ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

129/2015 01 diciembre de 2015

*Agnese Carlini**

ISIS: UNA NUEVA AMENAZA EN LA ERA DIGITAL

ISIS: UNA NUEVA AMENAZA EN LA ERA DIGITAL

Resumen:

El adviento de la Era Digital ha creado un nuevo campo de batalla. Las tecnologías modernas han establecido nuevos métodos de confrontación, instando las teorías clásicas sobre la guerra a hacer frente a las características peculiares del quinto dominio de conflictividad. Entre las amenazas a las que se enfrenta el espacio cibernético, la más inquietante es la del terrorismo cibernético, sobre todo el papel desempeñado por el Cibercalifato. Según algunos expertos, ISIS no existiría y no tendría tanto éxito si no hubiera hecho uso de la red. Como consecuencia de sus capacidades electrónicas ha ganado apoyo a nivel mundial, transformando internet en una posible herramienta de guerra.

El presente artículo propone un análisis del uso de la red por parte del grupo terrorista ISIS, con fines de reclutamiento, propaganda, recaudación de fondos y guerra psicológica, acentuando también las diferencias entre los grupos seculares terroristas y los yihadistas contemporáneos.

Abstract:

The advent of the Digital Age has created a new battlefield. Modern technologies have established new methods of confrontation, urging classic war theories to deal with the peculiar characteristics of the 5th domain of war. Among the threats that the cyberspace has to deal with the most worrying one is represented by cyberterrorism and especially by the Cybercaliphate. Some experts believe that ISIS would not have come into existence without the proper use of Internet; as a consequence of its electronic capacities it has gained support worldwide transforming the Web into a possible tool of war.

The present article proposes an analysis of the use of Internet from the terrorist group ISIS, with the purpose of recruitment, propaganda, fundraising and psychological warfare, highlighting as well the differences between terrorist secular groups and contemporary jihadists.

Palabras clave: Ciberterrorismo, Cibercalifato, ISIS, reclutamiento, guerra psicológica.

Keywords: Cyberterrorism, Cybercaliphate, ISIS, recruiting, psychological warfare.

INTRODUCCIÓN

El terrorismo empezó a amenazar la estabilidad global alrededor de los años 60 con la creación de grupos terroristas nacionales e internacionales. El final de la Guerra Fría y el proceso de descolonización desestabilizaron regiones enteras donde personas de diferentes culturas, tradiciones y religiones coexistieron pacíficamente durante décadas. Sin embargo, como consecuencia de la Revolución en Irán (1979), el terrorismo internacional experimentó un cambio drástico seguido por el resurgimiento del terrorismo religioso. El terrorismo religioso internacional ha demostrado ser la amenaza más desafiante, amenazante y asimétrica de todos los tiempos[1].

USO DE LA RED POR PARTE DE LOS TERRORISTAS

La comunicación siempre ha sido considerada una herramienta fundamental para la política, en tiempo de paz y de guerra. Independientemente de los medios adoptados, la comunicación necesita tiempo para poder producir sus efectos. Los medios modernos, organizados como una red, han demostrado una flexibilidad y adaptación alarmante a los continuos cambios tecnológicos, consiguiendo resultados más productivos y una mejor organización respecto a la piramidal de las actuales fuerzas de seguridad[2]. Hoy en día, la red juega un papel importante demostrando de todas formas sus pros y contras. El tiempo y el espacio han sido modificados profundamente; la red ha anulado la distancia entre las personas permitiendo la movilización de las masas. Los grupos terroristas religiosos contemporáneos ya no están inclinados exclusivamente a cometer ataques masivos sino que pueden contar con el uso de medios poco convencionales, una visión deformada de la sociedad, y por último un proceso nuevo y más eficiente de reclutamiento de militantes[3].

La Comunidad Internacional se enfrenta a un nuevo modelo de terrorismo, basado sobre todo en las creencias religiosas más que en los valores seculares. Bruce Hoffman, Director del Centro de Estudios para la Seguridad y del Programa de Estudio sobre la Seguridad en Georgetown University's Edmund A. Walsh School of Foreign Service ha establecido tres características para describir el terrorismo moderno religioso:

- Los autores deben usar escritos religiosos para justificar o explicar sus actos violentos o reclutar nuevos efectivos[4];

---

[1] GORI Emanuele *"L'evoluzione del terrorismo internazionale: il rischio di attacchi non convenzionali"*, 2008, pp.1-3. Disponible en: http://www.cssi.unifi.it/upload/sub/EVOLUZIONE%20TERRORISMO%20INTERNAZIONALE.pdf

[2] GAGLIANO Giuseppe *"Guerra psicologica. Saggio sulle moderne tecniche militari cognitive e di disinformazione"*, Fuoco Edizioni, 2012, pp 1-15.

[3] GORI, op. cit.

[4] Editado por CROMARTIER Michael. entrevista con Bruce Hoffman *"A Conversation with Bruce Hoffman and*

- Líderes Religiosos deben estar involucrados en funciones de liderazgo[5];
- El uso de imágenes apocalípticas por parte de los perpetradores para justificar sus acciones[6].

EL TERRORISMO RELIGIOSO CONTEMPORÁNEO

El terrorismo religioso internacional ha experimentado unos cambios considerables desde su resurgimiento en 1979 con el objetivo principal de extirpar la presencia occidental en la región de Oriente Medio y revolucionar su sociedad. Los actuales grupos terroristas usan la religión para legitimar sus ataques indiscriminados a diferencia de los grupos seculares que perpetraban ataques selectivos para no perder el apoyo de las masas. Hasta ahora, los ataques no convencionales han visto el uso de gases tóxicos contra el World Trade Center en 1993, gas Sarin en el metro de Tokio en 1995 y los ataques terroristas en 2001[7]. Desde entonces, la tecnología ha evolucionado de igual manera que las técnicas usadas por los terroristas. La evolución de la red y su presencia intrusiva en la vida cotidiana hace que la Comunidad internacional seas más vulnerable a los ciberataques.

El terrorismo cibernético representa una grave amenaza para la seguridad económica y de las naciones, especialmente en un momento en el que los grupos fundamentalistas están creciendo y se propagan rápidamente en todo el mundo gracias también al uso de la red. Mientras que los políticos, los expertos y los medios de comunicación se han centrado sobre todo en los riesgos procedentes del ciberterrorismo contra la red, son muy pocos los que han prestado suficiente atención a las actividades terroristas llevadas a cabo diariamente a través de Internet. En el siglo XXI la misma red utilizada durante la Guerra Fría, por parte de los servicios secretos estadunidenses contra la Unión Soviética, se ha convertido en un arma de doble filo a merced del terrorismo internacional. La web ha resultado ser una arena perfecta para los grupos terroristas ofreciendo: fácil acceso, poca o ninguna regulación, anonimato, un medio de comunicación rápido, efectivo y económico. La mayoría de las organizaciones internacionales tienen páginas webs donde poder promover sus ideologías, vender sus productos, animar a la gente a practicar su interpretación de la religión y por ultimo explicar la fabricación de armas para poder utilizar en contra de los infieles. Aprovechar la red ha representado un reto importante y un éxito inmenso para los grupos terroristas que anteriormente dependían de los medios de comunicación para publicar sus acciones.

Jeffrey Goldberg" in *Religion, Culture and International Conflict: a conversation*, Lanham, Md.: Rowman & Littlefield Publishers, 2005, pp 29-35.

[5] HOFFMAN Bruce *"Inside Terrorism"*, USA, Columbia University Press, 1999, p 90.

[6] Ian O. Lesser, Bruce Hoffman, John Arquilla, David Ronfeldt, Michele Zanini, Brian Michael Jenkins *"Countering the new terrorism"*, Santa Monica 1999, Chapter 2 pp 7-35.

[7] GORI, op. cit.

Gabriel Weimann, Senior Fellow en el United States Institute of Peace y profesor de comunicación en la Haifa University, ha identificado ocho maneras en las que los terroristas usan la red:

- **Guerra psicológica**- divulgando imágenes aterradoras como la decapitación de rehenes.
- **Publicidad y propaganda**- hoy en día los terroristas pueden manipular la información, su retrato y el de sus enemigos para poder justificar sus acciones.
- **Extracción de datos**- internet representa la "universidad libre de los terroristas". Según Dan Verton, ex oficial de inteligencia en la Marina estadunidense, "*las células de al Qaeda operan con la asistencia de extensas bases de datos que contienen potenciales objetivos americanos. Utilizan internet para recoger información sobre estos últimos, especialmente en el ámbito económico, y los softwares modernos les permiten analizar las deficiencias estructurales de las diferentes instalaciones y los potenciales efectos colaterales que podrían conllevar.*[8]"
- **Recaudación de fondos** - Al Qaeda dependió fuertemente de las donaciones a través de una fundación caritativa, ONGs, chat rooms y foros. Según los expertos, ISIS utiliza sobre todo la Red oscura (*dark web*) y Bitcoin[9] para recaudar fondos y para el proceso de reclutamiento. La posibilidad de que ISIS se esté refugiando en las redes anónimas ha sido remarcado también por Jimmy Gurule, ex Secretario General del Departamento del Tesoro en la presidencia George W. Bush y experto internacional en terrorismo y financiación del terrorismo. Gurule ha subrayado el hecho de que Bitcoin no este regulado y que entonces represente un riesgo y una brecha en el sistema que podría ser usada con propósitos criminales. Sin embargo ISIS, a diferencia de al Qaeda, es una organización que se auto financia gracias a la venta del petróleo en el mercado negro. El posible uso de Bitcoin para financiar organizaciones terroristas ha sido investigado por las agencias gubernamentales sobre todo después de un post donde se incitaba a ISIS a explotar el DarkWallet como plataforma de financiación[10].
- **Reclutamiento y movilización**- ambos Al Qaeda e ISIS han usado la web para reclutar y movilizar fundamentalistas mundialmente. Por su parte, ISIS lo parece aprovechar mejor que Al Qaeda gracias al contenido violento de los mensajes enviados por Internet. Compartiendo videos en las redes sociales aumenta el número de *foreign fighters* que se unen a ISIS diariamente. El proceso de

[8] VERTON Dan *"Black Ice: The invisible threat of cyberterrorism"*, McGrawHill/Osborne, 2003, p 109.
[9] Bitcoin: es una criptodivisa descentralizada concebida en 2009 por Satoshi Nakamoto.
[10] *"ISIS-Linked Blog: Bitcoin Can Fun Terrorist Movements Worldwide"*, July 2014, Coin Desk. http://www.coindesk.com/isis-bitcoin-donations-fund-jihadist-movements/

reclutamiento y movilización ha sido más efectivo del de Al Qaeda gracias a una propaganda más efectiva entre los jóvenes yihadistas[11].

- **Trabajo de red (*networking*)**: los grupos terroristas han experimentado un cambio radical. Las organizaciones jerárquicas seculares han dado paso a una de tipo descentralizado y horizontal. Ahora miembros de diferentes grupos pueden relacionarse, apoyándose mutuamente en sus acciones. Planear y coordinar ataques es más fácil y más barato.
- **Compartir información**: manuales y guías están disponibles en la red. Los terroristas comparten análisis y experimentos sobre la producción casera de productos para llevar a cabo ataques terroristas, planear asesinatos o métodos de guerrilla.
- **Planificación y coordinación**: Internet es una herramienta útil para poder planear y coordinar ataques simultáneos en diferentes partes del globo. Las chat rooms en la Red oscura se utilizan para enviar instrucciones sobre cómo, cuándo y dónde realizar ataques terroristas. Por ejemplo, Al Qaeda ordeno el uso del software "Pal Talk" a todos aquellos que estuviesen interesados en unirse a los "jihad brothers", sin miedo a que fueran monitorizados por el enemigo[12].

En 2014, Europa ha experimentado un aumento drástico de la amenaza yihadista que llevo a los ataques terroristas de Charlie Hebdo, en Paris, a principio de 2015 y a los homicidios de Montrouge y Portes de Vincennes. El Estado Islámico encarna una nueva idea de expansionismo, llevada a cabo a través de ataques convencionales además de estar apoyado por un ejército regular con el intento de asumir el control de nuevos territorios. La tendencia creciente de ISIS se debe sobre todo a la ideología yihadista que junta las practicas militares a las principales técnicas de guerrilla, acciones suicidas apoyadas por una avanzada capacidad de ciberterrorismo. Las operaciones de policía en Europa han demostrado, hasta ahora, como el área de la UE es tierra fértil para la radicalización y el reclutamiento de células terroristas[13].

El Daesh en la red

En los últimos meses, el ciberterrorismo ha causado mucha alarma entre los expertos, convencidos de que un ataque terrorista a los gobiernos o al sistema privado, contra el

[11] *"ISIS and Al Qaeda use social media, Web platforms differently to achieve different ends"*, Homeland Security News Wire, 14/10/2014. Disponible en: http://www.homelandsecuritynewswire.com/dr20141014-isis-and-alqaeda-use-social-media-web-platforms-differently-to-achieve-different-ends

[12] WEIMANN Gabriel "www.terror.net How modern Terrorism uses the Internet", Special Report No. 116, United States Institute of Peace, 2004, pp 5-11.

[13] Presidenza del Consiglio dei Ministri, Sistema di informazione per la sicurezza della Repubblica *"Relazione sulla politica dell'informazione per la sicurezza"*, 2014.

ejército y las estructuras financieras podría conllevar daños permanentes a la economía y al sistema nacional de seguridad. Los grupos terroristas islámicos han demostrado, a lo largo de los años, la capacidad de combinar de forma eficiente tácticas de guerrilla, explotando tecnologías avanzadas para maximizar sus objetivos. Hasta ahora el debate público se ha centrado más en no crear falsas alarmas entre la población en vez de examinar el peligroso aumento de los medios terroristas en el ciberespacio.

La guerra contra el terrorismo ha sido siempre objeto de considerables críticas, por parte de académicos, filósofos y de algunos partidos políticos, debido a la falta claridad de los objetivos occidentales en la lucha contra el terrorismo y cuánto tiempo llevaría. El terrorismo islamista fundamentalista es una red global que lleva al cabo una guerra asimétrica para crear caos, infundir terror y una sensación de vulnerabilidad.

Los grupos de terroristas islámicos modernos empezaron a usar el entorno cibernético con finalidad de propaganda, reclutamiento y entrenamiento, obtención de fondos, comunicaciones y targeting. El acceso facilitado a internet, la transmisión rápida y el mantenimiento económico de la presencia en línea, representan incentivos para los extremistas que quieren llevar al cabo su agenda de acciones terroristas[14]. Según Jaquelyn S. Porth[15], en los últimos años, se ha asistido a un aumento drástico de sitios web terroristas usados sobre todo para la creación de discursos, gráficos, blogs accesibles a todos y donde poderse especializar en la creación de bombas, llevar a cabo ataques terroristas y otras atrocidades. Los líderes yihadistas usan el web para incitar a la violencia contra occidente y los infieles, apuntando directamente a las mentes de los individuos.

> *"Internet ha expandido drásticamente la capacidad de los grupos radicales de reclutar, entrenar, motivar, y coordinar terroristas en vastas distancias sin tener un contacto directo. Los terroristas pueden consultar páginas webs para aprender las técnicas sobre como derribar helicópteros, ver videos de decapitaciones de rehenes, leer las cartas escritas por los kamikazes o escuchar los mensajes de los líderes militantes. Y aunque no hubiesen páginas webs, Internet permite la divulgación de mensajes radicales así como instrucciones operacionales enviadas por email.[16]"*

Recientemente la comunidad internacional ha visto como los Muyahidín, guerrilleros radicalistas islámicos, han desarrollado la guerra online conocida como yihad electrónica, donde se incita a los musulmanes a participar en la guerra contra el occidente[17]. Hasta

[14] WEIMANN, op. cit.
[15] Jaquelyn S. Porth es File Security Affairs Writer para el US State Department.
[16] Maine Senator Susan Collins, U.S. Senate Committee on Homeland Security & Governmental Affairs, 2007.
[17] ALSHECH E. *"Cyberspace as a combat zone: the phenomenon of Electronic Jihad"*, The Jerusalem Post, February 2007.

ahora, la comunidad internacional no ha sufrido ningún ataque terrorista en el quinto dominio pero, el grupo terrorista de ISIS parece particularmente atraído por el potencial de la red en términos de causar daños, reclutar a nuevos militantes y difundir un mensaje psicológico entre la población global. Sin embargo, el hecho de que la mayoría de las infraestructuras occidentales dependan de la tecnología de internet, transforma los potenciales beneficios de la red en el talón de Aquiles de la sociedad moderna. Los recientes ataques contra eBay, el departamento sanitario del estado del Montana o Sony han demostrado lo fácil que es para hackers expertos obtener información sensible y causar pérdidas masivas en el mercado financiero.

Diferencias con los grupos terroristas seculares

Hasta el éxito del año pasado, la Comunidad Internacional ignoraba la verdadera naturaleza del ISIS, subestimando las capacidades de este grupo de llevar la guerra hasta nuestras casas. El pequeño grupo terrorista, ahora controla vastas áreas de Siria, de Iraq y cada vez se acerca más a las costas del mediterráneo. Su líder, Abu Bakr al Baghdadi, ha instaurado el Califato cuyo objetivo principal es destruir la sociedad occidental, las culturas, sus costumbres y religiones que están en contra de la Sharia.

El ISIS pertenece a la línea dura de la escuela Yihadi-Salafista, basada en una interpretación extremista de las escrituras Islámicas. La fundación de la escuela yihadi se genera con la influencia de: la Hermandad Musulmana en Egipto y Salafismo. La primera, un movimiento sunita, fue fundado en 1928 emergiendo como una forma de activismo islámico contra el nacimiento del imperialismo occidental[18]. La idea de un califato echa raíces en esta escuela de pensamiento, *"El Islam requiere que la comunidad musulmana se una alrededor de un líder o jefe, el jefe del Estado Islámico, y prohíba a la comunidad musulmana dividirse en diferentes países […].[19]"* En cuanto a la ideología Salafista, el grupo esta sobre todo interesado en la purificación de la fe y erradicar la idolatría[20]. Ambos Al-Qaeda y el IS están afiliados a esta última teología, aunque IS ejerce una interpretación más extrema del Yihadi-Salafismo que se puede atribuir a su ex líder Abu Musab al-Zarqawi, que fue asesinado en 2006.

A diferencia de los grupos terroristas seculares, que dependían sobre todo en las armas convencionales y en los atentados con bombas en contra de determinados objetivos, esta nueva organización fundamentalista demuestra una fuerte capacidad de adaptación a las

[18] BUNZEL Cole *"From Paper State to Caliphate: The ideology of the Islamic State"*, The Brookings Project on U.S. Relations with the Islamic World Ana lysis Paper N. 19, Marzo 2015, pag.7.
[19] BUNZEL, op. cit. pag. 8.
[20] BUNZEL, op. cit. pag. 8. Mas información sobre el Salafismo en: "On the Nature of Salafi Thought and Action", by Bernard Haykel in Global Salafism: Islam's New religious Movement, ed. Roel Meijer (2009).

tecnologías del siglo XXI. Las redes sociales, como Facebook, YouTube, Twitter o Instagram han jugado un papel muy importante en el proceso de reclutamiento de nuevos terroristas.

El uso de Internet por parte de los grupos terroristas no debería ser ninguna sorpresa para occidente. Al-Qaeda antes que el IS uso la red como medio de propaganda y conseguir apoyos a nivel mundial. En cambio, lo que sí debería aumentar es la intención de prevenir ataques cibernéticos nocivos en contra de infraestructuras sensibles. *"El IS ya ha logrado suceso en usar las tecnologías, usando la web para el reclutamiento, la distribución de informaciones y tácticas atemorizantes a los terroristas […] hemos empezado a captar las señales de que las organizaciones terroristas están intentando obtener acceso a armas cibernéticas*[21]*."*

Algunos expertos están convencidos que IS todavía no tiene los medios apropiados para lanzar un ataque cibernético masivo contra Europa y EEUU, sin embargo hay cierta discrepancia entre las acciones y las convicciones. Michael Rogers, Director de la Agencia de Seguridad Nacional, recalca el hecho de que puede haber una dimensión cibernética en cualquier escenario donde las fuerzas occidentales estén despegadas[22]. Los yihadistas en Oriente Medio están mejorando sus capacidades para lanzar ataques contra EEUU y sus aliados; es solo una cuestión de tiempo antes de que las redes eléctricas sean derribadas y las naciones de todo el mundo sean incapaces de responder a ataques en los otros dominios.

Otra diferencia con los grupos terroristas secularistas es que el IS es económicamente fuerte como resultado de la exportación ilegal de petróleo, cuya rentabilidad es alrededor de los dos/tres millones de dólares al día encontrando a un aliado valioso en el mercado negro de Oriente medio. Esto implica que un alto porcentaje de este beneficio será reinvertido en tecnologías de encriptación para poder desarrollar su propio software de comunicación y responder a los ataques perpetrados por las agencias de seguridad occidentales[23]. Sin ir más lejos, en poco tiempo, ISIS ha conseguido desarrollar sus aplicaciones para los teléfonos y diferentes sistemas de mensajería. De momento, el grupo no representa una verdadera amenaza cibernética usando los medios sociales simplemente para reclutar y divulgar su interpretación del Corán. Sin embargo, un ejército yihadista cibernético podría pronto llegar a ser realidad así como lo es un Califato Islámico en Oriente Medio.

[21] David de Walt, chief executive of tech security company FireEye. Interview on the Financial Times.
[22] HAVERLUCK M.F. *"Isis threatening, hacking into more than one U.S news sites?"*, febrero 2015. Disponible en: http://onenewsnow.com/media/2015/01/02/isis-threatening-hacking-into-more-than-us-news-sites
[23] DETTMER J. *"Digital Jihad: ISIS, Al Qaeda seek a cyber caliphate to launch attacks on US"*, septiembre 2014. Disponible en: http://www.foxnews.com/world/2014/09/14/digital-jihad-isis-al-qaeda-seek-cyber-caliphate-to-launch-attacks-on-us/

Según Abdel Bari Atwan, escritor y periodista palestino, sin la tecnología digital sería bastante improbable que IS llegase a existir, menos aún que sobreviviera y se expandiera. Según el autor la mayoría de quienes participan o se sienten atraídos el ISIS son adolescentes o en sus veintes; un 89% es activo online de los que un 70% usa a diario los medios sociales pasando un total de 19 a 20 horas semanales en Internet. Aunque suene paradójico, por un grupo cuyo interés principal es el de hacer retroceder el mundo al tiempo de los cuatro primeros califas (Righteous Caliphs), el conflicto entre las tecnologías avanzadas del siglo XXI y la interpretación Salafita-Yihadista del Islam ha llegado a su fin cuando los líderes de los respectivos grupos terroristas se dieron cuenta del verdadero potencial de la red.

El primero en proponer la explotación de los medios sociales ha sido Awar al-Awlaki para difundir más rápidamente materiales yihadistas y reclutar nuevos terroristas. La tarea más difícil para ISIS es ajustarse a los cambios repentinos de la tecnología y contraatacar la propaganda negativa del enemigo. El jefe del departamento mediático de ISIS es Ahmed Abousamra, un Siriano nacido en Francia y crecido en Massachusetts. Graduado en IT se trasladó en Aleppo en 2011. El responsable de la actividad cibernética del califato es Abu Hussain Al Britani, hacker británico de Birmingham. Al Britani fue encarcelado en 2012 con la acusación de haber pirateado el perfil de Gmail del consejero especial del Ex Primer Ministro británico T.Blair, robando y publicando online información sensible. Entre los objetivos yihadistas están: el Pentágono, la página web del Departamento de Estado Estadounidense y sitios webs israelís como respuesta al conflicto contra Hamas. John Carlin, subprocurador de la División de seguridad del Departamento de Justicia EEUU, advierte que *"[…] estamos en un momento pre-9/11 en ámbito cibernético. […] Está claro que los terroristas quieren utilizar medios cibernéticos para causar cuanta más destrucción posible a nuestras infraestructuras.*[24]*"*

La importancia de la guerra digital fue en su momento subrayada por Abu Hamza Al-Muhajir, otro líder de Al-Qaeda, que creía que las futuras guerras se combatirían en el dominio cibernético reclamando hackers con talento a unirse a la Guerra Santa contra Occidente[25]. Si el IS tiene un equipo cibernético, se podría describir como un ejército y no como un simple grupo yihadista[26].

En septiembre 2014, Craig Giuliano, un ex funcionario del antiterrorismo en el Departamento de Defensa, declaró que el ISIS no tenía ni los medios ni el personal adecuado para llevar al cabo ataques cibernéticos contra EEUU. Mientras Francia y Occidente estaban todavía psicológicamente conmocionados por los ataques terroristas de Charlie Hebdo,

[24] DETTMER, op. cit.
[25] BARI ATWAN Abdel *"Islamic State: The Digital Caliphate"*, London, Saqi Books, 2015, p ix-xiv.
[26] Entrevista con COLONNA Antonella *"La cyberwar contro l'ISIS"*, febrero 2015. Disponible en: http://confini.blog.rainews.it/2015/02/02/la-cyberwar-contro-lisis-intervista-a-antonella-colonna-villasi/

algunas células cibernéticas a las dependencias de ISIS consiguieron entrar en la cuenta de twitter del periódico di Albuquerque y en la página web de Malaysia Airways visualizando el siguiente mensaje: *"Error 404- airplane not found. ISIS will win."* A principios de año, el cibercalifato consiguió piratear la cuenta Twitter de uno de los operarios del CENTCOM cuando accedió desde su ordenador particular a la red social, consiguiendo, de esta manera, acceder únicamente a los datos ahí almacenados. El mensaje que ISIS dejo fue bastante claro:

"Soldados americanos, estamos llegando, tened cuidados. ISIS" siguió *"En nombre de Allah, el más compasivo, el misericordioso, el CiberCalifato bajo los auspicios de ISIS sigue adelante con la Yihad cibernética. Mientras los EEUU y sus aliados están matando a nuestros hermanos en Siria, Iraq y Afganistán nosotros acabamos de penetrar vuestras redes y dispositivos personales y lo sabemos todo sobre vosotros. No tendremos ninguna piedad con los infieles. EL IS ya está aquí, estamos en vuestros ordenadores, en cada base militar. Con el permiso de Allah estamos en CENTCOM. ¡No nos pararemos! Sabemos todo sobre vosotros, sobre vuestras mujeres y vuestros hijos. ¡Soldados americanos! ¡Os estamos mirando! Aquí tenéis algunos datos confidenciales: ……*

¡No hay Dios que no sea Allah y Muhammad es su Profeta! ¡No hay ley sino la Sharia![27]"

El Comando aseguró enseguida que IS no comprometió ninguna operación militar y tampoco pudo acceder a información confidencial. El accidente fue descrito como un caso de ciber-vandalismo y que hay una diferencia fundamental entre un robo masivo de datos sensibles y piratear una cuenta de twitter[28].

El occidente esta sobre todo debilitado por los distintos enfoques al respecto; a expertos, el ejército y los gobiernos les falta eficiencia, una respuesta viable y cohesiva contra el terrorismo. Todavía se desconoce mucho sobre el ISIS y sus capacidades, sobretodo en términos de poder cibernético. Están poco claro los medios y la extensión de las capacidades hacker de ISIS, lo que se sabe con certeza es que la batalla contra los militantes fundamentalistas ha llegado físicamente a territorio occidental y pronto incluirá la dimensión cibernética.

James Lewis, experto de ciberseguridad del Center for Strategic and Internatinal Studies, en Washington DC, observo como *"…el episodio no demuestra tanto las habilidades de los agresores cuanto la ausencia de una respuesta rápida por parte de la víctima[29]"*, que debería

[27] U.S Central Command, Twitter Account @CENTCOM.
[28] Josh Ernets, current White House spokesman, nominated o May 2014 to replace Jay Carney.
[29] FREDIANI Carola entrevista a LEWIS James para el periodico italiano "l'Espresso" *"Isis, Al-Qaeda e la sfida del cyber terrorismo"*, febrero 2015. Disponible en:

ser causa de mayor preocupación. Hasta ahora, explica Lewis, los terroristas se han interesado más en los efectos causados por la propaganda online que en destruir las infraestructuras. Sin embargo, las cosas podrían evolucionar rápidamente si occidente no es capaz de responder de una forma efectiva y flexible. Por su parte Isaac Porche, un analista de ciberseguridad en RAND Corporation en Washington DC, opina de forma diferente. Porche describió el accidente como nada más que *una molestia a las relaciones públicas.* Es en esta gama de decisiones, según los expertos, que IS se está volviendo más fuerte y más impredecible.

Un estudio del Center for Strategic and International Studies demuestra que la guerra cibernética cuenta con un mercado más productivo que el del tráfico internacional de drogas. Si los ataques cibernéticos realizados hasta ahora contra EEUU, China y Alemania han causado daños alrededor de los 200 millones de dólares en 2013, es impensable saber lo que podría pasar si la lógica de ISIS se aplica a este nuevo dominio.

El ataque cibernético a CentCom tuvo lugar unos días antes de que el Presidente Barack Obama realizase un discurso a la Federal Trade Commission en Washignton DC sobre el proceso de expansión de la ciberseguridad.

"[…] Como nos han recordado durante este último año, incluyendo el ataque a Sony, la extraordinaria interconexión crea numerosas oportunidades, aun así inmensas vulnerabilidades para nosotros como nación y para nuestra economía, y para las familias individualmente."

El objetivo principal del Presidente Obama es lo de reforzar los vínculos entre el sector privado y el público para una respuesta cibernética más precisa y efectiva, con el propósito de codificar mecanismos para que el sector privado y los gobiernos puedan compartir información cibernética, y aumentar considerablemente las capacidades del sector privado para responder a los accidentes de ciberseguridad[30]. El Presidente americano expresó su inquietud ya en octubre 2014 y decidió financiar una iniciativa de ciberseguridad con 14 millones de dólares para el 2015.

La percepción del terrorismo, así como lo ha interpretado la Comunidad Internacional en la última década, ha evolucionado a un ritmo muy rápido, sobre todo en los últimos dos años en los que el occidente tuvo dificultades para responder. La capacidad cibernética de ISIS no debería extrañar a las sociedades occidentales, aunque no se les puede todavía considerar

http://espresso.repubblica.it/plus/articoli/2015/02/02/news/isis-al-qaeda-e-la-sfida-del-terrorismo-informatico-1.197769

[30] VOLZ Dustin *"Obama Cybersecurity Info Sharing Proposal"*. Disponible en: http://www.scribd.com/doc/252540856/Obama-Cybersecurity-Info-Sharing-Proposal

un grupo con capacidades tecnológicas catastróficas. La respuesta más efectiva después de los atentados a Charlie Hebdo ha sido por parte del grupo activista Anonymous. Desde su declaración de guerra, Anonymous ha eliminado numerosas cuentas de Twitter, YouTube y Facebook. Por su parte, Rai News- el primer canal de noticias en Italia- ha decidido no transmitir más los videos de ISIS con la intención principal de no promocionar las atrocidades y los mensajes que la organización quiere que veamos. La amenaza del ciberterrorismo se ha vuelto más realista que hace diez años, por lo tanto debería establecerse una colaboración más activa entre el sector privado y el público, las naciones y los gobiernos entre las organizaciones internacionales y regionales.

CONCLUSIÓN

La guerra contra el IS es una guerra total, que no se combate solo en el campo de batalla o a través de los servicios de espionaje sino en la arena digital también. Los próximos años verán como desafío principal el terrorismo yihadista y su intensificación a nivel regional y mundial. En términos de terrorismo doméstico, el Occidente será amenazado por el *homegrown terrorism*, como resultado de un proceso de radicalización dentro de la sociedad occidental inspirado principalmente por nuevos líderes carismáticos que se reconocen en las creencias del IS. El Daesh está invistiendo una gran cantidad de tiempo y de finanzas para sus medios de información y propaganda. Sorprenderse sobre el uso de la tecnología o fracasar en reconocer sus capacidades, demuestra una visión distorsionada de la superioridad de la sociedad occidental respecto a sus enemigos[31].

Si esta dimensión total de la guerra era impensable para cualquier grupo terrorista antes del 2014, ISIS ha demostrado hasta ahora su capacidad de aprovechar lo más posible este quinto dominio de conflictividad.

*Agnese Carlini**
Investigadora - Doctora en RRII

[31] LOMBARDI Marco *"IS 2.0 e molto altro: il progetto di comunicazione del califfato."* Parte del reportaje *"Twitter e Jihad. La comunicazione dell'Isis"*.