ACADEMIA DE LAS CIENCIAS
Y LAS ARTES MILITARES

Comunicaciones académicas

La disuasión frente a las amenazas híbridas en la era de la globalización

Miguel Ángel Ballesteros Martin
Academia de las Ciencias y las Artes Militares
Sección de Futuro de las Operaciones Militares

21 de octubre de 2022

El European Centre of Excellence for Countering Hybrid Threats (Helsinki), define la amenaza híbrida como la *Acción coordinada y sincronizada, que ataca deliberadamente las vulnerabilidades sistémicas de los Estados democráticos y sus instituciones, a través de una amplia gama de medios (políticos, económicos, militares, civiles y de información).*

La amenaza basada en una estrategia hibrida es tan antigua como la guerra entre sociedades organizadas. Sin embargo, en un mundo globalizado como el que vivimos, lo híbrido ha adquirido una nueva dimensión que favorece su empleo en la denominada «zona gris», que incluso puede desencadenar una guerra hibrida, cuyos efectos trascienden las fronteras de los contendientes. Un buen ejemplo fue la guerra del Yom Kippur de 1973, en la que los países árabes –a través de la OPEP– recortaron la producción de petróleo. Como consecuencia, en poco tiempo llegó a duplicar su precio, lo que provocó un aumento de la inflación y finalmente la recesión que duró varios años en los países importadores. El uso del petróleo como arma provocó una crisis económica cuyas consecuencias se sintieron más allá de Israel y sus aliados. De esta forma se evidenció que los efectos económicos de la guerra hibrida abarcaban más territorio que el de los contendientes y su duración es más larga que los de las operaciones militares.

Pero el mundo de hoy es muy diferente del de 1973. Con los avances tecnológicos, el ciberespacio y las capacidades que ofrecen las nuevas redes de comunicación, las denominadas TIC, se ha incrementado el campo de aplicación de las estrategias hibridas, mediante los ciberataques y la rápida difusión de las campañas de desinformación. En este contexto, la globalización ha permitido interconectar la mayor parte de la economía mundial, ampliar las cadenas de suministros para todo tipo de materiales, incluidos aquellos que son críticos para la seguridad nacional. Esto introduce nuevas variables en la ecuación de los conflictos, y la confrontación geopolítica, lo que obliga a un estudio y conceptualización de las estrategias hibridas, que se convierten en excelentes instrumentos para alcanzar objetivos geopolíticos a corto, medio y largo plazo.

La globalización favorece las posibilidades que ofrecen las estrategias hibridas que tienen lugar en la zona gris, lo que ha favorecido la asertividad de potencias regionales. Esto provoca una mayor rivalidad geopolítica.

Josep Baqués define la zona gris como *una competición estratégica entre dos o más Estados […] discurre por debajo del umbral de violencia política del conflicto armado menor situando la zona gris por debajo de la Guerra Hibrida*. Añadamos, que no son frecuentes las estrategias de disuasión para hacer frente a las amenazas hibridas en la zona gris, dado que aparentan ser menos peligrosas que las amenazas convencionales, lo que resulta muy atractivo para algunos regímenes autoritarios, que ven la posibilidad de aprovechar ese exceso de confianza de sus adversarios.

En los últimos diez años hemos sido testigos de cómo las estrategias hibridas se han transformado en amenazas hibridas, que acaban favoreciendo la aparición de conflictos híbridos en la zona gris, para finalmente acabar desencadenando guerras hibridas en las que hay operaciones de combate. Desde 2006, Rusia ha buscado el monopolio como suministrador de gas para toda Europa central, para desencadenar un conflicto en la zona gris para anexionarse Crimea en 2014 y finalmente desencadenar una guerra hibrida, invadiendo Ucrania en 2022. Todo ello con el objetivo geopolítico de llegar a controlar los espacios que formaron parte de la URSS.

El 9 de noviembre de 2012, el general ruso Valeri Gerasimov fue nombrado Jefe del Estado Mayor General y en febrero de 2013 publicaba un artículo titulado *El valor de la ciencia en la anticipación* sobre el conflicto hibrido, en donde describía las ventajas de saber combinar instrumentos convencionales como las operaciones militares con otras no convencionales como los ciberataques o las campañas de desinformación. Es lo que ahora muchos analistas denominan «doctrina Gerasimov». En ese artículo podemos leer: *El valor de la ciencia está en la*

capacidad de prever lo que sucederá o podrá suceder en el futuro, los nuevos desafíos exigen repensar las formas y métodos de llevar a cabo las operaciones de combate. Una invitación a revisar las doctrinas militares convencionales propias y ajenas.

Las amenazas híbridas pueden ir desde ciberataques a infraestructuras críticas, pasando por la interrupción de los servicios financieros, suministro de energía, hasta el socavamiento de la confianza pública en las instituciones gubernamentales o la profundización de las divisiones sociales mediante la polarización. E incluso la injerencia en procesos electorales de terceros países para acabar poniendo en riesgo los sistemas democráticos. Y todo ello aprovechando la dificultad de establecer la atribución de la autoría de los ciberataques, las injerencias, la desinformación o el empleo de mercenarios; así como la imposibilidad de establecer con rigor la relación causa efecto derivado de estas acciones. En este marco, los países democráticos –siempre respetuosos con las leyes nacionales e internacionales, con la libertad de expresión– son más propicios a sufrir campañas de desinformación y las injerencias en procesos electorales.

Volviendo al general Gerasimov, él considera que en el conflicto hibrido, la combinación de instrumentos no militares con operaciones militares, permite reducir la necesidad de estas últimas a la cuarta parte. Si sumamos a esta ventaja cuantitativa, la mayor facilidad para controlar la escalada del conflicto, se podrá conseguir que este permanezca en la denominada zona gris, sin llegar al combate abierto, evitando las acciones de represalia militar.

En 2014, un año después de que el general Gerasimov expusiera su doctrina, Rusia desencadenó un conflicto hibrido aprovechando el vacío de poder en Kiev, para anexionarse la península de Crimea, a la vez que promovía la rebelión del valle del Dombas, que se declaraba independiente con el nombre de Novorrosia, antigua región rusa en época de la zarina Catalina La Grande. Esto supuso una declaración de intenciones del Kremlin sobre su propósito de llegar a controlar las provincias de Luhansk, Donestk, Zaporizha, Kherson con Odesa, Mykolaiv a lo que hay que añadir Transnistria (Moldavia) y Crimea. Estos territorios en manos rusas dejarían sin salida al mar a Ucrania, estrangulando su economía.

La estrategia para hacerse con Crimea fue una combinación de operaciones militares que no debían alcanzar el uso de la violencia, manteniéndose en la denominada «zona gris». Para ello mezclaron operaciones militares encubiertas, despliegues en la frontera como medida de disuasión, etc. con otras acciones que van desde el bloqueo energético, la presión diplomática y la económica, ciberataques, campañas de desinformación, etc. Rusia había logrado su objetivo

de apoderarse de Crimea mediante un conflicto hibrido que se llevó a cabo en la zona gris.

Sin embargo, no se puede decir lo mismo de las acciones de rebeldes de Luhansk y Donetsk que con el apoyo de Rusia desencadenaron la guerra en el valle del Dombass, que se detuvo con un tenso alto el fuego fijado en los acuerdos de Minsk II firmados el 12 de febrero de 2015. Ucrania no disponía de una estrategia de disuasión frente a la amenaza hibrida rusa, más allá de su anhelada entrada en la OTAN. Tampoco los países de la OTAN y de la UE contribuyeron a definir una estrategia de disuasión frente a este tipo de amenazas a pesar de los avisos que supusieron los casos de Osetia del Sur y Abjasia en 2008.

Acciones de la UE y la OTAN frente a las amenazas hibridas

La constatación de la asertividad de Rusia mediante el empleo de las estrategias hibridas para alcanzar sus objetivos geopolíticos, puso a Occidente en alerta y en la reunión de Ministros de Asuntos Exteriores de la OTAN celebrada en Bruselas en diciembre de 2015, se aprobó la «Estrategia de la OTAN para hacer frente a las guerras híbridas», poniendo énfasis en la imprescindible complementariedad y coordinación entre la OTAN y la UE, y el refuerzo de los programas de apoyo a los países socios para el fortalecimiento de sus instituciones de seguridad y defensa. Por su parte el Secretario General Stoltenberg, afirmó que *lo híbrido es el lado oscuro de nuestro Enfoque Integral* y es que las amenazas hibridas requieren una estrategia basada en el enfoque integral.

Por su parte, el Parlamento Europeo (PE) ese mismo año, no alerta sobre la guerra hibrida perro sí pone el énfasis en el conflicto híbrido, indicando que es una «situación en la cual las partes se abstienen del uso abierto de la fuerza (armada) y actúan combinando la intimidación militar (sin llegar a un ataque convencional) y a la explotación de vulnerabilidades económicas, políticas, tecnológicas y diplomáticas». El PE sitúa la amenaza hibrida en la zona gris, olvidando la posibilidad de la escalada.

Poco después en 2016, se creó la *Hybrid Fusion Cell* (HFC) dentro del *EU Intelligence and Situation Centre* (EU INTCEN), como foco único a nivel europeo para el análisis de las amenazas híbridas. La célula recibe y analiza información clasificada y de dominio público relacionada específicamente con los indicadores y las alertas en materia de amenazas híbridas.

Ese mismo año, la Comisión Europea publicó la *Joint Framework on countering hybrid threats*, que trata de identificar las amenazas hibridas; organizar la respuesta de la UE, mejorar la concienciación de los Estados miembros y sus sociedades;

tratar de organizar la respuesta de la UE mediante el reforzamiento de la resiliencia de cada Estado miembro; a la vez que incentiva la prevención, la respuesta a las crisis y su recuperación y por último procura el aumento de la cooperación con la OTAN. Para conseguirlo, el documento refiere que es esencial a corto plazo, reforzar la capacidad de los Estados miembros y de la Unión para prevenir las amenazas híbridas, responder a ellas y recuperarse, de forma rápida y coordinada. El tiempo demostraría que se necesita algo más que coordinación.

También en 2016, el presidente del Consejo Europeo, el presidente de la Comisión Europea y el secretario general de la OTAN firmaron en Varsovia una declaración conjunta sobre siete ámbitos de cooperación, en donde destaca la lucha contra las amenazas híbridas.

En 2017 se creó el *European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)* en Helsinki, con el objetivo fomentar el diálogo estratégico y realizar actividades de investigación y análisis sobre las amenazas híbridas, así como estimular el desarrollo de nuevos conceptos y tecnologías en el sector privado y la industria para ayudar a los Estados miembros a reforzar su resiliencia.

Ya en 2018, la Comisión Europea publicó la *Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats*, en la que se repasa los avances conseguidos desde 2016 y se marcan nuevos objetivos como por ejemplo: mejorar la capacidad de detección de amenazas híbridas; mejorar las capacidades de comunicación estratégica de la UE; hacer frente a las campañas de desinformación y las interferencias híbridas por parte de gobiernos extranjeros; o el aumento de la resiliencia y de la disuasión en el sector de la ciberseguridad. Además, advierte que las amenazas hibridas apuntan a vulnerabilidades críticas y buscan crear confusión para dificultar la toma de decisiones y están diseñadas para ser difíciles de detectar o atribuir.

Por otro lado, las amenazas químicas, biológicas, radiológicas y nucleares (NBQR) generadas por medios no convencionales están dentro de una categoría propia debido al potencial daño que pueden causar. Como la atribución es difícil, estos desafíos requieren medidas específicas y coordinadas para contrarrestar; por ejemplo, detección de la transferencia de productos químicos peligrosos, reduciendo el acceso a ellos.

En 2019, se creó el *Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats* (HWP ERCHT), para ofrecer una visión horizontal de las cuestiones relacionadas con las amenazas híbridas y favorecer la coherencia y la cooperación entre la UE y sus Estados miembros. En especial en los ámbitos de la resiliencia estatal y social, la comunicación estratégica y la lucha contra la desinformación.

Ese mismo año 2019, el Consejo de la Unión Europea publicó las *Council Conclusions on Complementary Efforts to Enhance Resilience and Counter Hybrid Threats*, en las que se indica, entre otras cosas que: la responsabilidad de luchar contra las amenazas híbridas incumbe principalmente a los Estados miembros. Los esfuerzos a escala de la UE son de naturaleza complementaria y se llevan a cabo sin perjuicio de la responsabilidad exclusiva de los Estados miembros en cuestiones de seguridad nacional. La crisis energética y económica derivada de la invasión rusa de Ucrania, nos indica que la UE debe de tomar un mayor protagonismo en el diseño de planes de resiliencia energética, económica, tanto en materia energética, financiera, sanciones, cadenas de suministros, etc.

El documento también indica que la relación entre las amenazas híbridas y la seguridad económica es estrecha, aunque su responsabilidad sigue recayendo principalmente sobre los Estados miembros, debiéndose identificar y hacer frente a inversiones extranjeras directas que puedan afectar a la seguridad o al orden público. Con todo, la lucha contra las amenazas hibridas requiere un planteamiento global en el que se involucren el gobierno y la sociedad, y en el que se trabaje de manera más estratégica, coordinada y coherente en todos los sectores de actuación pertinentes. Algo que hoy es fundamental para hacer frente a la crisis energética, económica y militar derivada de la invasión rusa de Ucrania.

Por su parte la OTAN, ha implementado los Equipos de Apoyo Contra Amenaza Híbrida (conocidos como CHST71) que se pueden desplegar ante una crisis. Dada la experiencia de sus miembros en comunicaciones estratégicas, contrainteligencia o protección de infraestructuras críticas, sus expertos también asesoran en el establecimiento de estructuras de defensa orientadas a hacer frente a las amenazas hibridas.

Es necesario que las organizaciones internacionales como la OTAN y la UE deben tomar un mayor protagonismo en las medidas de disuasión frente a las amenazas hibridas.

Estrategias frente a amenazas hibridas

Las estrategias a realizar para contrarrestar las amenazas hibridas se basan en tres aspectos: detectar las amenazas híbridas, disuadir a los agresores híbridos, y ser capaces de responder a los ataques. La diversificación, complejidad, multiplicidad y latencia de las estrategias hibridas hacen que sea complicado evitar su materialización en todos los casos.

Las amenazas hibridas por su carácter multifacético y sus cambios constantes requieren sistemas integrados de información para facilitar la toma rápida de

decisiones. Esto es posible mediante un Sistema de Seguridad Nacional (SSN) con información digitalizada que aproveche la explotación de la información que puede proporcionar la Inteligencia Artificial.

La gestión de las crisis derivadas de conflictos o guerras hibridas requieren enfoques transversales basados en información holística de la situación, capacidades propias y posibilidades para una correcta toma de decisiones.

La Estrategia Nacional de Ciberseguridad 2019 ya establece en su Medida 6: *Desarrollar con los países de nuestro entorno una mayor conciencia sobre las Amenazas Híbridas, limitando su impacto sobre la soberanía e integridad de nuestros países*.

Y el Consejo de Seguridad Nacional decidió en 2020 adelantar la revisión de la ESN 2017 entre otras razones para establecer líneas de acción capaces de hacer frente a las amenazas hibridas. Y así la ESN 2021 establece que *su tercer objetivo es desarrollar la capacidad preventiva, de detección y respuesta frente a las estrategias híbridas*. Y al identificar y analizar los 16 riesgos y amenazas señala el grado de participación que pueden tener en las amenazas hibridas. Estableciendo líneas de acción para hacerlas frente como, por ejemplo:

LA 9: «Desarrollar el modelo de gestión integral de crisis en el Sistema de Seguridad Nacional a través de la elaboración de un reglamento de gestión de crisis; la implantación de un sistema de alerta temprana basado en indicadores…».

LA 10: «Crear la Reserva Estratégica basada en capacidades nacionales de producción industrial…».

LA 13: «Elaborar una Estrategia Nacional de Lucha contra las campañas de desinformación».

LA 20: «Potenciar la modernización y la productividad del ecosistema español industrial, mediante el impulso de la competitividad de sectores estratégicos clave para la Seguridad Nacional, en línea con lo establecido en el Plan de Recuperación, Transformación y Resiliencia».

LA 25: «Actualizar la Estrategia de Seguridad Energética Nacional para establecer objetivos y líneas de acción de acuerdo con el contexto de transición ecológica, energética y económica».

Desde el punto de vista organizativo, el Departamento de Seguridad Nacional (DSN) preside, desde 2018, el Grupo de Consulta sobre la Amenazas Hibridas, constituido por el MAUEC, el MINT, el MINISDEF y el CNI. Su objetivo es

intercambiar información entre distintos departamentos y organismos, consensuar y homogeneizar posturas nacionales, y alertar de los sucesos relacionados con este fenómeno o englobados en campañas de desinformación.

El DSN es también el punto de contacto para la Amenaza Hibrida ante las instituciones europeas.

En 2020 el Consejo de Seguridad Nacional aprobó un procedimiento para luchar contra las campañas de desinformación.

Por último, el Gobierno creó en 2018 el puesto de Embajador en Misión Especial para las Amenazas Híbridas y la Ciberseguridad, al igual que existe en otros países como Suecia y Finlandia.

Pero la naturaleza de la UE está mejor dotada para hacer frente a las amenazas hibridas en los asuntos no específicamente militares, por lo que la disuasión frente amenazas hibridas necesita la colaboración de OTAN y UE.

La disuasión frente a amenazas hibridas requiere:

- Una disuasión compartida frente a estrategias hibridas que, a partir de la disuasión y resiliencia nacional, se apoyan en la disuasión de la OTAN y de la UE, una política de atribución con los socios y aliados y sanciones eficientes.
- Luchar contra las campañas de desinformación dentro y fuera de las fronteras: con una mayor Cultura de Seguridad Nacional, potenciando el análisis crítico y fomentando la cohesión social
- Superioridad tecnológica y muy especialmente en el ciberespacio: Control del dato, Ciberseguridad, Alianzas industriales y Reservas de capacidades industriales (RECAPI).
- Mantener la iniciativa mediante el apoyo social, las cadenas de suministros propias y evitar los puntos débiles

Por eso debemos prevenir mediante la disuasión y actuar desde tiempos de paz, para lograr lo que decía Sun Tzu: «La victoria completa se produce cuando el enemigo no lucha ... y es vencido por el empleo de la estrategia».