ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

55/2018 10 de mayo de 2018

*Rafael José de Espona**

Guerra híbrida y capacidades estratégicas de la OTAN: aportaciones de Lituania, Letonia y Estonia

Guerra híbrida y capacidades estratégicas de la OTAN: aportaciones de Lituania, Letonia y Estonia

Resumen

La guerra híbrida ha transformado el panorama del conflicto y requiere potenciar capacidades al respecto. La OTAN está en la vanguardia de esta orientación, con destacada contribución de los aliados del Báltico. Se explicará la misión y actividad de los tres Centros de Excelencia (CoEs) que la OTAN dispone en Lituania, Letonia y Estonia en un marco convergente, relacionándolo con los cometidos de la División de Desafíos Emergentes (ESCD) y el Programa Ciencia para la Paz y Seguridad (SPS), bajo la premisa de que las capacidades relacionadas con estos ámbitos suponen de por sí un factor decisivo para plantear una campaña con relevante probabilidad de éxito.

Palabras clave

OTAN, guerra híbrida, ciberdefensa, seguridad energética, comunicación estratégica, guerra de información.

Hybrid Warfare and NATO strategic capabilities: contributions from Lithuania, Latvia and Estonia

Abstract

Hybrid Warfare has transformed the conflict overview and it demands to boost capabilities on the issue. NATO is on the cutting edge of this facing, which the relevant contribution of allies from Baltic region. It will be described mission and activity of the three Centers of Excellence (CoEs) that NATO allocates in Lithuania, Latvia and Estonia in a convergent framework, linking them with the tasks of Emerging Security Challenges Division (ESCD) and the Science for Peace and Security Programme (SBS), under the premise of considering that the capabilities linked to these areas mean by itself a key factor for planning a campaign with relevant probability of being successful.

Keywords

NATO, Hybrid Warfare, Cyberdefense, Energy Security, Strategic Communication, Information Warfare.

La guerra híbrida

La moderna *guerra híbrida* ha transformado la ciencia bélica y el panorama de tipología de conflictos, de lo que se deriva la necesidad de adecuar los medios de defensa al respecto[1]. El desarrollo de este concepto en el fondo parte de viejos problemas, sustancialmente basados en las actualizadas metodologías de hacer la guerra, prevalecer mediante la hostilidad, agredir o generar desestabilización, como la *Lawfare*[2]. Se parte de la premisa de que las capacidades relacionadas con este ámbito suponen de por sí un factor decisivo para plantear autónomamente una campaña con probabilidad de éxito.

La OTAN se encuentra en la vanguardia de esta orientación, desde que el Concepto Estratégico de 2010 impulsó los aspectos cibernético, energético y de comunicación estratégica en su perspectiva de defensa. La *División de Desafíos Emergentes* (ESCD-*Emerging Security Challenges Division*) establecida en 2010 se ocupa de riesgos y amenazas no convencionales, con secciones específicas relativas a Antiterrorismo, Ciberdefensa, Seguridad Energética, No-proliferación, Análisis Estratégico, Seguridad Económica y Política Nuclear. Por su parte, el *Programa Ciencia para la Paz y Seguridad* (SPS-*Science for Peace and Security*) promueve la investigación e innovación científica y el intercambio de conocimiento relacionados con actividades relevantes para la seguridad, de acuerdo con los objetivos de la Alianza, con un enfoque práctico y de aplicación operativa, englobando a científicos, expertos y funcionarios de países aliados y asociados. La especialización por materias encuentra en los distintos Centros de Excelencia de la OTAN (CoEs-*Centres of Excellence*) órganos de desarrollo de capacidades de acuerdo con la vanguardia técnica de cada sector, en perspectiva de apoyo a la transformación, funcionando en programas de

[1] COTTER, Bryan P., «De-escalation and Hybrid War: Mutually Supporting Strategies or Dangerous Brinkmanship?»*The Three Swords Magazine*, n.º 31 (2017), pp. 24-34. FLEMING, Brian P., *The Hybrid Threat Concept: Contemporary War, Military Planning and the Advent of Unrestricted Operational Art*, Fort Leavenworth (Kansas), School of Advanced Military Studies – United States Army Command and General Staff College, 2011, pp. 33-39. GARCÍA GUINDO, Miguel, MARTÍNEZ, Gabriel, GONZÁLEZ, Valera, «La Guerra Híbrida: Nociones preliminares y su repercusión en el planeamiento de los países y organizaciones occidentales», IEEE, DIEEET02-2014 (30 de marzo de 2015). SÁNCHEZ HERRAEZ, Pedro, «Comprender la guerra híbrida… ¿el retorno a los clásicos?», IEEE, Documento de Análisis 42/2016 (21 de junio de 2016). COLOM PIELLA, Guillem, «¿El auge de los conflictos híbridos?», IEEE, Documento de Opinión 120/2014 (24 de octubre de 2014). SÁNCHEZ HERRAEZ, Pedro, «La nueva guerra híbrida: un somero análisis estratégico», IEEE, Documento de Análisis 54/2014 (29 de octubre de 2014).

[2] MANDELBLIT, Avihai, «Lawfare: The legal front of the IDF», INSS - Military and Strategic Affairs, vol. 4 n.º 1 (abril 2012), pp. 51-57.

trabajo anuales —que evitan duplicidad de gastos o recursos— coordinados con el Mando de Transformación (ACT-*Allied Command Transformation*). Entre los Centros de Excelencia, los de ciberdefensa, seguridad energética y comunicación estratégica suponen ámbitos que confluyen precisamente en el campo de la *guerra híbrida*.

La región del Báltico, en el borde oriental de la OTAN, conforma un escenario geopolítico que continúa siendo una posición avanzada de alerta temprana sobre los vectores de acción exterior rusa y lugar de diáfana percepción del devenir de conflictos actuales como el acaecido en Ucrania. La implicación regional de la OTAN bajo su artículo 5 destaca, entre otros, por la misión permanente de Policía Aérea y el reciente despliegue permanente de unidades (*enhanced Forward Presence*-eFP), en un teatro de operaciones sobre el que se cierne la amenaza híbrida junto a la convencional[3]. La contribución de los tres aliados del Báltico —Estonia, Letonia y Lituania— a la Alianza Atlántica destaca cualitativamente por su condición de naciones anfitrionas de un Centro de Excelencia de la OTAN: en el caso de Estonia, del *Centro de Excelencia de Ciberdefensa Cooperativa* (*NATO CCD CoE*) creado en 2008, Lituania del *Centro de Excelencia de Seguridad Energética* (*NATO ENSEC CoE*) acreditado en 2012 y Letonia del *Centro de Excelencia de Comunicación Estratégica* (*NATO STRATCOM CoE*) establecido en 2014. Dentro del organigrama de la Alianza, la ESCD integra sus capacidades, que son convergentes. Asimismo, estos tres países participan en el *Centro Europeo de Excelencia contra las Amenazas Híbridas* (*Hybrid CoE*) junto a Alemania, España, Estados Unidos, Finlandia, Francia, Gran Bretaña, Holanda, Noruega, Polonia y Suecia.

Es propósito del presente estudio explicar sintéticamente la actividad y sinergias de dichos CoE, como aportación de los aliados bálticos a las capacidades de la OTAN para hacer frente a desafíos actuales y futuros de la guerra híbrida.

Ciberdefensa

A lo largo de la última década, la OTAN ha resaltado reiteradamente que los ciberataques suponen una de las nuevas amenazas a la que ha de hacer frente. Consecuentemente, de manera creciente se ha dotado de medios y recursos para ser

[3] RADIN, Andrew, *Hybrid Warfare in the Baltics. Threats and Potential Responses*, RAND Corporation, Santa Mónica, 2017.

capaz de garantizar la defensa en la dimensión ciberespacial. Las Fuerzas Armadas de los países aliados han conformado mandos conjuntos de ciberdefensa, y se ha incorporado el ámbito cibernético en los procesos de planeamiento. La política de la OTAN de 2011 en materia de ciberdefensa, ha marcado los objetivos y prioridades de la alianza en esta materia; subsiguientemente, la Cumbre de Chicago de 2012 integró la ciberseguridad en el programa *Smart Defence* de la Alianza enfocado al desarrollo de cibercapacidades por parte de los países aliados. El *iter* del conflicto en el caso de la ciberguerra se reviste de problemas de percepción y atribución —con implicaciones jurídicas complejas— y el ciberespacio se presta al devenir de la guerra híbrida tanto como teatro de operaciones como medio de acción en sí mismo[4]. Toda vez que la ciberdefensa es parte de los cometidos de defensa común de la OTAN, la Alianza ha reiterado que el derecho internacional ha de ser aplicado al ciberespacio. En julio de 2016, los aliados proclamaron que el ciberespacio se considera una 4.ª dimensión de las operaciones militares, junto a la tierra, mar y aire.

La OTAN y la UE implementan un Acuerdo Técnico de Cooperación en Ciberdefensa (de febrero de 2016) para el desarrollo constante de capacidades informáticas, modernización de redes, sistemas y soportes telemáticos, intercambio de información y mutua asistencia para prevenir, mitigar efectos y recuperar actividad tras un ciberataque. Para ello incluyen actividades de formación y ejercicios, así como la interacción con la industria a través de programas como el *Industry Cyber Partnership* de la OTAN.

Estonia fue el primer país de la OTAN que sufrió un ataque cibernético masivo, en primavera de 2007, y actualmente es la nación del mundo más integrada (en términos de actividad social y estatal) en el ciberespacio. Las lecciones aprendidas del ciberataque de 2007 han servido para percibir mejor la naturaleza y procedencia de las agresiones que en los 3 últimos años se proyectan contra Ucrania[5]. El Centro de

---

[4] LIBICKI, Martin C., *Cyberdeterrence and Cyberwar,* RAND Corporation, Santa Mónica, 2009. CARO BEJARANO, María José, «Nuevo concepto de Ciberdefensa de la OTAN», IEEE, Documento Informativo 09/2011 (marzo de 2011). LEJARZA ILLARA, Eguskiñe, «Ciberguerra, los escenarios de confrontación», IEEE, Documento de Opinión 18/2014 (21 de febrero de 2014).
URUEÑA CENTENO, Francisco J., «Ciberataques, la mayor amenaza actual», IEEE, Documento de Opinión 09/2015 (16 de enero de 2015). SINGER, P.W, FRIEDMAN, Allan, *Cybersecurity and Cyberwar. What everybody needs to know*, Oxford University Press, New York, 2014.

[5] JOUBERT, Vincent, «Five years after Estonia`s cyber attacks: lesson learned for NATO?», Research Division NATO Defense College Rome, Research Paper n.º 76 (May 2012). GEERS, Henneth (ed.), *Cyber War in Perspective: Russian Agression against Ukraine*, CCDCOE, Tallin, 2015. BAEZNER, Marie,

Excelencia de Ciberdefensa Cooperativa de la OTAN (*NATO CCD CoE*) fue establecido por Estonia en 2008 (España se encuentra entre las naciones fundadoras) como nación líder. Sus integrantes en 2017 son Alemania, Bélgica, República Checa, Eslovaquia, España, Estados Unidos, Francia, Gran Bretaña, Grecia, Holanda, Hungría, Italia, Letonia, Lituania, Polonia y Turquía como naciones patrocinadoras, a los que se adhieren Austria y Finlandia como contribuyentes (Suecia se encontraba en dicho proceso a finales de dicho año). Este CoE contribuye al conocimiento y competencias de la OTAN en el ámbito de ciberdefensa en los campos tecnológico y jurídico, en los escalones estratégico y operacional. El centro ha auspiciado la conformación del manual técnico *Tallinn Manual 2.0*, que constituye el principal análisis de la aplicación de la normativa jurídica internacional al ciberespacio. Como centro multinacional y multidisciplinar, organiza los más amplios y complejos ejercicios técnicos en ciberdefensa, los *Locked Shields*, caracterizados por incorporar elementos de vanguardia tecnológica. Con periodicidad anual —organizados desde 2010— los ejercicios de defensa cibernética cuentan con una red de trabajo acreditada, operan en tiempo real y han sido enfocados al adiestramiento de los expertos de seguridad para la acción práctica, en orden proteger redes de telecomunicaciones y gestión electrónica de información, la conferencia anual *CyCon* (acrónimo inglés de *cyber conflict*). Los distintos cursos de formación monográficos, conferencias, seminarios, estudios y publicaciones técnicas abarcan temáticas específicas como protección de infraestructuras críticas, aspectos tecnológicos y jurídicos.

Entre las tendencias de mejora de capacidades en ciberdefensa destacan la coordinación público-privada en CERTs, la Gestión de Crisis como la de verano de 2017 con el virus *Wanna Cry* o un fallo sistémico tipo *big one* en infraestructuras críticas. La ciberdefensa interacciona con el ámbito de seguridad energética especialmente en la protección de redes de gestión SCADA, y con el campo de la comunicación estratégica respecto de operaciones de información y psicológicas en el ciberespacio.

ROBNER, Patrice, *Cyber and Information warfare in the Ukrainan conflict*, Center for Security Studies, Zürich, 2017.

Seguridad energética

El concepto de seguridad energética desarrollado entre los expertos de la Alianza Atlántica desde 2010 ha proporcionado un enfoque integrado y multidimensional sobre el sector energético, de perfil funcional y sistémico, superando el clásico físico-territorial. Incorporando la denominada *smart energy*, mejora la eficiencia, la independencia y la resiliencia de los sistemas y subsistemas energéticos (eléctrico, gasístico, petrolífero y nuclear), reduciendo su vulnerabilidad y sensibilidad; en la dimensión estrictamente militar, particulariza la seguridad energética operativa[6]. La Cumbre OTAN de Varsovia de julio de 2016 ha destacado las múltiples implicaciones de la seguridad energética, señalando la crisis de Ucrania y la instrumentación del aprovisionamiento energético ruso y mostrando cómo el sector energético se encuentra entre los campos más afectados por las modernas técnicas de guerra híbrida[7].

Lituania, desde el primer momento de la transición postsoviética, ha buscado diversificar sus fuentes de aprovisionamiento energético —debido al monopolio de suministro ruso— así como integrar la «isla energética del Báltico» con la UE, lo que ha logrado con la puesta en operación de las terminales *offshore* de Butinge (de crudo, única vía de importación desde 2008), Klaipeda (de GNL, desde 2016) y las líneas de interconexión eléctrica *LitPol Link* con Polonia (terrestre) y *NordBalt Link* con Suecia (submarina). Como consecuencia de su experiencia en la transición tecnológica energética postsoviética y en su proceso estratégico de diversificación e integración energéticas en un entorno de conflictividad sectorial internacional, Lituania alcanzó la acreditación en 2012 de su *Centro de Excelencia de Seguridad Energética* (*NATO ENSEC CoE*). Además de Lituania como nación fundadora, tiene por miembros (en 2017) a Alemania, Estados Unidos, Estonia, Francia, Georgia, Gran Bretaña, Italia, Letonia y Turquía (encontrándose Finlandia en proceso de adhesión, y siendo contribuyentes Canadá y República Checa). Este centro asiste al mando estratégico de la OTAN y otras entidades civiles y militares de su entorno favoreciendo la interoperatividad y un conocimiento adecuado en la materia de seguridad energética,

[6] ESPONA, Rafael José de, «El moderno concepto integrado de Seguridad Energética», IEEE, Documento de Opinión 32/2013 (2 de abril de 2013). ESPONA, Rafael José de, «La seguridad energética en la OTAN», IEEE, Documento de Opinión 13/2010, octubre 2010. MARINO, Thomas, «Maintaining NATO's technological edge: Strategic adaptation and defense Research & Development», NATO Parliamentary Assembly – Science and Technology Committee Report (8 de octubre de 2017).

[7] MOLIS, Arunas, VAISNORAS, Tomas, «Energy Security through membership in NATO and the EU: interests and achievements of Lithuania», *Lithuanian Foreign Policy Review,* 2014 (Issue 32), pp. 13-32.

proponiendo soluciones concretas y eficientes según necesidades de las unidades y requerimientos de las misiones (teniendo en cuenta elementos que inciden al respecto, como el factor medioambiental y la limitación de costes). Para ello, el centro interacciona con el ámbito académico e industrial y crea redes de trabajo. Entre sus áreas temáticas de actividad se distinguen aspectos de propulsión de plataformas, logística del suministro energético en operaciones, protección de infraestructuras críticas y otras. Asimismo, los grupos de trabajo del CoE identifican futuras necesidades vinculadas al proceso de transformación de la OTAN. De las múltiples actividades que realiza, sobresalen los cursos de conciencia estratégica (ESSAC-*Energy Security Strategic Awareness Course*), la conferencia bianual IESMA (*Innovative Energy Solutions for Military Aplications*) que convoca a mandos de la OTAN y expertos militares junto con la industria energética para poner al día las innovaciones tecnológicas que proporcionan soluciones comercialmente disponibles o prototipos en proceso de lanzamiento, publicaciones técnicas (i.e. *Energy Security Operational Highlights*), seminarios *ad hoc*, estudios de campo (i.e. la evaluación del impacto del cambio cultural social sobre el marco de la seguridad energética) y desarrollo de prototipos (i.e. generador híbrido empleable en operaciones a nivel unidad de entidad batallón, presentado en EUROSATORY 2016).

Respecto de las tendencias relativas al incremento de capacidades en materia de seguridad energética, se destaca las mejoras en integración de elementos logísticos y de protección medioambiental a nivel seguridad energética operativa[8], la eficiencia energética (*Smart Energy*) y la Protección de Infraestructuras Críticas Energéticas (CEIP). La seguridad energética interacciona con el ámbito de la comunicación estratégica en aspectos como la orientación social al respecto de fuentes energéticas (a través de campañas de concienciación dirigida)[9] y con la ciberdefensa en cuestiones de gestión informática de redes energéticas (i.e. *software* SCADA empleado por los operadores de sistemas de transmisión eléctrico, gasístico o petrolífero).

[8] NUTTALL, William J., SAMARAS, Constanti, BRAZILIAN, Morgan, *Energy and the Military: Convergence of Security, Economic, and Environmental Decision-Making*, University of Cambridge, EPRG Working Paper n.º 1717, Cambridge Working Paper in Economics n.º 1752 (November 2017).

[9] https://enseccoe.org/en/newsroom/discussion-on-cultural-change/79

Comunicación estratégica

La comunicación estratégica (*StratCom*) se ha erigido recientemente en elemento vital para la Alianza Atlántica, que ha publicado una Política de Comunicación Estratégica y unas directivas para el mando estratégico. Su finalidad consiste en asegurar que las audiencias —favorables o adversarias— (en una nación o región donde la Alianza desarrolla operaciones) reciben adecuada, veraz y oportuna información que les permita entender las acciones llevadas a cabo y su intencionalidad, lo cual habría de detener las agresiones al tiempo que acercar los objetivos. Corresponde a los comandantes de la operación ponderar la velocidad y secuencia de diseminación de la información, de acuerdo con los requisitos de seguridad operativa. La conceptuación actual de la comunicación estratégica la integra como parte inherente al proceso de planeamiento y conducción de las operaciones, para su efectividad práctica. El entorno global de profusión informativa con empleo de tecnologías de telecomunicación de general acceso (i.e. Internet y telefonía móvil) implica que la difusión informativa tenga una cadencia lo más próxima al tiempo real, y que la evaluación de efectos sea rápida. La identificación y segmentación de audiencias potenciales perfiladas por sus percepciones, actitudes y creencias requiere una adecuada coordinación con órganos de Inteligencia, el desarrollo de adecuado análisis sociológico y la selección de canales de comunicación (tanto propios como a través de medios de masas) adecuados para el área de operaciones[10].

En Letonia se han sufrido directamente los efectos de las operaciones de información oponentes a los valores de la Alianza Atlántica[11] y, como parte de sus esfuerzos para contrarrestarlos y promover las capacidades de la OTAN en este ámbito, estableció en 2014 el *Centro de Excelencia de Comunicación Estratégica* (*NATO STRATCOM CoE*) ubicado en Riga. Además de esta nación fundadora, en 2017 son sus miembros —*sponsoring nations*— Alemania, Estonia, Gran Bretaña, Holanda, Italia, Lituania y Polonia (Finlandia y Suecia están asociados y Francia en proceso de adhesión). El CoE

[10] MAZÓN BORN, Diego (Pres.), «La comunicación estratégica», IEEE, Documento de Seguridad y Defensa 72 (marzo de 2017).
CAMBRIA, Antonino, «La importancia de la Comunicación Estratégica», IEEE, Documento de Opinión 42/2016 (2 de mayo de 2016). SALVADOR, Luis de, «Ingeniería social y operaciones psicológicas en Internet», IEEE, Documento de Opinión 74/2011 (18 de octubre de 2011).

[11] IASIELLO, Emilio J., «Russia`s Improved Information Operations: From Georgia to Crimea», *Parameters*, n.º 47-2 (2017), pp.51-63. CIZIK, Tomas, *Information Warfare as a Geopolitical Tool, Centre for European and North Atlantic Affairs*, April 2017.

tiene como finalidad poner a disposición de la Alianza capacidades reforzadas en comunicación estratégica, con modernos sistemas de simulación, medición y planificación. Como ámbitos concretos en los que actúa, sobresalen: la diplomacia pública que involucra las comunicaciones civiles y el apoyo social a las operaciones de la OTAN; los asuntos públicos para comprometer a la población y sus medios de comunicación en un adecuado nivel de información que permita comprender la actividades de la Alianza en curso; Operaciones de Información (INFOOPS) desarrolladas de modo parejo a las misiones militares; y operaciones psicológicas (PSYOPS) mediante el empleo de medios de comunicación y otros apropiados para las audiencias-objetivo a las que son dirigidas. Entre los estudios específicos que se han realizado en el CoE, cabe citar un monográfico sobre el extremismo violento, los medios para contrarrestar influencia hostil en países aliados, la campaña de información rusa en países nórdicos y bálticos, o la narrativa rusa sobre la Segunda Guerra Mundial. Este CoE apoya al *Comité Militar de Comunicaciones Estratégicas* de la OTAN a nivel políticas y doctrina, y analiza la implementación de dicha política a lo largo de su estructura de mando.

Al respecto de las tendencias de optimización de capacidades en materia de comunicación estratégica en el ámbito OTAN, se resalta la cooperación cívico-militar que involucra redes y agentes sociales, medios de comunicación de masas y agencias de información del mundo periodístico, cuya concienciación habrá de preservarles de las acciones hostiles.

El campo de la comunicación estratégica interacciona con el ámbito de seguridad energética especialmente en lo relativo a las acciones de influencia (i.e. generando temor a fuentes de energía)[12] y a la comunicación durante situaciones de gestión de crisis.

Con la ciberdefensa, la comunicación estratégica presenta interrelaciones respecto de la modelación del ambiente informativo en el contexto de acciones de *robot trolling* y también de operaciones de decepción del tipo *fake news* canalizadas por medios de comunicación y redes sociales (como ha acontecido en España en otoño de 2017 al

[12] ESPONA, Rafael José de, «Seguridad energética y guerra psicológica», IEEE, Documento de Opinión 66/2016 (1 de julio de 2016).

respecto de los disturbios provocados por la violencia separatista en su región catalana)[13].

Conclusiones y prospectiva

La globalización tecnológica ha aumentado simultáneamente la saturación informativa y la necesidad de medios cibernéticos y de suministro energético. La sociedad de la información, que incorpora como 4.ª dimensión el espacio virtual, presenta nuevos cauces para los conflictos y en este contexto se perfila la *guerra híbrida* contemplando un amplio espectro de fenomenología bélica soterrada, que —subyacente en permanente tensión— fluye por medio de tecnologías duales y afecta primariamente a la sociedad civil y sus servicios esenciales antes que a las Fuerzas Armadas.

Desde que en 2010 el Concepto Estratégico de la Alianza Atlántica apuntara los vectores del cambio en el ámbito de la defensa aliada, la OTAN ha desarrollado los 3 nuevos conceptos de ciberdefensa, seguridad energética y comunicación estratégica conformando una completa doctrina aplicable a conflictos de distinta naturaleza y curso.

Considerando que aquellos aportan capacidades que bastan para plantear por sí solas una campaña en sí misma (superando su empleo como mero multiplicador de fuerza cinética), sin menoscabo de la necesaria disuasión militar por medio de armas estratégicas y del clásico combate cinético, la defensa aliada deviene más compleja y requiere de una mayor interacción público-privada y cívico-militar (involucrando a la industria, operadores, tecnólogos y científicos).

Todo ello se percibe claramente en la región del Báltico, debido a la agresividad de potencias vecinas —antagonistas de la Alianza Atlántica— versadas en el empleo de dichos instrumentos. La experiencia propia de Estonia, Lituania y Letonia ha favorecido su desarrollo de capacidades analíticas y de trabajo que, puestas a disposición de la OTAN, han fructificado en la creación de los Centros de Excelencia especializados en ciberdefensa, seguridad energética y comunicación estratégica establecidos entre 2008 y 2014, los cuales mantienen una dinámica operativa alta.

En perspectiva de futuro, el devenir de la *guerra híbrida* y sus metamorfosis habrán eventualmente de prolongar su alcance, complejidad y sofisticación. Ante este

[13] MILOSEVICH-JUARISTI, Mira, *The «combination»: an instrument in Russia's information war in Catalonia*, Real Instituto Elcano, ARI n.º 92/2017 (2017).

panorama, la OTAN apunta a un incremento de capacidades en los citados ámbitos —ciberdefensa, seguridad energética y comunicación estratégica— los cuales, además, continuarán generando diversas interacciones que conviene tratar anticipadamente para la eficaz defensa aliada.

*Rafael José de Espona**
Instituto de RR. II. y Ciencia Política (TSPMI)
Universidad de Vilnius