¿Oportunidad o riesgo? Redes sociales y Fuerzas Armadas

Los avances tecnológicos que se han producido desde la década de 1970 en los campos de la informática, las telecomunicaciones o la robótica han cambiado nuestras vidas. No sólo estamos rodeados de muchos productos tecnológicos que facilitan y simplifican nuestro día a día; sino que también estos mismos productos han creado un mundo más interconectado y globalizado que nunca, una *sociedad en red* cuya característica fundamental es que ingentes volúmenes de información pueden transmitirse de forma casi instantánea a cualquier punto del globo, con un coste irrisorio, con una facilidad asombrosa y sin precisar de grandes bibliotecas físicas para almacenar tantos volúmenes de información. Ésta ha sido la base sobre la cual se ha erigido la Era de la Información y está siendo reemplazada por la Era del Conocimiento.

Más recientemente, la popularización de Internet y la facilidad de acceder a la red desde una amplia gama de dispositivos –desde los tradicionales ordenadores de sobremesa y portátiles hasta los más modernos *smartphones, tablets* o *Smart TVs*– ha permitido que ciudadanos de todo el mundo, incluidos los de los países en desarrollo o de regímenes autoritarios, tengan acceso a un volumen de información, comunicaciones y servicios antes impensables e inalcanzables.

No obstante, cualquier movimiento que hacemos en la red, cualquier exploración en los buscadores de Internet, cualquier página que visitamos o cualquier comentario que hacemos en las redes sociales virtuales proporciona una información muy valiosa para perfilar nuestra personalidad mediante la identificación de preferencias, gustos, intereses, ideología, estado civil, nivel educativo y cualquier otra información que pueda ser de interés para empresas, gobiernos, servicios de seguridad o delincuentes. Además, la agregación de estas informaciones procedentes de múltiples fuentes junto con los datos personales, bancarios, administrativos, económicos o académicos sienta las bases del *Big Data*, que en los próximos años se convertirá –si no lo ha hecho ya– en el "Gran Hermano" de la Era de la Información y donde nadie que tenga una identidad digital y presencia en la red podrá escapar a su control casi absoluto.

Si nos centramos en el ámbito militar, las tecnologías de la información no sólo han facilitado la consolidación de un *sistema de sistemas* –o la capacidad de cualquier sensor, plataforma, combatiente o arma para interactuar con el resto– que permite a los ejércitos modernos combatir en red tal y como ha demostrado la Revolución en los Asuntos Militares (RMA) liderada por Estados Unidos; sino también han motivado el surgimiento de un nuevo campo de batalla virtual: el ciberespacio. Considerado como la quinta dimensión del entorno operativo (tras la tierra, los mares, los cielos y el espacio), el ciberespacio es el dominio donde transita el grueso de los flujos de información y comunicaciones electrónicas civiles y militares de todo el globo. Aunque en esta dimensión coexisten una amplia gama de actores estatales y no-estatales con intereses, objetivos y capacidades muy distintas, en el ámbito militar las operaciones en el ciberespacio se orientarán a la protección, explotación, disrupción o destrucción de las redes, infraestructuras, equipos informáticos, sistemas tecnológicos o información almacenada para

Guillem Colom Piella
Doctor en Seguridad Internacional

Enrique Fojón Chamorro
Ingeniero Superior en Informática

Niño Palestino en el punto de mira de un soldado israelí.
(Fuente electronicintifada.net)

disuadir al enemigo de iniciar una acción militar, paralizar sus sistemas de defensa, desarticular sus fuerzas, erosionar sus capacidades de mando y control o colapsar completamente el país[1].

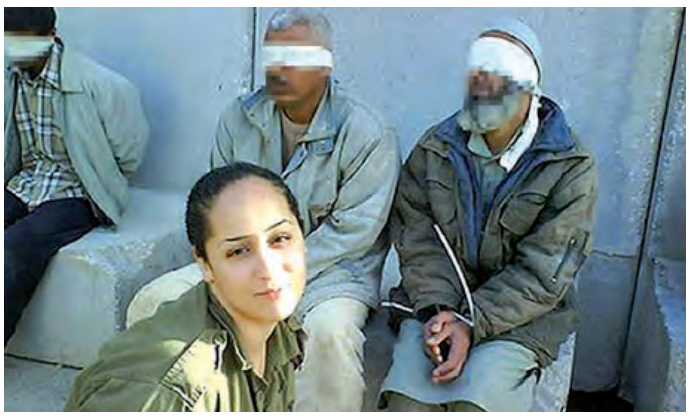
No obstante, a pesar de la enorme popularidad e importancia estratégica que ha adquirido la guerra en el ciberespacio, existe otro elemento vinculado con este dominio que cada vez está recibiendo una mayor atención: la guerra informativa. Y es que si bien ésta no es algo nuevo ya que el uso de la información y la propaganda ha sido una constante de todos los conflictos desde la antigüedad, en los conflictos recientes hemos observado como Internet –y muy especialmente las redes sociales virtuales– permite a cualquier actor, tanto estatal como no-estatal, realizar operaciones informativas con una facilidad y efectividad asombrosas. En efecto, tal y como hemos visto en Israel, Líbano, Palestina, Siria, Ucrania, Crimea o el Estado Islámico, el empleo de plataformas multicanal y redes sociales como *Facebook, Twitter, Instagram, Flickr* o *Youtube* permiten recopilar un vasto volumen de información sobre su enemigo susceptible de transformarse en inteligencia útil para las operaciones y también influir en la opinión pública propia, adversaria y neutral mediante actividades de propaganda y contra-propaganda[2]. Precisamente por ello, muchos ejércitos han integrado la dimensión cibernética en las labores de comunicación estratégica; realizan operaciones de información (INFOOPS) y operaciones psicológicas (PSYOPS) en el ciberespacio; llevan a cabo actividades de inteligencia de fuentes abiertas (OSINT) en Internet e incluso explotan la valiosa información que proporcionan las redes sociales virtuales (SOCMINT).

No obstante, aunque muchas fuerzas armadas se han subido al carro de las redes sociales de forma más o menos efectiva y con una estrategia más o menos clara, el uso personal que sus integrantes hacen de las mismas puede suponer tanto una amenaza para la seguridad nacional y un riesgo para las operaciones militares como representar un problema de comunicación pública. En este sentido, las Fuerzas de Defensa de Israel (FDI) son un buen ejemplo de ello. Aunque éstas constituyen el ejemplo paradigmático del uso y explotación de las redes sociales –tal y como se ha podido observar en la *Operación Pilar Defensivo* (2012) y en la

Operación Margen Protector (2014) como parte integral de su nueva doctrina *Dahiya* planteada tras el fiasco de la *Operación Recompensa Justa* (2006) contra Hezbollah– también están sufriendo varios problemas de difícil solución.

De hecho, según sus propias estimaciones, aproximadamente el 70% de sus oficiales y suboficiales y el 95% de su tropa disponen de perfil personal en Facebook. No obstante, su uso inadecuado provocó que en el año 2013 se prohibiera a los soldados pertenecientes a unidades de inteligencia y operaciones especiales compartir en las redes sociales virtuales fotografías que revelasen su condición de militar, máxime tras algunos episodios que pusieron en peligro la seguridad del país y la reputación de sus Fuerzas Armadas.

Más específicamente, en el año 2010 un soldado hebreo publicó en su cuenta personal de *Facebook* el mensaje: *"Limpiaremos Katana y el jueves volveremos a casa"*; Katana es un pequeño pueblo cercano a Ramala (Cisjordania). Al filtrarse esta información, las FDI se vieron obligadas a suspender la operación militar planificada. Paralelamente, entre 2011 y 2013, el número de fotografías compartidas por soldados dentro de instalaciones militares aumentaron de manera exponencial. De hecho, muchas de ellas fueron recopiladas por el grupo terrorista Hamas y utilizadas para confeccionar un pequeño catálogo de las capacidades militares de Israel[3]. Además, muchos soldados han compartido fotografías en situaciones inapropiadas, como es el caso de Eden Abergil posando con prisioneros palestinos. Ello motivó que la cúpula militar del país delimitara una "línea roja", aprobando un estricto código de conducta sobre el uso de las redes sociales en el que se contemplan importantes sanciones, incluidas penas de carcel, en caso de incumplimiento. Además, su puesta en marcha ha sido acompañada de diversas campañas de concienciación. De esta manera, en los pasillos de los cuarteles se pueden hallar avisos sobre los peligros que entrañan las redes sociales virtuales con carteles que muestran las fotos de Bashar Assad, Mahmoud Ahmadinejad y de Hassan Nasrallah acompañadas del texto *"Tienes tres nuevas solicitudes de amistad"*. Bajo las fotos, un mensaje muy claro: *"¿Crees que todo el mundo es tu amigo? ¡El enemigo usa las redes sociales para recopilar información acerca de las FDI!"*[5].



La soldado Eden Abergil posando con prisioneros palestinos. (Associated Press)

El servicio de mensajería instantánea Whatsapp también ha sido una importante fuente de problemas para las FDI y no debe descartarse que esta aplicación o sus equivalentes Telegram o Line puedan plantear graves problemas de seguridad para sus usuarios militares. De hecho, en 2013 doce oficiales de la Fuerza Aérea Israelí fueron condenados por compartir información clasificada como planos y coordenadas de vuelo, a través de esta plataforma. Y más recientemente, durante la Operación Margen Protector que se desarrolló en la franja de Gaza en verano de 2014, varios soldados fueron detenidos tras difundir a través de la misma red fotografías de varios soldados israelíes caídos en combate durante la incursión terrestre en Gaza. De forma similar, en el año 2013 el soldado Mor Ostrovski fue arrestado tras compartir en su cuenta de la red social de fotografía Instagram una imagen en la que se podía ver a un joven palestino en el punto de mira de su rifle.

Además, las redes sociales virtuales también pueden ser utilizadas por los soldados como medio de protesta. Por ejemplo, el pasado mayo una campaña realizada a través de *Facebook* de apoyo a un soldado israelí arrestado tras ser grabado mientras apuntaba con su arma a dos adolescentes palestinos en Cisjordania consiguió más de 120.000 *"Me gusta"*.

Del mismo modo, durante la actual escalada militar en Ucrania, el inadecuado uso de las redes sociales por parte de soldados rusos ha comprometido la Seguridad de la Operación (OPSEC) y puesto en duda la versión oficial de Moscú sobre su no implicación en el conflicto. En este sentido, las fotografías compartidas por el soldado Alexander Sotkinen en su cuenta de *Instagram* lo geolocalizaban dentro de las fronteras ucranianas, más concretamente entre los pueblos de Krasna Talycha y Krasny Derkul, ambos controlados por las fuerzas rebeldes. Otros soldados, como Vladislav Laptev o Mikhail Chugunov publicaron en su perfil de *VKontkte* –una red social rusa similar a *Facebook*– fotografías de los convoyes militares rusos desplazándose a la frontera ucraniana o declaraciones de que *"dispararon toda la noche contra Ucrania"* tal y como confirmó posteriormente la inteligencia estadounidense mediante fotografías de satálites[6]. No obstante, puede que el caso más conocido y controvertido de los riesgos –en este caso estratégicos y políticos– que entraña el em-

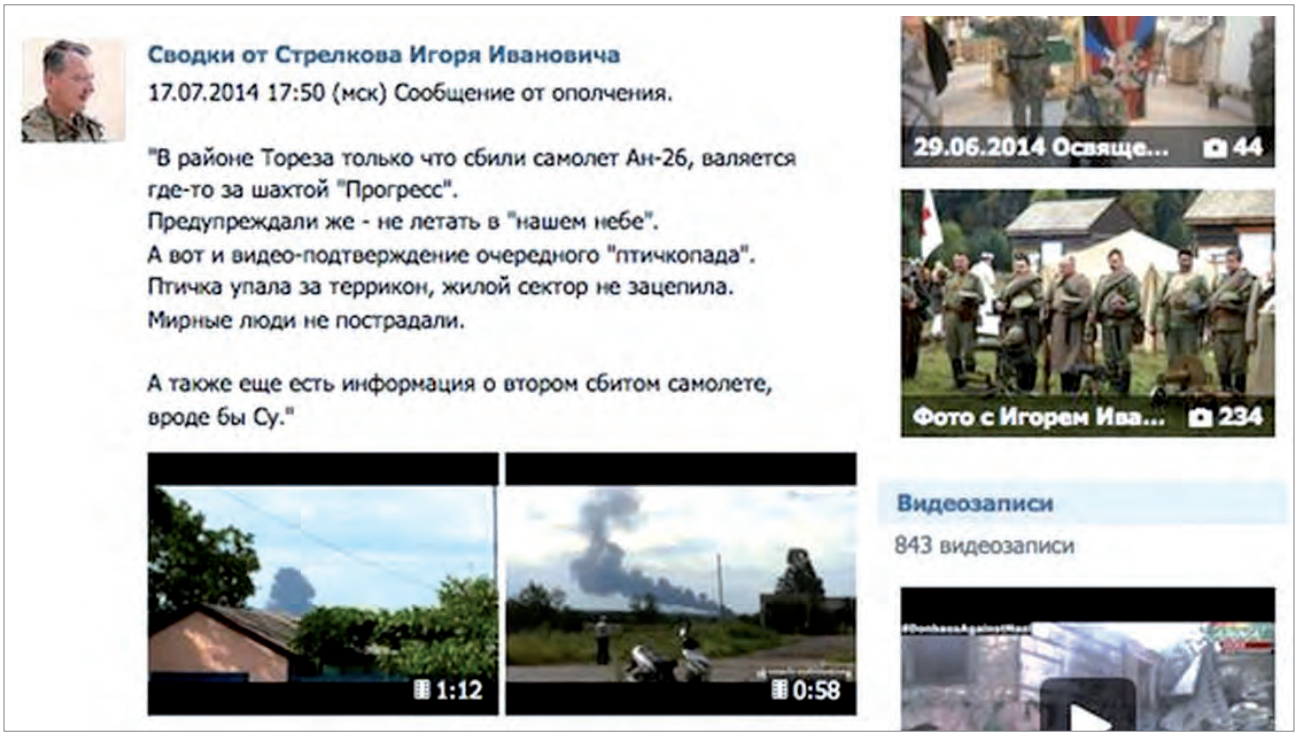
El soldado ruso Alexander Sotkinen en territorio ucraniano.
(Fuente Instagram)

pleo de las redes sociales para la seguridad de las operaciones militares es el caso de Igor Girkin, líder separatista de la autoproclamada República Popular de Donetsk, felicitándose en la red social *Vkontkte* de haber abatido un avión de transporte ucraniano *Antonov AN-26* cerca de la ciudad de Torez... un avión que resultó ser el vuelo *MH-17* de *Malaysia Airlines* y en el que murieron trescientos pasajeros[7]. Punto y a parte merecería el análisis de inteligencia empleando fuentes abiertas como redes sociales virtuales, fotografías y herramientas de geolocalización para identificar y situar al lanzador autopropulsado del misil superficie-aire *SA-11* (que formaba parte del sistema antiaéreo *BUK*) que derribó este avión[8].

Si nos desplazamos al otro lado del Atlántico también podemos observar que la preocupación del Departamento de Defensa estadounidense sobre el uso inapropiado de las redes sociales virtuales por parte de sus tropas durante las guerras de Irak y Afganistán ha ido aumentando. Y es que dejando de lado los múltiples problemas que han surgido a raíz de mantener abierta la geolocalización de los perfiles personales de los soldados en las redes sociales o publicar ciertas informaciones que ponían en riesgo la seguridad de las operaciones militares, en 2014 hemos podido observar otro caso que ha generado importantes controversias en Washington: la publicación en *Facebook* de una fotografía de catorce soldados estadounidenses en una posición poco respetuosa ante un ataúd –que según fuentes oficiales estaba vacío– cubierto con la bandera estadounidense[9].

Además del ejército estadounidense, las fuerzas armadas canadienses, británicas y australianas también han advertido a sus soldados acerca de los múltiples peligros que entraña la publicación de fotos personales y cualquier tipo de información sensible en las redes sociales como el geoposicionamiento de tropas, fotografías de soldados uniformados o ubicaciones tras confirmarse que operati-

Artilleria rusa desplegada en las fronteras de Ucrania.
Fuente Vkontkte)



Igor Girkin anunciando el derribo de un avion que resultaría el vuelo MH17. (Fuente Vkontkte)

vos de Al Qaeda estaban utilizando perfiles falsos en *Facebook*, simulando ser mujeres atractivas para entablar amistad con los soldados para realizar labores de inteligencia en redes sociales[10].

En conclusión, el empleo de las redes sociales en el ámbito militar no sólo se ha convertido en una importante herramienta de comunicación estratégica, sino también en una amenaza para la seguridad de las operaciones militares, un altavoz para las protestas de los soldados y un riesgo para la imagen y reputación de sus fuerzas armadas. Precisamente, todos estos elementos hacen que países que han participado en conflictos como Israel, Estados Unidos o Reino Unido monitoricen activamente la actividad de sus soldados para evitar que éstos cometan infracciones o cometan errores que pueden amenazar la seguridad de sus naciones, pero a su vez han abierto un interesante debate sobre el derecho a la privacidad de los miembros de las Fuerzas Armadas en el ámbito de las redes sociales. Sea como fuere, las redes sociales son una amenaza real para las Fuerzas Armadas y para la seguridad de las operaciones militares de todos los países avanzados ■

[1]SINGER, Peter y FRIEDMAN, Peter (2014): *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Nueva York: Oxford University Press o CLARKE, Richard y KNAKE, y Robert (2010): *Cyber War: The Next Threat to National Security and What to Do About It,* Nueva York: Harper Collins.

[2]BARRANCOS, David (2014): "Los Community Managers del terror: la propaganda de ISIS y su ofensiva sobre Irak", *Documento de Opinión del IEEE*, 82 (2014); DARCZEWSKA, Jolanta (2014): *The anatomy of Russian information warfare the Crimean operation, a case study*, Varsovia: Center for European Studies; STALINSKY, Steven y SOSNOW, Robert (2014): *From Al-Qaeda To The Islamic State (ISIS), Jihadi Groups Engage in Cyber Jihad*, Washington DC: The Middle East Media Research Institute o FOJÓN, Enrique; HERNÁNDEZ, Adolfo y COLOM, Guillem (2012): "Las redes sociales como herramienta de comunicación estratégica de las Fuerzas de Defensa de Israel durante la Operación Pilar Defensivo en Gaza", *Análisis del Real Instituto Elcano*, 94.

[3]GINSBURG, Mitch (23 de febrero de 2014): "Israel's army of Facebook addicts battles to keep its secrets", *The Times of Israel*.

[4]BRODERICK, Ryan (3 de junio de 2013): "Female Israeli Defense Force Members Pose In Lingerie For Racy Facebook", *Buzzfeed*.

[5]FOJÓN, Enrique y COLOM, Guillem (27 de agosto de 2014): "La guerra digital en el conflicto árabe-israelí", *La Razón*.

[6]SZOLDRA, Paul (21 de julio de 2014): "A Russian Soldier's Instagram Post May Be The Clearest Indication of Moscow's Involvement in East Ukraine", *Business Insider* o KELLEY, Michael (28 de julio de 2014): "US: These Satellite Photos Prove That Russian Troops are Shelling Ukraine", *Business Insider*.

[7]LUHN, Alec (20 de julio de 2014): "Three pro-Russia rebel leaders at the centre of suspitions over downed MH17", *The Guardian* y MOSENDZ, Polly (25 de septiembre de 2014): "Separatist Takes Credit for MH17 Shooting with Suspicious Media Post", The Wire.

[8]Bellingcat (seudo.) (2014): "Origin of the Separatists' Buk: A Bellingcat Investigation", *Bellingcat*, https://www.bellingcat.com/news/uk-and-europe/2014/11/08/origin-of-the-separatists-buk-a-bellingcat-investigation/

[9]MEMMOTH, Mark (18 de febrero de 2014): "Soldiers' 'Fun' Photo With Flag-Draped Coffin Sparks Outrage", *National Republic Radio*.

[10]AXE, David (9 de octubre de 2012): "Careful Who You Friend: Taliban Posing as "Attractive Women" Online", *Wired*.