre todo veraz. Consecuentemente, la legitimidad de las acciones derivadas de las decisiones políticas tiene que ser incuestionable.

En el caso de la OTAN, como organización, y de los países que la integran, con intereses comunes, se rigen por los principios de defensa colectiva y seguridad compartida. Estos principios se reafirmaron en la cumbre de la OTAN que tuvo lugar en Cardiff en 2014. Desde entonces, la OTAN ha impulsado una estrategia para potenciar sus capacidades de obtención de información en forma de capacidades ISR[4].

Sin embargo, muchas analistas militares se pueden preguntar si realmente las nuevas capacidades ISR de la alianza, materializadas con la plataforma RQ-4D, pueden cumplir en el escenario actual el cometido de obtener información creíble, relevante, contrastada, oportuna y veraz para asesorar a la cúpula política y militar de la OTAN.

2. El Sistema AGS

El Sistema de Vigilancia Terrestre de la Alianza, o AGS de sus siglas en inglés, permite al comandante conformar una imagen

[3] Inteligencia, Vigilancia y Reconocimiento conjuntos (JISR) de sus siglas en inglés.
[4] Inteligencia, Vigilancia y Reconocimiento (ISR) de sus siglas en inglés.

lo más completa posible de la situación en el campo de batalla, o conocer de primera mano qué es lo que está sucediendo en aquellos lugares en los que las autoridades políticas y militares tienen necesidades de información.

Este sistema de obtención se conforma de cinco RPA[5] RQ-4D, las estaciones de control, y el sistema de mando y control.

2.1. Misión

Según la Agencia de Gestión del AGS (2022), la misión principal del sistema de Vigilancia Terrestre de la Alianza es realizar vuelos de larga duración para vigilar la superficie terrestre o marítima, con el fin de proporcionar en tiempo casi real información sobre fuerzas amigas, neutrales y adversarias que sean de interés y utilidad operativa en todos los niveles de mando, desde el nivel político hasta el táctico. Por consiguiente, su finalidad es obtener un conocimiento de la situación antes, durante y después de las operaciones realizadas por la OTAN.

Adicionalmente y pese a que el procedimiento de empleo de este sistema está asociado principalmente al nivel estratégico y operacional, este puede apoyar las operaciones en el nivel táctico con ocasión de oportunidad.

2.2. Concepto de empleo

Aunque la adquisición del RQ-4D por parte de la OTAN empezó en 2019, EE. UU. lleva poniendo a disposición de la Alianza las capacidades de este RPA desde hace muchos años.

Según la NAGSF (2020), el RQ-4D se puede emplear en todo el espectro de las operaciones. Es decir, desde tiempo de paz hasta crisis que evolucionan a conflictos armados. El AGS, como sistema, proporciona un conocimiento de la situación que permite apoyar a las operaciones que se desarrollen en los dominios terrestre, marítimo y aéreo.

En estas condiciones, se identifican cinco tipos de misiones que puede desarrollar el sistema AGS:

- *Strategic Indications and Warnings* o indicadores y alertas estratégicas.

[5] Remotely Piloted Aircraft o aeronave pilotada remotamente.

- *Joint Operational Intelligence Gathering* u obtención de inteligencia en operaciones conjuntas.
- *Direct Support to Land forces*, *Maritime Forces AIRCOM*[6] o apoyo directo a las operaciones terrestres, marítimas o al mando aéreo de la OTAN.
- *Support to Special Operations Forces* o apoyo a las operaciones de fuerzas especiales.
- *Humanitarian and disaster relief* o asistencia a crisis humanitarias.

2.3. Sistemas y capacidades

2.3.1. Unidad de obtención

La Unidad de obtención está formada por un segmento aéreo, un segmento terrestre y un segmento de apoyo (NATO, 2021)which will give commanders a comprehensive picture of the situation on the ground. A group of 15 Allies is procuring the AGS system comprised of five NATO RQ-4D Phoenix remotely piloted aircraft and the associated European-sourced ground command and control stations. NATO will then operate and maintain them on behalf of all NATO Allies. The AGS NATO RQ-4D aircraft is based on the US Air Force Block 40 Global Hawk. It has been uniquely adapted to NATO requirements to provide a state-of-the-art Intelligence, Surveillance and Reconnaissance (ISR.

El segmento aéreo consta de cinco aeronaves pilotadas remotamente Global Hawk RQ-4D y elementos de control de vuelo del RPA. La aeronave tiene una longitud de 14,5 m, una altura de 4,7 m, una envergadura de 39,8 m y un peso de 6,781 kg, características que lo sitúan en los RPAS[7] de clase III. La velocidad máxima es de 575 Km/h, y puede alcanzar una altura máxima de vuelo de 60.000 pies (Kumar, 2021).

La autonomía de vuelo permite operar el RQ-4D durante 34 horas ininterrumpidamente (Osborn, 2021a), lo que posibilita cambiar las tripulaciones de vuelo sin que afecte a la misión del *Global Hawk*.

6 Mando Aéreo de la OTAN.

7 Remotely Piloted Aircraft System.

El RPA está equipado con el radar de última generación MP-RTIP[8]. Este sensor puede funcionar en modalidad M/GMTI[9] y como radar de apertura sintética (SAR) para proporcionar información de vigilancia e inteligencia geoespacial (GEOINT) casi en tiempo real de los dominios terrestres y marítimos (Vizcarra, 2018).

El sensor MP-RTIP permite obtener imágenes SAR con las que se pueden identificar objetivos a más de 200 km. De esta manera, es posible mantener las aeronaves lejos del alcance de los IADS[10] enemigos, o incluso cumplir su misión desde espacios aéreos de soberanía nacional de países aliados. Este sensor también posibilita crear patrones de vehículos u objetos en movimiento con la tecnología GMTI (Raimundo *et al.*, 2020).

Las capacidades del sistema permiten realizar misiones de obtención de información o de vigilancia en zonas de hasta 100.000 km^2, superficie que equivale a la extensión de terreno ocupada por Islandia.

El segmento terrestre consta de una serie de estaciones terrestres en configuraciones móviles y transportables, capaces de habilitar un enlace digital y procesamiento de datos, así como de dotar al sistema de capacidades de explotación e interfaces para la interoperabilidad (NATO, 2021)which will give commanders a comprehensive picture of the situation on the ground. A group of 15 Allies is procuring the AGS system comprised of five NATO RQ-4D Phoenix remotely piloted aircraft and the associated European-sourced ground command and control stations. NATO will then operate and maintain them on behalf of all NATO Allies. The AGS NATO RQ-4D aircraft is based on the US Air Force Block 40 Global Hawk. It has been uniquely adapted to NATO requirements to provide a state-of-the-art Intelligence, Surveillance and Reconnaissance (ISR.

Todas las operaciones de despegue, misión ISR y aterrizaje se controlan desde la MOB[11] o base principal de operación donde se encuentra el Centro de Operaciones del AGS en Sigonella (Italia) o NAOC[12] de sus siglas en inglés (Raimundo *et al.*, 2020).

8 Multi-Platform Radar Technology Insertion Program.
9 Indicador de objetivo móvil marítimo/terrestre.
10 Integrated Air Defense System.
11 Main Operations Base.
12 NATO AGS Operations Centre.

El segmento de apoyo incluye instalaciones dedicadas al respaldo de la misión en la base de operaciones principal de la NAGSF en Sigonella (NATO, 2021)which will give commanders a comprehensive picture of the situation on the ground. A group of 15 Allies is procuring the AGS system comprised of five NATO RQ-4D Phoenix remotely piloted aircraft and the associated European-sourced ground command and control stations. NATO will then operate and maintain them on behalf of all NATO Allies. The AGS NATO RQ-4D aircraft is based on the US Air Force Block 40 Global Hawk. It has been uniquely adapted to NATO requirements to provide a state-of-the-art Intelligence, Surveillance and Reconnaissance (ISR.

2.3.2. Centro de explotación

En el centro de explotación (PED), donde se procesa y analiza la información obtenida por el RPA, se producen y distribuyen unos productos preliminares de inteligencia. Este centro se encuentra dentro del NAOC (Raimundo *et al.*, 2020).

La información o elementos de información basados en imágenes y vídeos, por sí sola, puede llegar a carecer de valor militar si no se procesa e interpreta por analistas expertos en la materia. Por esta razón, el centro de explotación aporta el valor añadido a la información obtenida por la plataforma aérea RQ-4D.

2.3.3. Elemento desplegable

Como se ha visto hasta ahora, el sistema AGS ofrece enormes y variadas posibilidades de empleo. Esta variedad de misiones justificaría que la NAGSF fuera empleada en sitios remotos. Este hipotético empleo, en palabras del comandante del Ejército del Aire José A. Arrieta (2020), motivó que se tuviera que contar con un elemento de mando y control desplegable que sirviera a su vez como respaldo del NAOC en caso de que quedara inoperativo. Finalmente, se optó por la incorporación a las capacidades de la NAGSF de dos elementos de control del RQ-4D desplegables (DUCE[13]) y de dos tipos de entidades PED desplegables: seis MGGS[14] y dos TGGS[15], estas últimas con mayores capacidades operativas que las MGSS.

[13] Deployable Control Element.
[14] Mobile General Ground Station.
[15] Transportable General Ground Station.

2.3.4. Centro de entrenamiento y formación

Según el comandante del Ejército del Aire Miguel A. Palacios (2020), la NAGSF cuenta con una unidad de entrenamiento que es responsable de la formación y adiestramiento del personal que sirve al sistema AGS.

Pese al carácter novel de la NAGSF, los miembros de esta unidad han conseguido alcanzar un nivel de destreza y de experiencia significativo. Consecuentemente, esta unidad de entrenamiento también está formando a personal ajeno a la NAGSF en el campo del ISR conjunto a propuesta de las naciones aliadas (Stewart, 2020).

Además, un pequeño destacamento de la NAGSF está presente en SHAPE[16] y en la sede del Mando Aéreo Aliado (AIRCOM) como enlace para cuestiones operativas relacionadas con JISR y la integración del RQ-4D en las operaciones de la Alianza.

3. A2/AD ruso

Es importante aclarar que el concepto A2/AD no existe en la doctrina militar rusa. Al igual que la guerra híbrida, el A2/AD es un constructo occidental impuesta al pensamiento militar ruso sin valor intrínseco (Giles y Boulegue, 2019). Sin embargo, los foros militares de países occidentales y la propia OTAN son aceptantes de una realidad doctrinal que tiene por finalidad sintetizar en un modelo único un compendio de capacidades defensivas interoperables e íntimamente relacionadas. Por lo tanto, se parte de un marco teórico aceptado en el que se identifica un concepto para describir las capacidades que la FdR dispone para limitar o impedir la proyección del poder militar de la Alianza sobre regiones que están bajo su influencia o protección.

De forma genérica (Erdogan, 2018), el antiacceso se debe entender como aquellas acciones y capacidades, generalmente de largo alcance, diseñadas para evitar que una fuerza oponente entre en una zona o área defendida. Las acciones antiacceso tienden a atacar predominantemente a las fuerzas que se acercan por aire y por mar. Sin embargo, también pueden atacar a los sistemas con capacidades cibernéticas, fuerzas espaciales u otras fuerzas que las apoyan.

[16] Supreme Headquarters Allied Powers Europe.

De igual modo, la denegación de área se entiende como el conjunto de acciones y capacidades, generalmente de menor alcance que las antiacceso, diseñadas para limitar la libertad de acción del adversario dentro de la zona de operaciones. Las capacidades de denegación de área se dirigen al adversario en todos los dominios. La distinción entre antiacceso y denegación de área se difumina con facilidad en la aplicación, y pueden llegar a solaparse o sucederse. Además, es posible emplear muchos medios en el cumplimento de ambos fines (Erdogan, 2018).

El objetivo de este sistema es evitar que un adversario –EE. UU. o la OTAN– entre en la zona de influencia rusa mediante el empleo de armas de largo alcance, y niegue su libertad de acción en el caso de que la fuerza oponente consiguiera entrar en territorio ruso. Para llevar a cabo la estrategia A2/AD, Rusia se sirve de todo su arsenal de misiles, incluidos misiles tierra-aire, misiles balísticos antibuque, misiles de crucero, de sus sistemas de artillería de largo alcance y de sus sistemas de cohetes de lanzamiento múltiple (MLRS). Adicionalmente, completa su sistema defensivo con minas, RPAS, guerra electrónica, acciones en el ciberespacio y guerra submarina.

Una parte importante de los sistemas A2/AD es la denegación de acceso al espacio aéreo. Para ello (Erdogan, 2018), la FdR cuenta con un sistema de defensa aérea integrada (IADS) de múltiples capas, compuestos por modernos aviones de combate/ataque y misiles tierra-aire, fijos y móviles. Como se ha visto, todos estos sistemas son complementados con unidades de guerra electrónica y ciberespaciales. Es reseñable destacar la labor persistente de los sistemas de guerra electrónica y ciberespaciales que pueden funcionar ininterrumpidamente a voluntad del operador, sin más limitación que las propias de mantenimiento.

La propaganda rusa se ha encargado en los últimos años de difundir las capacidades que Rusia ha ido adquiriendo para oponerse a cualquier amenaza que osara venir del lado oeste de Europa. Según el Ministerio de Defensa ruso y otros medios de comunicación, Rusia dispone de medios ISR estratégicos capaces de detectar, localizar, identificar y seguir a las aeronaves y buques de superficie a gran distancia. Por otro lado, Rusia está desarrollando misiles antibuque –APR-3ME– de nueva generación capaces de destruir buques de la OTAN a mayor distancia. Estas nuevas capacidades no son más que una muestra de que Rusia ha llevado a las cotas más altas el desarrollo de sus sistemas A2/AD en la última década (Navy Recognition, 2021).

3.1. Principales sistemas del A2/AD ruso

Las plataformas móviles de misiles tierra-aire 9K317 Buk-M2[17], S-300[18] y S-400[19] son los sistemas que mayor alcance tienen de todos los que componen la defensa aérea de la VKS o Fuerza Aeroespacial de la FdR. Se debe destacar que el sistema S-400 puede llegar a tener un alcance de hasta 400 km, mientras que el alcance del S-300 se reduce a 200 km (Smura, 2016).

El Ministerio de Defensa ruso afirma que el misil de largo alcance más avanzado del S-400, el 40N6, tiene un alcance cercano a los 400 km y una altitud máxima de hasta 185 km. El S-400 se considera uno de los sistemas de defensa aérea de largo alcance más avanzados del mundo, aunque se valora que no es tan efectivo si los aviones vuelan a baja cota (Gady, 2018).

La Fuerza Aeroespacial (VKS) la integran unidades misiles de defensa aérea –en los que se incluye los misiles antibalísticos– y unidades de la Fuerza Aérea. Pese a que el PIB ruso es similar al español, las políticas de defensa de la FdR hacen que se destine más de un 3% de él al presupuesto de defensa. Este hecho permite que la VKS disponga de más de 850 aviones de combate y de 5 regimientos de defensa aérea (IISS, 2021).

Según Kofman (2020b), analista militar especializado en la región Rusa, la mayoría de la flota aeroespacial del VKS se ha modernizado o reemplazado en el último decenio con la finalidad de poder enfrentarse a cualquier amenaza aérea que trate de penetrar en el espacio aéreo ruso.

Lo mismo sucede con los regimientos de defensa aérea desplegados en zonas clave para impedir el acceso a fuerzas aéreas de la OTAN. Junto al despliegue de un batallón S-400 debe desplegar una unidad de defensa aérea de baja cota, tipo Pantsir S-1, representada en la figura 1, cuya misión principal es proteger a los batallones S-400 del ataque de misiles crucero de la OTAN o de un ataque de supresión de defensas aéreas (SEAD).

Por otro lado, otra capacidad necesaria para complementar el IADS es la capacidad ISR conjunta o JISR. Según el informe anual del IISS[20], *The MIlitary Balance 2021* (2022), la VKS dispone de

[17] Sistema con misil de medio alcance.
[18] Sistema con misil de largo alcance.
[19] Sistema con misil de largo alcance.
[20] The International Instutute for Strategic Studies.

una gran cantidad de medios ISR. Sin embargo, en relación con medios UAV[21], encuentra su techo tecnológico y operacional en sus sistemas MALE[22] Forpost (Searcher II). Es decir, medios que pueden considerarse de aplicación en el nivel de mando operacional, pero que se ven limitados tanto en el tiempo como en la altura de vuelo.

Figura 1. Sistema S-400 con batería Pantsir-S-1. Fuente: https://israelnoticias.com/militar/israel-pantsir-s1-rusia-siria/

En cuanto a la defensa costera, la Fuerza Naval rusa dispone de los sistemas móviles K-300P Bastion-P. Su modalidad de empleo está concebida para atacar a los buques de superficie que amenacen la costa rusa. Este sistema está equipado con misiles supersónicos P-800 Oniks/Jachont, cuyo alcance se estima en unos 300 km (Smura, 2016).

Los submarinos balísticos son otro elemento destacado del sistema A2/AD, estas naves tienen la capacidad de negar el acceso a las fuerzas de la OTAN que intenten amenazar las costas rusas a través de las cuencas que dan acceso a ellas. Estos submarinos tienen la capacidad de destruir objetivos terrestres con misiles de crucero Kalibr, con un alcance cercano a los 1500 km.

El desarrollo de unidades submarinas y sistemas de defensa de costa representa la continuación de la estrategia de «bastión marítimo» de la Guerra Fría, es decir, la creación de enclaves marinos controlados por las flotas de buques de superficie y sub-

21 Unmanned Aerial Vehicle.

22 Medium Altitude Long Endurance.

marinos, fuertemente defendidos con minas submarinas y unidades de defensa de costa (Smura, 2016).

Los misiles balísticos de corto alcance Iskander complementan a los misiles superficie-superficie Kalibrs[23] y a los misiles tierra-aire S-400 y S-300, los cuales se suman a todos los desafíos a tener en cuenta por las tropas de la OTAN en caso de conflicto con Rusia (Giles y Boulegue, 2019). Los misiles Iskander tienen un alcance de hasta 500 km y pueden portar ojivas convencionales o nucleares (MDAA, 2022).

Todos los sistemas de armas basados en misiles tienen asociados radares y otros dispositivos de localización. No obstante (Kofman, 2020a), las fuerzas rusas también utilizan otros radares sobre el horizonte como los sistemas Podsolnukh-E (OTH-SW) de onda superficial de alta frecuencia, con un alcance de más de 3000 km. Estos radares se despliegan en las bases donde están destacadas las flotas rusas o en instalaciones fijas ubicadas en la Rusia profunda.

Si bien es cierto que los batallones S-400 y S-300 desplegados a lo largo de la frontera este de Europa levantan un muro imaginario aparentemente impenetrable para ninguna fuerza aérea aliada, lo cierto es que esta barrera es porosa y penetrable en aquellas zonas ciegas para el radar o donde simplemente no se produce el solape entre las unidades que componen el IADS.

No obstante, la doctrina rusa contempla que esos espacios con menos posibilidades de detección deben ser reforzados con la cobertura y protección que otorgan las capacidades de guerra electrónica de las FAS rusas.

A modo de ejemplo, es relevante mencionar que los sistemas de EW Krasucha-4, el Moscow-1 y Borisoglebsk-2 son especialmente significativos, ya que son capaces de producir interferencias en las señales de radar, así como en las señales emitidas por satélites, aviones de reconocimiento, alerta temprana, drones y estaciones terrestres de control remoto hasta los 300 km de alcance (Smura, 2016).

3.2. Distribución del sistema ruso A2/AD

Del estudio y análisis realizado de todos los distritos militares en los que se organizan las FAS rusas, se puede asegurar que el

[23] Pueden ser lanzados desde submarino o buques de superficie.

Distrito Militar Occidental acoge a la fuerza más numerosa y mejor equipada de Rusia. El despliegue de fuerzas parece indicar que la prioridad de la FdR es fortalecer su flanco occidental, en el que Ucrania representa el mayor foco de tensión en su frontera oeste.

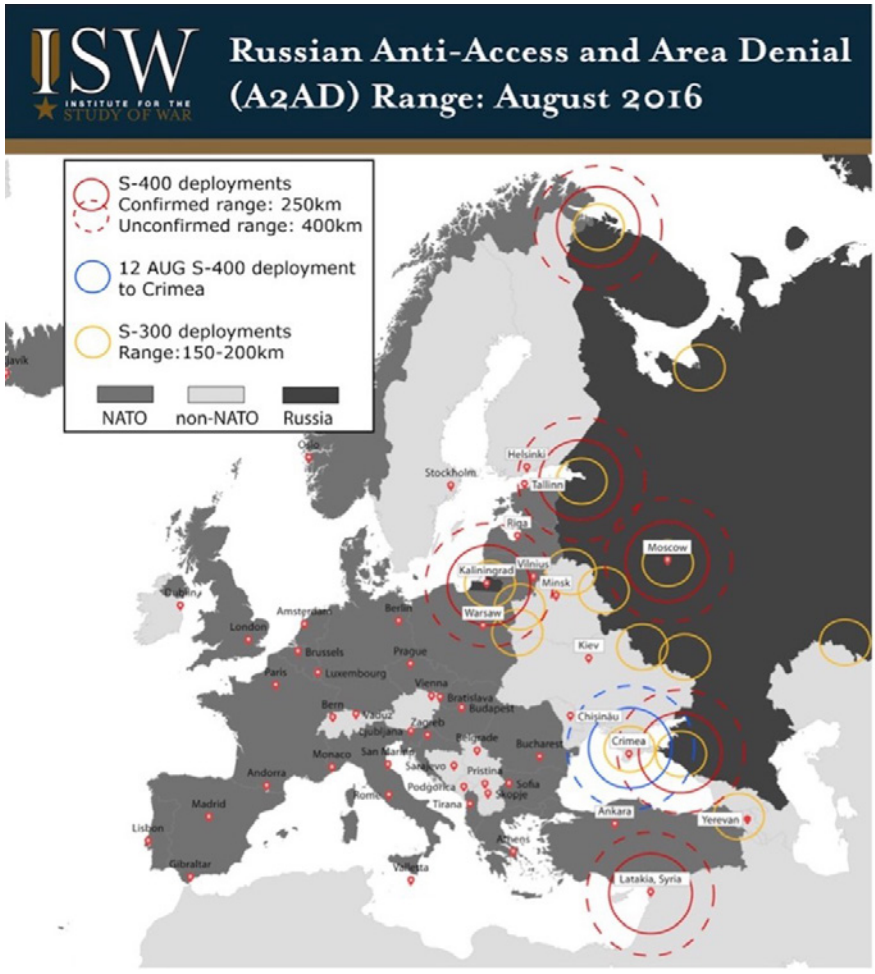

Figura 2. Aproximación del posible despliegue de unidades rusas que contribuyen a la defensa y denegación de área. Fuente: ISW

En los últimos años, el Ministerio de Defensa ruso ha aprobado el despliegue de un conjunto de unidades a lo largo de toda la frontera con Europa, como el descrito en la figura 2, que contribuyan a reforzar la estrategia A2/AD. Los enclaves más relevantes, por representar una verdadera amenaza para la Alianza, son Siria, Crimea, el mar Negro, Kaliningrado, el mar Báltico, el Ártico y el Cáucaso sur.

3.2.1. Siria

Los sistemas A2/AD desplegados en Siria cubren gran parte del Mediterráneo oriental y el mar Negro. Este despliegue sugiere que la FdR considera que las fuerzas de la Alianza son una amenaza creíble a través del Mediterráneo oriental. Estos medios desplegados en Siria, sin el apoyo de la Rusia continental, no son determinantes, pero son suficientemente capaces de complicar la entrada a Rusia de las fuerzas estadounidenses y aliadas por esta región (Giles y Boulegue, 2019).

Pese a que el presidente Putin retiró de Siria en 2016 una parte sustancial del contingente ruso, sobre todo aviones de combate y helicópteros, mantuvo las bases de Tartus y Latakia, y la base aérea de Hmeymim, situada esta última cerca de la ciudad portuaria de Latakia en Siria, defendidas todas ellas con los sistemas S-400 (Smura, 2016).

3.2.2. El mar Negro y Crimea

Desde su anexión en marzo de 2014 y su posterior militarización, Crimea se ha transformado en un puesto militar avanzado en el otro extremo de la frontera de Rusia con Europa Central, a imagen y semejanza de Kaliningrado. Desde el puerto marítimo de Sebastopol y a través de la península, las fuerzas armadas rusas han establecido un entorno A2/AD integral y de múltiples capas destinado a desafiar a los aliados de la OTAN en el mar y en el cielo (Giles y Boulegue, 2019).

Las unidades que contribuyen significativamente a la conformación del sistema A2/AD en la península de Crimea son la 128.ª Brigada de Defensa de Costa, la 19.ª Brigada de aviación naval de la Flota rusa del mar Negro (Smura, 2016). Todo este despliegue de unidades habilita el sistema A2/AD con los misiles S-300PM, S-400 (figura 3), así como los misiles de crucero Iskander y los K-300P Bastion-P.

El principal objetivo de Moscú en esta región es mejorar las capacidades antimisiles y antiaéreas para establecer una zona de denegación de área en esta zona. La flota rusa del mar Negro recibió su primer sistema de guerra electrónica Murmansk-BN, con más de 5000 kilómetros de alcance, diseñado para atacar las comunicaciones satelitales militares de alta frecuencia (Sukhankin, 2021).

Figura 3. Plataforma de tiro S-400 con cuatro lanzadores en Crimea. Fuente: livejournal.com

Los sistemas de armas de la Flota del mar Negro tienen alcance sobre las unidades de defensa contra misiles balísticos de la OTAN desplegados en la Base Aérea de Deveselu en Rumania. En comparación con Kaliningrado, las capacidades rusas A2/AD en el mar Negro proporcionan una mayor profundidad estratégica (Giles y Boulegue, 2019).

3.2.3. Kaliningrado

El Óblast de Kaliningrado es una de las regiones más pequeñas de la Federación Rusa, pese a su tamaño, su relevancia dista mucho de ser insignificante debido a su localización en el mar Báltico. De esta forma, Kaliningrado se ha convertido en un enclave fundamental para la defensa de Rusia y forma parte de un arco protector que abarca el Ártico, el mar de Barents, el mar Báltico, Crimea y el mar Negro. Además, es probablemente el foco de tensión más complejo y peligroso entre la OTAN y Rusia. Consecuentemente, su ubicación facilita ejercer una disuasión estratégica sobre Europa (Westerlund, 2017). Por lo tanto, no debe sorprender la existencia de un sólido despliegue de unidades militares en Kaliningrado, despliegue que se ha incrementado significativamente a raíz de la invasión de Crimea en 2014 y de la guerra de Ucrania en 2022.

De este modo (Giles y Boulegue, 2019), el enclave de Kaliningrado se erige en un puesto avanzado de defensa que es clave para la arquitectura regional A2/AD. Los medios A2/AD en Kaliningrado crean una barrera móvil de interdicción aérea, marítima y terrestre. Combinado con los sistemas continentales, el área donde puede actuar abarca los Estados bálticos, un tercio de Polonia, Estonia, Letonia, Lituania, el sur de Escandinavia y el golfo de Finlandia.

La flota báltica de Rusia, el 11.º Cuerpo de Ejército ruso y la 44.ª División de Defensa Aérea son las fuerzas militares desplegadas en el enclave de Kaliningrado. En el Óblast de Kaliningrado posiblemente se encuentren desplegados los sistemas de misiles tierra-aire S-400, S-300, Pantsir-S y Tor-M1; los sistemas de defensa de costa Bastion-P, equipado con misiles crucero P-800 Oniks; misiles balísticos Iskander-M junto con los misiles de crucero Iskander-K, OTR-21 Tochka, lanzadores de cohetes BM-21 y Kalibr, equipado este último en buques. Adicionalmente, se encuentran desplegados aviones de ataque Su-24s y cazas Su-27s, Su-35s y Su-30MS.

Como tal, Kaliningrado se presenta como la región que debe ser neutralizada por las fuerzas de la OTAN para garantizar el acceso sin restricciones y la libertad de acción en la zona del mar Báltico. Sin embargo, en caso de crisis, Moscú probablemente desplegaría rápidamente capacidades adicionales destinadas a oponerse estas fuerzas (Giles y Boulegue, 2019), supuesto que complicaría cualquier estrategia que se concibiera para neutralizar Kaliningrado.

3.2.4. El Ártico

La región del Ártico es una de las zonas con mayor interés geoestratégico del mundo por ser uno de los lugares donde se concentra una enorme cantidad de recursos naturales, y por donde transitarán las futuras rutas marítimas que aún están por dominar (Smura, 2016). Por consiguiente, esta región, en particular la península de Kola, es prioritaria para la FdR por su interés geoestratégico.

Esta motivación, basada en intereses comerciales y de acaparamiento del sector primario en la región, justifica la creación de un mando estratégico en el Ártico, en el que se incluye a la Flota del Norte, flota que es de vital relevancia por ser una de las dos que supuestamente cuentan con submarinos nucleares.

Junto a la Flota del Norte, despliegan otras unidades que contribuyen a la defensa aérea y a la ocupación de la costa. Todas estas fuerzas desplegadas, dependientes del mando estratégico del Ártico, proporcionan defensa aérea y de costa en múltiples capas (Giles y Boulegue, 2019).

Por otro lado, el Ministerio de Defensa ruso ha realizado una inversión significativa en infraestructuras con la finalidad de construir y modernizar bases que puedan albergar unidades con SU-34 y MIG-31, así como nuevas estaciones de radar de alerta temprana, junto con sistemas de guerra electrónica.

Todas estas fuerzas desplegadas permiten crear una barrera que podría negar el acceso a las fuerzas navales y aéreas de la OTAN. Sin embargo, las actuales capacidades de interdicción de Rusia en el Ártico siguen siendo incompletas y relativamente débiles en comparación con otras regiones (Giles y Boulegue, 2019).

3.2.5. El Cáucaso sur

La región del Cáucaso meridional también contribuye a la cobertura rusa de A2/AD. En 2016, el parlamento armenio ratificó un sistema regional bilateral de defensa aérea con Moscú. El despliegue de misiles tierra-aire S-300 en el Cáucaso sur fortaleció aún más las capacidades de interdicción de Rusia sobre la parte oriental del mar Negro y su frontera con Europa (Giles y Boulegue, 2019). Con este acuerdo, la FdR ha mejorado sustancialmente su capacidad antiacceso a través de su Distrito Militar Sur.

3.3. Valoración del A2/AD ruso

Se debe entender la estrategia A2/AD como una aproximación defensiva que trata de limitar los daños ante un ataque por la frontera occidental de Rusia. Esta estrategia se basa en la integración de un conjunto de sistemas defensivos que se solapan por capas. El estudio de las distintas capas induce a pensar que, inicialmente, la primera barrera defensiva en la que se basa la estrategia rusa comenzaría en el mar. Sin embargo, el análisis de las capacidades actuales indica que la burbuja defensiva que genera el IADS de la FdR es mucho más robusta que la que se inicia desde superficie marina, sobre todo, si se tiene en cuenta que la VKS ha sufrido una profunda modernización en los últimos diez años.

Evidentemente, la fortaleza del sistema defensivo no se debe basar en métricas que analicen individualmente cada uno de los sistemas que componen las capas defensivas, sino en el conjunto de todos ellos. Por lo tanto, tampoco se puede aventurar que la debilidad del sistema A2/AD comienza en el mar, ni que su inexpugnabilidad descansa en la solidez de su IADS.

En relación con la fortaleza del IADS, se debe destacar la significativa descompensación que hay entre las capacidades de defensa aérea y la capacidad JISR. Si bien es cierto que los radares rusos les confiere una gran ventaja en la detección temprana de medios aéreos 24/7, la capacidad de detectar medios en superficie, terrestre o marina, se ve limitada y descompensada por los UAV que dispone actualmente la FdR. Consecuentemente, la limitación JISR o descompensación respecto a otras capacidades del IADS puede hacer pensar que el sistema A2/AD encuentre su límite en el nivel táctico y, como mucho, en el operacional. Es decir, que su capacidad de detección es bastante sólida en el nivel táctico, y menos robusta en el nivel estratégico y operacional.

Respecto al IADS que opera desde la región del Ártico hasta el Mediterráneo oriental, se puede concluir que el fuerte despliegue de medios de defensa aérea hace que la penetración de la frontera oeste rusa sea una misión ardua. No obstante, es posible identificar brechas en el solape de las burbujas generadas por las unidades de defensa aérea y, sobre todo, en la región fronteriza entre Finlandia y la FdR, donde parece que la densidad de unidades del IADS es más reducida.

Por otro lado, se debe destacar el papel fundamental que desempeña el enclave de Kaliningrado, una región minúscula en el corazón septentrional de Europa, donde se agrupan una cantidad desproporcionada de unidades que conforman el A2/AD. Si bien es cierto que el agrupamiento de capacidades A2/AD en Kaliningrado le convierte en la principal amenaza dentro de Europa, la propia concentración le confiere una desmesurada vulnerabilidad e indefensión ante un ataque de la OTAN, que solo se puede descartar ante la posibilidad de desencadenar una guerra nuclear.

4. Posibles aproximaciones de la OTAN

Desde la caída del muro de Berlín en 1989, la opinión pública pocas veces había sentido que el poder militar de la FdR fuera

una verdadera amenaza para Europa hasta que se produjo la invasión de Crimea en febrero de 2014 y la guerra del Donbás dos meses más tarde. Por si hubiera alguna duda, esta realidad se confirmó definitivamente con la invasión de Ucrania en febrero de 2022.

Consecuentemente, este nuevo escenario geopolítico hace pensar que la OTAN y la Unión Europea tengan razones suficientes para estudiar cómo enfrentarse a la compleja maquinaria bélica rusa, particularmente, a las capacidades antiacceso en la frontera oeste de la FdR que limitarían notablemente la libertad de acción y ejecución de la Alianza en el flanco este de Europa.

Las capacidades militares de la OTAN y la aplicación de su doctrina permiten vislumbrar un paquete de posibles contramedidas basadas en aproximaciones directas e indirectas que hagan frente al sistema A2/AD.

Los sistemas A2/AD son muy complejos y su empleo depende en gran medida del adversario y del espacio de batalla en el que se deban aplicar. En consecuencia, el análisis de cualquier aproximación de la Alianza se debe realizar desde la más sencilla, la indirecta, hasta llegar a la aproximación más completa, la directa.

4.1. Aproximación indirecta

La sorpresa es un principio del arte de la guerra que nunca ha sido cuestionado a lo largo de la historia por ningún tratadista militar. Sun Tzu (2021) fue uno de los primeros pensadores militares en sugerir que nunca se debe prescindir de la sorpresa y el engaño en la concepción de cualquier operación militar, sin olvidar que los esfuerzos no se pueden mantener indefinidamente en el tiempo. De este modo, se ha aceptado doctrinalmente que los esfuerzos no solo deben graduarse y priorizarse en función de la amenaza y la importancia en la consecución de los objetivos del comandante, sino que deben permanecer ocultos al enemigo el máximo tiempo posible.

La aproximación indirecta en el campo del ISR conjunto se debe basar precisamente en estos conceptos, sorpresa, engaño y la graduación del esfuerzo en función de la amenaza. Es evidente que esta estrategia es solo plausible gracias al desarrollo tecnológico, el cual permite obtener información de posibles adversarios con cierta discreción, aunque no exenta de ciertas limitaciones y riesgos.

El desarrollo tecnológico permite que los medios de adquisición actuales puedan obtener información de potenciales enemigos sin invadir sus espacios de soberanía. Este aspecto es importante porque permite desarrollar un plan de obtención a largo plazo sin vulnerar el derecho internacional. No obstante, solo las capacidades ISR basadas en la observación desde satélite o en la obtención de información en el dominio ciberespacial pueden tener un alcance global. El resto de las técnicas de obtención se verán limitados en su alcance mientras se apliquen en el contexto de una estrategia indirecta.

> Pese a la evolución estratégica que haya tenido la OTAN desde su creación, la «naturaleza puramente defensiva de la Alianza, el énfasis en la prevención de la guerra» (Herreros, 2008: 26) y la necesidad de mantener el *statu quo* con la Federación de Rusia, se deduce que la principal estrategia de la Alianza en el empleo que haga de sus sistemas ISR en tiempo de paz va a ser en el marco de una aproximación predominantemente indirecta.

Se debe tener en cuenta que desde 2019, la NAGSF ha estado liderando el campo de la inteligencia, la vigilancia y el reconocimiento en el ámbito de la OTAN. Dada la naturaleza aérea de la NAGSF y la labor que realiza el CAOC[24] de Torrejón, responsable de mantener el conocimiento de las actividades aéreas en el sur de la OTAN, es fundamental para la planificación y ejecución de la misión de vigilancia aérea de la unidad AGS que la NAGSF tenga una buena coordinación y compenetración con el CAOC de Torrejón (AIRCOM PAO, 2021).

Por consiguiente, se puede concluir que el AIRCOM, a través del CAOC de Torrejón, aprobará rutas de vuelo que no provoquen una reacción del sistema A2/AD ruso.

En tiempo de paz hay unas áreas establecidas en las que se puede volar y cumplir las misiones encomendadas. Aun volando en estas zonas, las emisiones de los sistemas ISR de los aviones pueden llegar a ser consideradas como un acto hostil que desencadene una reacción rusa.

No obstante, dentro de la aproximación indirecta de la OTAN, la disuasión es una de las medidas más efectivas que se puede aplicar para evitar que la FdR considere airadamente la actividad ISR en la proximidad de sus fronteras como un acto hostil**.** En

[24] Centro de Operaciones Aéreas Combinado (CAOC) de sus siglas en inglés.

consecuencia, la OTAN debe convencer a los rusos, cada vez más capaces de materializar una agresión militar contra Occidente, de que cualquier acción contra la Alianza sea demasiado arriesgado y costoso (Colby y Solomon, 2016).

4.2. Aproximación directa

4.2.1. Ataques *Soft-Kill*

Los ataques *Soft-Kill* son aquellos que no requieren una acción cinética sobre el objetivo o grupo de objetivos. Dentro de los posibles ataques *Soft-Kill,* deben ser citados: la interferencia electrónica o *jazmín,* el uso de señuelos y ciberataques (Dalsjö *et al.*, 2019, pp. 47-49).

Interferencia electrónica[25] –Ataque Electrónico (EW-EA)– de radares de búsqueda, radares de adquisición o sistemas de mando y control.

De forma ilustrativa, se puede estudiar la operación «Tormenta del Desierto»[26] para ver la aplicación de este tipo de estrategia. En esta operación, el grupo de planeamiento americano valoró tres vías para ganar la batalla electrónica, para ello, identificaron los siguientes objetivos (Kopp, 1993): Primero, la supresión de las defensas aéreas enemigas –SEAD[27]– a través de interferencias, misiles antirradiación, señuelos y misiles guiados lanzados por aeronaves.

Segundo, neutralizar la red de mando y control con aviones EC-130 Compass Call[28]*,* hasta que los nodos clave pudieran ser destruidos por aviones de ataque.

Tercero, el uso de contramedidas electrónicas (ECM) a bordo de las aeronaves como última medida de salvaguarda en el caso de que no dieran resultado las medidas anteriores y el adversario estuviera en condiciones de disparar los misiles SAM contra las aeronaves norteamericanas (véase figura 4).

[25] Electronic jamming.
[26] Operation Desert Storm.
[27] Suppresion of Enemy Air Defence.
[28] Sistema de armas tácticas aerotransportadas que utiliza una versión muy modificada del fuselaje C-130 Hercules y puede neutralizar las comunicaciones de mando y control enemigo.

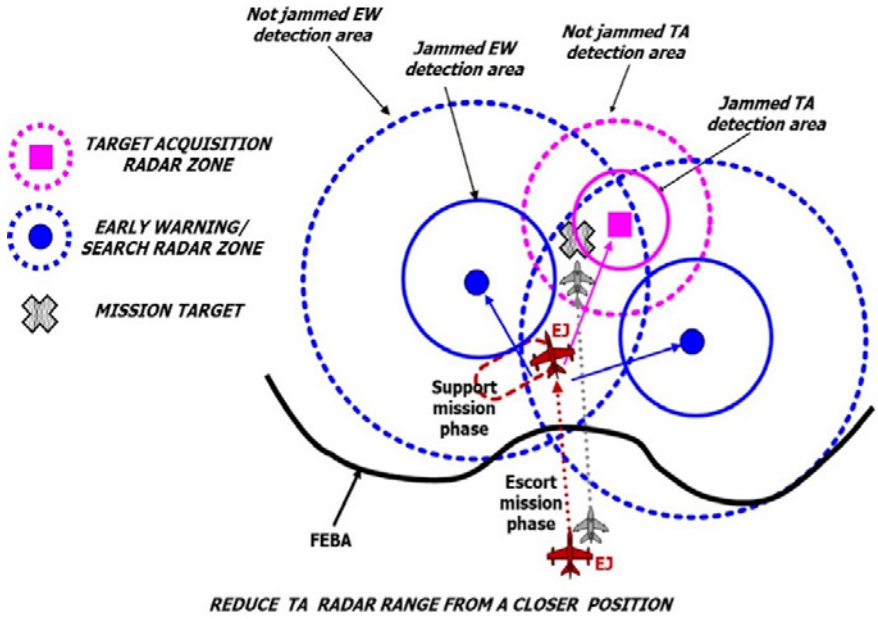

Figura 4. Escolta con capacidad de ataque electrónico aerotransportado. Fuente: Massimo Annulli https://www.emsopedia.org/entries/escort-jammer-task

No obstante, ser capaz de penetrar un sistema A2/AD por aire es una tarea con grandes riesgos. La mayoría de las plataformas aéreas requieren de un apoyo mutuo para poder sobrevivir (NSO, 2009). Este apoyo puede proporcionarse con aeronaves que realizan vigilancia, con otras que proporcionan protección electrónica, o con aquellas que proporcionan defensa física de los aviones de combate o de reconocimiento y vigilancia.

Decepción mediante el empleo de señuelos físicos o electrónicos que permiten engañar a las estaciones de radares o a los integrados en los misiles.

Las contramedidas como las tiras delgadas de papel de aluminio o bengalas generalmente son disparadas por aviones que se encuentran bajo la amenaza inminente de ataque de misiles.

Sin embargo, existen otras alternativas más ingeniosas a los señuelos convencionales, como fueron los usados en la primera guerra de Irak durante la operación «Tormenta del Desierto». Los pilotos de la Armada y el Cuerpo de Infantería de Marina lanzaron más de cien señuelos desde aviones F-18, con forma de aviones en miniatura, durante la noche en la que se inició la

operación «Tormenta del Desierto» en Irak (Evans, 1991). De este modo, los norteamericanos saturaron los radares enemigos con una masa confusa de objetos voladores que provocaron el fuego antiaéreo. Esta maniobra permitió que la defensa aérea iraquí encendiera sus radares, con lo cual, se hicieron visibles y pudieron ser atacados con misiles guiados.

Los ciberataques a los sistemas de vigilancia o mando y control son sin duda la medida que menos daños y bajas colaterales puede producir. Un ejemplo claro y reciente del empleo de estas tácticas y procedimientos se puede extraer del estudio de las operaciones aéreas que llevó a cabo la Fuerza Aérea Israelí (IAF) en 2007, para destruir la central nuclear de al-Kibar (Siria).

Dentro del marco de la operación bautizada como «Orchard», la Fuerzas de Defensa Israelíes (IDF) desarrollaron tres planes para alcanzar su objetivo: un ataque de la IAF contra varios lugares asociados al programa nuclear de Siria; un ataque de la IAF contra las instalaciones nucleares de al-Kibar; o una acción directa en al-Kibar por parte de unidades de operaciones especiales israelíes.

Finalmente, el Gobierno israelí eligió la segunda opción, un ataque de precisión de al-Kibar. Según Thomas Rid (2012: 16-17), el 6 de septiembre de 2007, un escuadrón formado por diez cazas F-16I y F-15I despegó de la base aérea de Ramat David (Israel) en lo que pensaron que era un ejercicio rutinario. Cuando se acercaron a la frontera con Siria, el escuadrón recibió la orden de atacar las instalaciones nucleares de al-Kibar; 18 minutos después al-Kibar había sido destruido.

Este ataque nunca se hubiera podido llevar a cabo sin que se hubiesen neutralizado previamente los sistemas de defensa aéreo sirios. Lo más sorprendente de esta operación fue que los sistemas de defensa aérea fueron neutralizados de la forma más discreta y aséptica posible. Supuestamente, la Unidad 8200[29] llevó a cabo un ciberataque que deshabilitó los sistemas de defensa aéreos sirios que defendían al-Kibar.

[29] La Unidad 8200 es la principal unidad de recopilación de información de la Dirección de Inteligencia Militar de las Fuerzas de Defensa Israelíes. Los soldados de la unidad están a cargo de desarrollar y utilizar herramientas de recopilación de información, analizar, procesar y compartir la información recopilada con los funcionarios pertinentes (IDF, 2017).

El empleo de un sabotaje cibernético previo al ataque aéreo permitió minimizar los daños colaterales. Una acción más cinética habría requerido la destrucción de muchas instalaciones de defensa aérea, lo que probablemente hubiese provocado la muerte de soldados y civiles.

Si bien el sistema de defensa aéreo sirio era uno de los más capaces del mundo, no pudo detectar a ninguno de los combatientes israelíes debido al ataque cibernético israelí (Rid, 2012: 17).

Al-Kibar estaba protegido por el sistema de defensa aérea Tor-M1 construido en Rusia que, a la sazón, se usaba para proteger las instalaciones nucleares iraníes. El aparente fracaso de estos sistemas llevó a Irán a comprar el sistema S-300 ruso en diciembre de 2007 (Gartenstein-Ross y Goodman, 2009).

4.2.2. Ataques *Hard-Kill*

Las acciones *Hard-Kill* se caracterizan por ser «cinéticas». Es decir, su finalidad es crear un efecto en el objetivo que provoque un cambio físico en su estado. Generalmente, implicará su destrucción física y daños en el personal y elementos mobiliarios que esté en las inmediaciones del objetivo.

Cuando se realiza un ataque *Hard-Kill* contra sistemas A2/AD se pretende inutilizar un centro de control, un radar, un puesto de tiro o incluso un misil en vuelo.

Los procedimientos y técnicas para inutilizar los sistemas A2/AD son múltiples, pero su conocimiento en detalle está reservado únicamente a aquellas unidades u organismos que tienen asignado este cometido. No obstante, existe mucha literatura sobre qué se debe atacar en los sistemas A2/AD. De forma generalista, se puede agrupar en cuatro categorías a los elementos que son objetivo en sí mismo de los ataques *Hard-Kill:* puestos de tiro, elementos de adquisición, puestos de mando o centros de control y las propias municiones.

Es reseñable que los sistemas A2/AD van más allá de los sistemas de defensa aérea. Aunque sí es cierto que estos sistemas son la principal amenaza para el *Global Hawk*.

Actualmente (Dalsjö *et al.*, 2019), el procedimiento más común del *Hard-Kill* es atacar los lanzadores de misiles y a sus sistemas de adquisición. Esto se puede hacer de manera deliberada y planificada, o como respuesta a una amenaza imprevista y ante la identificación de un objetivo de oportunidad.

Es importante destacar que, aunque es de interés especial para el componente aéreo, las operaciones contra los sistemas A2/AD no son exclusivamente una tarea de las fuerzas aéreas (Bonds *et al.*, 2017). Si la situación lo permite, las unidades terrestres, como las fuerzas especiales o la artillería de campaña, también pueden influir sobre el A2/AD; al igual que las unidades navales (especialmente los submarinos armados con misiles) si el objetivo es un barco o en la costa.

Más allá de poder neutralizar o destruir los sistemas de defensa aérea mediante el empleo de artillería de campaña de largo alcance, misiles balísticos o acciones directas con unidades de operaciones especiales, la opción militar que mejor rendimiento produce es el empleo de misiles antirradiación junto con los misiles o bombas guiados.

Pese a que el misil antirradiación ofrece la ventaja de que una vez disparado siga al blanco mediante un radar o sensor de seguimiento interno, es necesario que la fuente de emisión se mantenga activa. Un ejemplo claro de la dificultad que entraña las operaciones SEAD para destruir las unidades de misiles tierra-aire –SAM–, lo encontramos en el conflicto de Kosovo (1998-199). Los serbios, conocedores de las capacidades SEAD de la OTAN, consiguieron dificultar enormemente cualquier acción de la fuerza aérea aliada contra ellos apagando los radares. Con este simple, pero efectivo procedimiento, los serbios derribaron un F-117A con un sistema SAM S-1245M Neva, fabricado en la Unión Soviética en los años 60 (Oréjov, 2019).

Como parte de la guerra contra los sistemas A2/AD, se puede recurrir en última instancia a actuar contra el misil, ya sea un SAM o un misil balístico.

> Los misiles balísticos varían en alcance desde aproximadamente 120 a unas 10.000 millas. Una vez lanzados, los misiles tienen una fase de aceleración, mientras el motor cohete consume su combustible, a partir de ese momento, una vez finalizado el empuje del motor cohete, se inicia una fase balística o intermedia, para concluir con la fase terminal o de reentrada. La parte letal de un misil balístico es el vehículo de reentrada, que contiene y protege a la cabeza de combate del calentamiento producido por la fricción aerodinámica durante la reentrada en la atmósfera. La cabeza de combate puede disponer de alto explosivo, o tener cabezas nucleares, biológicas o químicas. Los misiles más grandes pueden dis-

poner de varios vehículos de reentrada y por tanto de varias cabezas de combate (Godínez, 2012).

Los sistemas contramisiles balísticos –BMD[30]– son una realidad. Distintas armadas cuentan con el sistema AEGIS norteamericano, como las fragatas F-100 españolas, armado con misiles estándar SM-3 que pueden interceptar misiles balísticos.

4.2.3. Tercera estrategia de compensación norteamericana

Cómo hacer frente a los sistemas A2/AD rusos es un verdadero reto para la OTAN. Por esta razón, lo más razonable es estudiar a las fuerzas armadas de EE. UU., las más poderosas del mundo, y analizar cómo afronta esta amenaza, cada vez más desarrollada.

La tercera estrategia de compensación es la aproximación que el Pentágono[31] ha articulado como respuesta a cualquier acción o alianza que pudiera limitar la proyección del poder militar a cualquier zona del planeta, independientemente de la estrategia A2/AD enemiga.

De este modo, se pretendería combinar los sistemas terrestres, navales y aéreos existentes con nuevos desarrollos que permitieran mantener la brecha cualitativa[32] frente a sus adversarios. Así, también se perseguiría reducir la dependencia logística y operativa que tiene EE. UU. de las instalaciones navales, aéreas y terrestres situadas en las regiones avanzadas. Además, de reducir la dependencia que tienen de sus satélites, en beneficio del aprovechamiento de la capacidad de proyección estratégica de su Fuerza Aérea y de su Marina.

Además, también se intentaría potenciar las enormes posibilidades que ofrecen sus RPAS de nivel estratégico, operacional y táctico, junto con su capacidad para realizar ataques estratégicos de precisión, susceptibles de batir cualquier objetivo enemigo (Colom, 2015).

Es interesante destacar que las dos estrategias de compensación anteriores tuvieron una validez de no más de 30 años. La primera en 1950, basada en la superioridad nuclear frente a la Unión Soviética; y la segunda de 1975, en la que se puso el foco

[30] Ballistic Missile Defence.

[31] Departamento de Defensa de los EE. UU.

[32] Especialmente en sistemas no-tripulados, inteligencia artificial, ciberespacio, guerra submarina, ataque estratégico o integración de sistemas.

en las armas guiadas para contrarrestar la paridad nuclear alcanzada por la Unión Soviética. EE. UU. pretende que esta nueva estrategia de compensación se cimente sobre los principios de la RMA[33] o revolución de los asuntos militares. Por lo tanto, según el exvicesecretario de Defensa, Robert Work (2016), la inteligencia artificial y los sistemas autónomos van a jugar un papel fundamental en esta estrategia.

Es evidente que uno de los objetivos en esta aproximación es conseguir una mayor desvinculación del hombre en los procesos de decisión y de ejecución en favor de la máquina. Otra lectura que se puede hacer de esta estrategia es la capacidad de aprendizaje de los sistemas, lo que extendería la validez de la estrategia más allá de los treinta años a las que llegaron sus predecesoras.

Por lo tanto, esta estrategia pensada a largo plazo otorgaría una ventaja tecnológica a los EE. UU. y a sus aliados que permitiría a los RPAS estratégicos operar en entornos altamente disputados con un alto grado de supervivencia en contraposición a los sistemas A2/AD.

Un claro ejemplo del progreso de esta estrategia aplicada en el campo de los RPAS es el desarrollo del RQ-180, el cual sustituiría al RQ-4B. Este UAV está siendo diseñado para volar en entornos disputados. Gracias a su diseño, tiene capacidad furtiva, a imagen y semejanza del F-22, un avión de combate de 5.ª generación, con los mejores avances tecnológicos aplicados a un avión que le hacen invisible a los sistemas de localización e identificación de sus enemigos.

Las innovaciones tecnológicas que se están aplicando en este RPAS hacen que sea invisible a los radares –tecnología furtiva o *stealth*–, lo cual es un salto cualitativo frente al RQ-4D, puesto que mejora su capacidad de supervivencia en un entorno altamente disputado (Rogoway, 2021).

5. Confrontación

«I think it's very possible that Putin has made a huge mistake in this invasion, that he's bitten off more than he can chew and that he's going to fail at his attempt to subdue Ukraine» (Fukuyama, 2022). Con estas palabras, el famoso politólogo estadounidense valoraba la execrable guerra de Putin en una entrevista conce-

[33] Revolution in Military Affairs.

dida a los pocos días de iniciarse la guerra. Ha sido una sorpresa para toda la comunidad internacional la habilidad que ha tenido el pueblo ucraniano para contener al todopoderoso Ejército del autócrata ruso, hecho que está haciendo reflexionar a todos los analistas militares acerca de las ideas preconcebidas que se tenían de la guerra moderna

¿Qué relación guarda la guerra en Ucrania y el sistema AGS de la OTAN? En principio no guarda una relación directa, más allá de la obvia necesidad de información de la OTAN de este conflicto. Por eso, el *quid* de la cuestión es el grado de fiabilidad de los supuestos contemplados, hasta la fecha, respecto a las capacidades atribuidas a las fuerzas armadas rusas.

Es un hecho que Putin ha reforzado sus fronteras con Europa en los últimos veinte años mediante el despliegue de nuevos sistemas de defensa aérea, basados fundamentalmente en los sistemas S-300 y S-400; sistemas de misiles balísticos; y misiles antibuque.

Esta colosal inversión rusa ha sido realmente barata si se tiene en cuenta que es el remedio más económico para oponerse a las capacidades militares de la OTAN, especialmente, al poder aéreo y naval. Consecuentemente, tal y como teorizan en la Agencia Sueca de Investigación de Defensa –FOI– (Dalsjö *et al*., 2019), no parece que el muro defensivo A2/AD sea tan infranqueable como se piensa.

El análisis de la cuestión radica en aislar el sistema A2/AD de la FdR y el AGS de la OTAN, y entender cuáles son los centros de gravedad (CoG[34]) de cada uno de los sistemas. Según la COPD[35] V3 (ACO, 2021), se entiende por centro de gravedad –en adelante CoG– aquella entidad que proporciona a un actor su fuerza, libertad de acción o voluntad de luchar. En suma, se deben tener en consideración los elementos esenciales que definen el CoG del AGS. Es decir, fines y objetivos, capacidades críticas[36], requerimientos críticos[37] y vulnerabilidades críticas[38].

[34] Center of Gravity o centro de gravedad.

[35] Comprehensive Operational Planning Directive.

[36] «Qué» debe ser capaz de hacer para lograr los objetivos identificados (ACO, 2021).

[37] Los medios, recursos y condiciones esenciales que permiten al CoG generar y mantener las capacidades críticas (ACO, 2021).

[38] Las debilidades, lagunas o deficiencias de los requerimientos críticos a través de los cuales se pueden proteger o explotar los CoG (ACO, 2021).

5.1. El A2/D como centro de gravedad en la defensa de la frontera Rusia-Europa

Habida cuenta de que el sistema A2/AD ruso está diseñado para defender su territorio mediante la integración de sistemas defensivos que operan en todos los dominios, se puede especular acerca de cuál de ellos es el menos consistente y, por tanto, prever por dónde se puede abrir una brecha que permita penetrar en el sistema A2/AD. Encontrar la vía por dónde empezar a desmantelar el sistema defensivo ruso es la clave de cualquier operación militar que se planee.

Consecuentemente, del estudio realizado sobre el sistema A2/AD de la FdR, se deducen el resto de los elementos esenciales del CoG.

Capacidades críticas:

El sistema A2/AD tiene la capacidad de evitar que un adversario entre en un área determinada. Adicionalmente, tiene la capacidad de limitar la libertad de acción del enemigo, en el caso de que consiguiera romper la barrera antiacceso y, consecuentemente, penetrara en el espacio de soberanía defendida.

Requerimientos críticos:

Si se analiza el sistema A2/AD como una amenaza para el sistema AGS, se puede acotar esta lista de requerimientos críticos a aquellos elementos que sí pueden generar un efecto potencial sobre él. En estas condiciones, los sistemas S-300 y S-400 son capaces de seguir al RQ-4D con sus radares de adquisición de largo alcance. Además, es destacable la capacidad de estos sistemas para atacar diferentes objetivos, principalmente aviones, aunque también puede atacar misiles balísticos y de crucero, no sin ciertas limitaciones asociadas a la velocidad de vuelo de estos últimos. Adicionalmente, el sistema S-400 dispone de sofisticados sensores que le confieren una peligrosa capacidad antisigilo (Hughes, 2019).

También se deben considerar las ya mencionadas capacidades de guerra electrónica y cibernéticas de las que, aun permaneciendo en el más absoluto anonimato, no se puede descartar que en determinadas condiciones pudieran generar efectos no deseados en alguno de los segmentos del AGS.

Vulnerabilidades críticas:

Si hubiera que elegir un dominio por dónde empezar a desmontar la barrera defensiva rusa en la frontera este de Europa, el dominio marítimo quizás adolecería de tener las mayores vulnerabilidades. Es importante destacar que la Alianza dispone de buques de guerra con sistemas antimisiles que limitarían los efectos de los misiles balísticos y también de los IADS, en apoyo a la maniobra naval que tendría por objetivo abrir una brecha en el sistema defensivo ruso. En el otro lado de la balanza, el IADS ruso, con los S-400 a la cabeza, probablemente sea la amenaza más plausible del sistema A2/AD (Kofman, 2019).

Del estudio realizado, se puede esgrimir el supuesto de que las zonas más disputadas, donde se produciría la batalla para romper el sistema A2/AD, serían la del mar Báltico y del mar Negro. En estas zonas las fuerzas navales de la Alianza y rusas sufrirían un alto grado de atrición. El factor desequilibrador en esta batalla sería el factor tecnológico, el cual, permitiría una mejor gestión de objetivos y la generación de la COP[39]. Así pues, una posible vulnerabilidad del A2/AD en la batalla naval es la posibilidad de que las fuerzas navales de la OTAN tengan potencialmente más probabilidad de alcanzar una superioridad tecnológica y de fuerzas, que provocaría la derrota de la marina rusa.

Como ya se ha visto a lo largo de este artículo, algunos analistas militares son escépticos sobre la verdadera efectividad de los sistemas de interdicción rusos en términos de alcance y eficacia de sus radares de adquisición; capacidades de sus misiles, y las limitaciones inherentes a la geografía (Giles y Boulegue, 2019).

Según los analistas de la agencia sueca FOI (Dalsjö *et al.*, 2019), los sistemas S-300 y S-400 son la mayor amenaza para el AGS, en particular, los sistemas desplegados en Kaliningrado. Sin embargo, se debe tener en cuenta que los sistemas de adquisición de su IADS, como el radar Nebo-M, aun con su alcance de hasta 1800 km, encuentran su limitación en la curvatura de la tierra y en accidentes geográficos, como cadenas montañosas, capaces de bloquear los sensores de los radares (Hughes, 2019).

Otra vulnerabilidad de los sistemas S-300 y S-400 es su capacidad para manejar múltiples objetivos simultáneamente. El radar de la unidad tipo batallón S-300 es capaz de adquirir doce objetivos simultáneamente, y su unidad de tiro puede disparar

[39] Common Operational Picture.

hasta veinticuatro misiles antes de realizar la recarga. Los procedimientos rusos determinan que se deben disparar dos misiles por objetivo. Por esta razón, es probable que, si se disparan un mínimo de doce misiles contra las unidades de tiro, se consiguiera disponer de un periodo de tiempo suficiente para poder atacar con cazabombarderos a estas unidades mientras recargan. Del mismo modo, se puede atacar una unidad tipo batallón S-400 disparando contra ella al menos treinta y dos misiles, ya que dispone de un máximo de sesenta y cuatro misiles antes de realizar la recarga (Dalsjö *et al.*, 2019).

5.2. La NAGSF como centro de gravedad en el ISR conjunto

La naturaleza de la NAGSF hace que su único fin sea monitorizar lo que está sucediendo en la superficie de la tierra para proporcionar al comandante el conocimiento de la situación antes, durante y, si es necesario, después de las operaciones de la OTAN (NAGSMA, 2022).

Si se toma en consideración el análisis realizado del sistema AGS, se pueden deducir el resto de los elementos esenciales que definen el CoG.

Capacidades críticas:

La NAGSF contribuye eficazmente en la obtención de información e inteligencia en operaciones conjuntas; también en el apoyo directo a las operaciones terrestres, marítimas y del mando aéreo de la Alianza; y, finalmente, en el apoyo a las autoridades que se determinen en la gestión de crisis humanitarias (NAGSMA, 2022).

Requerimientos críticos:

De los distintos segmentos que forman el sistema AGS, se puede considerar la plataforma aérea RQ-4D que es el recurso o activo del sistema que posibilita alcanzar el fin perseguido por el AGS. Una de las grandes ventajas de la aeronave del AGS es su permanencia en vuelo, más de 30 horas, y las posibilidades que otorga su sensor MR-RPTI.

Otro elemento determinante en la explotación de las imágenes y vídeos captados por la plataforma aérea es el centro de explotación (PED). Si bien es cierto que la inteligencia, fruto del análisis de imágenes y vídeos, puede ser elaborada en otros escalones de mando, el verdadero valor añadido del sistema AGS es la capaci-

dad de analizar y distribuir información e inteligencia en tiempo casi real gracias al centro de explotación de la NAGSF.

Vulnerabilidades críticas:

En un hipotético conflicto armado entre la FdR y la OTAN, pese a que la plataforma RQ-4D vuela a altitudes superiores a los 60.000 pies, la aeronave sería vulnerable a los sistemas de defensa aéreo, particularmente a los sistemas S-300/S-400 y a los aviones de combate de la Fuerza Aérea de la FdR (Rogoway, 2021). Esta afirmación se basa en el mero hecho de que la aeronave no tiene capacidad de combate aire-aire, y en la evidencia palmaria de que un Global Hawk puede ser derribado fácilmente por el IADS ruso, como ya le sucediera a un RQ-4A de la Fuerza Aérea de los EE. UU. en 2019 cuando fue derribado en el estrecho de Ormuz por una unidad iraní de artillería antiaérea con un sistema Buk-M2 de medio alcance (Osborn, 2021b).

Por lo tanto, es razonable concluir que, en un espacio de batalla altamente disputado donde la OTAN no haya alcanzado al menos la superioridad aérea, la NAGSF no podrá cumplir su misión con unas garantías de supervivencia razonables.

Por otro lado, los sistemas de navegación remotos y de comunicaciones del Global Hawk se basan en enlaces satelitales. Es evidente que las características y capacidades de este sistema se basan en la condición necesaria de mantener el enlace satelital, circunstancia que lo hace potencialmente vulnerable a un ciberataque contra la constelación de satélites o contra la propia aeronave.

Durante la investigación del último extremo, probablemente clasificado por la OTAN, no se ha encontrado una fuente bibliográfica creíble que pueda refutar esta vulnerabilidad. Consecuentemente, es plausible valorar esta vulnerabilidad debido al continuo desarrollo tecnológico en este campo, el cual podría permitir abrir una brecha tanto en los satélites dedicados al sistema AGS como en la propia aeronave o en las estaciones de control terrestres ubicados en Sigonella (Italia).

Finalmente, se puede indicar que la plataforma aérea RQ-4D presenta una vulnerabilidad en su propio diseño, ya que es perfectamente visible al radar. Aunque cuando fue diseñada existía la tecnología furtiva o *stealth*, su diseño no se basó en esta innovación, mejora que hubiese garantizado actualmente su supervivencia en un entorno disputado.

5.3. Confrontación de sistemas en tiempo de paz

Desde la firma del Tratado de Washington, la Alianza, en su relación con la extinta URSS y la actual Rusia, siempre se ha movido a lo largo del espectro del conflicto sin que se llegase al nivel de conflicto armado. Sin embargo, es cierto que ha habido ocasiones en los que ambos bloques han estado a punto de cruzar este peligroso umbral, como han sido las trece ocasiones documentadas en las que fuerzas de la OTAN y rusas se vieron envueltas en incidentes que podrían haber provocado una escalada armada o nuclear (Stout y Armstrong, 2015).

Una de las acciones que nunca se debe descartar por parte de la FdR es el empleo de los medios de guerra electrónica y de ciberataque. Estas capacidades pasan bastante desapercibidas, especialmente la posibilidad de actuar en el ciberespacio, cuya atribución entraña gran dificultad (Dalsjö *et al.*, 2019). Si Rusia fuera capaz deshabilitar los sistemas de navegación GPS[40], se vería comprometido el enlace de posicionamiento entre la aeronave y las estaciones terrestre, así como el control de la propia aeronave RQ-4D.

Por otro lado, la guerra de Putin está sirviendo para confirmar algunos de los supuestos planteados por teóricos y analistas militares de la OTAN. Un mes más tarde de que empezara la invasión de Ucrania, la Agencia de Seguridad Aérea de la Unión Europea (2022) –EASA– publico un boletín informativo en el que advertía sobre la posibilidad de que los sistemas de navegación de las aeronaves fueran degradados si se volaba cerca de la región de Kaliningrado, el mar Báltico, el mar Negro, al este de Finlandia y al este del mar Mediterráneo.

A tenor de las informaciones facilitadas por la EASA, se puede asegurar que las fuerzas armadas rusas tienen la capacidad de realizar acciones de guerra electrónica para atacar los sistemas de navegación de las aeronaves. No obstante, (Northrop Grumman, 2022) estas acciones *jamming* o *spoofing* para interferir la señal GPS del RQ-4D serían irrelevantes, ya que la aeronave dispone de sistemas *anti-jamming* que aseguran la integridad de las señales por vía satélite.

Por lo tanto, mientras que no haya una escalada en el conflicto entre el bloque de la Alianza y el bloque ruso, la NAGSF no debería realizar misiones ISR más allá de la frontera este de Europa para evitar que Rusia pueda justificar el empleo de sus sistemas S-300

[40] Sistema de posicionamiento global.

y S-400. Sin embargo, es inevitable que Rusia haga acciones cibernéticas que afecten a la misión del RQ-4D. Adicionalmente, en escenarios de máxima tensión, como el que está sucediendo en Ucrania desde febrero de 2022, se debe tener en cuenta que Rusia probablemente intensifique sus acciones de guerra electrónica en las zonas fronterizas y, consecuentemente, podrían influir en las comunicaciones y sistema de posicionamiento de la aeronave si los sistemas *anti-jamming* del RQ-4D no funcionaran correctamente.

5.4. Confrontación en una escalada del conflicto

El despliegue del sistema A2/AD ruso, desde el ártico hasta Siria, implica que la Alianza solo podrá alcanzar la superioridad de fuerzas después de neutralizarlo. En estas condiciones, la OTAN tendría que aislar en primera instancia a Kaliningrado con el fin de mitigar el efecto de las acciones de sus sistemas antiacceso en el corazón de Europa (Giles y Boulegue, 2019). Alcanzada esta condición, sería plausible plantear el estudio del resto de condiciones que se tuvieran que cumplir para suprimir las amenazas para el AGS del resto de sistemas del A2/AD.

De este modo, la OTAN, con EE. UU. a la cabeza, dispondrían de una interesante panoplia de posibilidades dentro de cada opción de respuesta militares para tratar de contrarrestar los efectos defensivos del sistema A2/AD ruso. De todas las capacidades del sistema antiacceso y de denegación de área de la FdR, la defensa aérea, la guerra electrónica y los ciberataques son el enemigo más letal para el AGS.

Según el análisis de vulnerabilidades críticas de los sistemas S-300 y S-400 –CoG del A2/AD frente al AGS– es factible considerar que estos sistemas de defensa aérea son una amenaza para aeronaves que vuelan a grandes altitudes. Sin embrago (Dalsjö *et al.*, 2019), el alcance efectivo del IADS ruso contra aeronaves tácticas o misiles que vuelan a menor altitud es menos efectivo. De esta manera, se reduce el alcance de sus armas considerablemente, probablemente, de 400 a 35 km.

Por consiguiente, se pueden plantear distintas acciones. La menos cinética sería el empleo de interferencias o señuelos con unidades de guerra electrónica terrestres o desde el aire con aviones equipados con estas capacidades. Por otro lado, la acción más letal sería la supresión de los sistemas S-300/S-400 y del radar de largo alcance Nebo, que sirve como sistema de alerta temprana, así como para la adquisición y seguimiento de objetivos.

Una misión SEAD con el apoyo de *jammers*[41] sería más que suficiente para eliminar este objetivo (Dalsjö *et al.*, 2019). Evidentemente, esta misión de supresión no es sencilla, pero sí que sería alcanzable. El ataque consistiría en saturar con *jammers* los radares enemigos, y en lanzar misiles contra las unidades de tiro para forzar la recarga, momento idóneo para actuar sobre las unidades S-300/S-400 (Hughes, 2019).

No obstante, el planteamiento más conservador indicaría que se debe evitar el vuelo de aviones de alto valor dentro de la burbuja defensiva de los sistemas S-300 y S-400 hasta que se hayan suprimido o neutralizado, sin olvidar los sistemas de defensa aérea de medio y corto alcance (Dalsjö *et al.*, 2019).

Consecuentemente, la supresión o neutralización de las unidades S-300/S-400 requiere un gran esfuerzo y un significativo desgaste de las unidades de combate de la fuerza aérea de la Alianza antes de que los objetivos sean neutralizados, y el sistema de defensa aérea esté lo suficientemente degradado para que pueda operar el RQ-4D con ciertas garantías de supervivencia.

Si bien es cierto que el CoG de la defensa aérea se basa en los sistemas S-300 y S-400, no se debe olvidar al poder aéreo ruso. Sin embargo, el seguimiento de las operaciones aéreas en la guerra en Ucrania permite vislumbrar un halo de esperanza para la OTAN para evaluar supuestos más favorables de los que se podían pensar antes del inicio de la guerra.

Antes de la invasión de Ucrania, la inteligencia estadounidense había pronosticado un ataque devastador del poder aéreo ruso. Sin embargo, un mes después del inicio de la guerra, los rusos no han conseguido la superioridad aérea. Según algunos analistas, se ha evidenciado una falta de coordinación de la fuerza aérea rusa con las fuerzas terrestres (Stewart y Ali, 2022).

Además de la acción del IADS y de la fuerza aérea, se debe sumar la acción de los sistemas de guerra electrónica dentro de los procedimientos empleados por los rusos en su estrategia A2/AD.

Finalmente, se debe recordar que las operaciones que se lleven a cabo en un hipotético conflicto armado OTAN-FdR serán en escenarios altamente demandados dentro del contexto de las operaciones multidominio. Por consiguiente, el elemento final de

[41] Aviones escolta con sistemas de guerra electrónica que producen interferencias en los sistemas de adquisición de los IADS.

análisis, dentro del espectro de las operaciones multidominio, es la capacidad de la FdR para llevar a cabo ciberataques. No obstante, y para sorpresa de algunos analistas, el conflicto de Ucrania ha servido para refutar una de las tesis menos discutidas y que han inducido a los analistas a considerar las poderosas habilidades cibernéticas de la Federación de Rusia como devastadoras y muy difíciles de contener.

A pesar de que semanas antes de que se produjera la invasión Ucrania se informó de numerosos ataques cibernéticos del GRU[42] (Zurdo, 2022), a partir del inicio de los combates el 24 de febrero de 2022, se pudo observar la inoperancia rusa para llevar a cabo ciberataques. Esta baja actividad cibernética tuvo su explicación en la acción de los equipos estadounidense de ciberseguridad, desplegados días antes de la invasión, cuya misión ha sido proteger las principales infraestructuras ucranianas. El trabajo de estos equipos permitió contrarrestar la capacidad cibernética de la FdR, hecho que refuta la tesis mantenida por muchos analistas de que las capacidades cibernéticas rusas podrían degradar en un alto grado las capacidades de mando y control de la Alianza en caso de conflicto bélico (Roca, 2022).

En adición a la defensa cibernética ofrecida por EE. UU., el viceprimer ministro ucraniano, Mykhailo Fedorov, ha conseguido organizar el denominado IT Army, un *ejército* de 300.000 hackers que tratan de proteger a Ucrania de los ataques rusos en la red que, hasta la fecha, ha resultado exitoso (Pearson, 2022).

Por consiguiente, queda demostrado en el conflicto de Ucrania que la Alianza sería capaz de contener la amenaza rusa en el dominio ciberespacial.

5.5. Valoración

Si bien es cierto que se han estudiado todas las capacidades o requerimientos críticos del sistema A2/AD, entendido como un sistema de sistemas, solo unos pocos pueden producir efectos sobre el AGS. Por lo tanto, el sistema A2/AD podría no ser considerado en sí mismo una amenaza para el RPAS desde el punto de vista doctrinal, ya que solo algunos de los elementos o sistemas verdaderamente representarían una amenaza para el AGS o la NAGSF, en calidad de entidades o actores.

[42] Departamento de Inteligencia Ruso o Glávnoye Razvédyvatelnoye Upravlenie.

Consecuentemente, se debe separar claramente qué sistemas del A2/AD ruso pueden producir efectos en el AGS en función de los dos escenarios o situaciones dentro del espectro del conflicto analizados en el estudio.

Por otro lado, se debe entender que, aun respetando la NAGSF los espacios de soberanía rusos, la FdR tratará en todo momento de realizar acciones sobre el sistema o parte del sistema AGS. Estas acciones serían del tipo ciberataque o ataque en el espectro electromagnético, las cuales, a la postre, serían difícilmente atribuibles a las FAS rusas. Igualmente, en el caso de que la plataforma RQ-4D por error, omisión o intencionadamente invadiera el espacio aéreo ruso, todos los sistemas del A2/AD atacarían la aeronave.

Por consiguiente, en tiempo de paz, existe una probabilidad sensiblemente baja de que ningún sistema del A2/AD pueda afectar a las misiones llevadas a cabo por la NAGSF en la frontera oriental de Europa. Sin embargo, en un escenario altamente disputado, todos los sistemas del A2/AD atacarían al sistema AGS en toda su extensión, incluidos los segmentos desplegados en Sigonella o en cualquier otra ubicación de Europa.

En la tabla 1, se muestra un análisis DAFO del sistema AGS:

ANÁLISIS DAFO AGS	
DEBILIDADES • Aeronave sin tecnología *stealth* • Aeronave no tiene contramedidas misiles tierra-aire o aire-aire • Enlace satelital puede ser alterado	**AMENAZAS** • IADS ruso: S-300, S-400, radares y cazas • Sistemas de guerra electrónica • Ciberataques
OPORTUNIDADES • Protección o apoyo de unidades ajenas a la NAGSF para neutralizar y superar el IADS ruso • Zonas no defendidas por el IADS ruso	**FORTALEZAS** • Larga persistencia sobre el terreno (+30 horas) • Altura de vuelo y alcance • Sensor de obtención de gran precisión con seguimiento de patrón de objetivos • Información en tiempo casi real • Sistema modulable y escalable • Capaz de obtener inteligencia sobre el objetivo sin exponer tripulación

Tabla 1. Análisis DAFO del AGS. Fuente: elaboración propia

6. Conclusiones

La amenaza que representa el concepto defensivo A2/AD para las misiones que pueda llevar a cabo la NAGSF se deben analizar desde el contexto de la situación. Es decir, dependiendo de en qué parte del espectro de conflicto se desarrollen las operaciones.

Consecuentemente, es factible concluir que las condiciones que se deben cumplir para que la NAGSF lleve a cabo su misión serán diferentes en función del escenario en el que se desarrollen. Es decir, un escenario en tiempo de paz o en un escenario en la que se haya producido una escalada en el conflicto. El estudio y confrontación de las capacidades de la FdR y de la OTAN para enfrentar el sistema A2/AD y el AGS determinan que la OTAN tiene una superioridad tecnológica que le permite contemplar la certeza de que la NAGSF pueda llevar a cabo su misión con una probabilidad relativamente baja de que las plataformas aéreas, así como sus estaciones de mando y control terrestre, se vean afectadas o comprometidas por la acción rusa en el espectro electromagnético y ciberespacial.

Sin embargo, el sistema de defensa aérea integrada sí que tiene la capacidad de causar efectos en el AGS, especialmente, a la aeronave RQ-4D. De todos los segmentos que conforman el sistema AGS, el elemento más vulnerable es la aeronave. Esto no quiere decir que la FdR no tenga la capacidad de atacar al resto de los segmentos o elementos del sistema, por ejemplo, mediante el uso de misiles balísticos o hipersónicos.

Por lo tanto, se puede afirmar que en tiempo de paz la NAGSF es probable que lleve a cabo su misión en la frontera con la FdR siempre que no invada sus espacios de soberanía. La limitación de la información que pueda obtener el RQ-4D vendrá condicionada principalmente por el sensor MP-RTIP y por la altura de vuelo. Sin embargo, el escenario político y de seguridad actual hace poco probable que Ucrania tampoco pueda ser sobrevolado con medios JISR de la OTAN sin provocar que la FdR desafíe a los países aliados y los arrastre al conflicto armado que mantiene con Ucrania.

Por otro lado, si las misiones de obtención se realizaran dentro de un contexto bélico, el alcance de los medios JISR solo encontrarían límite en las capacidades de la OTAN para destruir o neutralizar el IADS y las unidades de guerra electrónica. Sí es conveniente aclarar que el RQ-4D, pese a poder alcanzar altu-

ras de vuelo próximas a los 60.000 pies, la VKS tiene los sistemas de detección necesarios para localizar la aeronave, así como los medios aéreos y terrestres de interceptación para derribar el Global Hawk de la Alianza. Solo la tecnología Stealth[43] y las contramedidas activas podrían aumentar la capacidad de supervivencia de un RPA que opera aisladamente en un entorno altamente disputado. Es decir, innovaciones tecnológicas que no dispone la aeronave RQ-4D.

Llegados a este punto, es admisible teorizar sobre las condiciones que tienen que alcanzarse para que el AGS pueda operar en escenarios como el de Ucrania. De este modo, en un escenario bélico y prebélico, las plataformas RQ-4 del sistema AGS de la OTAN solo podrán realizar misiones de obtención, reconocimiento y vigilancia dentro del área de operaciones ruso cuando se degrade su sistema A2/AD.

De igual forma, la condición mínima necesaria para que el Sistema AGS opere en la zona de influencia rusa, con un sistema A2/AD degradado, será solo si se neutralizan los sistemas de defensa aérea y de ataque electrónico (EW).

Finalmente, no se debe obviar que para que las misiones del sistema AGS tengan éxito, ya sea en paz o en guerra, también se han tenido que establecer las medidas de ciberseguridad adecuadas para proteger el AGS frente a ciberataques que traten de afectar a cualquiera de los sistemas que controlan las comunicaciones y el sistema de navegación por GPS del RPAS.

Bibliografía

1. Libros

SUN, T. (2021). *El Arte de la Guerra*. 5.ª ed. Dojo Ediciones.

2. Artículos de revista de divulgación

Colom, G. (2015). Rumsfeld «Revisited»: la tercera estrategia de compensación estadounidense. En: *Revista UNISCI*. 0(38), pp. 69-88. doi:10.5209/rev_RUNI.2015.n38.49645

Evans, D. (1991). Air Decoys Fooled Iraq, Navy Reveals. En: *Chicago Tribune*. [Consulta: 21 de enero 2022]. Disponible en: https://www.chicagotribune.com/news/ct-xpm-1991-09-19-9103110068-story.html

[43] Tecnología que permite disminuir la firma radar para dificulta su localización e identificación.

Giles, K. y Boulegue, M. (2019). Russia's A2/AD Capabilities: Real and Imagined. En: *The US Army War College Quarterly: Parameters*. 49, p. 17. [Consulta: 15 de febrero de 2022]. Disponible en: https://press.armywarcollege.edu/parameters/vol49/iss1/4/

Godínez, A. S. (2012). La Defensa contra misiles balísticos. Posible participación de las Fragatas F-100. En: *Instituto Español de Estudios Estratégicos*. P. 29.

Herreros, J. L. (2008). La evolución del concepto estratégico de la OTAN y su efecto en la estructura de mandos. En: *Dialnet.* Pp. 25-54. [Consulta: 19 de marzo 2022]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/2864600.pdf

Kopp, C. (1993). Desert Storm - The Electronic Battle Parts 1 - 3. En: *Australian Aviation. Aerospace Publications*. Canberra, ACT, Australia, 1993(June). [Consulta: 21 de enero 2022]. Disponible en: http://www.ausairpower.net/Analysis-ODS-EW.html

Kumar, H. (2021). Características_Nato AGS RQ-4D Phoenix UAV, Italy. En: *Airforce Technology*. 12 octubre. [Consulta: 3 de enero 2022]. Disponible en: https://www.airforce-technology.com/projects/nato-ags-rq-4d-phoenix-uav-italy/

Navy Recognition (2021). Russia has launched serial production of APR-3ME air-to-submarine missile. En: *Navy Recognition*. [Consulta: 9 de febrero 2022]. Disponible en: https://www.navyrecognition.com/index.php/naval-news/naval-news-archive/2021/june/10375-russia-has-launched-serial-production-of-apr-3me-air-to-submarine-missile.html

Osborn, K. (2021b). The U.S. Military's Eye in the Sky: Why the Global Hawk Is a Powerful Asset. En: *The National Interest. The Center for the National Interes*t. [Consulta: 22 de febrero 2022]. Disponible en: https://nationalinterest.org/blog/buzz/us-militarys-eye-sky-why-global-hawk-powerful-asset-189182

Palacio, V. (2004). La imagen imperial del nuevo orden internacional: ¿es esto realismo político? En: *CIDOB d'Afers Internacionais*. N.º 64, pp. 7-28.

Pearson, J. (2022). Ukraine launches «IT army» takes aim at Russian cyberspace. En: *Reuters*. 27 febrero. [Consulta: 28 de marzo 2022]. Disponible en: https://www.reuters.com/world/europe/ukraine-launches-it-army-takes-aim-russian-cyberspace-2022-02-26/

Rid, T. (2012). Cyber War Will Not Take Place. En: *Journal of Strategic Studies*. 35(1), pp. 5-32. doi:10.1080/01402390.2011.608939

Rubio, A. R. (2016). El «telegrama largo» de Kennan: reflexiones desde el pasado y el presente. Real Instituto Elcano. 22 febrero. [Consulta: 21 de abril 2022]. Disponible en: https://www.realinstitutoelcano.org/el-telegrama-largo-de-kennan-reflexiones-desde-el-pasado-y-el-presente/

Smura, T. (2016). Russian Anti-Access Area Denial (A2AD) capabilities - implications for NATO. En: *Casimir Pulaski Foundation*. 27 noviembre. [Consulta: 23 de enero 2022]. Disponible en: https://pulaski.pl/en/russian-anti-access-area-denial-a2ad-capabilities-implications-for-nato/

Stewart, P. (2020). Alliance Ground Surveillance Force. En: *Joint Air Power Competence Centre*. 9 septiembre. [Consulta: 15 de marzo 2022]. Disponible en:

Alliance Ground Surveillance Force - Joint Air Power Competence Centre (japcc.org)

Stewart, P. y Ali, I. (2022). What happened to Russia's Air Force? U.S. officials, experts stumped. En: *Reuters*. 2 marzo. [Consulta: 29 de marzo 2022]. Disponible en: https://www.reuters.com/world/europe/what-happened-russias-air-force-us-officials-experts-stumped-2022-03-01/

Vizcarra, J. (2018). NATO E-3A and AGS Interoperability. En: J*oint Air Power Competence Centre*. 21 marzo. [Consulta: 15 de marzo 2022]. Disponible en:

NATO E-3A and AGS Interoperability - Joint Air Power Competence Centre (japcc.org)

3. Entrevistas

Fukuyama, F. (2022). *Vladimir Putin will fail at subduing Ukraine: Francis Fukuyama*. *Nikkei Asia*. [Consulta: 24 de marzo 2022]. Disponible en: https://asia.nikkei.com/Editor-s-Picks/Interview/Vladimir-Putin-will-fail-at-subduing-Ukraine-Francis-Fukuyama

Stoltenberg, J. (2021). Conferencia de prensa con el secretario general de la OTAN, Jens Stoltenberg, y el ministro de Asuntos Exteriores de Ucrania, Dmytro Kuleba. [Consulta: 4 de abril 2022] Disponible en: https://www.nato.int/cps/en/natohq/opinions_188554.htm .

Stoltenberg, J. (2022). Declaración del secretario general de la OTAN sobre el ataque no provocado de Rusia contra Ucrania. [Consulta: 4 de abril 2022]. Disponible en: https://www.nato.int/cps/en/natohq/news_192401.htm

4. Otros

ACO (2021). Comprehensive Operations Planning Directive Version 3.0. OTAN.

AIRCOM PAO, N. (2021). *NATO CAOC and AGS leadership compare notes*. *ac.nato.int*. [Consulta: 20 de enero 2022]. Disponible en: https://ac.nato.int/archive/2021/COMCAOCT_visit_NAGSF.aspx

Biden, J. R. (2021). Interim National Security Strategic Guidance. The White House. [Consulta: 10 de enero 2022]. Disponible en: https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf

Bonds, T. M. *et al*. (2017). *What Role Can Land-Based, Multi-Domain Anti-Access/Area Denial Forces Play in Deterring or Defeating Aggression?* En: *RAND Corporation*. [Consulta: 23 de enero 2022]. Disponible en: https://www.rand.org/pubs/research_reports/RR1820.html

Colby, E. y Solomon, J. (2016). For Peace with Russia, Prepare for War in Europe: NATO and Conventional Deterrence. En: *War on the Rocks*. [Consulta: 20 de enero 2022]. Disponible en: https://warontherocks.com/2016/04/for-peace-with-russia-prepare-for-war-in-europe-nato-and-conventional-deterrence/

Dalsjö, R., Berglund, C. y Jonsson, M. (2019). *Bursting the bubble Russian A2/AD in the Blatic Sea: Capabilities, Countermeassures and implicartions*.

EASA (2022). Global Navigation Satellite System Outage Leading to Navigation / Surveillance Degradation. En: *European Union Aviation Safety Agency*. P. 3. [Consulta: 20 de marzo 2022]. Disponible en: https://ad.easa.europa.eu/ad/2022-02#:~:text=EASA_SIB_2022_02.pdf%20(199%20kb)

Erdogan, A. (2018). Estrategia rusa A2AD y sus implicaciones para la OTAN. En: *Más allá del horizonte.* ISSG, 6 diciembre. [Consulta: 4 de enero 2022]. Disponible en: https://behorizon.org/russian-a2ad-strategy-and-its-implications-for-nato/

Gady, F. S. (2018). Russia's Military Receives Additional New S-400 Long-Range Air Defense Regiment. En: *THE DIPLOMAT*. [Consulta: 16 de enero 2022]. Disponible en: https://thediplomat.com/2018/07/russias-military-receives-additional-new-s-400-long-range-air-defense-regiment/

Gartenstein-Ross, D. y Goodman, J. D. (2009). The Attack on Syria's al-Kibar Nuclear Facility. En: *Jewish Policy Center*. [Consulta: 21 de enero 2022]. Disponible en: https://www.jewishpolicycenter.org/2009/02/28/the-attack-on-syrias-al-kibar-nuclear-facility/

Hughes, K. (2019). Why the S-400 Missile is Highly Effective -- If Used Correctly. 12 julio, p. 6. [Consulta: 27 de marzo 2022]. Disponible en: https://worldview.stratfor.com/api/v3/pdf/307597/Stratfor_WorldView-why-s-400-s400-missile-long-range-turkey-russia-syria-effective

IDF (2017). Dirección de Inteligencia Militar. En: *Israel Defense Forces*. [Consulta: 23 de enero 2022]. Disponible en: https://www.idf.il/en/minisites/military-intelligence-directorate/

IISS (2021). The Military Balance 2021. London (UK), Routledge.

Kofman, M. (2019). It's Time to Talk About A2/AD: Rethinking the Russian Military Challenge. En: *War on the Rocks*. [Consulta: 4 de enero 2022]. Disponible en: https://warontherocks.com/2019/09/its-time-to-talk-about-a2-ad-rethinking-the-russian-military-challenge/

Kofman, M. (2020a). A2/AD. En: *Russia Military Analysis*. [Consulta: 1 de marzo 2022]. Disponible en: https://russianmilitaryanalysis.wordpress.com/tag/a2-ad/

Kofman, M. (2020b). Russian A2/AD: It is not overrated, just poorly understood. En: *Russia Military Analysis.* 25 enero. [Consulta: 2 de marzo 2022]. Disponible en: https://russianmilitaryanalysis.wordpress.com/2020/01/25/russian-a2-ad-it-is-not-overrated-just-poorly-understood/

MDAA (2022). Iskander-M (SS-26) - Alianza de Defensa de Defensa de Misiles. En: *Missile Defense Advocacy Alliance*. [Consulta: 20 de febrero 2022]. Disponible en: https://missiledefenseadvocacy.org/missile-threat-and-proliferation/todays-missile-threat/russia/iskander-m-ss-26/

NAGSMA (2022). NATO Alliance Ground Surveillance Management Agency. [Consulta: 11 de marzo 2022]. Disponible en: https://www.nagsma.nato.int/About/AGSGeneralInformation/Pages/default.aspx

NATO (2021). Alliance Ground Surveillance (AGS). En: *NATO*. [Consulta: 3 de noviembre 2021]. Disponible en: http://www.nato.int/cps/en/natohq/topics_48892.htm

Northrop Grumman (2022). Anti-Jam MilSatCom Overview. En: *Northrop Grumman*. [Consulta: 25 de marzo 2022]. Disponible

en: https://www.northropgrumman.com/anti-jam-milsatcom-overview

NSO (2009). AJP-3.3.2 (A) Allied <joint Doctrine for Close Air Support and Air Interdiction. Bruselas (Bélgica): Nato Standardization Office.

Oréjov, J. (2019). Lo sentimos, no sabíamos que era invisible: cuando un viejo misil ruso derribó un F-117 de EE. UU. [Consulta: 23 de enero 2022]. Disponible en: https://es.rbth.com/historia/83386-misil-ruso-derribo-f-117-ee-uu

Osborn, K. (2021a). Global Hawk Surveillance Drones Heading Back to the Future of Their Glory Years. En: *Warrior Maven: Center for Military Modernization*. [Consulta: 22 de febrero 2022]. Disponible en: https://warriormaven.com/air/global-hawk-drones-surveillance

Roca, J. (2022). Evolución de la situación en Ucrania. ESFAS. 28 marzo. Madrid.

Rogoway, T. (2021). The RQ-180 Drone Will Emerge From The Shadows As The Centerpiece Of An Air Combat Revolution. The Drive. [Consulta: 23 de febrero 2022]. Disponible en: https://www.thedrive.com/the-war-zone/39882/how-the-rq-180-drone-will-emerge-from-the-shadows-as-the-centerpiece-of-a-warfighting-revolution

Stout, M. y Armstrong, B. (2015). 12 Other Clashes and Close Calls with the Russians. En: *War on the Rocks*. [Consulta: 25 de marzo 2022]. Disponible en: https://warontherocks.com/2015/11/12-other-clashes-and-close-calls-with-the-russians/

Sukhankin, S. (2021). Crimea: The Expanding Military Capabilities of Russia's Area Denial Zone in the Black Sea. En: *Jamestown*. [Consulta: 22 de febrero 2022]. Disponible en: https://jamestown.org/program/crimea-the-expanding-military-capabilities-of-russias-area-denial-zone-in-the-black-sea/

Westerlund, F. (2017). Russia's Military Strategy and Force Structure in Kaliningrad. Suecia: Swedish Defence Research Agency, p. 2. [Consulta: 16 de febrero 2022]. Disponible en: https://www.foi.se/download/18.7fd35d7f166c56ebe0bbfe7/1542369070079/RUFS-40_Military-strategy-and-force-structure-in-Kaliningrad_FOI-Memo-6060.pdf

Work, R. (2016). Remarks by Deputy Secretary Work on Third Offset Strategy. En: *U.S. Department of Defense*. [Consulta: 9 de marzo 2022]. Disponible en: https://www.defense.gov/

News/Speeches/Speech/Article/753482/remarks-by-deputy-secretary-work-on-third-offset-strategy/

Zurdo, P. (2022). Ucrania, cronología de ciberataques y ciberinteligencia. En: *infobae*. [Consulta: 28 de marzo 2022]. Disponible en: https://www.infobae.com/opinion/2022/03/04/ucrania-cronologia-de-ciberataques-y-ciberinteligencia/ .