Las acciones ciberelectromagnéticas y el futuro de la guerra electrónica

Félix Pérez Martínez
Director de la ETSIT de la UPM
Academia de las Ciencias y las Artes Militares
Sección de Prospectiva de la Tecnología Militar

Las actividades de la Guerra Electrónica y la Ciberdefensa se basan en el uso masivo de las tecnologías de la información y las comunicaciones, pero su desarrollo histórico ha recorrido caminos separados. Además, en aspectos tecnológicos, doctrinales y operativos, las diferencias entre ambas actividades han sido muy importantes.

La Guerra Electrónica, con muchos más años de existencia, se asociaba fundamentalmente al uso y control del espectro electromagnético, por el contrario, la Ciberdefensa siempre se ha asociado a la protección y ataque de sistemas de información que tradicionalmente han estado constituidos por redes de ordenadores convencionales (redes de área local), con gran capacidad de computación, que se conectaban entre sí mediante enlaces dedicados muy seguros.

En Guerra Electrónica las tecnologías críticas estaban asociadas a la generación, radiación, detección y proceso de señales de radiofrecuencia y electroópticas, mientras que las amenazas en el ámbito de la Ciberdefensa se introducían por puertas externas e internas asociadas a las vulnerabilidades del software.

En los últimos años, esta situación está cambiando a consecuencia de dos fenómenos de índole muy diferente pero interrelacionados entre sí: los cambios en las características de los escenarios de conflicto y la convergencia y dualidad de las tecnologías utilizadas.

Nuevos escenarios operativos

Lejos ya los tiempos de la de la Guerra Fría, los conflictos actuales son mucho más complejos como consecuencia de múltiples factores: la globalización, los cambios

demográficos y de entorno, la descomposición de algunos estados, la propagación de ideologías y movimientos radicales, la aparición de nuevos entornos de conflicto –como el ciberespacio–, la escasez de algunos recursos y un largo etc.

Además, y a consecuencia de algunos de los factores indicados, junto a los conflictos convencionales, en la última década han aparecido nuevos tipos como los asimétricos, de creciente sofisticación a medida que se facilita y abarata el acceso a las tecnologías emergentes, e híbridos, donde los enfrentamientos se libran simultáneamente en los ámbitos militar y civil.

A modo de resumen, se puede afirmar que las operaciones militares se han modificado significativamente perdiendo importancia las características cuantitativas de las mismas (masa y volumen) para ganarla los factores cualitativos (oportunidad, indetectabilidad, precisión, sostenibilidad, escalabilidad, acciones y efectos). En este contexto, las acciones de Guerra Electrónica y Ciberdefensa, además de incrementar su valor, deben adaptarse a este tipo de operaciones para contribuir a lograr ventaja (por ejemplo, física, temporal o condicional) sobre adversarios de muy diversa naturaleza. Pero no es un camino fácil.

Acciones ciberelectromagnéticas

De hecho, tras la caída del Muro de Berlín, la Guerra Electrónica sufrió un significativo parón, concentrándose su desarrollo en los sistemas de autoprotección de plataformas y personas.

En este sentido es muy significativa la reducción de capacidades operativas que se produce en el Ejército de EE. UU. («Telecomunicaciones militares para el despliegue de fuerzas en misiones humanitarias y de mantenimiento de la paz». Grupo de Trabajo de Defensa y Seguridad del Colegio Oficial de Ingenieros de Telecomunicación, GTDS-COIT. 2013).

Al mismo tiempo se desplegaron masivamente los sistemas de información en el ámbito militar –como ocurrió en el campo civil- y con ello un incremento exponencial de sus vulnerabilidades. Las actividades y medios asociadas a la Ciberdefensa crecieron exponencialmente y consumieron –y siguen consumiendo– muchos recursos que inevitablemente se detrajeron de los dedicados a los ámbitos de la Guerra Electrónica, entre otros muchos. No ocurrió lo mismo en Rusia (Fernando Manrique Montojo. «Panorama de la guerra electrónica en Rusia». Documento de Opinión IEEE 11/2019. Instituto Español de Estudios Estratégicos. Madrid. España. 5 de febrero de 2019. http://www.ieee.es/Galerias/fichero/docs_opinion/2019/DIEEEO11_2019FERMAN-ejercitoRusia.pdf).

El consecuente desequilibrio se puso de manifiesto en el conflicto del Donbáss, iniciado el año 2014 en el este de Ucrania, cuando las limitaciones operativas de las actividades de Guerra Electrónica de los ejércitos de la OTAN se evidenciaron. A partir de este momento se acelera la convergencia entre los ámbitos operativos de Guerra Electrónica y Ciberdefensa

que se concreta en lo que se conoce como acciones ciberelectromagnéticas (Cyber electromagnetic activities. FM 3-38. https://publicintelligence.net/us-army-cema/).

Un concepto que, curiosamente, se había definido bastantes años antes, pero cuya importancia táctica es ampliamente reconocida a partir de este momento.

La figura 1 es relativamente antigua y representa una vista funcional de las relaciones y fronteras entre las operaciones de Guerra Electrónica (óvalo marrón), Inteligencia Electrónica (óvalo azul) y Ciberdefensa (óvalo rojo). Es una modificación realizada por Isaac R. Porche III et al. («Redefining Information Warfare Boundaries for an Army in a Wireless Word». United States Army. RAND Corporation monograph series. 2013. https://www.rand.org/pubs/monographs/MG1113.html).

Es evidente que en términos teóricos es difícil establecer una separación clara entre los distintos ámbitos.

La posibilidad de emplear efectos combinados entre los tres tipos de operaciones ha sido considerada desde hace casi dos décadas, pero hasta hace pocos años ha sido más un planteamiento teórico que una realidad, la prueba es que eran llevadas a cabo por unidades militares diferentes. En estos momentos es inevitable la convergencia entre las actividades de Guerra Electrónica y la Ciberdefensa en un contexto caracterizado por la aparición de los combates híbridos y la creciente importancia del uso militar de técnicas y tecnologías civiles en muy rápido desarrollo.

Figura 1. Visión funcional de la convergencia entre la Guerra Electrónica, la Ciberdefensa y la Inteligencia Electrónica

Posiblemente fueron Rohret y Jimenez de los primeros que en su artículo de 2012 (David Rohret & Abuid Jimenez. «Convergence of Electronic Warfare and Computer Network Exploitation/Attacks Within the Radio Frequency Spectrum». Proceedings of ICIW 2012,

The 7th International Conference on Information-Warfare & Security), pusieron de manifiesto que la utilización de protocolos IP en los sistemas de radiocomunicaciones facilita su ataque, pues su protección está orientada a las vulnerabilidades de la red y no a las de los efectos combinados. Lo demostraron en tres casos: un sistema de comunicaciones de banda ancha entre una plataforma aérea y tierra, un sistema de comunicaciones por satélite y una red de sensores.

Otro caso bastante conocido de utilización de efectos combinados en el ámbito civil es la perturbación de sistemas comunicaciones móviles 3G y 4G para que conmuten a sistemas 2G, mucho más vulnerables. Algo similar puede hacerse con las redes WiFi. En definitiva y frente a los ataques clásicos de Guerra Electrónica, en la actualidad deben realizarse buscando los efectos combinados característicos de las acciones ciberelectromagnéticas.

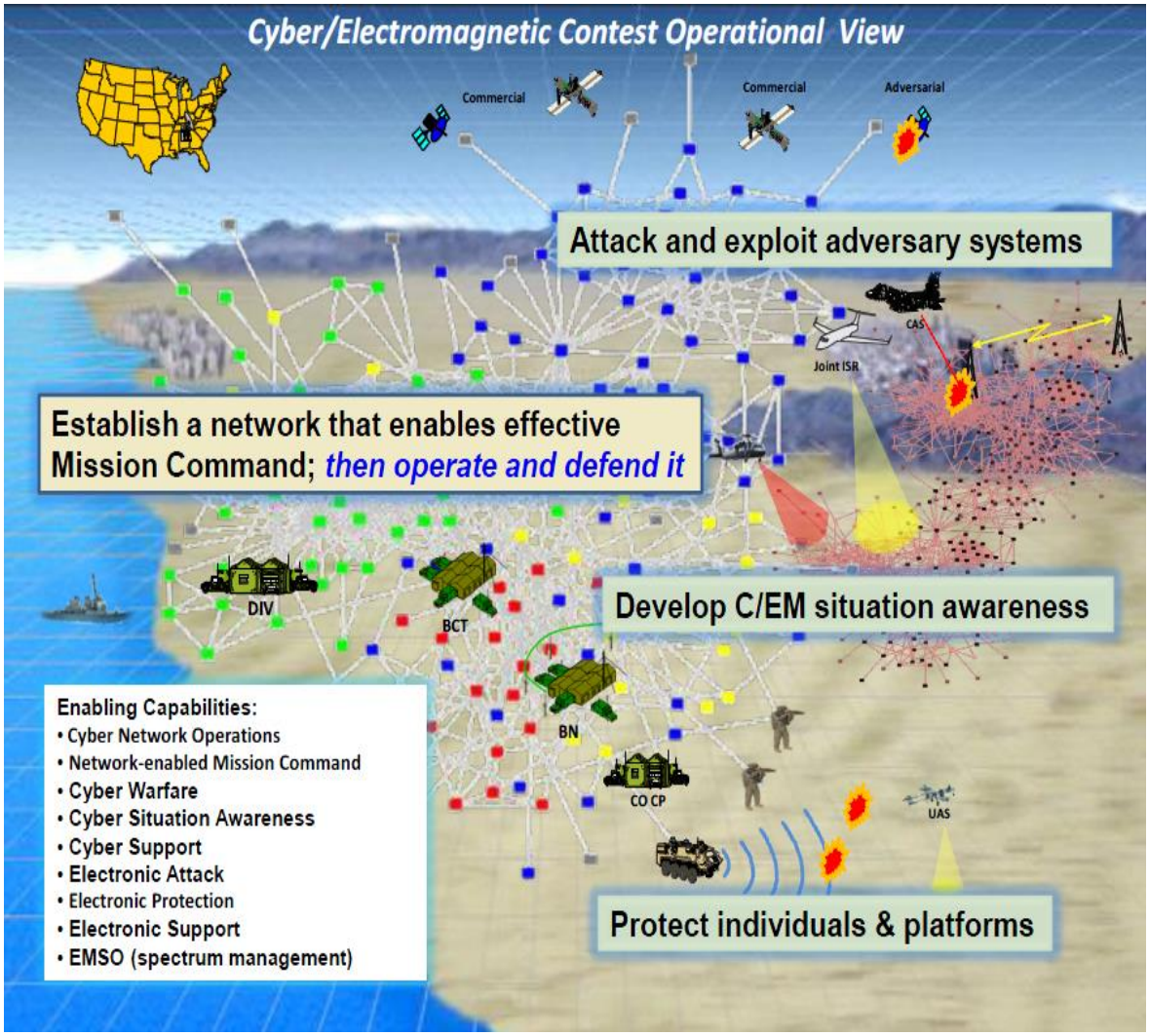

Figura 2 Acciones ciberelectromagnéticas (vista operativa)

El futuro de la guerra electrónica

Como resultado de todo lo anterior la Guerra Electrónica está sometida a un proceso de transformación que producirá cambios estructurales en numerosos aspectos.

Organización, doctrina y operaciones

La nueva visión CEMA (*Cyber and ElectroMagnetic Activities*), representada en la figura, implica la combinación de las actividades en ambos ámbitos. Su implementación implica importantes cambios estructurales, doctrinales y operativos en las Fuerzas Armadas, un reto tan importante o más que la transformación tecnológica que se comentará a continuación.

Nuevas técnicas y tecnologías

En este aspecto son dos los retos más importantes a los que se enfrentarán los futuros sistemas de Guerra Electrónica: la adaptación al nuevo entorno ciberelectromagnético y la necesidad de combatir la amenaza más importante en los próximos años: las nuevas generaciones de misiles supersónicos.

Ambos retos implican cambios sustanciales en las arquitecturas empleadas hasta ahora en los sistemas de Guerra Electrónica. Las nuevas arquitecturas estarán completamente digitalizadas, incluso en sus etapas de radiofrecuencia, y serán capaces de implementar sistemas adaptativos, multifuncionales y reutilizables capaces de trabajar en entornos cambiantes y con una significativa reducción de costes
(Qinghan Xiao. «A Conceptual Architecture of Cognitive Electronic Warfare System». The Tenth International Conference on Advance Cognitive Technologies and Applications. 2018.
http://www.thinkmind.org/index.php?view=article&articleid=cognitive_2018_3_10_40012
Barry Trimmer. «Trend in Defence Electronics: Thecnological Convergence in Radar and EW». Microwave Journal September 2011.
https://www.microwavejournal.com/articles/11683-trends-in-defence-electronics-technological-convergence-in-radar-and-ew).

Para soportar estas arquitecturas, además de las tecnologías clásicas de generación, detección y proceso de señales de radiofrecuencia y electroópticas, se requieren otras tecnologías claves como son su integración en UAS (*Unmanned Aircraft Systems*) y la introducción masiva de técnicas de inteligencia artificial. Esta última tecnología permitirá que los sistemas de ciberguerra aprovechen los datos para adaptarse a las situaciones cambiantes del combate. Es el camino a un escenario más complejo en el que combatan sistemas de Guerra Electrónica autónomos: los UAEWS *«Unmanned and Autonomous EW Systems»*.

A modo de conclusión, el futuro de la Guerra Electrónica estará determinado por tres tendencias de convergencia entre ámbitos que hasta hace unas décadas estaban muy separados:

a) la Ciberdefensa y la Guerra Electrónica que convergen en los nuevos conflictos ciberelectromagnéticos;
b) la convergencia tecnológica, fruto de la digitalización, entre los diversos sistemas de defensa que utiliza el medio radioeléctrico para conseguir sus objetivos y,
c) la convergencia entre las aplicaciones de seguridad y de defensa y las tecnologías desarrolladas en los sectores civiles y militares.

Todo ello augura una transformación muy importante de los actuales sistemas de Guerra Electrónica en los próximos años.