Documento
Opinión

112/2022 15 de diciembre de 2022

Carlos Javier Frías Sánchez *

Ucrania: la guerra de los teléfonos móviles

Ucrania: la guerra de los teléfonos móviles

Resumen:

Una de las características más originales de la guerra de Ucrania está en el uso de las redes de telefonía móvil, por parte de ambos bandos. Ucranianos y rusos han hecho un empleo intensivo de las redes de telefonía móvil, con finalidades que se extienden desde la comunicación de los gobiernos con la población civil, a las comunicaciones civiles y militares, pasando por acciones propias de guerra en el ámbito cognitivo o el empleo de aplicaciones para teléfonos móviles ligadas a la inteligencia o a los apoyos de fuegos. Las operaciones en Ucrania ofrecen una perspectiva nueva y, en algunos aspectos, sorprendente, del papel que pueden cumplir las redes de telefonía móvil en las operaciones militares actuales.

Palabras clave:

Teléfonos móviles, GSM, Starlink, ámbito cognitivo, aplicaciones informáticas, comunicaciones.

Cómo citar este documento:

FRÍAS SÁNCHEZ, Carlos Javier. *Ucrania: la guerra de los teléfonos móviles*. Documento de Opinión IEEE 112/2022. https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO112_2022_CARFRI_Ucrania.pdf y/o enlace bie[3] (consultado día/mes/año)

NOTA:** Las ideas contenidas en los ***Documentos de Opinión son responsabilidad de sus autores, sin que reflejen necesariamente el pensamiento del IEEE o del Ministerio de Defensa.

Introducción

Una de las características más originales de la guerra de Ucrania está en el uso de la telefonía móvil, por parte de ambos bandos. En realidad, en nuestra experiencia en combate, la telefonía móvil no ha tenido ningún papel relevante (si es que ha tenido alguno). En cualquier caso, la expansión actual de la telefonía GSM (*Global System for Mobile communications* – sistema global de comunicaciones móviles) ha tenido lugar después de los últimos conflictos principales combatidos por los ejércitos modernos en ambiente de «alta intensidad», por lo que es un actor relativamente nuevo en nuestra experiencia militar.

Las operaciones en Ucrania ofrecen una perspectiva nueva y, en algunos aspectos, sorprendente, del papel que pueden cumplir las redes de telefonía móvil en las operaciones militares actuales.

¿Qué es el sistema GSM?

El sistema de telefonía GSM se compone de cuatro elementos principales: los terminales móviles (nuestros teléfonos); las «antenas» que se colocan en puntos elevados (cuyo nombre técnico es «base *transceiver station*» o BTS; un número variable de estas antenas están controladas por un procesador denominado «base *station controller*»); el sistema que controla la red, permitiendo el acceso de los terminales autorizados a ella, y asignando para gestionar la comunicación la antena mejor situada para hacerlo (*Network Switching System* —NSS— o sistema de conexión de red); y, finalmente, el sistema que gobierna el conjunto y que permite comunicarlo con otros medios de comunicación (otras redes GSM, la telefonía móvil o Internet, por ejemplo).

Este tipo de telefonía se denomina «celular» porque el sistema divide el espacio en «células», que es como se conoce al espacio comprendido entre tres de estas «antenas» o BTS. De una forma muy simplificada, cuando un terminal que se encuentra dentro de una de estas células intenta establecer una comunicación, el NSS le asigna a la antena que recibe más potencia de señal. Comparando la potencia de la señal emitida por el teléfono a cada una de las tres torres de telefonía que conforman una célula, el sistema conoce con cierta aproximación la posición del teléfono dentro de cada célula. Es importante saber que los teléfonos móviles emiten continuamente información al sistema, incluyendo la identificación física del terminal, el operador de telefonía móvil que tiene contratado, su número de teléfono y otros datos. Es decir, incluso sin intentar llamar, los

teléfonos emiten información, y, consecuentemente, las compañías propietarias de las BTS reciben los datos suficientes como para identificar el terminal concreto, la compañía de telefonía móvil que le da servicio, el número de teléfono asociado al terminal, la célula donde se encuentran y su posición aproximada dentro de esta célula.

El sistema de telefonía móvil GSM es el más extendido en el mundo de la telefonía móvil. La mayoría de la red en Europa es del tipo GSM 4G LTE (*Long-Term Evolution*), que permite una elevada tasa de intercambio de datos, permitiendo la conexión a Internet.

Ucrania y la red GSM

El Estado ucraniano nace de la descomposición de la Unión Soviética. En el momento de la independencia, Ucrania carece de una estructura administrativa moderna, faltando funcionarios, oficinas, procedimientos administrativos, bases de datos… La creación del Estado ucraniano coincide con el comienzo de la expansión de Internet y de la telefonía móvil GSM. Una de las grandes ventajas de la telefonía GSM cuando se emplea para acceder a Internet es que el coste de desplegar las redes de antenas BTS es muy inferior al de crear redes de cables fijos, en las grandes extensiones de terreno de Ucrania. Consecuentemente, el Estado ucraniano se apoya muy frecuentemente en aplicaciones que permiten a los ciudadanos acceder a multitud de servicios básicos del gobierno (en 2019 se lanzó un programa gubernamental significativamente llamado «El Estado en tu *smartphone*»). Ucrania dispone también de muchos técnicos informáticos, lo que da al Estado ucraniano la capacidad de desarrollar aplicaciones propias o la de adaptar las existentes a sus necesidades.

Ucrania dispone de cuatro proveedores de servicios digitales, a los que se suman dos operadores «ilegales» en las provincias separatistas de Lugansk y Donetsk, con un total de unos 59 millones de líneas para una población de 43,81 millones de habitantes, lo que da una idea de la difusión de la telefonía móvil en el país[1].

La red GSM y la invasión rusa de Ucrania

La invasión rusa de Ucrania es el primer conflicto entre dos Estados avanzados desde el final de la Guerra Fría. En realidad, desde la guerra de las Malvinas, solo la guerra del Golfo de 1991 y la posterior invasión de Irak en 2003 han implicado combates

[1] Mc DAID, Cathal. The Mobile Network Battlefield in Ukraine. Part 1, *ENEA, Adaptive Mobile Security*. 4 de abril de 2022. Disponible en: The Mobile Network Battlefield in Ukraine - Part 1 (adaptivemobile.com)

convencionales entre ejércitos dotados de armamento moderno y capacidades comparables en alguna medida. Y, en los años transcurridos desde estos conflictos, uno de los campos donde la tecnología ha avanzado más es el de Internet, con la telefonía móvil como el medio de acceso a la red global más extendido. En consecuencia, no es sorprendente que los oficiales de planeamiento ruso no prestasen especial atención a la telefonía móvil: era un campo que escapaba a su experiencia previa y, muy posiblemente, a su educación profesional.

En realidad, tampoco Ucrania, estaba mejor adaptada a hacer uso de la telefonía móvil en el marco de su esfuerzo de guerra. Sin embargo, el hecho de que el conflicto se desarrollase en suelo ucraniano implica necesariamente que la red de telefonía móvil existente en la zona en la que se desarrollan los combates está bajo el control de las autoridades ucranianas, a través de las compañías de telefonía móvil propietarias de las antenas BST.

La lógica militar nos lleva a pensar que una de las primeras medidas del ejército ruso debería haber sido la neutralización de la red de telefonía móvil: en realidad, los ejércitos hacen un importante esfuerzo en dotarse de radios con importantes capacidades de guerra electrónica, que aseguren las comunicaciones entre sus diversos elementos. Una de las primeras acciones en combate es tratar de destruir las redes de comunicaciones del enemigo, al tiempo que se preservan las propias. En este sentido, las redes de telefonía móvil en manos de los ucranianos constituyen una potente herramienta de mando y control en manos del gobierno ucraniano y, en consecuencia, debían ser un objetivo preferente del Ejército ruso: en teoría, sin telefonía móvil, el gobierno ucraniano perdía gran parte de su capacidad de comunicarse con su población (y con sus unidades militares y estas entre sí), al tiempo que la red de radios de combate rusa debería asegurar las comunicaciones del ejército ruso… Las radios tácticas rusas más modernas son las R-187P1 *Azart*, radios teóricamente muy capaces, con tecnología SDR (*Software-Defined Radio*), que operan en las bandas de VHF y UHF, en frecuencia modulada (FM), con alcances máximos de 4,12 y 40 km, según el modelo concreto. En escalones superiores se emplean las R-168-5UN-2, con versiones en HF (350 km de alcance máximo) y VHF (con alcance máximo de 20 km)[2]. Estas radios son modernas y

[2] Mc DERMOTT, Roger. «Moscow Promotes Military Communications Systems for 21st Century Conflict», *Eurasia Daily Monitor,* Vol. 17, núm. 31. 4 de marzo de 2020. Disponible en: https://jamestown.org/analyst/roger-mcdermott/

capaces, pero se han suministrado en número escaso (unos pocos centenares para todo el ejército) y, aparentemente, han presentado problemas de calidad (baterías chinas de duración muy escasa o problemas con los cifradores). Al no existir un número suficiente de ellas, las unidades rusas han tenido que utilizarlas en modo compatible con radios más antiguas, en modo de frecuencia y fija y sin cifrar, lo que las ha hecho muy vulnerables a la interceptación[3] (las comunicaciones militares rusas en HF, sin cifrar, han sido interceptadas incluso por radioaficionados en todo el mundo, grabadas y puestas en internet a disposición del público)[4]. Como consecuencia, las unidades rusas experimentaron una rápida degradación de sus comunicaciones radio: por un lado, sus equipos se demostraron menos capaces de lo esperado (en autonomía y en calidad del cifrado), por otro, el número de equipos de radio disponibles era muy inferior a las necesidades y, finalmente, el empleo de BTG (*Battalion Task Groups* – unidades tipo batallón interarmas) como el principal «peón de maniobra» de las Fuerzas Armadas rusas tuvo el efecto de hacer operar a estas unidades muy separadas unas de otras y muy alejadas también de su escalón de mando superior (el «ejército interarmas», en inglés *Combined Arms Army* o CAA). En efecto, al desaparecer en la organización rusa los escalones intermedios (la brigada, la división, el cuerpo de ejército…), las comunicaciones de los BTG se revelaron de un alcance demasiado reducido (estaban pensadas para enlazar con el cuartel su brigada, desplegada a pocas decenas de kilómetros, no con el de su CAA, situado a cientos de kilómetros).

Como consecuencia, las unidades rusas tuvieron que recurrir al empleo de la telefonía móvil… ucraniana. Y, en consecuencia, no se podían permitir su destrucción.

Por su parte, el gobierno ucraniano empleaba la telefonía móvil para mantener los servicios públicos esenciales y para mantener el contacto con su población (por ejemplo, el discurso diario del presidente Zelenski se emite en un canal de Telegram)[5]. Para ello, el gobierno tomó tres medidas importantes: autorizó el *roaming nacional* o *de emergencia* (es decir, cualquier terminal de cualquier compañía ucraniana podía conectarse a

[3] CRANNY-EVANS, Sam y WITHINGTON, Dr Thomas. «Russian Comms in Ukraine: A World of Hertz». 9 de marzo de 2022. Disponible en: Russian Comms in Ukraine: A World of Hertz | Royal United Services Institute (rusi.org).

[4] MYRE, Greg. **«**How does Ukraine keep intercepting Russian military communications?». 26 de abril de 2022. Disponible en: How does Ukraine keep intercepting Russian military communications? : NPR

[5] Mc DAID, Cathal. «The Mobile Network Battlefield in Ukraine. Part 2». *ENEA, Adaptive Mobile Security*. 31 de marzo de 2022.
Disponible en: The Mobile Network Battlefield in Ukraine - Part 2 (adaptivemobile.com)

cualquier BTS, independientemente si pertenecía a su proveedor de servicios de telefonía móvil o a otro), impuso la gratuidad del servicio y prohibió el *roaming* de los teléfonos con tarjetas SIM rusas o bielorrusas o la emisión de llamadas desde móviles ucranianos hacia Rusia o Bielorrusia[6].

Esta última medida dejaba (en teoría) sin comunicaciones GSM a las fuerzas armadas rusas. Los rusos reaccionaron de dos formas: por un lado, haciéndose con todas las tarjetas SIM ucranianas que pudieron localizar, y por otro empleando dispositivos tipo *SIM box* o *SIM bank*[7] (aparatos que reciben comunicaciones de SIM de un operador ruso y las convierten en comunicaciones realizadas con otro SIM ucraniano, evitando así la prohibición de emplear tarjetas SIM rusas en la red ucraniana). Estos dispositivos requieren un cierto número de tarjetas SIM de entrada rusas y otro número de tarjetas SIM de salida ucranianas), obtenidas estas últimas normalmente por requisa. Tras capturar una primera *SIM box* rusa a mediados de marzo, los ucranianos comenzaron a rastrear la presencia de estos dispositivos, siendo capaces de detectar la presencia de estas *SIM boxes* y *SIM banks* por su localización (muchas tarjetas SIM emitiendo desde una sola localización geográfica) y por el elevado número de comunicaciones que efectuaban (la *SIM box* capturada en marzo hacía más de un millar de llamadas diarias) y anulaban la conectividad de las tarjetas SIM ucranianas empleadas por las *SIM boxes* y *SIM banks* rusas. De la misma forma, las tropas rusas comenzaron inmediatamente a requisar los teléfonos móviles de los civiles ucranianos, para utilizarlos de forma bien particular, bien oficial. Los civiles ucranianos cuyos teléfonos habían sido requisados por los ocupantes informaban a sus proveedores de servicios, que, a su vez lo comunicaban al gobierno ucraniano. De esta forma, las fuerzas armadas de Ucrania saben qué terminales móviles ucranianos están siendo empleados por los rusos.

Sin embargo, los ucranianos pronto se dieron cuenta de las ventajas militares que les otorgaba su control de la red GSM. Así, en lugar de anular las tarjetas SIM empleadas por los rusos, comenzaron a grabar las conversaciones, con el fin de obtener inteligencia y, en ocasiones, identificar a los usuarios rusos que las empleaban. Algunas fuentes aseguran que el alto número de generales rusos caídos en combate está relacionado con la identificación de sus teléfonos móviles por parte de los ucranianos, localizando su

[6] Mc DAID, Cathal. «The Mobile Network Battlefield in Ukraine. Part 1». *ENEA, Adaptive Mobile Security.* 4 de abril de 2022.
Disponible en: The Mobile Network Battlefield in Ukraine - Part 1 (adaptivemobile.com)
[7] Ibíd.

posición y atacándolos cuando se encontraban dentro del alcance de las armas ucranianas[8].

Como hemos citado, los terminales móviles emiten continuamente hacia las BST de la red GSM. Los ucranianos aprovecharon esta circunstancia para localizar los teléfonos rusos activados, obteniendo con elevada precisión la posición de los soldados que los portaban. En ocasiones, los ucranianos eliminan periódicamente la prohibición de *roaming* de los teléfonos rusos, aprovechando para emitir propaganda hacia estos terminales y como incentivo para que los soldados rusos mantengan activados permanentemente sus teléfonos, con el fin de comunicarse con sus familias aprovechando esas «ventanas de conexión».

El control de la red GSM permite también al gobierno ucraniano «dominar el relato»: el gobierno ucraniano decide qué terminales móviles pueden emitir y cuáles no dentro del territorio ucraniano. Puesto que los combates se desarrollan en Ucrania, solo los teléfonos autorizados por el gobierno ucraniano pueden conectarse a Internet. En consecuencia, al resto del mundo nos llegan casi exclusivamente imágenes de medios rusos destruidos o capturados, siendo verdaderamente excepcional ver fotos o vídeos de pérdidas ucranianas. Para poder emitir estas imágenes, los rusos necesitan obtener las fotos y después transportar el terminal o el soporte físico de las imágenes hasta un lugar con cobertura GSM propia, lo que supone un elevado retraso, que perjudica a la inmediatez típica de las publicaciones en Internet. Esto crea una imagen de los resultados de los combates mucho más favorables a Ucrania de lo que es la realidad.

De la misma forma, el control de la red GSM y el uso habitual de teléfonos móviles por parte de la mayoría de la población civil ucraniana permite al gobierno del presidente Zelenski difundir sus mensajes a la población civil ucraniana, al tiempo que le permite un amplio margen para bloquear la propaganda procedente de Rusia. Así, el ciudadano medio ucraniano solo recibe la información que su gobierno quiere difundir, lo que supone una importante herramienta para mantener la moral de combate. De la misma forma, las alertas de ataques aéreos o de presencia de UAV rusos se difunden vía aplicaciones de telefonía móvil.

Por su parte, el Ejército ruso, consciente de esta debilidad, ha comenzado a desplegar antenas BTS pertenecientes a los proveedores de telefonía móvil de las regiones

[8] As Russian Troop Deaths Climb, Morale May Be an Issue - The New York Times (nytimes.com)

separatistas de Lugansk y Donetsk en las zonas donde combaten sus fuerzas[9]. Al mismo tiempo, ha comenzado a destruir las antenas BST ucranianas en las zonas donde las fuerzas rusas disponen de cobertura radio (donde se concentran en espacios reducidos muchas fuerzas, permitiendo el enlace radio en alcances de pocos kilómetros, como en el frente del Dombás o en Jersón) o donde disponen de cobertura GSM proporcionada por esas compañías de telefonía de las regiones separatistas.

Ucrania ha recibido también el apoyo de la compañía *Starlink*, que proporciona acceso a Internet empleando satélites en órbitas bajas. Para ello, en lugar de las BTS utiliza terminales portátiles de enlace con los satélites. Por ello, en general, el acceso vía *Starlink* lo emplean las Fuerzas Armadas Ucranianas, que son las que han recibido estos terminales específicos.

Además de este empleo de la telefonía GSM, Ucrania ha modificado algunas de las aplicaciones que empleaban los ciudadanos para comunicarse con su gobierno, para que apoyen su esfuerzo de guerra[10]. Algunos ejemplos:

- Una aplicación destinada a informar sobre violencia de género consistía en un icono en el teléfono móvil que activaba un mensaje a la policía si un ciudadano presenciaba un episodio de violencia de género. El mensaje en cuestión incluía la localización del terminal que emitía la alerta. Esta aplicación se emplea hoy por los ciudadanos ucranianos para informar de la presencia de tropas rusas.
- Otra aplicación estaba destinada a informar a los Ayuntamientos de desperfectos en el mobiliario urbano. En este caso, además de la geolocalización, se incluía una foto del desperfecto: una acera rota, un bache, una papelera caída… Esta aplicación la emplean hoy los ciudadanos para enviar fotos de los medios desplegados por las tropas rusas de ocupación, lo que permite identificar el tipo de unidades y, en muchos casos, incluso a qué unidad concreta pertenecen[11].

[9] Mc DAID, Cathal. «The Mobile Network Battlefield in Ukraine. Part 3». *ENEA, Adaptive Mobile Security*. 25 de abril de 2022.
Disponible en: The Mobile Network Battlefield in Ukraine - Part 3 (adaptivemobile.com)

[10] HARWELL, Drew. «Instead of consumer software, Ukraine's tech workers build apps of war». *The Washington Post*. 24 de marzo de 2022. Disponible en: Here are the apps Ukraine created to combat the Russian invasion - The Washington Post

[11] Mc DAID, Cathal. «The Mobile Network Battlefield in Ukraine. Part 2». *ENEA, Adaptive Mobile Security*. 31 de marzo de 2022.
Disponible en: The Mobile Network Battlefield in Ukraine - Part 2 (adaptivemobile.com)

- Una aplicación desarrollada sobre la base de la anterior se denomina *GIS Arta*[12] y está destinada a que puedan solicitarse fuegos desde cualquier terminal móvil. La aplicación toma una foto del objetivo sobre el que se pide fuego, y la envía junto con la localización y la identidad del teléfono solicitante, vía Internet, a las Fuerzas Armadas Ucranianas. Con la posición del teléfono y la foto del objetivo, el sistema emplea la cartografía digital de la zona para obtener las coordenadas del objetivo y asignarle, si se estima oportuno, un medio de fuego para batirlo (artillería de campaña, RPAS, cohetes, misiles…). La identidad del terminal permite asignarle una determinada fiabilidad, en función de la experiencia previa de las solicitudes realizadas.
- El gobierno ucraniano también emplea la información de que dispone gracias a estas aplicaciones para informar a su población de la presencia de tropas rusas en determinados lugares[13], con el fin de identificar corredores libres para poder escapar de las zonas ocupadas, o para informar de las zonas minadas que se han identificado. La publicación de estos datos supone un incentivo para que los ciudadanos compartan, vía móvil, la información sobre estos aspectos de que dispongan, como medio de contribuir a la seguridad de sus conciudadanos. Adicionalmente, algunas organizaciones privadas hacen una función similar, recopilando información proporcionada por los ciudadanos y difundiéndola más rápidamente que el propio gobierno (que necesita confirmar la información antes de su publicación o que la retrasa por motivos de interés militar).

El amplio uso de estas aplicaciones por parte de las Fuerzas Armadas de Ucrania implica un cambio de paradigma. En el combate tradicional, los medios de inteligencia son escasos, y el problema principal está en la priorización y la asignación de los limitados medios disponibles para obtener el máximo rendimiento. Cuando cada ciudadano es, potencialmente, un «sensor», el problema pasa a ser la gestión de una cantidad ingente de información, de fiabilidad muy variable, mientras que los medios específicos de inteligencia deben dedicarse a cubrir las zonas en las que no hay estos sensores o a complementar o confirmar la información recibida por ellos. La información procedente

[12] *GIS Arta*, automated command and control system. Disponible en: GIS ARTA
[13] VILLARREAL, Mary. «Ukraine's Digital Government Services App Converted Into an Instrument of War», *Stillness in the Strom*. 10 de abril de 2022. Disponible en: Ukraine's Digital Government Services App Converted Into an Instrument of War - Stillness in the Storm

de los proveedores de servicios móviles son otra potente fuente de información sobre el despliegue de las fuerzas invasoras, pero supone igualmente una cantidad ingente de información a procesar.

Algo similar ocurre con las aplicaciones dedicadas a solicitar apoyos de fuegos: los observadores avanzados de artillería (OAV) son un recurso muy escaso, que, hasta hoy, precisaban medios muy específicos para ejecutar sus tareas en combate (brújulas, planos, telémetros, radios…). Con las aplicaciones informáticas citadas, cada ciudadano es un OAV potencial, y no precisa más que su teléfono móvil y una conexión a la red de GSM, y de ella a Internet, para cumplir su función. Nuevamente, el problema deja de ser de escasez, para pasar a ser de abundancia y de gestión.

Sin embargo, la utilización por parte de los ciudadanos ucranianos de estas aplicaciones plantea importantes problemas, legales y morales. Hay pocas dudas de que un civil que informase por radio de los movimientos de las fuerzas de un ejército de ocupación sería considerado como un espía, sufriendo los rigores de esta condición. Pero todavía hay más, un civil que apuntase un sistema de designación de objetivos capaz de solicitar fuegos sobre una unidad militar sería considerado como un combatiente, perdiendo cualquier protección que el derecho internacional otorga a los civiles no combatientes… Y sin embargo, con estas aplicaciones, algo tan inocuo y omnipresente como un teléfono móvil puede convertirse en cualquiera de las dos cosas, y un gesto tan aparentemente inocente como pulsar un icono en la pantalla táctil o tomar una foto puede ser considerado, con razón, como un acto hostil por parte de los ocupantes.

Conclusiones

La red GSM puede ser un nuevo espacio de confrontación, si, como en Ucrania, los dos bandos la necesitan. Esta situación, en realidad, no es nueva: algo similar ocurre en la práctica totalidad del continente africano, donde los conflictos armados rara vez afectan a la infraestructura de telefonía móvil, de la que todos los bandos contendientes dependen.

El dominio de la red de telefonía móvil permite al Estado seguir funcionando y mantener el contacto entre la población y las autoridades, y constituye una red de comunicaciones más resistente que la que depende de infraestructuras fijas, más vulnerables y más difíciles de reparar. Como consecuencia, el defensor tendrá siempre un gran interés en mantener el sistema operativo.

Adicionalmente, como hemos visto en Ucrania, el control de la red GSM implica también el control sobre el acceso a Internet en el campo de batalla, por lo que resulta un elemento fundamental para controlar el relato de lo que sucede en él. Este control permite trasladar al exterior solo aquella información que favorece los intereses de quien controla la red de telefonía móvil

La emisión continua de los terminales de telefonía móvil supone una gran vulnerabilidad para las fuerzas militares que los emplean, especialmente si dependen de una red GSM controlada por el enemigo o que pueda estar infiltrada por él. La capacidad de la red GSM de localizar los terminales, grabar sus conversaciones e, incluso, desencriptarlas, implica que el proveedor de servicios GSM conoce casi en tiempo real la localización de todo el personal que porta un teléfono móvil activado y que es capaz de identificar con cierta seguridad al que ocupa puestos de responsabilidad, si realiza comunicaciones con su teléfono móvil. Y esto es válido tanto para conflictos «simétricos», por ejemplo el de Ucrania, como para operaciones de estabilización, ya sea en Afganistán, en Irak o en cualquier rincón de África. Los teléfonos móviles son muy peligrosos para las unidades militares, y no precisamente por el riesgo de que se publiquen fotos poco favorecedoras. Las crecientes distancias de despliegue obligan a las fuerzas militares a replantearse los alcances de sus comunicaciones radio (y, como consecuencia, de la tecnología que emplean para ellas), so pena de tener que depender de un medio tan arriesgado como la telefonía GSM.

En cualquier caso, es necesario que las acciones que impliquen a la red de telefonía móvil reciban la atención necesaria en los planes operativos. En el caso de Ucrania, las medidas adoptadas (*roaming* nacional, prohibición del *roaming* de los teléfonos rusos o bielorrusos, gratuidad del servicio, posibles aplicaciones de uso militar…) fueron posibles en gran parte porque estaban previstas desde tiempo de paz (varias se implementaron la misma noche de la invasión), y porque existía un conocimiento adecuado de la forma de funcionar de estas redes entre los mandos militares ucranianos. Por parte rusa, la decisión de destruir o conservar la red de telefonía móvil ucraniana vino determinada por la insuficiencia de sus comunicaciones radio, lo que no dejó otra alternativa viable a corto plazo.

Es posible afirmar que la decisión de qué hacer con la red de telefonía móvil en la zona de combate debe ser uno de los elementos básicos contemplados en todo plan de operaciones en el campo de batalla moderno.

*Carlos Javier Frías Sánchez**

General de Brigada
Director de la Escuela de Guerra del Ejército