

Daesh en la 'Deep Web': las profundidades de la Red al servicio de la 'yihad'

[Andrés Ortiz Moyano](#)



La versatilidad del Estado Islámico en el uso de nuevas tecnologías y la propaganda del terror alcanza su cénit en el Internet profundo.

Parece ya evidente que una de las principales características de Daesh, que ha asombrado a propios y extraños, es la extraordinaria versatilidad que demuestra en sus distintas actividades.

Desde la proclama del califato por parte de Al Baghdadi a mediados de 2014, se han ido progresivamente conociendo con mayor detalle los distintos aspectos sobre los que se basa la utopía *yihadista*: financiación, logística, política social, capacidad militar... y comunicación. Efectivamente, en general se puede estar muy de acuerdo en que Daesh ha revolucionado la propaganda, el mensaje y los canales de información desde el enfoque terrorista. Es más, podemos establecer que su revolución mediática ha sido tan poderosa que ha reescrito las bases del mensaje del terror.

Esta importancia se traduce en un extremo cuidado de sus contenidos tanto en el fondo como en la forma, que encuentran una difusión extraordinaria en la tecnología actual: sencilla, barata y altamente eficaz. Bien conocidas son las actividades del Estado Islámico en las redes sociales, foros virtuales o aplicaciones móviles. Igualmente notorias son las acciones de su centro de comunicación Al Hayat y sus distintas delegaciones, cuyo organigrama es parte fundamental en la propia estructura de Daesh (tanto es así que el director de comunicaciones, Al Adsnani, tiene tratamiento de emir, y los distintos trabajadores cobran bastante más que un soldado raso. La coalición internacional ha puesto precio a las cabezas de estos personajes y son ya objetivos prioritarios).

Así pues, ante esta realidad, debemos asumir que el Estado Islámico no escatima esfuerzos en utilizar tecnología puntera, potente y, sobre todo, eficaz a la hora de difundir su mensaje. Como consecuencia de este patrón, los tentáculos *yihadistas* se clavan incluso en el Internet más desconocido y profundo: la *Deep Web* (*Internet profundo*).

En las profundidades

Una explicación prosaica del *Internet profundo*, sin tecnicismos, se suele ilustrar con la imagen de un iceberg: la punta es la web que todos conocemos y usamos a diario, y la inmensidad oculta corresponde a esa red paralela cuyo tamaño se estima es 500 veces mayor que la anterior.

Pero, ¿cuál es la auténtica particularidad de la *Deep Web*? Pues, básicamente, que al no estar indexadas las páginas web que encontramos, la navegación por ella es totalmente anónima. Esta característica supone una oportunidad obvia para actividades delictivas. (Sin embargo, la mayor parte de la *Deep Web* no se dedica a ello, sólo un porcentaje pequeño llamado *Dark Web*, *Internet oscuro*, por el mercado negro que allí impera). Acceder no es ninguna tarea titánica, por lo que, a pesar del desconocimiento generalizado de éste, cualquiera puede acceder y navegar libremente sin necesidad de vastos conocimientos.

La presencia del extremismo en la *Deep Web* es notable. Desde hace años se sabe de la existencia de foros extremistas pertenecientes a Al Qaeda y otros grupos radicales; ahora es Daesh quien se ha subido al carro. Sin embargo, en los últimos meses se ha repetido el mismo patrón de actividad que vemos en las redes sociales. Ya no es tan fácil acceder a esos foros, sino que hay que esmerarse más en la búsqueda para localizarlos y acceder. Debido a la guerra declarada por compañías como Twitter y Facebook, por ejemplo, las grandes cuentas *yihadistas* han desaparecido, pasando ahora a una actividad mucho más sutil a través de perfiles infinitamente más pequeños pero difíciles de encontrar. En la *Deep Web* el patrón es similar, antes el ingreso en los foros era muy sencillo (existían algunos muy conocidos como Al

Fida o Shoumoukh al Islam, que acabaron desapareciendo), y ahora hay que bucear un poco más. En cualquier caso, no es, ni mucho menos, una tarea imposible. Son foros en inglés y árabe principalmente, como Islamic State, aunque muchos captadores utilizan otras lenguas como el portugués o el propio castellano.

Es en estos foros y en otros generalistas donde actúan algunos captadores. Principalmente, existen dos tipos: los activos y los pasivos. Los primeros son aquellos que rastrean la Red (son más activos en el Internet superficial) en busca de usuarios que demuestren su apoyo a Daesh a través de la difusión de contenidos extremistas (es el caso que relata la periodista francesa Anne Erelle en su *En la piel de una 'yihadista'*). En cuanto a los segundos, los más habituales en la *Deep Web*, son aquellos que ofrecen su ayuda para unirse a la *yihad* y esperan ser contactados por posibles candidatos. Es una estrategia lógica, ya que un usuario extrañamente contactará con un captador pasivo 'al descubierto', sino que recurrirá al anonimato de las profundidades para interesarse.

Paralelamente, cabe destacar que en este entorno asistimos a la difusión de los contenidos más virulentos, inéditos en los medios convencionales y en páginas web de información. Ejecuciones de toda clase y a cualquier persona (hombres, mujeres, niños y ancianos), matanzas de minorías religiosas como los yazidíes, sermones y proclamas de los jefes de Daesh, sugerentes anuncios de captación, todo tipo de amenazas a los enemigos del califato... y siempre jaleado por innumerables seguidores que se retroalimentan en contenidos, consejos y algunos documentos.

Por ejemplo, resulta relativamente sencillo conseguir auténticas guías del buen *yihadista*. Unas te recomiendan qué comer y cómo entrenar para estar en forma y saber usar un AK-47, una granada o un cuchillo; otras te aconsejan sobre cómo viajar a Siria o Irak desde el país en el que te encuentres (recomiendan a franceses viajar a Turquía desde España y luego cruzar la frontera).

Incluso existen inquietantes tertulias entre supuestos candidatos a *lobos solitarios* para atentar por su cuenta en Occidente y algunos países musulmanes. Si bien muchos de estos usuarios son cuentas falsas de meros mirones o incluso infiltrados de las fuerzas de seguridad de Estados democráticos, el inmenso número de participantes sugiere que, en efecto, muchos de ellos son verdaderos terroristas.

Actividades complementarias

Se ha demostrado que, en ocasiones puntuales, Daesh y otros grupos terroristas han comprado armas en la *Dark Web*. No es en absoluto difícil acceder a tiendas donde comprar pistolas,

ametralladoras, escopetas, granadas o bazucas. No obstante, cabe recordar que el principal flujo de armamento de los *yihadistas* ha sido, hasta ahora, gracias a los botines de guerra tras sus victorias sobre el desmoralizado ejército iraquí. Así, el Estado Islámico disfruta ahora de la logística militar americana que en su día fue donada a Bagdad.

Por otro lado, se antoja necesario destacar un denominador común en todos los mensajes lanzados por Daesh en la *Dark Web*, que no es otro que la financiación del califato a través de donaciones a cuentas de Bitcoins. Todos los foros, todos los usuarios afines y todos los hilos de debate encontrados están coronados tanto por una *sura* (verso del Corán) como por un número de cuenta corriente de esta moneda virtual.

Debe hacerse hincapié en que éstas, lógicamente, no conforman el grueso ni de su financiación ni de su armamento, pero sí arroja una clarificadora luz sobre el hecho de que están dispuestos a utilizar todas las herramientas a su alrededor posibles.

Luces necesarias en las sombras de Internet

Las prestaciones de la *Deep Web*, decíamos, ofrecen unas excepcionales oportunidades para actividades delictivas. Es una tecnología relativamente reciente (poco más de una década) y su conocimiento actual es muy escaso. Tanto que genera una mitificación perniciosa a la hora de comprender las claves de su funcionamiento. Es, precisamente, ese prejuicio el que, con conocimiento y uso, las sociedades tecnológicas actuales deben derribar, como se está demostrando, al nuevo terrorismo. En este sentido, el *yihadismo* internacional con Daesh a la cabeza ha marcado un perturbador antecedente.

En el lado opuesto, las unidades de ciberterrorismo de las fuerzas de seguridad occidentales son cada vez más activas en estos entornos y, a pesar de las dificultades que plantean, su eficiencia mejora cada año. De ahí la obligación de los usuarios a conocer y comprender, pues los nuevos campos de batalla son tan terrenales como virtuales.

Debate [*Daesh, una sofisticada maquinaria de propaganda*](#) con motivo de la presentación del libro *#Yihad. Cómo el Estado Islámico ha conquistado Internet y los medios de comunicación* el jueves 21 de enero a las 10h.

Fecha de creación

19 enero, 2016