

ISSN: 2539-0015 (en línea)

TRIARIUS

Volumen 2 - Nº 35



15 de agosto de 2018



Arabia Saudí



2539-0015

Boletín de Prevención y Seguridad ante el
Terrorismo y las Nuevas Amenazas



ISSN: **2539-0015** (en línea)

Medellín - Colombia

Volumen **2** - Número **35**

15 de agosto de **2018**

Editor

Douglas Hernández

Analistas Triarius

Ulises León Kandiko, Aldo Baggio,
Haylyn Hernández, Francisco
Javier Blasco, Douglas Hernández,
Montserrat López.

Este boletín es una publicación del **Observatorio Internacional sobre el Terrorismo y las Nuevas Amenazas**. Se produce de manera quincenal, en formato pdf, y su distribución es gratuita.

Información de Contacto:

Douglas Hernández

Medellín, Colombia

Móvil: (+57) 321-6435103

director@fuerzasmilitares.org

hernandez.douglas@hotmail.com



Editorial

En esta oportunidad, el experto argentino en ciberseguridad Ulises León Kandiko, nos presenta valiosos elementos que nos inducen a prepararnos para luchar contra el ciberterrorismo. En su artículo hace una introducción al problema, con ejemplos históricos, y muestra distintas vulnerabilidades del mundo moderno -que tienden a incrementarse- y que podrían ser explotadas por ciberterroristas, e incluso por gobiernos interesados en causar graves daños a la infraestructura de un adversario. Prestemos atención.

Nuestro amigo italiano, Aldo Baggio, nos trae un breve pero preocupante análisis sobre la mafia nigeriana, que no solo opera en África, sino que también ha llevado sus tentáculos a Europa, concretamente a Italia. Este tipo de organizaciones criminales, con comprobados nexos con grupos terroristas, parecen proliferar por el mundo, haciendo necesario que quienes trabajamos en procura de un mundo seguro y en paz, nos esforcemos más cada día, y muy especialmente, cooperemos con nuestros pares de otros países.

Haylyn Hernández, desde Colombia, nos introduce en los más recientes hechos políticos ocurridos en ese país, en particular en cuanto a la contienda electoral por la presidencia de la república, donde el electorado fue puesto a escoger entre la izquierda y la derecha, cada una con propuestas de fondo que van a marcar el futuro inmediato del país, y en donde las mayorías se inclinaron por la derecha. ¿Qué pasará con el proceso de paz, o con el tema de la producción y tráfico de drogas ilícitas?

El Coronel Blasco desde España, nos ofrece una interesante introducción a la OTAN y a su historia, al mismo tiempo que relaciona aspectos geopolíticos contemporáneos, cruzados con los intereses y acciones del gobierno de Donald Trump y su política de "América Primero". Todo ello con el fin de hacer prospectiva en relación con el futuro de la alianza, y en particular para valorar el papel que allí tendrá (o no tendrá más) España. Como siempre, una lectura interesante.

A paso seguido, y en el marco de la seguridad de la información, se presenta un ejercicio académico producto del Master en Seguridad de la Información del Security College US. Este material nos dará algunas ideas sobre este ámbito operativo, que cada vez es más importante frente a un creciente número de amenazas, y que además representa oportunidades laborales para quienes se interesen por estos temas.

Finalizamos esta entrega, con un interesante análisis de la señora Montserrat López, quien desde España nos ilustra sobre el uso de los medios de comunicación -y en particular las redes sociales- por parte de los grupos terroristas para reclutar, adoctrinar y radicalizar a nuevos seguidores y así adelantar su Yihad.

Esperamos que estos contenidos, diversos y atractivos, sean de interés y utilidad para nuestros lectores.

¡Conocer para vencer!

Douglas Hernández

Editor



Este boletín tiene versión en inglés.

Triarius 35, Contenido:

Cómo combatir el Ciberterrorismo, p.4
Por Ulises León Kandiko (Argentina)

Nigerian Mafia, p.10
Por Aldo Baggio (Italia)

Reconfiguración política de Colombia ¿realidad o utopía?, p.12
Por Haylyn Andrea Hernández Fernández (Colombia)

España y la OTAN, p.15
Francisco Javier Blasco, Coronel (r) ET (España)

Seguridad de la Información. Clasificación de Activos, p.22
Por Douglas Hernández (Colombia)

Autoadocctrinamiento: Yihad Mediática, p.32
Por Montserrat López Melero (España)



Fuerzas
Antiterroristas del Mundo

TRIARIUS

Vaya un saludo muy especial para las mujeres que trabajan en seguridad, defensa, inteligencia y contraterrorismo. En particular para aquellas que son asiduas lectoras de nuestra revista. Queremos contarles que el <http://www.securitycollege.us/> tiene este año ofertas especiales para mujeres en sus distintos cursos de capacitación. Ellos tienen la idea de cualificar a las mujeres y ayudarlas a elevar sus competencias, para así minimizar las diferencias de género que en ocasiones se presentan en lo laboral. Revisa su portafolio.

En portada, miembros de la **Special Security Force de Arabia Saudita**. Unidad con amplia experiencia en la lucha contra el grupo terrorista al-Qaeda. Ver al final de la revista.

TRIARIUS privilegia la libertad de expresión, sin embargo, la responsabilidad por lo dicho en los artículos, es exclusiva de sus autores.

Agradecimiento muy especial a los analistas internacionales que de manera gratuita nos han enviado sus artículos para este número.



SHIELD AFRICA
A b i d j a n 2019

Cómo combatir el Ciberterrorismo

Por Ulises León Kandiko (Argentina)



Por el incremento de la dependencia tecnológica, cada vez somos más vulnerables.

La primera vez que expuse sobre el tema fue en el año 2003, y pasaron 5 años hasta que me animé a escribir sobre el Ciberterrorismo, hoy a poco más de 15 años de estar tratando con el tema, veo que pese al desarrollo y evolución que el mismo ha tomado es poco lo que desde las áreas legislativas se trabaja, particularmente en los países de la región. Esto dado a que tienen la falsa premisa de que el Ciberterrorismo es solo Islamista y que sus únicos enemigos son Estados Unidos de Norteamérica y Europa.

Sin perjuicio de ello, y como siempre digo, uno tiene la obligación de “evangelizar”, y en este sentido es que retomo al tema. Como si se tratase de cualquier otra amenaza que atenta contra la Seguridad Pública o lo que algunos entienden como la Seguridad Nacional (sacándose de encima todo tapujo ideológico), vamos a tratar de ver cómo se puede combatir al Ciberterrorismo.

En primer lugar, hay que tomarlo como una amenaza a la Seguridad, por la particularidad del tipo de amenaza, primero trataremos de respondernos estos interrogantes:

1. ¿Qué prevemos que los terroristas quieran hacer en el ciberespacio?

2. ¿Cómo podemos prevenir estas acciones?
3. ¿Cómo podemos ser proactivos contra estas acciones?

Al primer interrogante ya lo he tratado en varios de mis artículos anteriores y ponencias, pero para hacerlo breve, esto se refiere a:

- El ciberataque en sí.
- Planificación y Coordinación de ciberataques.
- Propaganda y Reclutamiento.

En cuanto al segundo interrogante, nos lleva inexorablemente a tratar de conocer cuáles son esas acciones, conocer al enemigo y sus técnicas y tácticas para poder prevenir. En ese sentido veamos algunos casos desde los inicios:

Los Tigres de Tamil

El primer acto caracterizado de ciberterroristas, identificado por las autoridades de inteligencia, fue llevado adelante por los Tigres de Tamil, terroristas guerrilleros en Sri Lanka en 1998. Las embajadas de Sri Lanka recibieron 800 correos electrónicos por día durante más de dos semanas con un mensaje que decía "Somos los Tigres Negros de Internet y

estamos haciendo esto para interrumpir tus comunicaciones".

Aum Shinrokiyo

En 2000, una investigación descubrió que el gobierno japonés había estado usando software desarrollado por una compañía asociada con Aum Shinrokiyo (Akhgar, Staniforth, & Bosco, 2014). Se informó que Aum había recopilado datos confidenciales sobre armas nucleares, a lo que previamente habían discutido las compras con Rusia en 1993 (RAND Corporation, 2005).

Prueba del generador Aurora

En 2007, un ataque cibernético experimental titulado "Prueba del generador Aurora". Los investigadores descubrieron que al alterar remotamente el software de un generador de energía podían provocar que las turbinas prendieran fuego y, por lo tanto, eventualmente causen daños graves al generador. Este es un ejemplo de una amenaza relevante de los ciberterroristas en los Sistemas de Control Industrial (ICS). En un informe sobre la infraestructura de estos sistemas de control y su amenaza potencial por terroristas, Dana Shea (2003) cita: "Las tecnologías de sistemas de control industrial a menudo se emplean en industrias de infraestructura crítica para permitir que un único centro de control administre múltiples sitios. Los sistemas de control industrial se implementaron originalmente como redes aisladas y separadas. Fueron vistos como sistemas seguros que protegían ubicaciones remotas de ser físicamente violadas y maltratadas. Por ejemplo, se creía que el establecimiento de sistemas de control remoto en presas protegía contra la liberación ilegal del agua represada, ya que no se podía acceder a válvulas ni interruptores accionables manualmente".

Al-Shahab

En 2011, el medio de comunicación de Al-Qaeda, Al-Shahab, publicó un informe en el que pedía que los "Ciber Jihadistas" atacaran a compañías y gobiernos que se oponen a sus creencias. El columnista del medio decía: "Aconsejamos a los expertos en este campo que se dirijan a los sitios web y las redes de las grandes empresas y los gobiernos de los países que atacan a los musulmanes. Deben enfocarse en sitios web de redes administradas por centros de medios que luchan contra el Islam, la Jihad y los muyahidines ". Además, el informe del medio detallaba la negación distribuida de los ataques al Servicio realizados por el pirata informático Michael Calce en febrero de 2000 y cómo funcionan los ataques DDoS.

En 2012, un informe publicado por el Comité del Senado de USA sobre Seguridad Nacional y Asuntos Gubernamentales detalló un video del grupo terrorista Al-Qaeda, en el que se pedía ataques cibernéticos contra la infraestructura crítica de USA, incluida la red eléctrica y el suministro de agua (Clohery, 2012). Se supone que estos ataques cibernéticos están destinados a explotar vulnerabilidades en ICS, similares a las descubiertas en la "Prueba del Generador Aurora". Al comentar sobre el video de Al Qaeda, el senador estadounidense Joseph Lieberman afirmó que "el Congreso debe actuar ahora para proteger al público estadounidense de un posible ataque devastador a nuestra red eléctrica, sistema de suministro de agua o redes financieras" (Freeman, 2014). Aunque esta no es la única amenaza potencial que vemos del terrorismo cibernético, es evidente que los ataques potenciales como este representan una gran amenaza para la sociedad.

Nightmare

En 2012, un grupo de hackers pro-palestinos titulado "Nightmare" implementó un ataque de Denegación de Servicio Distribuido en los sitios web de la Bolsa de Tel Aviv, Tel Al Airlines y First International Bank of Israel.

Terrorismo telefónico

Entre el 11 y el 14 de septiembre de 2017 cientos de amenazas de bomba falsas realizadas por personas que llamaron anónimamente se hicieron contra los principales edificios públicos de toda Rusia. Los perpetradores realizaron llamadas falsas en más de 30 ciudades, lo que llevó a la evacuación de escuelas, hoteles, hospitales, aeropuertos, estaciones de tren, universidades y centros comerciales. El Kremlin llamó a las amenazas 'terrorismo telefónico'. Hasta la fecha, no se han encontrado dispositivos explosivos, lo que deja en claro que el motivo era propagar el miedo y la interrupción.

Fake News

A fines de 2017, un ejemplo cercano de la variante de Ciberterrorismo patrocinado por un Estado, esta es la situación hostil entre Qatar y sus vecinos. No es simplemente un caso de realismo hiper ofensivo o diplomacia de poder, sino que los lados opuestos se están atacando mutuamente a través de la red. Un ejemplo reciente de esto es el pirateo de los sitios / ministerios de medios del gobierno de Qatar para difundir noticias falsas e intentos de derribar sitios

web rivales. Es una nueva forma de guerra de información motivada políticamente.

Obviamente lo visto no es excluyente, hay multiplicidad de ataques y herramientas, por ejemplo:

- Phishing.
- Watering Hole.
- Ransomware.
- Escaneo.
- Spear-Phishing.
- Denegación de servicio distribuida.
- Ataque a cadena de suministro.
- Explotación de Día Cero, etc.

¡¡SEGUNDOS FUERA!!

(expresión pugilística que usa el árbitro)

Debemos ser razonables al asumir que las amenazas potenciales discutidas hasta ahora en este artículo pueden ser implementadas en cualquier momento, sin previo aviso. La mayor parte de nuestra infraestructura digital ya cuenta con una gran cantidad de defensa. Tales tecnologías actuales incluyen: firewalls, sistemas de protección con contraseña, cifrado de clave (por ejemplo, 3DES, RSA), estenografía, sistemas de detección de intrusos, Secure Socket Layer (SSL), IPsec, listas de control de acceso, etc. Cuando se discuten actos de terrorismo en general, la responsabilidad de la prevención normalmente recae en los gobiernos y las organizaciones nacionales.

En los últimos años, las vulnerabilidades en los softwares y las nuevas tecnologías han demostrado que la seguridad no suele estar a la vanguardia de la prioridad durante su desarrollo. Un claro ejemplo de ello lo verán en el artículo que publiqué antes: *Avatares de una Flota del Siglo XXI: Proteger la flota de ciberataques*.

También, varios expertos han referido que es un mito patrocinado por el gobierno que el cifrado es la única barrera para combatir con éxito el terrorismo en línea. El empleo o realización de tests de penetración, comprobación de códigos de las plataformas existentes y por supuesto el empleo de Equipos Rojos es vital para prevenir, pero y ¿cómo lo combatimos además? Es la sumatoria de múltiples herramientas, algunas tecnológicas y otras humanas, que a través de Inteligencia y Ciberantiterrorismo lograremos combatir y obtener resultados positivos, algunas de ellas son:

Uso de OSINT

El uso masivo de la internet inexorablemente sirve para la recopilación de información e inteligencia en

preparación para actividades delictivas, terroristas o de otro tipo, de igual forma sirve para quienes combaten esas actividades. La cultura actual de intercambio de información, en particular por aquellos que no son bastante de mediana edad, proporciona una gran cantidad de datos que pueden ser aprovechados por delincuentes, terroristas y por supuesto por quienes combaten a ambos.

Francamente, todo lo relacionado con la vida de algunas personas ahora se publica para que todos lo vean. De hecho, se podría decir que es más difícil encontrar a alguien que no tenga un perfil en lugar de uno que sí. La inteligencia basada en fuentes abiertas se ha convertido ahora en un arte especializado (o ciencia), ayudado principalmente por la estupidez de muchas personas.

El sitio web "Please Rob Me" extrajo el perfil y la información de ubicación de usuarios y generó una alerta cuando esos usuarios no estaban en casa, principalmente porque "tuitearon" que estaban en otro lugar. Este nivel de recopilación de inteligencia de código abierto ha sido ampliado por otros en un servicio de mapas para que cuando los usuarios envíen un Tweet y su GPS registre su posición, estos datos se envíen a un sitio de asignación y su ubicación se muestre para que todos los vean.

La gran cantidad de webcams disponibles en Internet permite realizar un reconocimiento de objetivos desde la comodidad de la oficina. Es cierto que muchas "cámaras de tráfico" oficiales han acumulado retrasos de unos minutos, sin duda para reducir su utilidad en tiempo real para los delincuentes y permitir a las autoridades cortar la alimentación si es necesario, pero hay una gran cantidad de otras webcams disponibles para ver. Muchos de ellos se difunden vía web intencionalmente con fines de marketing en hoteles, restaurantes y zonas turísticas, pero otros son cámaras de seguridad locales que no han sido protegidas y pueden ser utilizadas por cualquier persona.

Uso de BA

El "Business Analytics" tiene muchas aplicaciones comerciales, especialmente en el campo de la investigación de mercado y la capacidad de respuesta del cliente a nuevos productos y servicios. Pero créanlo o no, también tiene aplicaciones en el mundo de la ciberseguridad.

Esta es la ciencia de analizar conjuntos de datos de seguridad extremadamente grandes en tiempo real, lo que permite la revelación muy rápida y extremadamente precisa de las tendencias ocultas que residen en ellos. Con la capacidad ahora de llevar a cabo este tipo de investigaciones muy sofisticadas,

se puede predecir futuras amenazas basadas en estas variables:

- El momento de un ataque basado en el Ciberespacio.
- Las secuencias específicas de tales instancias y ocurrencias.
- Cualquier diferencia discernible que se haya obtenido de los conjuntos de datos de seguridad.
- Trazar las tendencias de riesgo y el comportamiento del ciberataque en tiempo real.

Plataformas como la de "Security Analytics" pueden ser empeladas para encontrar incluso la causa raíz de cualquier tipo o clase de violación de seguridad que pueda ocurrir. Además, se pueden crear modelos predictivos para construir los perfiles de futuros vectores de ciberataque y compararlos con los valores de referencia del comportamiento normal a fin de establecer el nivel de riesgo apropiado.

Un método que se utiliza actualmente es el de Machine Learning. Este es un proceso en el que la construcción de modelos predictivos es totalmente automática, y se utilizan algoritmos matemáticos especializados para analizar literalmente todos los conjuntos de datos de seguridad con el fin de "aprender" iterativamente de ellos. Desde aquí, se puede descubrir cualquier idea oculta, ya que estos algoritmos no se han programado para mirar un período de tiempo específico, sino que se ven en el marco de tiempo completo.

Sun Tzu y la Ciberinteligencia

Parafraseando al reconocido maestro del Arte de la Guerra, quien decía "si conoces al enemigo y te conoces a ti mismo, no debes tener miedo del resultado de 100 batallas", en este sentido y con ello en mente sumando algunas operaciones de Ciberinteligencia y claro está algo de lo que ya vimos y con un buen análisis podremos conocer a nuestro enemigo. Para ello nada mejor que utilizar las propias plataformas de los Ciberterroristas, investigando o haciendo operaciones de ciberinteligencia por ejemplo sobre los sitios web terroristas, los que pueden revelar las condiciones subyacentes de conflictos específicos, incluyendo los factores que conducen para atacar a adversarios particulares, hasta inclusive determinar el uso de armas particulares para determinados objetivos. Este estudio de marco conceptual, desarrollado por Marc Sageman, se basa en seis pasos secuenciales:

El primero se basa en la necesidad de identificar a la insurgencia terrorista en su manifestación física. Esto implica un amplio espectro de actividades en las tácticas que se aplican, ya sea por ejemplo uso de

armas portátiles de bajo impacto, uso de dispositivos explosivos de medio o alto impacto o el empleo de dispositivos químicos bacteriológicos y/o nucleares.

El primero se basa en la necesidad de identificar a la insurgencia terrorista en su manifestación física. Esto implica un amplio espectro de actividades en las tácticas que se aplican, ya sea por ejemplo uso de armas portátiles de bajo impacto, uso de dispositivos explosivos de medio o alto impacto o el empleo de dispositivos químicos bacteriológicos y/o nucleares.

En segundo lugar, es necesario identificar las conductas ideológicas de los grupos insurgentes, especialmente aquellas que son radicales que van acompañadas de un alto contenido cultural, étnico y/o religioso.

En tercer lugar, es crucial examinar las condiciones Pre-estructurales que son la base de una insurgencia y/o actividad terrorista; es decir centrarse en las condiciones sociales, los accesos a los servicios básicos, a los derechos igualitarios, a las protecciones civiles, a la libertad y a la calidad de vida en general. Según esta teoría la injusticia social, el descontento popular, la enajenación en general y el sentido de la crisis social son ingredientes dominantes para una erupción del terrorismo en esta sociedad.

En el cuarto paso es importante estudiar la aparición de los tipos de líderes que se movilizan en estas subculturas de los individuos que son susceptibles o influenciados por este tipo de conductores. Los rasgos más característicos y necesarios para un liderazgo eficaz son la de aquellos con personalidades carismáticas que pueden transformar los agravios y frustraciones en una agenda política para la acción violenta, para la radicalización de sus partidarios, para reclutar y movilizar a personas que hasta sacrificarían sus vidas para la causa; asimismo tienen la habilidad para atraer a otros sub-grupos que lo ayuden a cumplir con sus objetivos e imponer una disciplina terminante sobre el resto del grupo.

Las relaciones entre los grupos terroristas, sus simpatizantes y el apoyo que reciben de la comunidad pueden verse como una estructura piramidal, donde el grupo terrorista se encuentra ubicado en el ápice de la pirámide y los simpatizantes junto con el apoyo comunitario serían la base de la misma.

El quinto paso está relacionado con los factores externos que influyen en la decisión de llevar adelante un ataque terrorista, generalmente de carácter precipitado. Vale decir, esto surge como una reacción a un acto realizado por un actor externo y no deseado, como puede ser el caso de las reuniones mantenidas por el presidente de EE.UU. junto con su par Israelí

en Camp David, usando esta negociación como pretexto para incrementar los ataques Palestinos en territorio Israelí; otro ejemplo ha sido el de la publicación de dibujos animados controversiales que satirizaban la conducta del Islamismo.

Los insurgentes como los terroristas persisten o perduran en un cierto plazo. El sexto paso, es por lo tanto crucial examinar los factores que sostienen tales brotes en un cierto plazo. Estos factores incluyen las causas originales sin resolver que continúan conduciendo las acciones primarias de los grupos terroristas, tales como los ciclos de venganza, la necesidad de un grupo de proporcionar una razón de ser, la aparición de actividades criminales provechosas y finalmente una sensación de no poseer ninguna opción cierta más que continuar con su lucha armada porque ofrece la única alternativa al encarcelamiento o la muerte por las autoridades.

Es gracias al estudio realizado por Marc Sageman que se cuenta con una metodología para que los analistas antiterroristas, a través de la penetración en sus sitios web, puedan desmembrar los factores subyacentes que conducen a las acciones terroristas y/o insurgentes.

PR0B4BL3 3V0LUC10N D3L C1B3RR3RR0R1SM0

Lamentablemente hay que tener presente que la seguridad fue una idea de último momento en la creación de las computadoras, por lo que tanto los gobiernos como la esfera privada solo recientemente reconocen el daño potencial inherente a Internet. Es dable esperar que la delincuencia y el Crimen Organizado como así todas las redes asociadas continúen explotando los rincones ocultos de Internet, como Darknet, o Internet normal para llegar a las víctimas.

Al mismo tiempo, es probable que haya un crecimiento significativo en las amenazas planteadas por el Ciberterrorismo, particularmente dado que las empresas y los gobiernos aún deben proporcionar un marco integral para mitigar los ataques. Al mismo tiempo, los legisladores deberán asumir su rol y tratar de introducir leyes que prohíban los actos terroristas en línea y obligar a las empresas a cumplir con ciertos protocolos de seguridad.

Lugares donde convergen nuestros mundos físicos y virtuales serán posibles zonas de ataque cibernético. Como tal, Internet of Things está proporcionando los vectores de ataque perfectos para los ciberterroristas, donde la infraestructura civil y gubernamental está cada vez más informatizada. Estos incluyen desde dispositivos inteligentes, como las luces y hornos hogareños, hasta objetivos a gran escala, es decir,

infraestructura energética, sistemas de control del tráfico aéreo y bases de datos gubernamentales. Estos pueden no solo servir para difundir el miedo y la destrucción, sino que pueden resultar en la adquisición de información altamente secreta.

Al pensar en el concepto futuro de una ciudad inteligente (integración de las TIC's e IoT para gestionar los activos de una ciudad), si sufriera un ciberataque masivo, el daño sería de una magnitud nunca antes visto, aunque ya hubo incipientes casos como el de Atlanta (ver Smart Cities bajo ciberataque). Como así también puede suceder con Fuerzas Armadas y claro esta los ciberterroristas son conscientes de ello,

El terrorismo cibernético dirigido por un estado nacional será una gran amenaza para 2020, y toda organización debería prepararse.

Esa es la palabra del informe *Threat Horizon 2020 del Information Security Forum (ISF)*, que postula que grupos terroristas, organizaciones criminales, hacktivistas y hackers trabajan en diversas colaboraciones y configuraciones para convertir cada vez más el dominio cibernético, lanzando ataques contra infraestructuras críticas nacionales. que causa destrucción generalizada y caos. Además, sus actividades no tomarán en cuenta las barreras terrestres o la legislación.

"En los próximos dos años, los líderes empresariales enfrentarán decisiones regulares y complejas sobre la protección de su información y sistemas críticos. Las soluciones existentes que se han utilizado durante años serán expuestas como inadecuadas ", dijo Steve Durbin, director general de ISF. "Solo las organizaciones que entienden este entorno complejo y que cambian rápidamente se mantendrán firmes e inquebrantables. Aquellos que no están preparados y son incapaces de responder rápidamente se desmoronarán mientras se defienden de una avalancha de ataques cibernéticos poderosos día a día ".

Mas allá de la predicción del fin del mundo, el informe también predice que la tecnología superará a los controles. Las capacidades que parecían imposibles hace poco tiempo se desarrollarán extremadamente rápido, ayudando a quienes las ven venir y obstaculizando a quienes no lo hacen. Los desarrollos en tecnología inteligente crearán nuevas posibilidades para organizaciones de todo tipo, pero también crearán oportunidades para atacantes y adversarios al reducir la efectividad de los controles existentes. La información previamente bien protegida se volverá vulnerable.

Además, según la ISF, la presión sesgará el juicio. Los controles y métodos existentes para gestionar el

riesgo de la información se verán sometidos a una gran tensión por una avalancha de nuevas tecnologías, regulaciones y presiones sobre los empleados. Las organizaciones que tienen un buen historial de obtención de información estarán en riesgo de complacencia, ya que consideran que la forma en que siempre han hecho las cosas continuará funcionando en el futuro, una actitud peligrosa que tomar.

"En los próximos años, los cimientos del mundo digital de hoy temblarán violentamente", dijo Durbin. Los atacantes innovadores y decididos, junto con los cambios sísmicos en la forma en que las organizaciones llevan a cabo sus operaciones, se combinarán para amenazar incluso a los establecimientos más fuertes. Solo aquellos con preparaciones robustas se mantendrán altos".

C3RR4ND0 1D34S

Es notable que una gran parte de nuestro ciberespacio se construye sin tener en cuenta la seguridad y las organizaciones pueden no ser plenamente conscientes de los riesgos de las tecnologías que están utilizando. Por lo tanto, un método valioso para desarrollar la prevención contra las amenazas Ciberterroristas, antes que puedan materializarse, es trabajar fuertemente en Ciberinteligencia, Inteligencia, Operaciones de Ciberinteligencia y Cibercontrainteligencia.

A menudo los terroristas no tienen legislación a seguir, a lo sumo algunas buenas prácticas para causar mayor daño e impacto, y no están preocupados por las consecuencias de la identificación antes o durante un ataque. Concluir que

es de vital importancia para el reconocimiento preliminar, la defensa y la acción para identificar a los atacantes se realiza en la naturaleza más rápida. La detección de intrusiones es una de las áreas más activas de investigación dentro del Ciberterrorismo en los últimos 20 años (SANS Institute, 2003). Crear barreras seguras, tanto dentro de nuestros sistemas como físicamente, es necesario para identificar los ataques que ocurren con el fin de implementar el método correcto de mitigación. Muchas de estas técnicas, como se discutió anteriormente, incluyen los gustos del cifrado. El empleo de contraseñas, podría ser visto como uno de los métodos más antiguos de detección de intrusos. A medida que estos métodos se utilizan más ampliamente, las vulnerabilidades se vuelven más comunes.

Si bien es cierto que una gran parte de la capacidad cibernética global recae en actores Estatales, eso podría significar buenas noticias, malas noticias o ambas para aquellos que buscan prevenir el surgimiento de un ciberterrorismo verdaderamente destructivo. El casi monopolio de los Estados en las capacidades cibernéticas podría ayudar a comprar suficiente tiempo y espacio para prevenir ataques ciberterroristas exitosos mientras se lleva a cabo una estrategia integral para reducir las causas subyacentes regionales y locales del terrorismo. Alternativa o concurrentemente, como refería la Evaluación de Amenazas de la Comunidad de Inteligencia de USA, los Estados que ya disfrutaban de cierto éxito en la búsqueda de actividades cibernéticas inescrupulosas podrían ver el patrocinio de ciberterroristas como una forma conveniente de avanzar en sus propias agendas.

Fuente de la Imagen: <http://www.latejedora.es/wp-content/uploads/2015/12/ciberterrorismo.jpg>

Ulises León Kandiko

(Argentina) Licenciado en Seguridad, egresado del Instituto Universitario de la Policía Federal Argentina. Docente del IUPFA en la carrera de Ciencias de la Seguridad, analista, Director de Planificación Aérea del Ministerio de Seguridad de la Provincia de Buenos Aires. Especialista en cyberterrorismo e inteligencia criminal.



AIG
American Intelligence Group

Mafia Nigeriana

Por Aldo Baggio (Italia)



Algunas armas incautadas a elementos de la mafia nigeriana (Black Axe) en Italia.

La mafia nigeriana también conocida como "Langdan", nombre de la ciudad homónima del estado africano, se desarrolló alrededor de los años ochenta cuando, tras la crisis del petróleo, como resultado de la guerra declarada por Egipto y Siria a Israel, la OPEP decide aumentar el precio de barril e imponer el embargo sobre el petróleo crudo a los países pro-israelíes, parte de la clase dominante de Nigeria para no perder sus privilegios pidió el apoyo de algunos criminales, que podían proliferar sin perturbaciones, asumiendo cada vez más una connotación transnacional.

La estructura de la asociación delictiva es horizontal y, según el DNA (Dirección Nacional Antimafia), consiste en bandas agresivas, los cultos, que están flanqueados por grupos más organizados y sólidos que son verdaderas empresas delictivas que se benefician del tráfico de seres humanos, la explotación de la prostitución y el tráfico de drogas y, sobre todo, las estafas por medio de la web.

También es perturbador el descubrimiento en Castelvolturno, en el Casertano, un bastión de la mafia nigeriana en Italia, de un arsenal de armas destinadas a la organización terrorista islámica Boko Haram que domina en el norte de Nigeria, que con una astuta estratagema se desmonta y transfiere con el acompañamiento de burbujas en el que los productos se clasifican como carpintería metálica, y escapan a cualquier control, incluso por el hecho de

que no existe una referencia legislativa específica en la materia, especialmente a nivel internacional según el último tratado ATT (Tratado de Comercio de Armas), el problema es que no hay una definición técnica para tales armas.

Confirmando la naturaleza peligrosa de la asociación criminal, hay diversa información, en particular cito la de la Embajada de Nigeria en Roma en 2011 y la DIA 2016:

«Me gustaría llamar su atención sobre la nueva actividad criminal de un grupo de nigerianos pertenecientes a sectas secretas, prohibidas por el gobierno debido a actos violentos de vandalismo: desafortunadamente los antiguos miembros de estas sectas que lograron entrar en Italia, de nuevo fundaron la organización aquí, principalmente con fines delictivos "»

«Entre las estructuras criminales de origen africano, la más generalizada parece ser la nigeriana, formada por varias células criminales independientes y con estructuras operativas diferenciadas pero interconectadas, ubicadas en Italia y en otros países europeos y extraeuropeos. Las recientes investigaciones llevadas a cabo por la policía ponen de relieve cómo los consorcios en cuestión han tomado la forma de verdaderas asociaciones delictivas, utilizando el modus operandi típico de las mafias autóctonas, incluida la fuerte propensión a operar en empresas transnacionales ".

Fuente de la Imagen: <https://najuju.files.wordpress.com/2015/11/mafia-nigeriana-675.jpg?w=300&h=122>

Aldo Baggio. (Italia) Guardia de seguridad en COOPSERVICE, Bologna.



LISA Institute

Security Education

Paseo de la Castellana, 91, 4ª Planta (Madrid, España)



REINVENTANDO LA FORMACIÓN EN
SEGURIDAD e INTELIGENCIA

Fórmate Online con Expertos.
Cuando quieras. Donde quieras.

CURSOS CON INSCRIPCIONES ABIERTAS

INTELIGENCIA

- Curso de Experto en Análisis de Inteligencia
- Curso de Analista de Inteligencia
- Curso de Redacción de Informes de Inteligencia
- Curso de Sesgos y Esquemas Mentales

TERRORISMO

- Curso de Introducción al Terrorismo
- Curso de Protocolos de Autoprotección Terrorista
- Curso de Prevención del Estrés Postraumático
- Curso de Análisis Interno de Procesos de Radicalización

15%

Código de Descuento: **TRIARIUS15**

(Promoción válida hasta fin de existencias)

Inscríbete ahora en www.LISAINSTITUTE.com

Reconfiguración política de Colombia ¿realidad o utopía?

Por Haylyn Andrea Hernández Fernández (Colombia)

El escenario político en Colombia, desde el pasado 11 de marzo cuando se llevaron a cabo las elecciones legislativas y las Consultas Interpartidistas Populares, ha estado marcado por la polarización debido a las constantes prácticas clientelistas, distorsión de las ideas de los candidatos, estigmatización de sus ideologías políticas e información falsa que circulaba por redes sociales.

La primera vuelta, que se realizó el 27 de mayo, dejó como candidatos a la presidencia a Iván Duque, por el Centro Democrático, con el 39,14% de los votos y Gustavo Petro, por Colombia Humana, con el 25,08%. El candidato de centro, Sergio Fajardo, estuvo muy cerca del candidato de la Colombia Humana, con el 23,73% de los votos (Registraduría Nacional de Estado Civil, 2018a). Pero, tras lo que algunos analistas consideraron ‘malos cálculos

políticos’ en el sistema de alianzas con el ex candidato Humberto de la Calle, no hubo unificación de los votos de los electores que se identificaban con una opción de centro que representaba un cambio de la política tradicional colombiana y se alejaba de una campaña populista que ganaba adeptos rápidamente, así que la respuesta por parte del electorado estuvo dispersa. De esta manera, la contienda electoral delegaba a los ciudadanos la titánica tarea de elegir el presidente para el periodo 2018-2022 con opciones de extrema derecha e izquierda.

Por tercera vez, Duque y Petro se midieron durante la campaña presidencial en la segunda vuelta que tuvo lugar el pasado 17 de junio, donde finalmente se eligió al candidato Duque como presidente electo, obtuvo 10.373.080 votos y Petro quedó en segundo lugar con 8.034.189 votos.

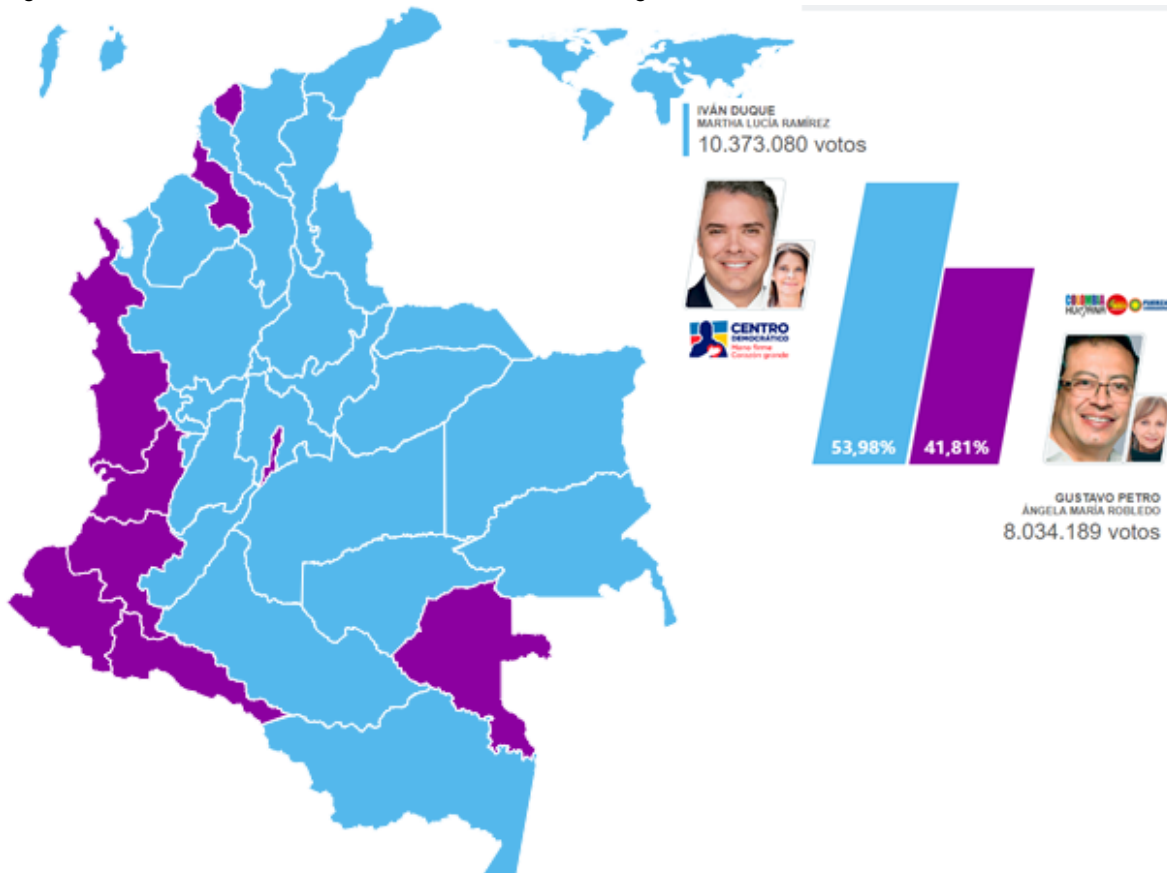


Figura 1. Resultados segunda vuelta. Adaptado de: Registraduría Nacional de Estado Civil. (2018b, junio 17). Elecciones Presidencia de la República.

Más allá de una lectura parcial de los resultados, se deben destacar varios factores que influyeron para llegar al panorama actual. Es necesario tener en

cuenta que tanto Petro como Duque cambiaron, en algunos aspectos estratégicos, sus discursos. Por un lado, Petro había anunciado que de ser elegido

presidente su primer acto sería convocar una Asamblea Nacional Constituyente, esta propuesta causó polémica, ya que, si bien es cierto que el país necesita reformas, especialmente en materia de justicia, la trascendencia de una decisión de este tipo pone en jaque a los ciudadanos y a las instituciones que si bien tiene problemas, siguen funcionando.

Tras pasar a la segunda vuelta, el candidato negó que convocaría la Constituyente, es decir, estaba haciendo cambios estructurales a su programa de gobierno, incluso, como acto simbólico, el candidato firmó en mármol lo que se denominaron los '12 mandamientos' para disipar los miedos que se generaban de su posible llegada al poder. "No expropiaré, no convocaré a una Constituyente y manejaré los recursos públicos como recursos sagrados", fueron algunas de las promesas del candidato, que, junto a figuras políticas como Antanas Mockus, ex candidato presidencial, y Claudia López, fórmula vicepresidencial de Fajardo, formalizaron una alianza, que pese a tener diferencias políticas programáticas, pero no éticas, se consolidaban como la opción más fuerte ante la negativa de aceptar el regreso del uribismo al poder. De esta manera, pretendían persuadir a quienes aún tenían la duda de votar en blanco (ya que los excandidatos Fajardo y De la Calle habían anunciado públicamente que votarían en blanco y esto podría influir en el electorado que los había apoyado en la primera vuelta) o apoyar a Petro (Semana, 2018).

Por su parte, el Centro Democrático, partido del presidente electo, Iván Duque, afirmó que iba a hacer 'trizas' los Acuerdos de Paz, así lo declaró su director, Fernando Londoño, anunciando que todo su esfuerzo para las elecciones de 2018 se concentraría en arremeter contra el Acuerdo del gobierno Santos con las Fuerzas Armadas Revolucionarias de Colombia - FARC-EP-, ya que de esa manera se encontraría una oportunidad de revalidar una agenda más 'justa' (Cuervo, 2017). Sin embargo, el discurso del uribismo ha ido evolucionando a medida que la campaña electoral iba perfilando a Duque como posible ganador. Después de desestimar las iniciales declaraciones del partido, se habló de que se harían cambios estructurales y, finalmente, terminó en modificaciones estructurales. Duque se desmarcó de Uribe y enfatizó en que se pretende lograr una paz con justicia, donde haya verdad, reparación y cumplimiento de penas satisfaciendo los anhelos de las víctimas, es decir, no haría trizas el Acuerdo.

Lo que es evidente es que la estrategia de los candidatos fue maleable en la medida en que el proceso electoral iba avanzando y las propuestas políticas se adaptaban a lo que el electorado quería

escuchar, lo cual no garantiza que sus propuestas, específicamente las del presidente electo, ya que es quien va a ejecutar, se cumplan a cabalidad.

Algunos aspectos que se deben destacar tras los comicios son los siguientes: (i) fueron las elecciones más pacíficas de la historia, la Registraduría Nacional destacó que fue una jornada exitosa ya que no hubo traslado de puestos de votación por razones de orden público, esto gracias a la política de paz del presidente Juan Manuel Santos, pero paradójicamente, ganó la estructura política que más oposición representa a su gobierno. (ii) Pese a las posturas de los líderes políticos de centro, que una vez culminada la primera vuelta anunciaron su intención de voto en blanco, finalmente los electores se inclinaron por elegir alguna de las opciones y se disipó la duda con respecto al alto porcentaje del voto en blanco que se esperaba, el cual finalmente llegó solo al 4,20%, si bien tuvo cierto incremento con respecto a la primera vuelta (1,76%), no tuvo ningún impacto inmediato. (iii) Petro logró que la izquierda llegara a tener la votación más alta en la historia de Colombia, así que a mediano y largo plazo y con un dinamismo activo del partido político de Colombia Humana, la izquierda es una opción real de gobierno; así se evidenció además en el discurso de Petro tras conocerse el resultado electoral, en lo que el excandidato denominó como 'el segundo chico', haciendo referencia a la apuesta por llegar a las alcaldías y gobernaciones para hacer oposición férrea, el control político es inminente. (iv) Al presidente electo, por su filiación política con el Centro Democrático, además de enfrentar los desafíos que la presidencia representa, le resta sortear un control vehemente de la oposición que estará representada por Petro desde el Senado, además debe deslindarse de los legados de su padrino político que van desde el autoritarismo, la parapolítica, la mafia, el narcotráfico, la corrupción y el clientelismo, un reto que debe convencer, además de los ocho millones que apoyaron a Petro, al 47% de ciudadanos que se abstuvieron de votar y de quienes se desconoce su inclinación política, ya que gran parte del país desconfía de las instituciones y cree que su voto está lejos de cambiar la realidad, por lo cual el abstencionismo sigue siendo un desafío.

Iván Duque asume, particularmente, tres procesos claves del gobierno Santos: (i) Acuerdos de Paz, (ii) Extradición de Jesús Santrich y, (iii) la Justicia Especial para la Paz -JEP-. En cuanto a los Acuerdos, se debe tener en cuenta el avance e impacto positivo que ha tenido en el país, más allá de diferencias pragmáticas, los Acuerdos están en función de los ciudadanos, así que el margen de maniobra es

limitado, a menos que sea algo para mejorar el Acuerdo a través del consenso. Ariel Ávila argumenta acertadamente al respecto lo siguiente:

El riesgo de hacer trizas los acuerdos de paz no está en que las Farc regresen a las armas, eso difícilmente ocurrirá. El riesgo está en que en la medida que no se haga una transformación del campo, no se profundice la democracia y se siga en la política errada de lucha contra el narcotráfico de los últimos 20 años, Colombia está condenada a vivir una nueva ola de violencia, tal vez ya no política, si no más criminal. Por ello, la implementación del acuerdo es fundamental para que Colombia avance como una sociedad y supere la violencia que parece repetirse cada cierto tiempo. (Ávila, 2018)

La extradición de Santrich para Duque es inminente, toda vez que se compruebe que el jefe del partido Farc cometió el delito de narcotráfico después de la firma del acuerdo de paz con el Gobierno, además, el presidente electo considera que debe ser la justicia ordinaria la que resuelva la situación jurídica ya que la JEP no tiene ley estatutaria. Y es precisamente ésta última la que está causando revuelo, la JEP, entendida como componente de justicia del Sistema Integral de Verdad, Justicia, Reparación y no Repetición, creado por el Acuerdo de Paz entre el Gobierno Nacional y las FARC-EP (Jurisdicción Especial para la Paz, 2018), aún no se aprueba en el Senado pese a que la Cámara de Representantes avaló el proyecto. Como medida de choque, el gobierno Santos decidió convocar a sesiones extraordinarias y pidió que cada miembro de la corporación asuma su responsabilidad en la

aprobación o no de la iniciativa. La negativa se generó luego de que el presidente electo le pidiera a su bancada esperar a que la Corte Constitucional se pronunciara frente al proyecto, moción que fue atendida no solamente por el Centro Democrático sino por otras fuerzas políticas (Bonces, 2018).

Además, el nuevo mandatario sugirió retrasar la votación de la reglamentación para la JEP hasta después del 20 de julio, ya que entran en funciones los nuevos congresistas: "Me parece que le da la legitimidad si ese trámite se empieza a surtir a partir del nuevo Congreso que tomará posesión el próximo 20 de julio" (CNN, 2018).

A tan solo escasos días desde que se eligió al candidato Duque, el presidente más joven de la historia, ya se evidencian rifirrafes políticos con el gobierno saliente, así que en el empalme político, que está próximo a realizarse, se esperaría que los temas antes mencionados tengan especial atención y se lleguen a compromisos que superen diferencias políticas para que prime la estabilidad del país y de sus ciudadanos.

Por otro lado, le resta al presidente demostrar autonomía y autoridad de su gobierno que se posesionará el próximo 7 de agosto, frente a los fantasmas que le preceden a su aliado, el senador, Álvaro Uribe, a quien Duque propuso como presidente del Congreso, dada la votación histórica a nivel individual en las pasadas elecciones al Congreso, hecho que pone en tela de juicio el deslinde político esperado por muchos colombianos, solo resta esperar la consolidación del nuevo gobierno y el control político de la oposición.

Referencias

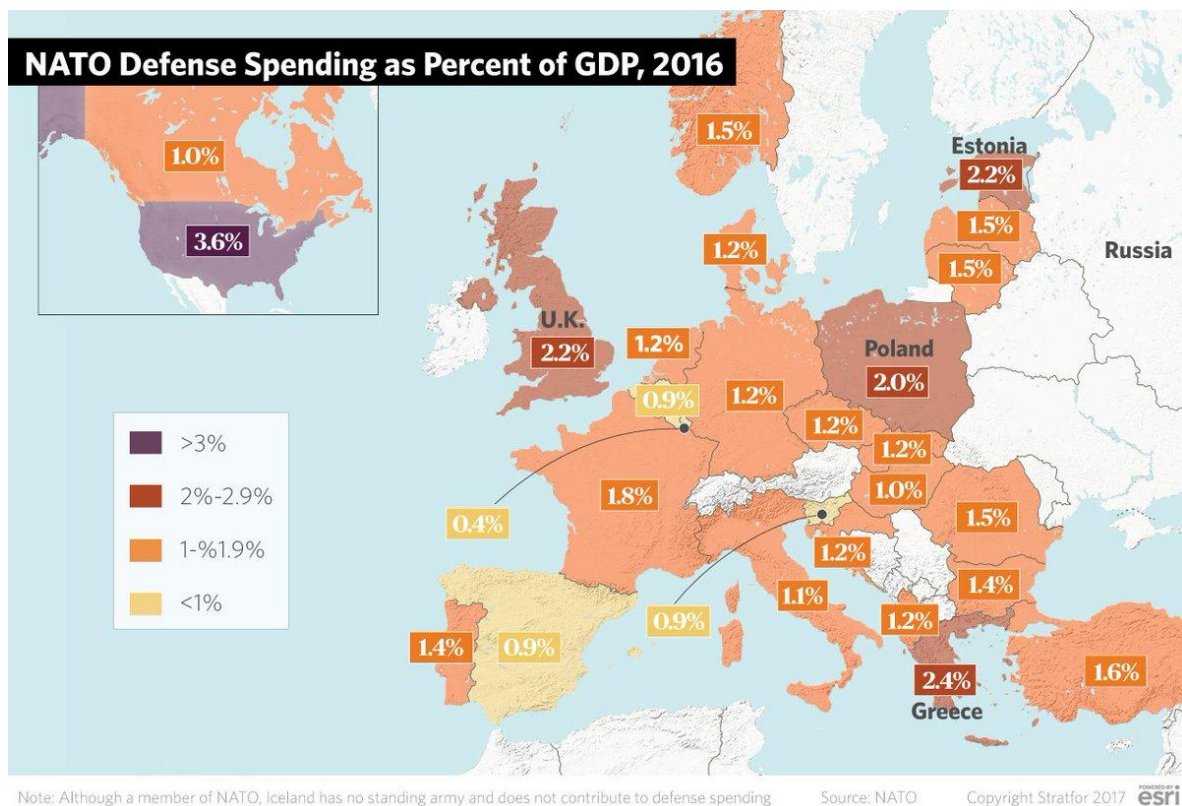
- Ávila, A. F. (2018, junio 13). Los ciegos que no quieren ver. Recuperado a partir de <https://www.semana.com/opinion/articulo/los-ciegos-que-no-quieren-ver-columna-de-ariel-avila/571049>
- Bonces, E. (2018, junio 20). Aún no se aprueba la JEP en Senado. Recuperado a partir de <http://www.elcolombiano.com/colombia/politica/aprobacion-de-la-justicia-especial-para-la-paz-en-el-senado-EY8890314>
- CNN. (2018, junio 19). Colombia: ¿qué está pasando con la Jurisdicción Especial para la Paz y por qué aplazaron su reglamentación? CNN. Recuperado a partir de <https://cnnespanol.cnn.com/2018/06/19/jep-colombia-senado-aprobacion-reglamentacion/>
- Cuervo, J. I. (2017, junio 1). Hacer trizas el acuerdo [Text]. Recuperado 21 de junio de 2018, a partir de <https://www.elespectador.com/opinion/hacer-trizas-el-acuerdo-columna-696539>
- Jurisdicción Especial para la Paz. (2018). Jurisdicción Especial para la Paz. Recuperado a partir de <https://www.jep.gov.co/Paginas/JEP/Jurisdiccion-Especial-para-la-Paz.aspx>
- Registraduría Nacional de Estado Civil. (2018a, mayo 27). Elecciones Presidencia de la República. Recuperado a partir de <https://presidente2018.registraduria.gov.co/resultados/html/resultados.html>
- Registraduría Nacional de Estado Civil. (2018b, junio 17). Elecciones Presidencia de la República. Recuperado a partir de <https://presidente2018.registraduria.gov.co/resultados/2html/resultados.html>
- Semana. (2018, junio 9). 12 mandamientos: el mensaje de la alianza Mockus, Petro y Claudia López. Recuperado a partir de <https://www.semana.com/nacion/articulo/12-mandamientos-de-la-alianza-de-mockus-petro-y-claudia-lopez/570590>

Haylyn Andrea Hernández Fernández

(Colombia) Magister en Seguridad y Defensa Nacionales de la Escuela Superior de Guerra de Colombia. Profesional en Relaciones Internacionales y Estudios Políticos de la Universidad Militar Nueva Granada. Amplio conocimiento y competencias en análisis de problemáticas nacionales e internacionales, estudio de relaciones de entidades del sistema internacional y capacidad de exploración en nuevos campos de estudio. Analista de Inteligencia en AIG Colombia.

España y la OTAN

Francisco Javier Blasco, Coronel (r) ET (España)



Gastos en defensa de los miembros de la OTAN como porcentaje del Producto Interno Bruto.

El tema de la OTAN, su finalidad, continuidad en el tiempo tras su verdadero origen o razón de ser, financiación y orientación de cara al futuro suele ser muy recurrente desde la caída del telón de acero y el derrumbamiento del bloque socialista. Como todos sabemos, la OTAN es un club privado que a modo de una Alianza firme trabaja en la defensa de unos intereses y del suelo común de sus miembros o socios; quienes se comprometen a intervenir, incluso militarmente, cuando cualquiera de ellos se viera amenazado directa o indirectamente. Compromiso de máximos, que solo se ha invocado una vez tras los atentados de 11-S en EEUU.

Una Alianza cuya participación, adhesión y diferente grado de integración en su estructura de mando y control es voluntaria y se basa en un complejo sistema de compensación. Son los propios EEUU los que, tradicionalmente, porque les ha podido interesar por cuestiones de liderazgo y por incapacidad, dejadez o aprovechamiento del resto, vienen corriendo con la inmensa mayoría de los gastos en defensa del conjunto. Miembro, además, cuyas aportaciones en personal y material incluso en operaciones de mucho riesgo, de forma permanente o por largos periodos de tiempo y fuera de su territorio natural supera exponencialmente las de cualquiera de

sus miembros, e incluso las de todos juntos al unisono.

El origen de la Alianza fue claro y no tuvo otro motivo que el evitar que se repitieran fenómenos como los que indujeron a dos guerras mundiales en Europa en poco más de un cuarto de siglo y al mismo tiempo, defenderla de las crecientes y constantes amenazas de la entonces URSS -protagonizadas en aquellos momentos por el famoso cerco ruso a la ciudad de Berlín- tras el fin de la segunda guerra.

Para dejar clara su posición y blindarse ante posibles ataques militares, los aliados de Estados Unidos decidieron finalmente suscribir, en abril de 1949, el Tratado -conocido por el nombre del Tratado del Atlántico Norte o de Washington, por haberse firmado en dicha ciudad- con el que se oficializaba la creación de la OTAN. Los países firmantes de ese primer tratado fueron EEUU, Bélgica, Canadá, Dinamarca, Francia, Islandia, Luxemburgo, Italia, Noruega, Países Bajos y Reino Unido.

España, no sin un largo, tortuoso, titubeante y muchas veces antagónico proceso de adhesión -protagonizado por el PSOE en dicho momento- se unió a la OTAN en 1982 y tras varios procesos de integración, culminó su incorporación plena a la estructura militar integrada el 1 de enero de 1999.

Actualmente son 29 los países que la conforman, aunque Islandia no aporta fuerzas por no disponer de permanentes estructuras militares. Todas las decisiones se toman de forma unánime y de común acuerdo. No hay ninguna votación o decisión por mayoría.

Tras caer el telón de acero en 1989 y posteriormente desmembrarse la URSS, hubo que, tras años de ciertas reinventiones y adaptaciones, transformar la Organización, su estructura, cometidos y misiones ampliando el foco a otros aspectos de la seguridad y la defensa común, aunque se focalizaran en lo que se conoce como “fuera de área” y que, durante muchos años, no habían sido contemplados.

Pertenecer a este tipo de clubs no es gratis, por mucho que bastantes políticos así lo puedan o quieran interpretar. No solo la predisposición y obligación en su caso, de aportar fuerzas y acudir en defensa de uno o de gran parte de la colectividad, entrando en guerra contra el agresor, si fuera preciso, es un factor de costo económico, social, militar y político para todos los miembros. La participación colectiva supone un constante sistema de adaptación y normalización a las tácticas, técnicas y procedimientos dictados por la Alianza; pero fundamentalmente, sobre los materiales y sistemas de todo tipo. Esto conlleva una gran adaptación a las nuevas tecnologías y la transformación o adquisición de nuevos materiales bélicos, que no suelen ser de bajo coste.

En la OTAN se lleva varios años insistiendo en un factor importante para el logro de dicha normalización y que consiste, además de los logros alcanzados -tras muchos años de esfuerzos- sobre la interoperabilidad de sus materiales y municiones, en alcanzar cada país miembro un gasto en defensa cercano o superior al 2% del PIB. Compromiso, que, tras haber sido tratado verbalmente en muchas ocasiones, fue llevado al papel, por primera vez, en la famosa Cumbre bianual de la OTAN que en 2014 se celebró en Gales.

Para dicha fecha, aunque por lo bajini, todos los países se comprometieron alcanzar tal cifra en un plazo de diez años [1]. Los países miembros por diversos motivos geopolíticos y económicos derivados de la crisis de 2008, tal y como bien se reflejan en la referencia, llevaban muchos años reduciendo gastos y costes en defensa y la situación derivada de tanto recorte en el gasto había alcanzado un punto demasiado crítico para la mayoría de los países y la operatividad de la Alianza en su conjunto a no ser que se produjeran cambios importantes al respecto.

La llegada de Trump a la Casa Blanca ha supuesto, como en casi toda la política interna y externa norteamericana, un cambio profundo y el impulso a la toma de decisiones de fuerte calado y acciones de presión sobre temas que, aunque ya estaban decididos por previos presidentes y que sus propias cámaras exigían un arreglo o acuerdo mucho más racional, seguían casi enquistados y muchos de ellos, durmiendo el sueño de los justos.

Trump con su idea y campaña fundamental de “America First” encontró en el punto de los gastos y el grado de participación e implicación de cada miembro en la OTAN un fulcro o punto de apoyo fundamental, para mover a los demás hacia algo positivo y, al mismo tiempo, y no le falta razón, reducir en una gran parte los gastos de EEUU dedicados a defender Europa casi en exclusiva y poder dedicar dichos esfuerzos materiales y personales en otros focos mucho más acordes con sus intereses nacionales del momento; Asia-Pacífico y ciertas áreas o regiones en Oriente Próximo y Medio.

Recuperar el compromiso individual y colectivo de Gales, por tanto, no es nada nuevo, ni un acto achacable solo a Trump como se quiere hacer ver por parte de determinados medios de comunicación y círculos políticos interesados en hacer una campaña de desprestigio y contra propaganda sobre el personaje. Otra cosa, son sus formas de decir las cosas o los poco refinados y nada diplomáticos actos gestuales que emplea cuando está disconforme con la persona, el país o grupo de ellos, que se sienten frente a él en cualquier foro o momento de discusión política.

Recientemente se ha sabido la existencia de ciertas cartas a casi una decena de países aliados de la OTAN en las que él, personalmente, ha tratado de leer la cartilla a los respectivos gobiernos, y que sirves de aviso previo de la tormenta que al respecto se pudo desencadenar durante la Cumbre de la OTAN en Bruselas de los días 11 y 12 de julio. Todos conocemos, por experiencias previas, que este personaje no se corta ante nadie ni ante ningún foro por importante o aparente que este sea. Baste recordar sus actuaciones estelares, peleas, discusiones y portazos dados en la pasada reunión del G-7.

Son memorables y poco agradables las imágenes de sus caras largas y de disgusto presentadas frente a Merkel y con el propio Rey de España a diferencia con visita llena de amores -aunque con posteriores y casi instantáneas grandes decepciones- con Macron y su esposa, todas ellas en la Casa Blanca. Los gestos, las cortas palabras y de poco halago en aquellas otras dos visitas, ya marcaron una premonición de que algo no funcionaba bien y, que como suele decirse, podría empeorar.

Aquí están las causas y sus razones de aquellos malos humos; Trump sabía perfectamente que Alemania y España -dos de los tres/cuatro puntales de la nueva Europa- no estaban por la labor de cumplir con sus compromisos en defensa. Ambos, unos por coalición y otros por usurpación de gobierno, están bajo una o egida o corriente socialista “moderna y algo extraña” que hoy en día, se muestra muy reacia a cumplir con temas de calado referentes a la cooperación internacional y, fundamentalmente, al aumento de los gastos en seguridad y defensa, por entender, que estos les alejen de sus programas de otros gastos a manos llenas en temas, que ellos titulan como “Sociales”; pero, que en muchos casos, no suponen más que un atencivo despilfarro

propagandístico y de partido. Planes E, cheques bebé, etc...

España ha sufrido como muy pocos una crisis económica y financiera desde 2008 que le ha llevado a políticas de austeridad en grandes y pequeños gastos, entre los que, como no debía ser menos, entran y muy de lleno, la Seguridad y la Defensa. Las políticas de recortes nos han llevado a reducir en mucho nuestros consumos y evitar grandes desgastes de material en ejercicios y maniobras. Nuestras Unidades de primera línea o sobre las que se basan la mayor parte de los despliegues en el exterior, al menos inicialmente y en momentos de tensión, están súper saturadas y sus materiales al borde de la inoperatividad por sus numerosas participaciones, aunque mayoritariamente y en los últimos años, estas sean a base de pequeños destacamentos y con pocos movimientos sobre el terreno.

La necesidad de cubrir mínimamente las plazas de clase de tropa en los años anteriores a la crisis en las que había trabajo -muy bien remunerado- para todos en cualquier especialidad y, principalmente en la construcción, hizo que se fueran reduciendo las exigencias psicofísicas e intelectuales de los escasos aspirantes a integrarse en las FAS. Además, y para aumentar su número, los respectivos gobiernos cometieron el gran error de mejorar, en mucho, las condiciones y contratos laborales de los aspirantes, facilitando su continuidad en el empleo durante muchos años y poniendo grandes trabas a la rescisión de sus contratos. Un trabajo casi a la carta y para el que se te buscaba a lazo. Como consecuencia de todo ello, tras muchos años posteriores plenos de restricciones, nos encontramos, con unas FAS, muy o bastante envejecidas de media; que no fueron ni son hoy en día, las más capaces psicofísicamente para realizar dichas labores y que en un alto porcentaje dedican los mejores efectivos, recursos económicos y gran parte del mejor material a labores muy plausibles y loables pero de escaso valor militar para la Alianza (la UME).

La falta de un mayor número de Unidades adiestradas para las rotaciones iniciales en las aperturas de misiones y el empecinamiento político de figurar en todo tipo de misiones propias, de la OTAN, la UE o la ONU, hace que las mismas Unidades con sus personas y materiales se vean implicadas en diferentes escenarios con muy poco espacio de tiempo entre las diversas actuaciones. Situación, que redundan en el comportamiento humano por el cansancio que supone y los problemas de conciliación familiar, principalmente entre las mujeres soldados, cuyo número va en aumento y que, debido a una mayor permanencia en filas, se suelen casar con otros soldados; matrimonios que en muchos casos y, como es natural, las lleva a tener hijos lo que supone un hándicap para poder seguir cumpliendo con su labor y contrato profesional. En definitiva, cambiar simplemente de boina, de reglas de enfrentamiento o de escenario con las mismas fuerzas de forma casi permanente y sin periodos de

reposo, adaptación y conciliación suficientes no es la mejor fórmula para dotar estas misiones.

Tras haber pasado una gran parte de mi vida profesional dedicado a diversos aspectos que tienen mucho que ver con las operaciones y el desgaste del material como: seis años piloto de pruebas de helicópteros y jefe de mantenimiento en dos Unidades de las Fuerzas Aeromóviles del Ejército (FATMET); siete de oficial de Estado Mayor en Mando de Apoyo Logístico (MALE); más de dos como fundador y Jefe de Planes Operaciones y Seguridad del Mando de Apoyo Logístico a las operaciones de Apoyo a Bosnia (MALOG A/B), dos periodos de operaciones de seis meses en Bosnia y Kosovo; tres años en el Cuartel General de la OTAN, AFSOUTH (Nápoles) durante la operación de entrada y pacificación de Kosovo, Jefe de uno de los Regimientos que más contribuyen con hombres y bajas en las operaciones de Paz (Isabel Católica nº 29 de la BRILAT) y segundo Jefe de la Nato Reaction Force nº 6 (NRF-6) -primera liderada por España y en la que participó como país mayor contribuyente de medios y fuerzas- creo poder decir con bastante acierto y conocimiento de causa que los medios, materiales y municiones empleados por las FAS tanto en los periodos de entrenamiento como en operaciones de cierta intensidad necesitan de importantes programas de mantenimiento, revisión, sustitución e incluso de modificaciones y reformas o adaptaciones a los nuevos componentes o medidas para su protección o mejora de funcionamiento.

Todos los materiales terrestres marítimos y aéreos están sujetos a dicho tipo de operaciones de mantenimiento en mayor o menor grado de complejidad y coste. En muchos casos, estas macro revisiones o adaptaciones de actualización suponen no solo un gran periodo de tiempo para su ejecución, sino que precisan ingentes cantidades de dinero para ello. Todos estos procesos son muy afectados cuando por restricciones o recortes presupuestarios se ven aplazados en el tiempo, limitados en su alcance y profundidad e incluso eliminados. Cosa que, para nuestra desgracia, ha ocurrido y sigue arrastrándose en una gran parte de nuestros materiales críticos e importantes por lo que estos pueden llegar a quedar inoperativos, son menos eficientes por no acoger los sistemas más modernos o pierden compatibilidades con sus homólogos en otros ejércitos.

Los que tenemos cierta experiencia en estos menesteres somos conscientes de esta gran lacra y deficiencia, pero también se conocen por las casas fabricantes de los materiales originales, quienes, normalmente, llevan a efecto dichas reformas o modificaciones. Un Ejército que realiza o aplica durante un largo periodo de tiempo la mayoría de los principales planes de modernización, pierde gran parte de sus cualificaciones y capacidades y eso, no es un secreto de estado, se conoce en todo el entorno industrial y militar de las alianzas.

Los nuevos medios empleados en la guerra moderna a base de capacidades para el ejercicio de las guerras electrónicas; los medios de comunicación de datos por todo tipo y redes, incluidas las cibernéticas;

capacidades de visión todo tiempo y ambiente y el empleo generalizado de potentes y efectivos sistemas de misiles inteligentes, contra misiles y drones precisan también de unas potentes inversiones que no se cubren con pequeños escauceos en estas tecnologías.

España, a pesar de que todo el mundo le reconoce su fuerte mejora en la situación de su economía e industria, sigue estando a la cola de los países que invierten menos en seguridad y defensa. Concretamente, en la OTAN tenemos el honor de ser el tercer país que menos invierte de todos los miembros, nuestra ratio en este gasto es algo menor del 1% y solo superamos en ello, y por los pelos, a Bélgica y en algo más a Luxemburgo. Como todos sabemos, dos grandes referentes internacionales por sus capacidades de todo tipo.

Trump sabe en qué situación se encuentran nuestras fuerzas y material por sus propios informes militares y por lo que le comentan sus principales industrias de armamento; quienes, a su vez y a modo de compensación de inversiones en la defensa de Europa, tienen la capacidad y patente para realizar la mayor parte de dichas modificaciones y modernizaciones en dichos materiales. Por ello, es imposible engañarle y menos con burdos mensajes por parte de nuestro presidente o de su cada vez más falaz o escurridizo ministro de exteriores. Quienes con sus declaraciones al respecto insultaron la inteligencia de propios y a extraños el pasado día 3 de los corrientes.

Declaraciones como que, aunque España gaste menos del 2% del PIB en Defensa, "lo gastamos de una forma muy activa" porque "nuestras Fuerzas Armadas son prácticamente las únicas que participan en todas las misiones de la OTAN a través de todas las fuerzas: aire, tierra, mar y fuerzas especiales". Desde el Gobierno se destaca que España ha desplegado 1.161 efectivos en misiones de la OTAN [2], 616 con la ONU y 757 con la Unión Europea. Además de formar parte de la Coalición contra el DAESH, donde 581 españoles colaboran en la formación del ejército iraquí. Pero, ambos obvian que España no ha participado en operación de combate alguna en ninguna parte -ni siquiera en Libia, Siria e Iraq a pesar de habérsenos invitado e insistido en ello- desde que salimos en fuerza de Iraq y posteriormente de Afganistán. Por mucho que presumamos de números, hay que reconocer que las misiones en las que actualmente participamos tienen mucho de testimoniales, nada decisivas militarmente, bastantes son de carácter de enseñanza militar específica y policial y con un grado de riesgo muy limitado en la mayoría de los casos por no tener previsto su entrada en combate.

Además, gran parte de nuestra participación en misiones de la ONU y de la UE se realiza fundamentalmente en benéfico propio -a fin de evitar o controlar, de diversos modos, el flujo de refugiados hacia España a través de Marruecos y Mauritania- y siempre a cargo de fondos procedentes de otros apartados de los presupuestos o de las mismas

organizaciones para las que desplegamos. Fondos, que permiten rellenar, parcialmente algunas necesidades, que, por otro lado, serían imposibles de cubrir de otra forma [3]. Tema que el mismo ministro, insistiendo en su error de arrogancia y desprecio a los demás, lo zanjó con: "Somos el único país de la Unión Europea que ha participado en todas las misiones militares de la UE; o sea, que gastamos menos de lo que dice la OTAN, pero lo utilizamos muy bien", según informó Europa Press [4].

Expresiones y afirmaciones todas ellas muy vendibles y comprables en el mercado interno, máxime cuando, últimamente, el número de palmeros al gobierno ha aumentado notablemente. Pero, tratar de engañar y vender humo externamente contra realidades palpables es una tarea muy difícil, máxime, cuando el otro tiene bien claros los datos sobre la mesa.

Algunos ya advertimos públicamente, que una vez les diera tiempo a los asesores de Trump a desempolvar la escasa información que tuvieron sobre Sánchez tras su inesperada toma del poder en España, dada la insignificancia que hasta entonces podía plantear, y vieran que es discípulo directo y aventajado de Zapatero, el hombre que humilló a su bandera en un desfile militar en Madrid y abandonó ante el enemigo un flanco de las fuerzas americanas en Iraq saliendo de prisa y corriendo, incluso dejando in situ gran parte del material propio por las prisas de la desordenada, por rápida e inesperada, retirada, nos mirarían con lupa y nos leerían pronto y bien la cartilla.

Sánchez lleva un mes en el gobierno de España tras acceder con el apoyo más antinatural pensable; no ha realizado ni una sola conferencia de prensa o declaración de programa e intenciones de todo tipo en nuestro territorio desde entonces y que ha engañado a propios y extraños en muchos de sus pasos dados y totalmente contrarios a sus declaraciones previas; que pretenciosamente ha querido liderar acciones en Europa casi enquistadas relacionadas con el tema de la migración y ha vuelto a casa con más de lo mismo y alguna ración extra y que busca todo tipo de efectos especiales y fuegos de artificio. El mismo Sánchez, en pocos días deberá lidiar con un toro bravo, que, aunque él mismo y los medios aparenten no darle la importancia y el eco que tiene; personalmente, no se me antoja nada fácil, máxime por los avisos dados tanto por el toro como por el torero.

Si pretende acudir a Bruselas con los mismos, poco profundos y hasta casi jocosos discursos oficiales que han hecho tanto él como su ministro de exteriores tras la carta recibida de Trump y la visita del Secretario General de la OTAN, puede que consiga el efecto totalmente contrario al pretendido. En estos temas de gasto en grado sumo y máxima defensa y ante las chulerías de los demás, las reacciones del presidente norteamericano pueden ser funestas e incluso letales. Todos sabemos que tener Unidades o Cuarteles Generales internacionales desplegados en territorio nacional produce provechosos y variopintos réditos e incluso prestigio al país que los acoge; de ahí que los aliados estén siempre en liza para albergar este tipo de unidades. Ahora mismo estamos en un proceso de

acoger uno de ellos de tipo aeronaval para el mando de la Operación Atalanta procedente del Reino Unido como consecuencia derivada del Brexit.

La OTAN no cuenta con mecanismos de expulsión entre sus estatutos y reglamentación; pero tampoco estos dicen nada en contra de aquello, por lo que se puede presuponer, que dicha posibilidad pueda ser planteada ante determinadas circunstancias y por alguien con la suficiente fuerza y capacidad de otro tipo de amenazas [5] para ello -en su día y en ciertos mentideros se llegó a barajar la posibilidad de expulsar a Grecia y/o a Turquía por causas diferentes pero, en ambos casos, se incluía un cierto y muy peligroso acercamiento a Rusia-.

No es casualidad que cartas similares hayan sido enviadas a otros ocho países de la OTAN entre los que se encuentran Alemania e Italia, lo que hace suponer que la Administración norteamericana pueda estar empezando a pensar proponer, bajo una fuerte presión del socio más rentable y capaz, barajar una OTAN a dos velocidades como importante medida de convicción, a su vez, sobre los miembros más díscolos; o, lo que sería aún pero, como el paso previo a una gran reducción en algunos países, si es que estos, voluntariamente y sin causa justificada, no se avienen a cumplir con lo ya largo tiempo acordado.

España, por tanto, podría estar entre ellos, por dos importantes motivos: no seguir estrictamente lo marcado en la Alianza y por estar jugando con dos barajas a la vez, al mismo tiempo que se niega a incrementar su gasto, ofreciendo Unidades a iniciativas militares de mucha menor entidad dentro de Europa, pero fuera de la OTAN y la UE [6]. Iniciativas, pequeñas pero que, sin duda, distraen y restan esfuerzos e inversiones en la propia Alianza.

Los Estados Unidos comandados por Trump no se arredran a la hora de lanzar sus amenazas tanto a amigos y aliados como a extraños o enemigos; las hace de forma grosera y con muy poco o ningún tacto diplomático; pero, son suficientemente fuertes y entran en efectividad a las pocas horas de pronunciarlas. Estas mencionadas cartas, no son un buen presagio y, personalmente, no pienso que las haya remitido y firmado personalmente, tal y como parece, como un simple aviso a navegantes sin graves consecuencias. No tengo ninguna información de primera mano al respecto, pero tras estudiar sus comportamientos y decisiones drásticas y a la vista de lo que ha sucedido en otros casos de vital importancia, mucho me extrañaría que solo fuera así. En cualquier caso, y aunque dicha posibilidad no estuviera ni por asomo en el horizonte, insisto en la necesidad de bajar las ínfulas o humos nacionales al intervenir España en Bruselas ya que, el quedar muy

significado y acorralado en un organismo como la OTAN supone siempre un paso atrás en la toma en consideración frente a los compromisos internacionales, una pérdida de prestigio dentro la Alianza y una falta de credibilidad para futuras intervenciones o propuestas en las que España se vea involucrada directa o indirectamente tanto en aquella como en la propia UE y en otros organismos internacionales. Pecados estos muy difíciles de ser perdonados y que, sin duda, supondrían un largo calvario y penar por los pasillos de las relaciones y lugares de enjuagues a varias bandas.

Las repetidas demostraciones españolas de grandeza y los muchos apoyos a iniciativas de todo tipo en la UE sobre temas de diferente calado y máxime aquellos referentes a las Políticas Comunes de Seguridad y de Defensa de la UE y los deseos de un posible liderazgo en la mayoría de ellas [7], podrían quedar anuladas, sino enterradas, si se nos enmarcase definitivamente como proscritos en la Alianza por no cumplir con los compromisos tantas veces asegurados.

Quedar España aislada militarmente teniendo en los flancos y a tan cortas distancia a quien tenemos, principalmente por el sur, supondría una desprotección mayúscula y un auténtico caramelo fácil de ser disputado y devorado cual apetitoso bollo en la puerta de un colegio a la hora de la salida de los alumnos.

Espero que las cúpulas militares y de la seguridad e inteligencia del CNI, que no han sido tocadas por la “mano divina” tras el cambio de gobierno, sigan teniendo todas sus ideas tan claras tal cual, al parecer, las tenían hace algo más de un mes y sean capaces de convencer a la nueva ministra y al presidente del error de seguir por dicho camino.

Entramos en la OTAN -tras muchas dudas y cambios radicales de posturas internas- de la mano del PSOE y puede que sea este mismo partido el que, tras años de beneficios mutuos, nos saque de ella, por aquello de “a mí nadie me dice lo que debo hacer, ni cuanto, ni en que tengo que gastar mi dinero”. No me extrañaría nada que en este punto -tal como ya se constata en otros muchos de cierto calado en la política nacional vistos hasta el momento- también tenga algo o mucho que ver el indiscutible compañero de fatigas de Pedro, Pablo Iglesias y, que la doctrina a este respecto emane del muy conocido ideario de aquel que, incomprensiblemente y de la mano del PSOE en el gobierno, fue JEMAD; Julio “el rojo” como ya se le llamaba en sus tiempos de cadete en S. Javier, quien ya se ha pronunciado varias veces, y no bien, sobre la OTAN y sigue teniendo un puesto de importancia o relevancia ideológica en Podemos.

Referencias y Notas

[1] <https://sites.google.com/site/articulosjavierblasco/las-dificultades-de-la-otan-actual-a-la-hora-de-tomar-decisiones>

[2] A lo largo de 2017, España ha estado presente en las siguientes operaciones y misiones de la OTAN cubriendo las dimensiones área, marítima y terrestre:

- En Turquía se ha contribuido a la protección de su población contra la amenaza de misiles balísticos mediante el despliegue de una batería antiaérea Patriot y más de 140 efectivos.
- En Letonia, en la Presencia Reforzada Avanzada, con más de 330 efectivos formando parte del batallón liderado por Canadá, aportando medios terrestres de gran capacidad. La participación española ha supuesto, de hecho, el primer despliegue en el exterior de medios mecanizados y acorazados de cadenas -seis carros de combate "Leopardo 2E", dos carros "Leopardo 2ER" de recuperación, catorce vehículos de combate de infantería VCI "Pizarro" y quince transportes oruga acorazados (TOA)-.
- España ha contribuido durante cuatro meses a la misión de Policía Aérea en el Báltico con un destacamento de 4 aviones en Estonia, donde hemos llegado a contar con cerca de 130 efectivos.
- En Afganistán, en la misión Apoyo Decidido ("Resolute Support") hasta un máximo de 95 pax. en misión de instrucción y asesoramiento en Operaciones Especiales.
- En las fuerzas navales permanentes de la OTAN, con una aportación muy significativa de medios navales y de efectivos.
- En el Mediterráneo en la operación "Sea Guardian".

<http://www.exteriores.gob.es/RepresentacionesPermanentes/OTAN/es/quees2/Paginas/EspañaOTAN.aspx>

[3] Hay muchos países que basan gran parte de sus necesidades militares en los ingresos por participar en misiones sufragadas por Organizaciones Internacionales.

[4] <http://www.elmundo.es/espana/2018/07/03/5b3b30c946163f564f8b4608.html>

[5] Baste recordar los abandonos de EEUU bajo la presidencia de Trump de acuerdos de mucha trascendencia para el mundo sin, aparentemente, haber calibrado sus consecuencias. No quisiera imaginar que sería de la OTAN, si Trump, disgustado por o, gracias a la falta de rigor en otros, la abandona y el Reino Unido culmina su Brexit.

[6] <https://mundo.sputniknews.com/defensa/201807011080039292-francia-presidente-quiere-crear-un-ejercito/>

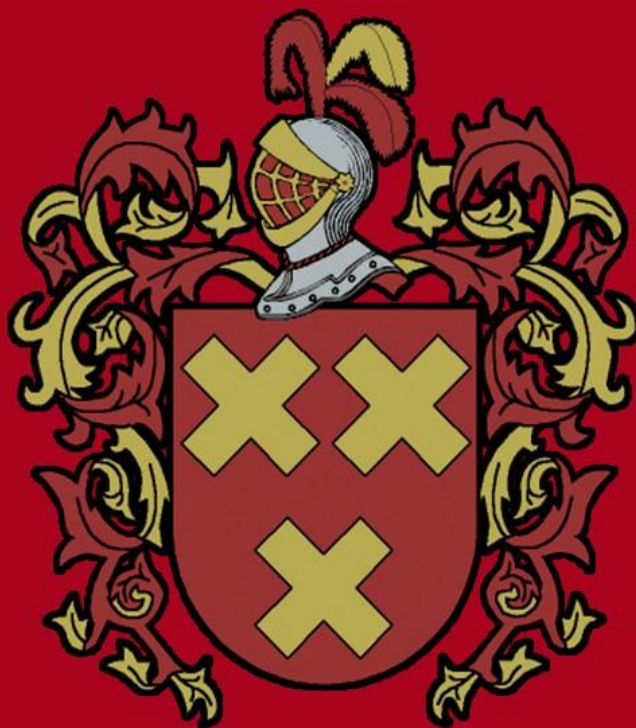
[7] https://elpais.com/internacional/2017/11/13/actualidad/1510587099_967631.html

Fuente de la Imagen: <https://pbs.twimg.com/media/C4vdDeLXAAEJzMR.jpg>

Francisco Javier Blasco

(España) Coronel del Ejército de Tierra, en la reserva. Fue Director Adjunto del Centro de Inteligencia de las Fuerzas Armadas (CIFAS) y Jefe del Departamento de Proliferación; Agregado de Defensa en la República Checa y la República Eslovaca; 2º Jefe de la Brigada Hispano-Italiana en la Región Oeste (KFOR) en Kosovo; Profesor principal del Ejército de Tierra en la Escuela Superior de las Fuerzas Armadas (ESFAS) del CESEDEN, entre otros cargos de gran importancia.

ANIVERSARIO NÚMERO 15



www.fuerzasmilitares.org

2003-2018

15

¡Siempre en Vanguardia!

Seguridad de la Información. Clasificación de Activos

Por Douglas Hernández (Colombia)



El presente es un ejercicio académico, desarrollado en el marco del Master en Seguridad de la Información del Security College US. Los errores y omisiones son atribuibles únicamente al autor, quien se encuentra en proceso de formación. Bienvenidas las críticas constructivas y observaciones.

Requerimientos

- a) Escoja un sector de la industria privada o pública, por ejemplo, si desea tomar el sector educación, y realizar una breve descripción del comportamiento de esta área definiendo cual es el bien o el servicio que se ofrece, cuáles son las grandes empresas de este sector, etc. (OSINT)
- b) Del sector que haya escogido debe tomar como ejemplo una empresa para el ejercicio. Ejemplo "politécnico Colombo Andino." debes hacer la búsqueda de la información acerca de esta empresa escogida, determinar sitios oficiales, redes sociales, organización, procesos, certificaciones que posee, junta directiva, y toda la información que pueda obtener a través de OSINT. (Documente el proceso y las herramientas usadas).
- c) Una vez realizada la búsqueda inicial vamos a asumir que la empresa le ha contratado para implementar un sistema de gestión de seguridad de la información y dentro del primer paso que estamos desarrollando vamos a realizar la fase de identificación y clasificación de los activos de información. Ejemplo: para el politécnico su principal bien a proteger es la información de los estudiantes, su servicio es la educación por lo tanto el principal activo de información es la aplicación donde se alimentan las bases de datos de estudiantes. Se debe identificar por lo menos 10 activos de información por proceso identificado en el punto b. Para ello se recomienda realizar una tabla con la identificación de los activos. Recuerde que puede investigar metodologías para la clasificación de los activos de información o crear su propio método.
- d) Una vez realizada la tabla debe documentar por qué se considera un activo valioso, determinando cuales son las amenazas, riesgos e impacto sobre cada uno de los activos.

Solución

Para el presente ejercicio académico escojo a la empresa SUMIMEDICAL perteneciente al sector salud de la República de Colombia. Mi interés por esta empresa radica en que soy su cliente, y esta es una buena oportunidad para saber más sobre ella.

El Sector Salud en Colombia

En Colombia, el Sistema General de Seguridad Social en Salud (SGSSS), es el marco en el que prestan su servicio las entidades afiliadas al sistema. La Ley Estatutaria 1751 del 16FEB2015 señala que el sistema de salud es “el conjunto articulado y armónico de principios y normas; políticas públicas; instituciones; competencias y procedimientos; facultades, obligaciones, derechos y deberes; financiamiento; controles; información y evaluación, que el Estado disponga para la garantía y materialización del derecho fundamental de la salud.”

En el SGSSS interactúan distintos agentes públicos y privados, entre los que hay un permanente flujo de información y también de recursos. En el centro del sistema están los pacientes. Se supone que el servicio de salud debería ser oportuno, eficaz y de calidad, pero las quejas de los usuarios y los escándalos son constantes. ANDI (2016) llama la atención sobre una cadena intersectorial que agrega valor a los servicios que se prestan en el SGSSS y hace posible la atención en salud de la población. Allí las IPS establecen relaciones de mutuo beneficio con la academia -por ejemplo- con la que “colabora en investigación y en formación del futuro recurso humano del sector. También con una gran diversidad de proveedores de servicios y productos, en muchos casos especializados para el sector, y que están en permanente actualización y mejora.”

A continuación, se presenta un esquema que muestra a los principales actores del Sistema General de Seguridad Social en Salud.



Imagen N° 1 Actores del Sector Salud en Colombia. Fuente: ANDI (2016)

Hay que mencionar también a actores estatales, como la Procuraduría General de la Nación, la Contraloría General de la República, la Fiscalía, la Defensoría del Pueblo y la Rama Judicial, que tienen una injerencia notable en el sector a través de sus decisiones.

Administración y Prestación de los Servicios de Salud

La Ley 100 de 1993 delega en tres entidades la administración y prestación de los servicios de salud dentro del SGSSS:

1. Entidades Promotoras de Salud (EPS).
2. Administradoras del Régimen Subsidiado (ARS), e
3. Instituciones Prestadoras de Servicios (IPS).

Los servicios brindados por estas entidades, giran alrededor del contenido del Plan Obligatorio de Salud¹ (POS) de cada uno de los regímenes existentes (contributivo o subsidiado).

Las EPS y las ARS esencialmente son compañías aseguradoras (administran los riesgos y el dinero que remunera este servicio), mientras que las IPS son las que proveen directamente el servicio. A continuación, una breve reseña de cada tipo de entidad, según Santa María, García, Rozo y Uribe (2007):

“Entidades Promotoras de Salud (EPS)

Son compañías de seguros encargadas de prestar o garantizar directa o indirectamente la prestación del POS a los afiliados al RC. Estas instituciones están además encargadas de promover la afiliación de los grupos no cubiertos y del recaudo de las cotizaciones que se dirigen a las subcuentas del Fondo de Solidaridad y Garantía (FOSYGA). El FOSYGA, es el órgano que administra la financiación del SGSSS, para lo cual administra las cotizaciones de los afiliados a las EPS, garantiza la compensación entre personas de distintos ingresos y riesgos, así como la solidaridad del sistema, entre otras. Las EPS reciben posteriormente (por parte del FOSYGA) un pago per cápita o UPC por afiliado.

Administradoras del Régimen Subsidiado (ARS, hoy EPS-S)

Estas administradoras (compañías de seguros también) se encargan, además de prestarle servicios a los afiliados al RS, de atender los requerimientos del RSP. De la misma forma que en el RC, los beneficiarios del RS tienen derecho a elegir libremente la aseguradora según sus preferencias.

Instituciones Prestadoras de Salud (IPS)

Las EPS y las ARS contratan los servicios ofrecidos por las IPS, es decir, los hospitales o centros de salud de carácter público, privado, mixto, comunitario o solidario. Estas entidades están encargadas de ofrecer el contenido del paquete de servicios básicos, en términos de medicamentos y procedimientos al que acceden los afiliados del SGSSS (POS), y de ofrecer servicios a los vinculados, que no cuentan con ningún tipo de cobertura (o que tienen un subsidio parcial). Las IPS pueden ser de diferentes niveles (del I al IV), dependiendo de la complejidad de los servicios que ofrecen (donde los niveles III y IV corresponden a enfermedades bastante complejas o de ‘alto costo’).” (p.26-27)

Las Mejores EPS

El Tiempo (2018) señala que desde el año 2013 el Ministerio de Salud viene realizando una Encuesta de Evaluación de los Servicios de las EPS. Para el año 2017 fue realizada a 24.586 personas de 95 municipios en 28 departamentos del país, así como en el Distrito Capital, buscando medir la oportunidad del servicio, la satisfacción de los usuarios, y los trámites de las empresas aseguradoras.

En el Régimen Contributivo las 10 mejores EPS según la encuesta reseñada fueron:

1. EPS Suramericana.
2. Aliansalud EPS.
3. Sánitas EPS.
4. Compensar EPS.

¹ El Plan Obligatorio de Salud, es el conjunto de servicios de atención en salud a los que tiene derecho un usuario, cuya finalidad es la protección de la salud, la prevención y curación de enfermedades, incluye el suministro de medicamentos para el afiliado y su grupo familiar junto al reconocimiento de indemnizaciones en caso de incapacidad por enfermedad y maternidad. La definición del POS estaba a cargo de la Comisión de Regulación en Salud (CRES) hasta diciembre de 2012 cuando dicha entidad fue liquidada y sus funciones fueron asumidas por el Ministerio de Salud y Protección Social.

5. Salud Total EPS.
6. Nueva EPS.
7. Coomeva EPS.
8. Famisanar EPS.
9. Servicio Occidental de Salud SOS EPS.
10. Comfenalco Valle EPS.

En cuanto al régimen subsidiado, las 10 mejores EPS para el 2018, resultaron ser:

1. Comfasucre.
2. CCF de La Guajira.
3. Comfacor.
4. Comfaorienté.
5. Coosalud EPS.
6. CCF Cajacopi Atlántico.
7. Ecoopsos ESS.
8. Ambuq ARS.
9. Comparta.
10. Asociación Mutual SER.

Las Mejores IPS

Según un estudio de Merco Salud, realizado en el año 2016 y presentado por DINERO (2016), las siguientes son las mejores 10 IPS (Clínicas y Hospitales) de Colombia:

1. Fundación Valle del Lili.
2. Fundación Santa Fe de Bogotá.
3. Hospital Pablo Tobón Uribe.
4. Fundación Cardio Infantil Instituto de Cardiología.
5. Centro Médico Imbanaco.
6. Hospital Universitario de San Vicente Fundación.
7. Fundación Clínica Shaio.
8. Fundación Cardiovascular de Colombia.
9. Clínica del Country.
10. Clínica de Marly.

La revista América Economía presentó un estudio de clínicas y hospitales en el que se muestra otro ranking de calidad para el 2017². Básicamente aparecen las mismas instituciones, en diferente orden.

Asuntos varios

Una estadística de interés en relación con el sector salud, tiene que ver con el número de hospitales y clínicas, y con cuantas camas están disponibles para atender a la población. DINERO (2016), nos señala que:

En el país existen cerca de 1.800 hospitales y clínicas, y de ellas casi 52% corresponde al sector público y el restante a instituciones privadas. En total suman unas 80.000 camas hospitalarias; es decir, que Colombia está entre 1,6 y 1,7 camas por cada mil habitantes, por debajo de la media de la región, cuyo indicador por el mismo número de habitantes se ubica en cerca de dos.

El sector salud en Colombia se financia en más del 75 % con recursos públicos, desafortunadamente los escándalos de corrupción son frecuentes. Jaime Arias, presidente ejecutivo de Asociación Colombiana de Empresas de Medicina Integral (Acemi), citado por DINERO (2017) indica que existen tres factores principales que hacen que el sector sea proclive a la corrupción:

- Por el sector salud pasa mucho dinero: \$50 billones al año.
- Es un sector muy fragmentado, descentralizado, repartido en todos los municipios del país que crea deficiencias en su control.

² <https://www.pulzo.com/economia/ranking-mejores-hospitales-colombia-2017-PP393641>

- Es “opaco” tanto en información técnica como en información financiera.
- Adicionalmente, Gabriel Mesa gerente general de EPS Sura y de la junta directiva de Acemi, citado por DINERO (2017), nos dice que entre las principales debilidades y retos que enfrenta el sector, se encuentran:
- La falta de transparencia en los aspectos financiero, calidad, servicios, derechos y deberes.
 - Falta de gobernanza de la información.
 - Debilidad de los sistemas de información.
 - Vigilancia y control poco efectivo.
 - Politización de la salud.

SUMIMEDICAL

Sumimedical es una entidad del sector salud en Colombia.

Cómo obtener más información

En términos de Inteligencia de Fuentes Abiertas (OSINT), es posible obtener información mucho más específica sobre esta empresa, sus directivos y su personal, siguiendo algunos procedimientos sencillos y legales. La información que es posible recolectar en las fuentes abiertas, da a quien investiga un perfil detallado del blanco, visibilizando posibles vulnerabilidades. Algunas fuentes de información abierta son:

- Se puede conocer lo que dice SUMIMEDICAL de si misma a través de su website: <http://www.sumimedical.com/>
- Sabemos que forma parte de una unión temporal, por lo que ese website también es de interés: <https://redvitalut.com/>
- También es importante conocer sobre su socio en la unión temporal: <http://www.ipsuniversitaria.com.co/es/>
- Se puede conocer lo que dicen otros sobre SUMIMEDICAL indagando en Internet. Colocando como criterio de búsqueda el nombre de la empresa y palabras como “problemas”, “quejas”, “reclamos”, “demanda”, “ente de control”, “felicitaciones”, “conmemoración”, “celebración”, entre otras.
- Es posible obtener el Número Único de Información Tributaria (NIT) de la empresa, escribiendo en Google SUMIMEDICAL+NIT. En los resultados de la búsqueda aparece el siguiente enlace: <https://redvitalut.com/politica-de-privacidad/> donde se señala que el NIT de SUMIMEDICAL es el **900.033.371-4**
- A partir del NIT se puede solicitar en Cámara de Comercio el Registro Mercantil de la empresa, de donde se obtendrán datos esenciales sobre su constitución, funcionamiento, y responsables.
- Otra posibilidad es consultar el Registro Único Empresarial y Social (RUES), de las Cámaras de Comercio de Colombia, donde a partir de un criterio de búsqueda, se obtendrá una información parcial tanto del Registro Mercantil (como el NIT), así como del Registro Único de Proponentes. http://versionanterior.rues.org.co/RUES_Web/Consultas
- Si en el Registro Mercantil aparece un representante legal, también estarán sus datos de identificación, tales como su número de Cédula de Ciudadanía (DNI), un dirección física, un número de teléfono y una dirección de e-mail. Estos datos a su vez permiten obtener más información.
- A partir del número de cédula (DNI), se pueden obtener datos en las siguientes entidades públicas:
 - Contraloría - Determinar si el sujeto es deudor moroso del Estado. <https://www.contraloria.gov.co/control-fiscal/responsabilidad-fiscal/certificado-de-antecedentes-fiscales/>
 - Procuraduría - Determinar si el sujeto posee antecedentes disciplinarios, penales, contractuales, fiscales y de pérdida de investidura (esto si es o ha sido funcionario público). <https://www.procuraduria.gov.co/porta/Antecedentes-disciplinarios.page>
 - Registraduría - En qué lugar vota y cual es su número de mesa de votación. Es usual que las personas voten muy cerca de su lugar de residencia. <https://www.registraduria.gov.co/>
 - Policía Nacional - Es posible conocer si la persona tiene antecedentes penales, o es requerido por una autoridad judicial. <https://antecedentes.policia.gov.co:7005/WebJudicial/>
 - SISBEN - Al consultar su nivel del Sisben se obtiene una confirmación del municipio de residencia, así como un indicio del estrato socioeconómico del sujeto del que se busca información. <https://www.sisben.gov.co/atencion-al-ciudadano/Paginas/consulta-del-puntaje.aspx>

- SIMIT (Sistema Integrado de información sobre Multas y sanciones por Infracciones de Tránsito). Si el sujeto tiene un vehículo y ha recibido alguna sanción, el sistema arrojará el número de placa del vehículo en cuestión. <https://consulta.simit.org.co/Simit/indexA.jsp>
- La rama judicial tiene un servicio de consulta, donde se puede saber si una persona o empresa está involucrado en algún proceso judicial activo, señalando el número del proceso correspondiente, la ciudad y departamento, así como el juzgado en el que se lleva dicho proceso. <https://procesojudicial.ramajudicial.gov.co/Justicia21/Administracion/Ciudadanos/frmConsulta.aspx> También hay servicios de pago que brindan esa información: <https://www.expedientes.co/> - <http://www.monolegal.co/> - <http://datajuridica.com/>
- En Colombia existen entidades que manejan información crediticia comercial y bancaria, a la que se podría acceder para obtener información de una persona de interés. En este caso se necesita de un tercero que esté afiliado al servicio de consulta.
 - Antecedentes historial crediticio comercial: <https://www.procreditoenlinea.com/servicio-procredito>
 - Antecedentes historial crediticio bancario: <https://www.datacredito.com.co/>
- Con el nombre completo del sujeto, el nombre de la empresa y su correo electrónico, se puede intentar obtener fotografías de las personas de interés, su familia y relacionados, a través de las distintas redes sociales, personales e institucionales, así como en la prensa.
- También se puede consultar en la Superintendencia de Industria y Comercio, sobre marcas, patentes, distintivos, que la empresa pudiese tener registrados. <http://www.sic.gov.co/consulta-de-base-de-datos>
- Otra fuente de información sobre las empresas, pueden ser las asociaciones y gremios del sector, tanto los websites oficiales, como sus redes sociales y publicaciones físicas o virtuales. Para el caso de SUMIMEDICAL, podrían ser: Asociación Colombiana de Empresas de Medicina Integral (ACEMI) <https://www.acemi.org.co/> y la Asociación Colombiana de Clínicas y Hospitales de Colombia (ACHC) <http://achc.org.co/>

Es importante entender claramente qué es lo que hace la empresa a la que se estudia, para ello son útiles el registro mercantil que se obtiene en Cámara de Comercio, la información del website oficial, así como las leyes que cobijan el sector. Es buena idea esquematizar las funciones medulares de la empresa, para así visualizar más fácilmente sus vulnerabilidades.

Se deben identificar las instalaciones físicas de la empresa. Para el caso de SUMIMEDICAL, cuáles son sus sedes y qué se hace en cada una de ellas. Las sedes físicas deben estar clasificadas de acuerdo a parámetros como: ciudad, tipo de instalación, cantidad de empleados que laboran allí, si es una sede gerencial, administrativa u operativa.

Sede Administrativa

Calle 33 # 74E-31

Sedes Operativas (Atención de Pacientes)

Sede Prado Cra. 45 #55-53

Sede Laureles Circular 3ª #74-52

Sede Envigado Cll. 37 sur #37-23

Sede Bello Cll. 44 # 49b – 90, Interior del hospital Marco Fidel Suárez.

Sede Caucasia Cra. 14A#21-15

Sede Turbo Cra 14B # 101 - 72 Barrio Baltazar

Sede Estadio Calle 47D # 70-113

Sede Argentina Calle 57 # 46 – 43

Sede Itagüí Cra. 49 # 51-40, 4º piso

Sede Rionegro Cra. 49 # 50 – 58, Locales 108 – 109

Sede Apartadó Carrera 106 C # 99 c 17 Barrio los Almendros

Sede Quibdó Cra. 1 # 26A-91, Barrio Roma

Sede Apoyo Terapéutico Calle 45e # 73-40

Servicios Farmacéuticos

Ed. Vicente Uribe Rendón, local 9908 carrera 46 #52-36

Activos de Información

Un Activo de Información, es el elemento de información que la Organización recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentre presente en forma impresa, escrita, en papel, transmitida por cualquier medio electrónico o almacenado en equipos de cómputo, incluyendo software, hardware, recurso humano, datos contenidos en registros, archivos, bases de datos, videos e imágenes. (Agencia Nacional de Defensa Jurídica del Estado 2016, p.3).

Para una organización del sector salud, como SUMIMEDICAL, los activos de información más valiosos son, a criterio del autor:

1. La historia clínica de los pacientes.
2. La base de datos de los pacientes con su información de contacto y datos personales.
3. El software operativo (donde el médico vacía la información médica de los pacientes).
4. El software administrativo (donde se controlan aspectos administrativos y financieros).
5. El Balance General.
6. El Estado de Pérdidas y Ganancias.
7. El Flujo de Caja.
8. El Inventario de Activos.
9. La base de datos de empleados y otro personal vinculado.
10. Los expedientes detallados de los empleados.
11. La nómina.
12. Las proyecciones de mercado.
13. Las decisiones estratégicas.
14. Los planes de corto, mediano y largo plazo.
15. Los datos de organización y análisis de los planes y medidas de seguridad física de las instalaciones.
16. Los datos de organización y análisis de los planes y medidas de seguridad de la información.

Estos activos de información deben ser clasificados de acuerdo a los criterios de Integridad, Confidencialidad y Disponibilidad, con el fin de que se les brinde la protección adecuada en el marco de la seguridad de la información.

A los efectos de este ejercicio académico, se tomará como referencia la metodología empleada por Colciencias (2016) en su manual de seguridad de la información, adaptándola a este ejercicio.

Clasificación de los Activos de Información

CONFIDENCIALIDAD		
Información	Individuo, entidad o proceso no autorizado accede al activo de información.	
Hardware	Alguien conoce que existe el elemento o su configuración o accede al activo sin autorización.	
Software	Individuo, entidad o proceso no autorizado conoce la existencia o parametrización del activo.	
Servicio	Alguien conoce su existencia o configuración o hace uso no autorizado del activo.	
Persona	Se hace uso inadecuado de la información privilegiada a la cual se tiene acceso por cargo o función que desempeña.	
Criterio	Descripción	Explicación
3	Alto	El conocimiento o divulgación no autorizada de la información que gestiona este activo impacta negativamente la imagen y el personal de SUMIMEDICAL.
2	Medio	El conocimiento o divulgación no autorizada de la información que gestiona este activo puede tener consecuencias moderadas que a corto plazo pueden perjudicar e impactar negativamente la misión y objetivos institucionales de SUMIMEDICAL.
1	Bajo	El conocimiento o divulgación no autorizada de la información puede ocasionar un impacto pequeño o inexistente a este activo y puede impactar negativamente la misión y los objetivos institucionales.

Tabla N° 1 Criterio de Confidencialidad para la Clasificación de los Activos de Información. Fuente: Adaptado de Colciencias (2016).

INTEGRIDAD		
Información	Se pierde la completitud, exactitud o precisión del activo de información. Ejemplo: Errores de procesamiento de los sistemas.	
Hardware	El activo no efectúa las actividades de procesamiento o su función correctamente o es alterada su configuración indebidamente. Ejemplo: cuando se daña un elemento o parte del activo o funciona inadecuadamente.	
Software	Se valora la completitud, exactitud o precisión de la parametrización del activo. Ejemplo: modificación la configuración del software lo que puede llevar a errores en la información a procesar.	
Servicio	Se valora la completitud, exactitud o precisión del servicio. Ejemplo: Que el servicio se presta en las condiciones óptimas y acordadas.	
Persona	La persona produce datos errados o incompletos o de acuerdo con su rol toma decisiones equivocadas, por capacidades o aptitudes inadecuadas para desempeñar el rol o función.	
Criterio	Descripción	Explicación
3	Alto	La pérdida de exactitud y estado completo del activo impacta negativamente la prestación del servicio de SUMIMEDICAL.
2	Medio	La pérdida de exactitud y estado completo del activo impacta negativamente no sólo a la misión, si no los objetivos institucionales de SUMIMEDICAL.
1	Bajo	La pérdida de exactitud y estado completo del activo puede tener un impacto pequeño o inexistente.

Tabla N° 2 Criterio de Integridad para la Clasificación de los Activos de Información. Fuente: Adaptado de Colciencias (2016).

DISPONIBILIDAD		
Información	No se puede acceder al activo de información por el personal que está autorizado.	
Hardware	No se puede acceder al activo de información por el personal que está autorizado.	
Software	No se puede acceder al activo de información por el personal que está autorizado.	
Servicio	No se puede acceder al activo de información por el personal que está autorizado.	
Persona	La persona no se encuentra disponible para el proceso.	
Criterio	Descripción	Explicación
3	Alto	La falta o no disponibilidad del activo de información impacta negativamente la prestación del servicio e impacta negativamente a SUMIMEDICAL.
2	Medio	La falta o no disponibilidad del activo de información impacta negativamente los procesos de SUMIMEDICAL.
1	Bajo	La falta o no disponibilidad del activo de información puede tener un impacto pequeño o inexistente.

Tabla N° 3 Criterio de Disponibilidad para la Clasificación de los Activos de Información. Fuente: Adaptado de Colciencias (2016).

De Acuerdo con esta guía, se procede a clasificar los activos de información antes especificados. Asignando en cada caso el valor numérico señalado en "criterio", los ítems que obtengan los puntajes más altos en un rango que va de 3 a 9, serán los activos más críticos dentro de dicho inventario. La norma de clasificación será la siguiente:

- Calificación total entre 3 y 4 el riesgo será BAJO.
- Calificación total entre 5 y 7 el riesgo será MEDIO.
- Calificación total entre 8 y 9 el riesgo será ALTO.

De acuerdo a los parámetros anteriores, se presenta la siguiente clasificación:

Activo de Información	Valoración			
	Confidencialidad	Integridad	Disponibilidad	Total
La historia clínica de los pacientes.	3	3	3	9
La base de datos de los pacientes con su información de contacto y datos personales.	3	3	3	9

El software operativo (donde el médico vacía la información médica de los pacientes).	2	3	3	8
El software administrativo (donde se controlan aspectos administrativos y financieros).	2	2	2	6
El Balance General.	1	1	1	3
El Estado de Pérdidas y Ganancias.	1	1	1	3
El Flujo de Caja.	1	1	1	3
El Inventario de Activos.	1	1	1	3
La base de datos de empleados y otro personal vinculado.	1	2	2	5
Los expedientes detallados de los empleados.	1	2	2	5
La nómina.	1	3	3	7
Las proyecciones de mercado.	1	1	1	3
Las decisiones estratégicas.	2	1	1	4
Los planes de corto, mediano y largo plazo.	2	1	1	4
Los datos de organización y análisis de los planes y medidas de seguridad física de las instalaciones.	3	2	3	8

Tabla N° 4 Clasificación de los Activos de Información de SUMIMEDICAL. Fuente: Elaboración propia (2018).

De este modo, tenemos que los activos de información críticos de SUMIMEDICAL, son:

- La historia clínica de los pacientes.
- La base de datos de los pacientes con su información de contacto y datos personales.
- El software operativo (donde el médico vacía la información médica de los pacientes).
- Los datos de organización y análisis de los planes y medidas de seguridad física de las instalaciones.

Medidas de Seguridad Propuestas

El análisis preliminar muestra que la información referida a los pacientes es el activo de información más delicado de SUMIMEDICAL, así como el software con el que esa información se ingresa, almacena, comparte (internamente) y se modifica. En torno a este activo de información -entendido como una base de datos virtual-, existen elementos de infraestructura física, hardware, redes informáticas, servicio de Internet, servicio eléctrico, y un personal con acceso directo a dicho activo.

También se considera crítico el activo de información representado por todos los datos referidos a la seguridad física de instalaciones.

De manera concurrente, si la información de la seguridad física cae en malas manos, un delincuente podría violar la seguridad de las instalaciones de la empresa, y de esta forma tener acceso directo o indirecto a los servidores, a los medios de almacenamiento, a los archivos y expedientes físicos, y a todos los bienes y recursos críticos de la organización.

De esta forma es necesario extremar la seguridad física de las instalaciones, así como la seguridad de las redes informáticas. Teniendo en cuenta especialmente las vulnerabilidades que presenta el recurso humano.

Principalmente se recomienda:

1. Incrementar las medidas de seguridad física, en todas las sedes de SUMIMEDICAL.
2. Incrementar las medidas de seguridad informática, para proteger especialmente los datos de los pacientes.
3. Capacitar continuamente al personal de SUMIMEDICAL, en cuanto a medidas de seguridad personal, familiar, y de seguridad de la información.
4. Asegurar que todos los procesos institucionales tengan trazabilidad, de manera de poder reconstruir las distintas acciones que incidan en los activos de información críticos. No solo para hallar culpables de errores o presuntos delitos, sino también como medida disuasiva.
5. Tomar todas las medidas necesarias para garantizar la confidencialidad, integridad y disponibilidad de los activos de información críticos, y con ello garantizar la continuidad del servicio que presta la empresa. Entre estas medidas, podemos destacar: tener generadores eléctricos auxiliares que permitan a los servidores informáticos, CCTV, sensores y alarmas, continuar funcionando; Invertir en modernos firewall que protejan las redes internas, y mantenerlos actualizados; Invertir permanentemente en la formación del personal de sistemas, para que se mantengan al tanto de las últimas novedades del sector, en especial en temas de seguridad de la información.

A modo de conclusión

En el desarrollo de este ejercicio académico, se pudo verificar que (en Colombia) es relativamente fácil recopilar información de empresas y personas. Lo que puede convertirse en una vulnerabilidad, en el entendido de que se pueden identificar los diferentes procesos, así como los activos de información críticos para la organización, con la intención de afectarlos de forma negativa.

En el caso de SUMIMEDICAL, encontramos que los activos de información críticos están referidos a su actividad medular: la prestación de servicios médicos. Se recomienda asegurar las instalaciones físicas, así como la información de los pacientes.

Es muy importante destacar lo fácil que es obtener información personal de alguien, y a través de esta información un tercero malintencionado puede abordarlo con el fin de tener acceso a información de la empresa. De esta forma, el ámbito personal y familiar puede poner en peligro la seguridad de la organización. Por ello, las capacitaciones sobre seguridad de la información, deben incluir -por ejemplo- medidas preventivas y conducta recomendada en redes sociales. Podemos imaginar que un empleado puede ser seducido, sobornado, extorsionado, secuestrado (él o sus familiares), amenazado o torturado, con el fin de proporcionar información confidencial sobre la empresa, su personal, o sus activos de información, también para proporcionar acceso no autorizado a las instalaciones.

Los empleados deben estar instruidos para tomar medidas preventivas en su vida privada, para que esta no afecte la seguridad de la organización donde labora.

Referencias:

- Agencia Nacional de Defensa Jurídica del Estado (2016). *Guía de Inventario de Activos, Clasificación y Publicación de Información*. Recurso en línea, consultado el 4 de julio de 2018. Disponible en: https://www.defensajuridica.gov.co/servicios-al-ciudadano/ley_transparencia/Documents/guia_inventario_activos_clasificacion_publicacion_de_informacion_130916.pdf
- ANDI (2016). *Contexto actual del Sector Salud en Colombia*. Recurso en línea, consultado el 2 de julio de 2018. Disponible en: <https://encolombia.com/economia/economiacolombiana/sector-salud/informe-sostenibilidad/contexto-sector-salud/>
- Colciencias (2016). *Manual Inventario de Activos, Clasificación, y Publicación de la Información*. Recurso en línea, consultado el 1 de julio de 2018. Disponible en: http://www.colciencias.gov.co/sites/default/files/upload/paginas/g104m02-manual-de-activos-de_informacion.pdf
- DINERO (2016). *Las mejores IPS de Colombia en 2016*. Recurso en línea, consultado el 2 de julio de 2018. Disponible en: <https://www.dinero.com/edicion-impresa/informe-especial/articulo/las-mejores-ips-de-colombia-en-2016/238782>
- DINERO (2017). "Los recursos públicos son sagrados, pero más los de la salud": gerente EPS Sura. Recurso en línea, consultado el 2 de julio de 2018. Disponible en: <https://www.dinero.com/pais/articulo/corrupcion-en-el-sector-de-la-salud-en-colombia/243376>
- El Tiempo (2018). *Estas son las mejores EPS de Colombia, según encuesta*. Recurso en línea, consultado el 2 de julio de 2018. Disponible en: <http://www.eltiempo.com/vida/salud/ranking-de-las-mejores-eps-de-colombia-en-2018-196510>
- Santa María, M., García, F., Rozo, S., y Uribe, M. (2007). *Un diagnostico general del sector salud en Colombia: Evolución, contexto y principales retos de un sistema en transformación*. Recurso en línea, consultado el 2 de julio de 2018. Disponible en: http://www.med-informatica.net/FMC_CMCB/VeeduriaCiudadana/CIDMEDvcacelapss/SaludRetosRegulacion_MauricioSantamaria_cap1_final.pdf
- Fuente de la Imagen: <http://www.esan.edu.pe/apuntes-empresariales/2016/05/13/seguridadmayoprincipal.jpg>

Douglas Hernández

(Colombia) Fundador y director del website www.fuerzasmilitares.org, ejerce como periodista especializado en seguridad y defensa. Es colaborador de la Air and Space Power Journal -revista institucional de la USAF-, y de la revista brasilera Segurança & Defesa. Es Sociólogo y Magister en Educación de la Universidad de Antioquia (Medellín, Colombia), estudiante de Doctorado. Posee un Diplomado en Relaciones Internacionales.



Autoadocinamiento: Yihad Mediática

Por Montserrat López Melero (España)



Resumen

Este artículo pretende ilustrar la posibilidad de una radicalización del terrorismo yihadista a través de las redes sociales. Se enfoca a través de una sentencia de la Audiencia Nacional de España –39/2016, de 30 de noviembre- tras la reforma del Código Penal en el 2015. El objeto de investigación es un nuevo enfoque de la radicalización hacia una red terrorista, radicalización como proceso de transformación para adoptar ideas islamistas radicales, con una ideología extremista, con efectos negativos y desalentadores.

Palabras clave: Autoadocinamiento; Terrorismo yihadista; Radicalización; Yihad mediática.

Introducción

La incorporación a la organización terrorista del autodenominado Estado Islámico a través de las redes sociales no es novedad, lo que se está introduciendo es el método de la radicalización, el deseo de participación de algunos individuos al movimiento yihadista ha dado lugar en España, por vez primera, a lo que se ha denominado como *yihad mediática*, autoadocinamiento. Una radicalización a través de las nuevas tecnologías es, por ello, importante y especialmente comprender este nuevo fenómeno de involucración.

Concepto de radicalización:

Podemos definir la *radicalización* como el proceso de adopción de un sistema de valores o creencias extremistas incluyendo la disposición de usar, apoyar o facilitar la violencia como método para llevar a cabo algo cambio social. La Comisión Europea define la *radicalización* como el fenómeno en virtud de cual las personas se adhieren a opiniones, puntos de vista e ideas que pueden conducirles a cometer actos terroristas³.

Es la Policía Canadiense Real⁴ la que establece una definición al fenómeno, entendiéndolo como “una previa exposición de los individuos a determinados mensajes ideológicos y la posterior aceptación por parte de estos

³ Comisión de las Comunidades Europea, Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre la captación de terroristas, “Afrontar los factores que contribuyen a la radicalización violenta”, Bruselas, 21 de septiembre de 2005, COM, 2005, p. 2.

⁴ National Security Criminal Investigations, *Radicalization: A Guide for the Perplexed*, Hereinafter, Royal Canadian Mounted Police, 2009.

de creencias procedentes de visiones extremistas.” Ahora bien, es uno de los Comités del Senado de EEUU en 2007 (*Senate Committee on Homeland Security and Governmental Affairs*) el que realmente vincula el término de radicalización con conducta antisocial y, por tanto, con la posibilidad de una conducta y comportamiento violentos, así asevera que la radicalización “implica el proceso de adopción de un sistema de creencias extremistas, incluyendo la voluntad de utilizar, apoyar o facilitar la violencia, como un método para lograr el cambio social”⁵. De esta definición, se deduce que el proceso de radicalización ha de tener un proceso en etapas, y una duración en el tiempo, durante el cual el sujeto, caracterizado por una falta de madurez psicológica, está expuesto a creencias, a merced de su voluntad, a través de las redes sociales. Afinando un poco más la cuestión, se plantea que pueden darse dos posibilidades en la radicalización, de un lado, aquellos sujetos que ya tienen raíces en Occidente, pero por factores, como la frustración en la sociedad, se ven inmersos en un proceso de radicalización y, por otro lado, aquellos que teniendo ya un comportamiento radical llevan su conducta al país donde llega su fin como objetivo⁶. En ambas situaciones, hay un periodo de tiempo y de espacio, en la mayoría de ellos, acompañados de un intermediario que les guía sobre cómo finalizar una etapa y cómo, y cuándo, iniciar la siguiente, así le informa de cuándo está preparado para el acto final. Como estudiaremos, en el autoadoctrinamiento no existe tal figura, pero no por ello quiere decir que se esté cometiendo errores en las fases de radicalización, las pautas las pone uno mismo. La radicalización es un proceso y no un estado.

Existen diversos estudios de radicalización en España, pero escasos respecto al *autoadoctrinamiento*. Los estudios españoles han abordado la yihad individual cuando son las organizaciones terroristas las que llaman a la acción, las que captan a sus nuevos integrantes a través de las redes sociales, una modalidad de reclutamiento. Paralelamente se han abordado cuestiones relativas a la estrategia de la organización terrorista, especialmente al *Daésh*, en cuanto a la utilización de internet, como principal medio de difusión de sus ideas. No obstante, se afirma, que existía una mayor preocupación por las causas de los conflictos violentos, que no se incluían estudios o estrategias sobre la radicalización y el reclutamiento⁷.

Ahora bien, la Sentencia de la Audiencia Nacional 39/2016, de 30 de noviembre, es el primer precedente en la doctrina jurisprudencial española sobre el autoadoctrinamiento, se fundamenta que sigue siendo “atractiva” la idea de la yihad individual para las organizaciones terroristas, si bien, el método de captación es diferente, a través de mensajes específicos, ideas abrumadoras en las redes sociales, se produce una nueva estrategia de adoctrinamiento. Se determina que las redes sociales siguen siendo el principal operador o fuente de captación en los procesos de radicalización, afirmando que las redes sociales virtuales son totalmente eficaces y efectivas para formar actores terroristas.

Estamos, por tanto, ante los nuevos *lobos solitarios*, denominados *radical solitario* por Wiktorowicz⁸, el autor afirma que no es el perfil que más predomine en el proceso de radicalización, o como acertadamente se indica *virtual self- recruitment*⁹. Es decir, una manera autodidacta de acometer el proceso de radicalización hacia la violencia fundamentalmente a través de los numerosos recursos que la red ofrece¹⁰. Marc Sageman¹¹, manifestó que los lobos solitarios eran “jóvenes radicalizados a través de Internet que están dispuestos a sacrificar sus vidas por una causa sin haber tenido una relación orgánica, bien con Al Qaida Central o bien con grupos terroristas yihadistas salafistas afiliados o próximos a ella”. La psicología del hombre va un paso más allá, a través de las redes sociales de internet es posible el autoadoctrinamiento. Lo que significa que cuenta con cierta estrategia en la comunicación.

⁵ Senate Committee on Homeland Security and Governmental Affairs, “Threat of Islamic Radicalization to the Homeland,” 110 th Cong., 1 st sess., March 14, 2007, p. 4.

⁶ CANO, M.A., *Generación Yihad. La radicalización islamista de los jóvenes musulmanes en Europa*, Dykinson, Madrid, 2010, p. 64.

⁷ ROGELIO ALONSO, P., “Procesos de radicalización y reclutamiento en las redes de terrorismo yihadista”, *Cuadernos de Estrategia*, nº 141, La Inteligencia, factor clave frente al terrorismo internacional, Ministerio de Defensa, Instituto español de estudios estratégicos, Centro Nacional de Inteligencia, 2009, p. 21.

⁸ QUINTAN, WIKTOROWICZ. “*Islamic Activism. A Social Movement Theory*”, Bloomington, Indiana University Press, 2004, pp. 1-33.

⁹ NEUMANN, PETER, ROGERS, BROOKE, ALONSO, ROGELIO Y MARTINEZ, LUIS. «*Recruitment and Mobilisation for the Islamist Militant Movement in Europe*», King’s College London, diciembre de 2007, pp. 87-90.

¹⁰ ROGELIO ALONSO, P., “Procesos de radicalización y reclutamiento en las redes de terrorismo yihadista”, *Cuadernos de Estrategia*, nº 141, La Inteligencia, factor clave frente al terrorismo internacional, Ministerio de Defensa, Instituto español de estudios estratégicos, Centro Nacional de Inteligencia, 2009, p. 37.

¹¹ SAEGEMAN, M., *Leaderless Jihad*, University of Pennsylvania Press, 2008, p. 5.

Premisas del autoadoctrinamiento:

En base a los informes de expertos antiterroristas, la importancia de Facebook en la captación y radicalización es elevada, además de que “son rápidas, eficaces y llegan a todas partes en especial a la gente joven”¹². Teniendo en cuenta la definición de radicalización de la Comisión y adaptándola al autoadoctrinamiento se pueden señalar las siguientes premisas:

- a) Se trata de un fenómeno novedoso en el método. El sujeto asume unas ideas extremistas terroristas, las justifica y acepta la justificación dada por la organización terrorista.
- b) Se trata de un fenómeno en auge. Se puede señalar que no era un fenómeno que prevalecía en el ámbito español. Hay que tener en cuenta el contenido del mensaje y la puesta en escena del mismo. Las organizaciones terroristas tienen especial cuidado en la puesta en escena, pero el que se autoadoctrina no repara en plasmar sus emociones a través de internet.
- c) El proceso de autoadoctrinamiento es evolutivo. Tiene unas fases en las que el sujeto cada vez tiene una conducta más agresiva, dirigidos a hacer realidad su convicción. Requiere una temporalidad en el que la intensidad va variando en deseos y/o en vulnerabilidad. La neutralización por parte de la organización terrorista no es imposible pero sí improbable.

A lo anteriormente indicado, se ha de añadir las siguientes características: las imágenes que se utilizan; la música salmódica que le acompaña; y según la sentencia citada, se califican como vibrantes y enardecedores; los tonos de voz en los discursos, el método y las técnicas agresivos utilizados en los vídeos, los flashes intercalados. Todo ello permite, a la doctrina jurisprudencial, afirmar que “sigue el proceso de adoctrinamiento a través de las redes diseñado por Estado Islámico (E.I.), inspirado en los principios promulgados por el líder de Al Qaeda en su fatua Frente Islámico Mundial para la Yihad contra judíos y cruzados, y en el libro *Llamada a la resistencia Islámica Mundial*, que aboga por la acción de activistas solitarios, [...] con un programa de adoctrinamiento que desarrolla en los jóvenes musulmanes un estado mental que los avoca al activismo militante”¹³.

Se trata de analizar la influencia de las redes sociales en los jóvenes, existen diversos estudios entre los que cabe mencionar a Christakis y Fowler¹⁴, demuestra que los adoctrinados por la vía de redes virtuales pueden ser aún más peligrosos, en cuanto a ideas y en cuanto a la obligación de imposición de las mismas a todos los ciudadanos, incluso, a lo que hay que añadir que es más difícil o se le añade la dificultad en cuanto a control de los mismos.

Es necesario señalar las etapas por las que se pasa para demostrar que en el caso de autoadoctrinamiento en España el sujeto ha pasado por todas: el victimismo, culpabilización, solución y activismo.

Victimismo. Caracterizado porque “se inculca en el musulmán la idea de que toda la *umma* (comunidad de fieles) es víctima de las acciones que ejerce Occidente. Es esa fase en la que hay una mayor presencia de los fieles en las ideas del terrorismo islamista, ideas aceptadas”. Desde el punto de vista social y cultural, es acertada e interesante la reflexión de Giovanni Sartori, aunque si bien lo hace respecto de la televisión, asevera que “[...] ésta no es sólo un mero instrumento de comunicación, sino que también es un instrumento antropogénico: un medio capaz de generar un nuevo tipo de ser humano”¹⁵; es decir, hay una asimilación de conceptos, hay un conocimiento de una “realidad” proyectada a través de imágenes que “arrinconan al razonamiento abstracto y la reflexión crítica”¹⁶, es una manera o instrumento sutil de transformar al individuo y la vida en sociedad. No obstante, es más acertada la denominación de *cultura de la virtualidad real*, afirmada por Castells¹⁷, es decir, lo virtual se está convirtiendo en una realidad para nosotros.

Desde la Victimología, hablamos de una víctima con tolerancia a la actitud de los terroristas; es Dussel¹⁸ quien asevera que “toda tendencia fundamentalista tiene un componente de intolerancia, la aceptación del otro en la verdad dogmática es el fruto de la derrota en una guerra fundamentalista; y se pretende ser una *guerra justa* en

¹² <http://www.elconfidencialdigital.com/seguridad/fabricar-yihadista>

¹³ Sentencia AN, 39/2016, de 30 de noviembre, fj. 3.

¹⁴ CHRISTAKIS, N.A y FOWLER, J.H., *Conectados*, Taurus, Barcelona, 2010, pp. 17-46.

¹⁵ SARTORI, G., *Homo videns. La sociedad teledirigida*, Taurus, Madrid, 1998, p. 36.

¹⁶ SARTORI, G., *Homo videns. La sociedad teledirigida*, Taurus, Madrid, 1998, p. 36.

¹⁷ CASTELLS, M., *La galaxia Internet*, Areté, Barcelona, 2001, p. 230.

¹⁸ Dussel, E., *Deconstrucción del concepto «tolerancia»*, 2006, p. 2. Disponible en <http://www.afyl.org/info.html>

tanto opina que es guerra en defensa y propagación de la verdad (sea revelada, cultural, etc.) del grupo triunfador". M. Akaarir no ha nacido yihadista, pero tiene un perfil victimológico que es aprovechado por los captores convirtiéndose en el objetivo perfecto para ser radicalizado.

La *culpabilización*, es aquella en la que el sujeto está en la posición mental de que se equipara al musulmán, no se identifica con las víctimas. Se considera mal musulmán, y tiene asumido los postulados del autodenominado Estado Islámico, es la fase en la que el sujeto es un instrumento de proclamación de los mensajes, haciendo suyo los mensajes, comparte la causa, comparte imágenes y las difunde por la red social internet. Aquí ya se observa el posicionamiento, deja atrás sus ideas e incluso el idioma en el que normalmente habla en sociedad pudiéndose cambiar por el árabe.

La *solución*, en la que ante la frustración a todo lo que está haciendo en Occidente, pretende y necesita establecer una solución en base a una reivindicación social. Los sujetos que llegan a esta etapa ven como solución la violencia contra todos aquellos que son considerados como infieles.

Y la etapa de *activismo*, aquella en que la violencia está justificada y el sujeto está preparado para matar y para morir por la causa.

Enfoque

Al abordar el tema, se vislumbra un problema fundamental, en el autoadoctrinamiento existen *auto fases*. Nuestra legislación penal castiga a quienes se *adiestran o adoctrinan de manera autónoma*, es el 575.2 del Código Penal que dictamina que: "[...] Se entenderá que comete este delito quien, con tal finalidad, acceda de manera habitual a uno o varios servicios de comunicación accesibles al público en línea o contenidos accesibles a través de internet o de un servicio de comunicaciones electrónicas cuyos contenidos estén dirigidos o resulten idóneos para incitar a la incorporación a una organización o grupo terrorista, o a colaborar con cualquiera de ellos o en sus fines. [...] quien, con la misma finalidad, adquiera o tenga en su poder documentos que estén dirigidos o, por su contenido, resulten idóneos para incitar a la incorporación a una organización o grupo terrorista o a colaborar con cualquiera de ellos o en sus fines".

Ha quedado demostrado que desde febrero de 2015 hasta abril de 2016 (fecha en la que fue detenido Akaarir) accedió, de forma repetida, "a ciertas páginas de internet con contenido yihadista radical violento difusoras de los fines del Estado Islámico", la mayoría de las cosas que leía las aceptaba, las guardaba, e incluso las publicaba en su muro de Facebook.

Análisis

Respecto a la etapa de *victimismo*, Akaarir se caracteriza por el excesivo tiempo buscando y captando información del terrorismo yihadista en las redes sociales. La sentencia indica que "había superado ya la inicial fase de victimismo [...] (El musulmán es una víctima) a este periodo corresponde la búsqueda, visión, guarda y publicación de vídeos y mensajes en el que se muestra el sufrimiento de niños musulmanes o el trato que se da a las minorías musulmanas en sus países por los países de occidente, o el trato a aquéllas en sus colonias". A esta primera etapa corresponde los siguientes mensajes del acusado:

- Publicó fotografías de varios policías golpeando a un musulmán, y un solar con cadáveres calcinados. Ambas fotografías llevaban de origen la misma leyenda (en árabe) "así está la situación de los musulmanes en Burma. El Profeta de Allah dice que quien no se preocupa por la situación de los musulmanes no es musulmán. Pido tu promesa por Allah de que si ves esta Imagen dale a compartir para que llegue a los demás. Comparte la causa".
- Publicó una fotografía, un musulmán en posición de oración sobre su espalda, de rodillas y las manos juntas, un cristiano en posición de oración, y de pié sobre los hombros de este último, un judío con un libro la mano. Este dibujo lleva en árabe, una leyenda, dice "Este dibujo es un trabajo que lo ha hecho un artista español. Se cabrearon los judíos, aunque están por encima de los cristianos y el Islam por debajo. Porque saben que cuando se levante el musulmán se caerán todas las demás religiones" "Que Dios le valore al islam y a los musulmanes. El musulmán que diga amén".
- El 15 de septiembre de 2015, publicó un video, tomado de la página de Amer Kharat Kiwan procedente de #FreeSyria.
- Publicó un video cogido de la página HIBAPRESS añadiéndole el comentario "Mira como tratan y castigan los musulmanes en Bangladesh, compartir este video para que lo vea todo el mundo". Las fotografías de la página Khalid Rofking Orgullo; la foto del presidente sirio cubierto de sangre con un

hacha de carnicero en la mano, junto a niños y mujeres muertas, la leyenda "250.000 + syrian Killed. Since 2011 Uprising. Syrian are besieged, bereaved, displaced, bombed, gassed, sniped, massacred, detained, tortured, raped, mutilated, starved, by Saturnino Regime for almost 4 years [...] Word remains silence". En árabe, "se pide a todos los amigos compartir la foto de este asesino en las páginas del Facebook y hacer muchos comentarios para llenar a Facebook [...] Para este asesino". Este video recibió críticas de usuarios puesto que se demostró que las imágenes no corresponden a España, sino a un país latinoamericano; mensajes en árabe "Alá es grande" "Los judíos odian la palabra Allah es Grande. ¿Cuánta gente odia a los judíos? Que escriban "Allah es Grande" "Allah es Grande, Allah es Grande." "Allah llévanos al paraíso para encontrar pan". Otras imágenes se intercalan con flashes de imágenes de guerra: bombas sobre una mezquita, imágenes de niños muertos. Hombres arrastrando y golpeando a dos mujeres, niños muertos. Una persona, con la cara cubierta con un trapo, enterrada viva hasta el cuello. Imágenes de un helicóptero abatido con guerreros triunfantes, armados, sobre él. Todo ello, acompañado de música salmódica; publicó un vídeo de repudio de los Chiies, imágenes de individuos autoflagelándose y la leyenda "Nosotros los repudiamos ante Allah. Nos distanciamos de este dicho ante Allah. No son nuestros hermanos. Son los hermanos de Satanás", se le añadió la leyenda "Para el que quiera saber quiénes son los malditos chiyis".

- Publica un video con el título "Nasheed en uno de los momentos dice: "Si nuestro sol se convierte en el oscurecimiento, si nuestra tierra se convierte en cenizas, sí intimidan a nuestro pueblo bajo el gatillo, si creen que somos un grupo débil, lo juro, lo juro, lo juro, nos van a encontrar en cada rio, en ese momento se van a subir unas banderas, las banderas de la yihad" los guardó y publicó en su muro añadiéndole el comentario siguiente en árabe "El mejor nasheed del yihad. Allah nos hará ganar y no perder".

Se concluye de esta primera etapa, que en primer lugar las intervenciones en el muro de su Facebook eran esporádicas, convirtiéndose, posteriormente en una mayor presencia en la red, con mensajes más frecuentes y con imágenes más violentas, sangrientas, y existe un progresivo cambio en los comentarios, son en castellano y de construir las frases en tercera persona se empieza a hacer en segunda persona. Esta etapa supone la *cultura de la virtualidad real*, es fundamental, desde el punto de vista de la Criminología, ya que de ella se extrae una peculiar conducta del sujeto que se traduce en perfil de la personalidad, supone un amplio campo de estudio para la ciencia empírica de la Criminología, ya que supone esa parte en la que se está construyendo la identidad de cada sujeto, en el que las nuevas tecnologías influyen de forma acelerada sin necesidad de que exista interacción personal y/o directa, o al menos esa interacción ya no tiene relevancia ni importancia en el proceso de radicalización.

En cuanto a la segunda etapa, la *culpabilización*, la Sentencia de la Audiencia Nacional, manifiesta que es aquella en la que Akaarir se equipara al musulmán que no se identifica con las víctimas y que no "ayuda" mediante la difusión en la red de esta "situación de masacre" como un mal musulmán. Hay un claro posicionamiento del sujeto, donde de forma indirecta impone órdenes a los demás, así ante un vídeo de dos menores jugando, y la imagen de sus cadáveres al lado, escribe "no salgas antes de decir Que Allah les perdone, [...]". Es a partir de aquí, cuando deja su castellano en los mensajes y comienza con el árabe, asume los principios y valores del *Daésh*, muestra su incondicional apoyo a través de los mensajes. La sentencia de la Audiencia asevera, acertadamente, que "Así, se podría llegar a considerar que Akaarir está realizando a su manera la *yihad mediática*", además, "se tipifica la conducta del autodidacta, que por sí mismo lleva a cabo su adiestramiento o adoctrinamiento de manera autónoma"¹⁹.

En la tercera etapa, *solución*, el odio que tiene hacia los europeos se convierte en una solución práctica para el sujeto. Dicta la sentencia que "Sobre la base, general, de la frustración existente dentro de la comunidad musulmana no solo motivada por unas deficientes perspectivas económicas (frustración por sentirse menospreciados) sino también por la reivindicación social de unos derechos en materia de libertad religiosa que consideran que no se han respetado [...] muestra unas claras simpatías por grupos terroristas, se embebe de su ideario y lo busca en las redes sociales".

Y, por último, en el *activismo*, en el que se justifica la violencia y se prepara para la muerte, escribe con el grito de guerra yihadista (*Allah'akbar Allah!*), es aquí, con esta fase, cuando el acusado recoge de forma directa mensajes procedente del *Daésh*, así como plasma videos de preparación para la muerte, caracterizada por ser

¹⁹ Sentencia AN, 39/2016, de 30 de noviembre, fj. 3.

heroica, asume y desea la muerte por sus ideas y principios; apoyad el vídeo con "no hay Dios más poderoso que Allah "para que no lo quiten" incluyendo en árabe la leyenda "Alaho akbar alah" "estamos en la guerra Santa la tercera guerra mundial contra el Islam 80 países contra un Estado: Irak y siria".

Las investigaciones en el Facebook demuestran que siempre subía sus comentarios en favor del terrorismo yihadista por la noche y durante los fines de semana. Comentarios denunciando la masacre de los chiíes a musulmanes suníes, sobre la situación de los palestinos en Gaza, eran comunes y frecuentes. La decisión que toma es individual, pese a que está influenciada por un grupo. Existe una lealtad absoluta, que proviene de una imposición indirecta, no es reclamada por los integrantes. Por lo que, como manifiesta Alonso Pascual, no se imponen sobre ellos mecanismos de desindividuación que contribuyan a subyugar su personalidad²⁰.

Si bien, internet juega un papel fundamental en el proceso de radicalización. Pudiendo llegar a ser la única fuente para ser radicalizado, como en la presente sentencia objeto de análisis. Se afirma, en este sentido, que este *grupo social* (los jóvenes) se alimenta de información, casi exclusivamente, en la red, de ahí que los radicalizadores, sabedores de ello y quizás tan jóvenes como los propios radicalizados la utilicen en consecuencia²¹.

Conclusiones

Varias son las conclusiones que se pueden extraer del análisis de la sentencia. En primer lugar, se comprueba que la radicalización yihadista abarca mucho más que el proceso inicial, se centra en mecanismos de redes sociales que influyen en la psicología individual, y se ha demostrado que es una figura atractiva de participación, y cómoda, si bien la participación puede ser inestable en cuanto a proceso y en cuanto a radicalización. El grado de implicación variará según la personalidad de los sujetos, y será gradual en función de la implicación con el tiempo en las ideas radicales de los miembros de la organización terrorista. Se demuestra que la radicalización es un estado y proceso secuencial pudiendo ser sólida, eficaz, efectiva y duradero o permanente.

La yihad mediática es un proceso de radicalización peculiar y particular de reclutamiento que puede no tener ningún tipo de éxito, especialmente si tenemos en cuenta las primeras fases del fenómeno. El compromiso del "futuro recluta" dependerá de la personalidad del mismo, no siempre estaremos ante esta transformación desalentadora, ahora sí demuestra la autonomía que tienen algunos sujetos en aceptar ideas radicales y tener una sobre estimulación adecuada para tener la influencia de la organización terrorista en todo el proceso de radicalización.

Fuente de la Imagen: <http://www.jewishpress.com/wp-content/uploads/social-media.jpg>

Montserrat López Melero

(España) Doctora en Derecho UAH. Profesora Acreditada Derecho Penal y Grado de Criminología UNIR.

²⁰ ROGELIO ALONSO, P., "Procesos de radicalización y reclutamiento en las redes de terrorismo yihadista", en Cuadernos de Estrategia, nº 141, La Inteligencia, factor clave frente al terrorismo internacional, Ministerio de Defensa, Instituto español de estudios estratégicos, Centro Nacional de Inteligencia, 2009, p. 36.

²¹ http://politica.elpais.com/politica/2014/08/07/actualidad/1407436014_813390.html, 7, Agosto, 2014

Fuerzas Antiterroristas del Mundo

Audentes fortuna iuvat



Arabia Saudí Fuerzas Especiales de Seguridad

El 12 de mayo de 2003, un grupo de militantes de al-Qaeda, fuertemente armados, ingresaron por la fuerza a complejos residenciales en Riad, matando a 36 personas, incluyendo a 9 estadounidenses. Este asalto dio paso a una oleada de terrorismo, que se manifestó con atentados con carro bomba, asesinatos selectivos, y ataques suicidas. Arabia Saudita venía de una década de relativa calma, por lo que estos sucesos fueron más estremecedores. En el año 2004 los ataques alcanzaron su clímax, dando como resultado la muerte de más de 60 personas, entre ellos varios extranjeros.

Esta campaña de violencia terrorista, habría sido orquestada por militantes de al-Qaeda, con el objetivo de desestabilizar al país y afectar/derrocar a la monarquía saudita. El gobierno de este país respondió al reto, fortaleciendo sus Fuerzas Especiales de Seguridad, estos son equipos antiterroristas, organizados, entrenados y equipados para hacer frente a este fenómeno. Operan bajo la dirección del Ministerio del Interior.

De esta forma, durante los tres años siguientes, las Fuerzas Especiales de Seguridad se enfrentaron a los militantes de al-Qaeda en las zonas urbanas del país, debilitando todas sus estructuras, hasta dar con la captura y ejecución del jefe de esa organización en Arabia Saudita.

Durante ese periodo intenso hubo muchas lecciones aprendidas, que ahora hacen parte del plan de estudios de las Fuerzas Especiales de Seguridad de Arabia Saudita, que ahora sumas unos 10.000 hombres, distribuidos en lugares estratégicos del país.

Los miembros de las FES, deben pasar por un entrenamiento bastante riguroso, que está diseñado para preparar a los comandos para cualquier contingencia que pueda presentarse en el curso de las operaciones,



que van desde la protección de convoyes VIP, respondiendo contundentemente a los agresores, hasta la búsqueda y recuperación de rehenes en poder de elementos hostiles, asaltos a todo tipo de instalaciones, desactivación de bombas y artefactos explosivos improvisados, operaciones aerotransportadas y de paracaidismo, tiro de precisión, y vigilancia humana y/o electrónica.



Las instalaciones de entrenamiento cuentan con una cancha de asalto urbano, consistente en una estructura cuyas paredes son ajustables para simular distintas configuraciones. A un lado hay un fuselaje completo de un avión de pasajeros para que los comandos puedan practicar tácticas, técnicas y procedimiento contra la interferencia ilícita (secuestro de aeronaves). También hay pistas que semejan el fuselaje de helicópteros, desde las que los comando practican las operaciones helicoportadas. Hay unas torres elevadas desde las que practican rapel y asalto aéreo. También hay lugares designados para entrenar el combate cuerpo a cuerpo. Ha trascendido que el entrenamiento militar básico dura tres meses, luego del cual sigue otro mes de capacitación básica de seguridad. Entonces los comandos en formación son seleccionados para especializarse en distintos aspectos de las Fuerzas Especiales. Dependiendo de la especialización, esta puede durar desde dos meses, hasta siete.

Todo el personal recibe un entrenamiento bastante extenso en el tema de los explosivos. En especial lo referido a los artefactos explosivos improvisados y las trampas explosivas. Entre las lecciones aprendidas que se han incorporado al entrenamiento de las Fuerzas Especiales de Seguridad de Arabia Saudita, está precisamente el empleo por las organizaciones terroristas, de objetos cotidianos y de apariencia inocente para activar potentes y mortales explosivos. Esto va desde abrir un libro (un Corán), mover un maletín, recoger un objeto del piso, abrir una puerta, enderezar un cuadro de la pared, recoger un osito de peluche, encender una luz, entre otros. Resulta que la sociedad saudí está fuertemente segregada según el género. Esto afecta todos los órdenes de la sociedad, incluyendo a las fuerzas de seguridad. De este modo hay mujeres en la policía que se encargan de los asuntos que competen a las mujeres, y policías hombres que atienden los asuntos que involucran a los hombres. Sin embargo, al parecer no hay mujeres comandos en el seno de las Fuerzas Especiales de Seguridad.



MITIGA RIESGOS EN TU ORGANIZACIÓN

ANTES, DURANTE Y DESPUÉS

IMPLEMENTA CONTROLES QUE REDUZCAN LOS RIESGOS

Auditorias e implementación de estándares en seguridad física, electrónica, de la información, realización de visitas domiciliarias, verificación de antecedentes, pruebas de lealtad, poligrafía pre-emplero y específica. Investigaciones.

MÁS QUE CONSULTORES, SOMOS TUS ASESORES DE CONFIANZA

PREGUNTA POR LOS PAQUETES EMPRESARIALES Y KIT PYME TOTAL

contáctanos info@mastersecurityconsulting.com

+57 3165479295