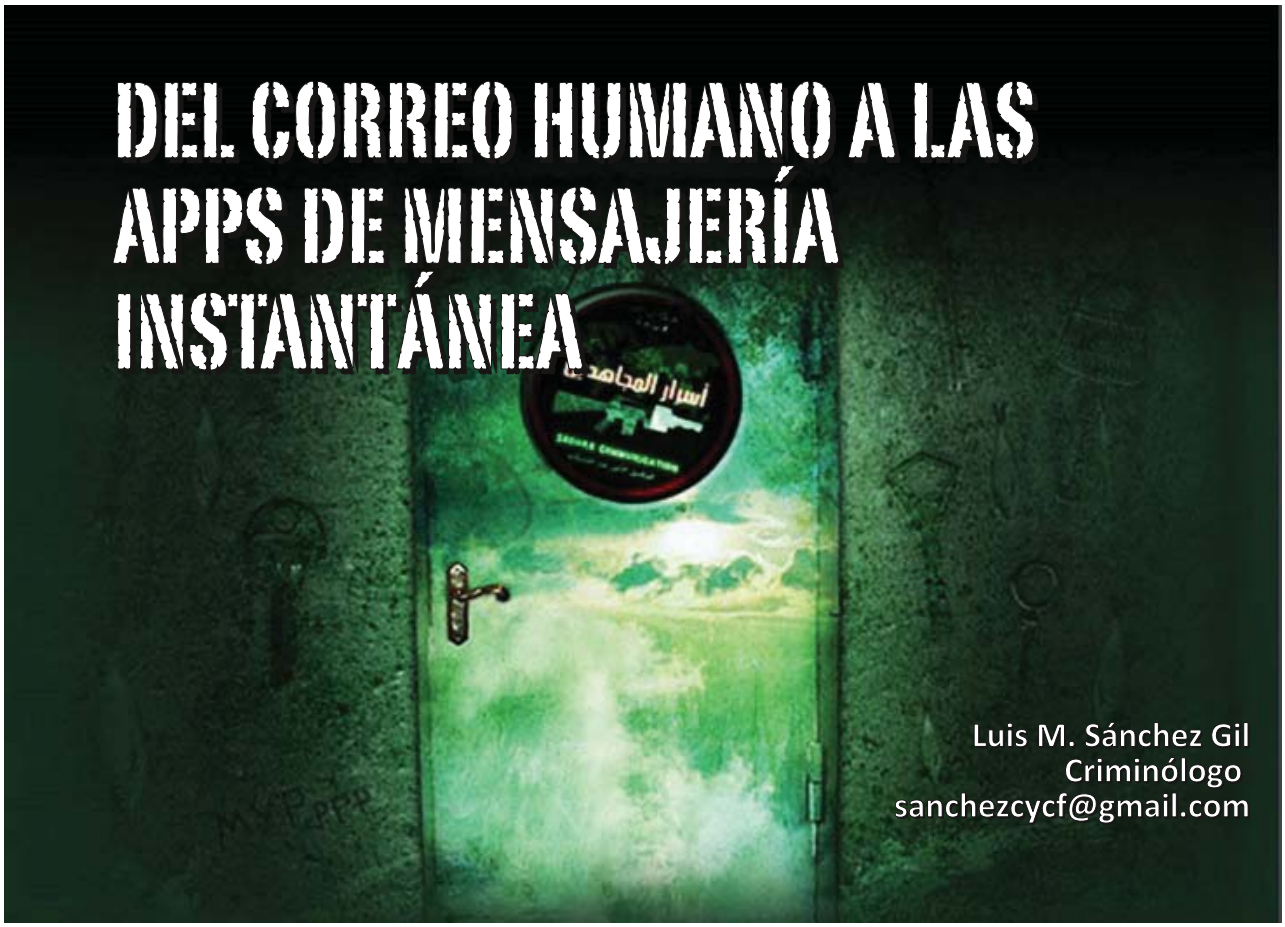
DEL CORREO HUMANO A LAS APPS DE MENSAJERÍA INSTANTÁNEA



Luis M. Sánchez Gil
Criminólogo
sanchezcycf@gmail.com

Los estados, sus organismos e instituciones extraen continuamente lecciones de los ataques contra su seguridad nacional, de los errores cometidos en las operaciones antiterroristas,... De igual manera, los grupos insurgentes y las organizaciones terroristas también evolucionan a partir de sus experiencias y de las continuas contiendas que mantienen con los servicios de inteligencia, los cuerpos de seguridad o las fuerzas armadas, etc., siendo, en numerosos casos, visibles sus lecciones aprendidas.

Las comunicaciones en el seno de un grupo terrorista constituyen un instrumento fundamental a través del que se transmiten discursos ideológicos, directrices de estrategia militar, etc. Sin embargo, no solo conforman una herramienta que facilita sus actividades sino que, en muchas ocasiones, sirven a los agentes antiterroristas como elemento delator y localizador de estas organizaciones o individuos. Precisamente una de las dificultades que se presentan a la hora de interceptar la acción de un terrorista individual (a menudo mal denominado "lobo solitario") es el menor nivel de interacción que este presenta en comparación con las células o grupos -por muy reducidos que sean-.

Las grandes organizaciones terroristas como Al Qaeda (AQ) o el Daesh son plenamente conscientes de lo expuesto con anterioridad, lo que provoca

que permanentemente se esfuercen para alcanzar mejoras en la seguridad de sus comunicaciones. Un aspecto que se lleva al extremo cuando se trata de interacciones que implican la participación de individuos que se sitúan, dentro de la jerarquía del grupo, en las posiciones más altas. Por suerte, a pesar de todos los esfuerzos que los terroristas realizan para que sus comunicaciones pasen inadvertidas, los agentes de la lucha antiterrorista -empleando distintas técnicas que van desde la utilización de elementos tecnológicos hasta el uso de informadores- consiguen interceptar las cadenas de comunicación y, con cierta frecuencia, llegar a través de ellas a sus actores. Un ejemplo público y muy conocido es el de la interceptación de una llamada efectuada desde un teléfono satelital por Abu Ahmed al Kuwaiti (correo humano de Osama Bin Laden -en aquel tiempo número uno de AQ-) que tras meses de trabajo desembocó en la denominada "Operación Gerónimo", en la que fuerzas especiales de los Estados Unidos dieron muerte a Bin Laden e intervinieron una ingente cantidad de documentación. De tal manera que los terroristas, a menudo, cuidan sus formas de comunicación e implementan sus sistemas de seguridad.

Por suerte, a pesar de todos los esfuerzos que los terroristas realizan para que sus comunicaciones pasen inadvertidas, los agentes de la lucha antiterrorista -empleando distintas técnicas que van desde la utilización de elementos tecnológicos hasta el uso de informadores- consiguen interceptar las cadenas de comunicación y, con cierta frecuencia, llegar a través de ellas a sus actores.

Tradicionalmente, las organizaciones yihadistas han utilizado el correo humano, usando -en los últimos años- las memorias USB como soporte para la transmisión de los mensajes. En cambio, a pesar de que parece constituir un canal seguro, para lograr un aceptable nivel de seguridad se requiere la participación de un elevado número de intermediarios lo que, a su vez, incrementa el riesgo de interceptación y ralentiza el tránsito entre emisor y receptor. Por ello, los grupos islamistas han optado por servirse de la tecnología, no sin adoptar algunas precauciones en su labor operativa. Entre los métodos que las organizaciones terroristas islamistas han empleado para proteger sus interacciones de posibles interceptaciones se encuentra la técnica de *dead dropping*. El *dead dropping* consiste en la utilización de una cuenta de correo (sirviéndose de proveedores de servicios de correo electrónico convencionales) para escribir un mensaje sin destinatario y grabarlo en la carpeta de borradores. En otro lugar, desde un dispositivo diferente, pero empleando igual usuario y contraseña, otra persona accede a la misma cuenta de correo electrónico y, a continuación, a la carpeta de borradores en que se aloja el texto introducido anteriormente por otro individuo. De esta forma se hace efectiva la comunicación sin necesidad de que el mensaje transite por la red de una cuenta a otra. A su vez, el receptor puede repetir el proceso para dar una respuesta y, del mismo modo, la conversación se puede prorrogar lo que sus participantes deseen. Este método fue utilizado, por ejemplo, en el curso de los preparativos del 11-M en las

comunicaciones entre Amer Azizi y sus interlocutores locales de la propia red 11-M (intercambiando mensajes entre Afganistán, Pakistán y España), dificultando con esta técnica el esclarecimiento de la trazabilidad de los mismos (Reinares, 2014). Aunque es una práctica que no solo ha sido empleada por los terroristas sino que también ha servido a algunos servicios de inteligencia para intercambiar mensajería entre miembros e informadores.

con esta finalidad cabe destacar *Asrar al-Mujahideen 2.0* (también conocido como *Secret Mujahideen 2.0*) lanzado por el *Global Islamic Media Front* (GIMF) *Technical Center*. Su gran difusión con la publicación de un artículo bajo el título de "Asrar al-Mujahideen: Sending & Receiving Encrypted Messages" en el número 1 de la revista *Inspire*, -producida por Al Qaeda en la Península Arábiga (AQAP)- lo convirtió en un instrumento muy popular. Su funcionamiento es sencillo y

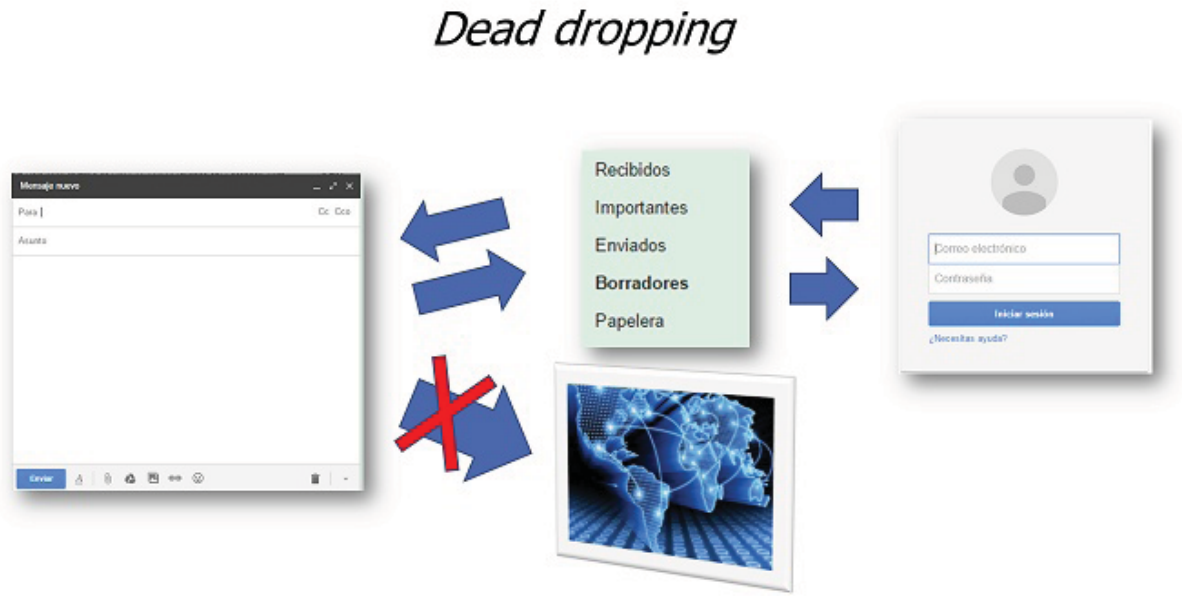


Ilustración 1. Fuente: elaboración propia

Sin embargo, con el paso del tiempo, los agentes de la lucha antiterrorista tomaron consciencia del uso de esta metodología por parte de dichos grupos yihadistas, reaccionando en consecuencia. Circunstancia que, a su vez, propició que estas organizaciones terroristas evolucionaran y potenciaran el uso de los *softwares* de encriptación en sus comunicaciones. Sin lugar a dudas, entre los programas empleados

aparece perfectamente desarrollado en el citado volumen de *Inspire* (mostrando, incluso, capturas de pantalla). *Asrar al-Mujahideen* opera con una clave pública (a modo de dirección de recepción) y una privada que los usuarios emplean para enviar los mensajes cifrados y transformar las comunicaciones recibidas a un lenguaje "en claro" que haga posible su lectura. Además, AQAP apunta una serie de pautas para evitar fallos

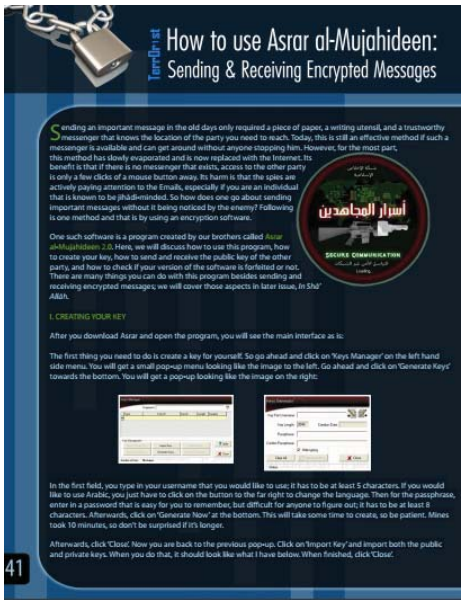


Ilustración 2. Fuente: *Inspire*

de seguridad en el uso de este programa como es la recomendación de alojarlo en un dispositivo de memoria USB (en lugar de hacerlo en un disco duro interno) a fin de dificultar el acceso al mismo a los agentes de lucha antiterrorista cuando el equipo en cuestión se encuentre de forma regular conectado a la red. Una muestra del extendido uso de este *software* es su utilización en las comunicaciones por parte de importantes iconos del terrorismo islamista como, por ejemplo, Anuar al-Aulaki (Storm, Cruickshank y Lister, 2015), caracterizado por ser una figura de gran relevancia en el plano ideológico de AQ y considerado líder de AQAP hasta su muerte en una operación de la inteligencia estadounidense en el año 2011.

En febrero de 2013 el Centro Técnico de GIMF facilitaba a los actores islamistas una nueva herramienta: *Asrar al-Dardashah*. Este nuevo instrumento constituye, en lo básico, una evolución del *software* anterior (*Asrar al-Mujahideen*) en tanto que opera como plataforma de chat, siendo publicitado como «el primer programa islámico para mensajería instantánea cifrada» (GIMF, 2013).

Sin embargo, los grupos yihadistas no se han detenido en los *softwares* criptográficos, destacando en la actualidad por el excelente aprovechamiento que muestran de las tecnologías de la información y la comunicación (TIC). El análisis de los últimos actos de terrorismo islamista evidencia el uso de *apps* de mensajería instantánea comerciales, como *WhatsApp* o *Telegram*, por parte de los terroristas durante la planificación, preparación y ejecución de sus ataques. Las medidas de seguridad que dichas plataformas adoptan para el cifrado de los mensajes blindan también las comunicaciones de los actores terroristas. Además, a la seguridad de los *softwares* hay que sumar la de los dispositivos que se emplean, siendo buen ejemplo de la problemática la disputa protagonizada en los últimos meses por *Apple* y el FBI en relación al cifrado de los dispositivos *iPhone* vinculados a los terroristas de San Bernardino.

En definitiva, las organizaciones terroristas son conscientes de la importancia de sus comunicaciones y se esfuerzan por conseguir que estas se efectúen de forma segura. Los terroristas aprenden continuamente de las medidas adoptadas por los servicios antiterroristas que interceptan sus conversaciones y frustran sus acciones, actuando en consecuencia. ■

REFERENCIAS

Al-Malahem Media. (2010). "Asrar al-Mujahideen: Sending & Receiving Encrypted Messages". *Inspire*, 1, 41-44.

Global Islamic Media Front´s Technical Center. (2013). Download Asrar al-Dardashah. Recuperado el 7 de mayo de 2016 de http://gimfmedia.com/tech/en/asrar-al-dardashah/

Reinares, F. (2014). *¡Matadlos!* 1ª Ed. Barcelona: Galaxia Guternberg

Storm, M., Cruickshank, P. y Lister, T. (2015). *Mi Vida en Al Qaeda*. Barcelona: Península.