XXVII Curso Internacional de Defensa

Amenaza híbrida

La guerra imprevisible

Jaca. 30 de septiembre a 4 de octubre. 2019

MINISTERIO DE DEFENSA

CÁTEDRA "MIGUEL DE CERVANTES"

XXVII Curso Internacional de Defensa
Jaca, del 30 de septiembre
al 4 de octubre de 2019

Amenaza híbrida
La guerra imprevisible

Dirigido por la «Cátedra Miguel de Cervantes»
Academia General Militar – Universidad de Zaragoza

MINISTERIO DE DEFENSA

CATÁLOGO GENERAL DE PUBLICACIONES OFICIALES
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

NIPO: 083-20-052-3 (edición en línea)
NIPO: 083-20-051-8 (impresión bajo demanda)
ISBN: 978-84-9091-465-6

Fecha de edición: mayo 2020

Maqueta e imprime: Ministerio de Defensa

https://publicaciones.defensa.gob.es/

ÍNDICE

Índice

Página

Página

Página

PRESENTACIÓN

PRESENTACIÓN

D. MIGUEL ÁNGEL SANTAMARÍA VILLASCUERNA
Coronel director de la Cátedra Cervantes

Finalizada la XXVII edición del Curso Internacional de Defensa y gracias a la favorable disposición de ponentes y comunicantes, hemos querido plasmar en este libro de actas las diferentes exposiciones realizadas, con la esperanza de que las mismas puedan servir como material de consulta a los asistentes o incluso a aquellos otros que no pudieron asistir, colaborando con ello a la difusión de la cultura de seguridad y defensa.

En esta ocasión hemos querido dedicar este curso a tratar el tema: «Amenaza híbrida», concepto probablemente poco conocido, pero con toda seguridad las amenazas que representa están permanentemente presentes entre nosotros.

El término «amenaza híbrida», es definido por el glosario de terminología del Estado Mayor de la Defensa como: «Aquella que emplea todo tipo de instrumentos de poder, procedimientos convencionales, junto a tácticas irregulares y a actividades terroristas, crimen organizado, nuevas tecnologías, ataques en el ciberespacio, presión política y múltiples tipos de herramientas de información y desinformación incluyendo las noticias falsas y la mentira en sí misma».

Para la Unión Europea, la «guerra híbrida» implica la utilización de armas como la desinformación o los ciberataques, usar el chantaje económico o energético, recurrir a la provocación en las calles e incluso al terrorismo para alentar, por ejemplo, un conflicto latente. Por ello insiste en aumentar la conciencia de que estas amenazas son reales y en que debemos de mejorar la resiliencia, incluso en las circunstancias más difíciles.

Hace no mucho tiempo, en un enfrentamiento, en una guerra, se conocía perfectamente quién era el enemigo, incluso su potencial y territorio de procedencia. Más recien-

temente, debido a la escalada de actos terroristas, raramente se conoce la identidad de los individuos que perpetran los atentados, pero sí se conoce a los grupos terroristas de los que forman parte, pues ellos mismos lo manifiestan públicamente.

Pero existe una hipótesis mucho más peligrosa, la que el concepto amenaza hibrida representa, no saber quién es el enemigo, dónde se encuentra, en definitiva, de dónde procede la amenaza, aunque sí debemos dar por seguro que esta amenaza se encuentra presente entre nosotros, en nuestro ordenador, en nuestro móvil, intentando perpetrar ataques a redes públicas o privadas para generar grandes pérdidas económicas o incluso denegación de servicios esenciales tales como la luz o el agua, o manipulando las redes sociales para generar engaños y desorientación en los ciudadanos y con ello la pérdida de confianza en los gobiernos establecidos.

Cuando se habla de seguridad y defensa, quizás existe la tentación de a priori pensar en los que portamos uniforme, pero hoy en día, en el complejo mundo en que vivimos, el concepto defensa se ha visto enormemente modificado, y como se ha dicho, las amenazas se encuentran entre nosotros. Combatir estas amenazas, a las que constantemente podemos vernos sometidos, es tarea de los gobiernos, instituciones y organizaciones, pero esta labor no se antoja fácil, pues a menudo uno de los objetivos de estas amenazas es la tergiversación de la verdad y con ello que la población pierda la confianza en sus gobiernos.

Pero como individuos no podemos ni debemos ser ajenos a estos asuntos, sino que debemos de adoptar unos hábitos de conducta que nos protejan contra todos estos bulos, contra todas estas amenazas a que estamos expuestos, entre ellas cibernéticas, y esta ha sido la pretensión de esta XXVII edición del Curso Internacional de Defensa: proporcionar los conocimientos suficientes, en especial a los jóvenes que son quienes con posterioridad mayor transferencia de los mismos pueden hacer a nuestra sociedad, de manera que todos los asistentes dispongan de criterio propio y tengan una mayor conciencia de la necesidad de perder un poco de su comodidad en favor de un considerable aumento de su seguridad.

CONFERENCIA DE INAUGURACIÓN

AMENAZAS HÍBRIDAS

Dª ELENA GÓMEZ DE CASTRO
Directora general de Política de Defensa
del Ministerio de Defensa
(Texto no facilitado)

PONENCIAS DEL ÁREA 1
Mirando al futuro

ÉTICA Y LÍMITES DE LA LIBERTAD DE OPINIÓN Y DE PRENSA

D. ÁNGEL GÓMEZ DE ÁGREDA
Coronel jefe del Área de Análisis Geopolítico de la División de Coordinación y Estudios de Seguridad y Defensa (DICOES)

ÉTICA Y LÍMITES DE LA LIBERTAD DE OPINIÓN Y DE PRENSA

D. ÁNGEL GÓMEZ DE ÁGREDA
Coronel jefe del Área de Análisis Geopolítico de la División de Coordinación y Estudios de Seguridad y Defensa (DICOES)

Poner límites a la libertad de opinión, de expresión o de prensa, más allá de lo que marca la Constitución cuando habla de la difusión de noticias veraces, resultaría en un grave perjuicio para mucho más que esas libertades. La restricción en los puntos de vista disponibles para abordar un asunto cualquiera minimiza las posibilidades de encontrar todos los ángulos útiles en su interpretación. La verdad solo puede alcanzarse desde un estudio multidisciplinar de la realidad, sin preconcepciones, apriorismos ni sesgos.

En este sentido, decía George Orwell que «si la libertad significa algo es el derecho a decirle a la gente aquello que no quiere oír». Orwell es el autor de 1984, la novela en la que la sombra del Gran Hermano adopta un papel protagonista y en la que el Ministerio de la Verdad tiene por principal misión de distorsionarla en beneficio del Estado. El Ministerio desarrolla el «doble-pensar» y la «neolengua» en los que el medio, el lenguaje, se convierte en lo importante en detrimento del objeto representado por el mismo.

La utilización real de la neolengua moderna —que se adorna con un gran parecido al lenguaje políticamente correcto que se impone en los últimos años— pretende, efectivamente, limitar la libertad para decirle a la gente aquello que no quiere oír. Los cauces por los que un creciente porcentaje de la población recibe la información, las redes sociales, estudian el comportamiento ofrecido por los datos y metadatos de los internautas para servirles solamente aquel discurso que se alinea con sus preconcepciones y que garantice una mayor permanencia del usuario en el entorno de la red.

Eso encierra a la población en cámaras de eco aisladas de cualquier narrativa hostil a su relato por unas burbujas de filtros que dejan fuera cualquier visión alternativa de la realidad. Ahí dentro, grupos de personas homogéneas en su forma de pensar con respecto a un aspecto concreto exacerban y radicalizan su discurso por la mera fuerza del

ego. La necesidad de pertenencia al grupo se ve garantizada por la misma existencia de la red. Sin embargo, la necesidad de realización personal y de destacar solamente puede satisfacerse llevando los postulados comunes al grupo hacia posiciones más extremas a las que el resto de sus componentes se irán desplazando en base a la aceptación que reciba.

La verdad se convierte, de este modo, en el sustento de la libertad. No ya de la libertad de expresión, sino de la libertad en un sentido más amplio. Solamente el conocimiento presta un fundamento suficiente para construir sobre él una capacidad de decidir de forma racional más allá de las corazonadas y los caprichos.

Ese conocimiento que lleva a la verdad tiene que basarse, evidentemente, en datos y en información veraz, y en una capacidad mínima para relacionar entre sí las distintas piezas de información que se vayan obteniendo. No basta con tener acceso, como es el caso, a más información que en ningún otro momento en la historia, también es necesario tener la voluntad para acceder a ella a pesar de que otras opciones más cómodas estén disponibles por defecto.

Desgraciadamente, en el viejo dilema entre la seguridad y la libertad, ambas se han degradado significativamente en beneficio de la comodidad. En general, se acepta de muy buen grado cualquier producto que se nos ofrezca que sea cómodo, que sea de acceso inmediato y que sea —al menos aparentemente— gratuito. Envuelto en una capa de *marketing* y sin pretensiones de durar indefinidamente en la lista de prioridades del consumidor, ese producto tiene muy buenas posibilidades de instalarse en la cesta de los deseos por poco útil que sea.

Hemos perdido libertad y seguridad en favor de la comodidad. Y lo hemos hecho desde el mundo digital. Degradamos nuestra seguridad regalando nuestros datos, nuestros unos y ceros, nuestro «yo digital» a empresas que los integrarán para ver a través de nosotros y poder sacar el mayor partido de nuestra desnudez. Esas mismas empresas, basándose en los datos que les acabamos de regalar, generarán un producto por el que pagaremos gustosamente porque se adecúa a nuestros gustos y convicciones. Ese producto, sin embargo, tiene por finalidad principal retenernos dentro del feudo de la compañía para que sigamos proporcionando datos al tiempo que nuestra capacidad de elección se ve mermada por los sesgos que introduce para retenernos allí.

Es lo que Tim Cook, el CEO de Apple, denomina «jardines amurallados». Las plataformas ofrecen un entorno amigable, agradable y, sobre todo, cómodo en el que pastemos la información que nos van proporcionando. Dentro de ese jardín reina soberana la compañía porque se trata de un mundo virtual pobremente regulado por los poderes del mundo físico hasta el momento. Está rodeado de una muralla cuya función principal no es tanto la protección frente a las amenazas exteriores como dificultar la huida de los clientes apacentados del interior de la red.

Eso explicaría que Miguel de Unamuno tomase como divisa «Antes la verdad que la paz», contraponiendo ambos términos en lugar de los de libertad y seguridad. La verdad como base de la libertad es, sin embargo, la primera víctima de todas las guerras, por

lo que la falta de paz también supondría la de verdad, aunque lo contrario no sea necesariamente cierto.

A esa verdad se contraponen los «hechos alternativos» de los que hemos sido testigos últimamente en algunas instancias de la política internacional como la inauguración del presidente Trump. La jefa de prensa de la Casa Blanca, Kellyanne Conway definió así lo que antes se habría calificado como una burda mentira o manipulación. Un «hecho alternativo» es una mentira que un grupo concreto acepta como verdad consensuada para acomodarla a su narrativa. Es un autoengaño colectivo que refuerza al grupo que da cobijo a los sujetos que lo componen.

En este contexto, cualquier afirmación es válida en tanto suficiente número de personas esté dispuesta a endosarla. No hay ningún problema en incurrir en contradicciones manifiestas entre distintas versiones de la verdad, porque el conocimiento no llega a generarse ya que los datos permanecen aislados y solamente se exponen contra el fondo de la situación que se pretende modificar. El dato se aprehende, se consume y se descarta de forma inmediata, salvo que pueda resultar de utilidad circunstancialmente para apoyar alguna otra narrativa. Según se vaya descubriendo su falta de coherencia, puede descartarse sin rubor en base a la nueva verdad que se quiere «vender».

Versiones disparatadas de un hecho son perfectamente aceptables. Y, cuando dejan de serlo, tampoco existe ningún problema en reformularlas para que se amolden al nuevo contexto generado por realidades incontestables. Negar la mayor es siempre un recurso a disposición del manipulador. Si no podemos cambiar el actor o el argumento, cambiaremos el escenario y, con él, la obra entera se ve bajo una luz diferente.

El control del relato se vuelve, por lo tanto, fundamental. No el control de la información, sino el de la conformación de las noticias en relatos. La iniciativa en este caso es requisito ineludible porque, en los cortos plazos que se manejan, las contranarrativas pierden toda credibilidad y utilidad. Lo importante es sentar las bases sobre las que se asienta la verdad y dejar luego que el público vaya encajando las piezas que se le vayan sirviendo sobre esa base sesgada.

Sin iniciativa en el relato no existe la posibilidad de dirigir la conversación y, por lo tanto, de establecer una visión de la realidad.

Del mismo modo, por mucho que las audiencias ya no puedan ser —teóricamente— segmentadas al tener todo el mundo acceso a la totalidad de la red disponible, el mensaje se diseña, distribuye y dirige únicamente a un público fiel y casi cautivo. Se trata de movilizar seguidores y de hacer lo contrario con los detractores. En ningún momento se pretende hacer cambiar de bando a los convencidos, solamente a los indecisos y, casi siempre, a través de la presión social que se ejerce sobre ellos.

Robert Cialdini lo expresa muy gráficamente en su libro *Persuasión*. El condicionamiento que puede realizarse a través de los medios tecnológicos actuales apunta más hacia una actividad previa a la conformación del relato que a un cambio en el contenido del mismo una vez que ha sido estructurado. Es la movilización afectiva de los partida-

rios lo que se busca, más que la ampliación de las bases que constituyen estos grupos alineados con una postura.

La construcción del relato no es, desde luego, un tema novedoso. Pero sí lo es la capacidad casi indiscriminada de acceder a dicha construcción o manipulación de los sentimientos para actores que están muy por debajo del nivel estatal o que no tienen recursos económicos prácticamente ilimitados. La democratización del acceso a la información ha venido acompañada de una similar para la creación de contenidos.

Estas capacidades se vienen utilizando dentro de los ejércitos desde tiempos inmemoriales. El ejemplo clásico más recogido en la literatura es, precisamente, la obra de Julio César sobre la *Guerra de las Galias* que, más allá de ser un recuento histórico de las campañas que el genial general libró en lo que entonces eran los confines del imperio, tenía una función de elaboración de un relato sobre su propia figura de cara al acceso al puesto de Cónsul y, eventualmente, a la formación de un triunvirato en el que él constituía la figura en principio más débil.

Sin embargo, la comunicación estratégica parece haberse quedado pequeña para la nueva realidad de la guerra que se libra EN la gente, frente a la que se ha estado peleando entre la gente o en los campos de batalla abiertos. Las novenas divisiones de Estado Mayor mutan su nombre por el de «influencia» fusionando muchas de las tácticas, técnicas y procedimientos relacionadas con el entorno cognitivo y sensitivo del combate.

También, como adelantábamos, actores no estatales están alimentando el fuego de las narrativas desde las plataformas que les ofrece, principalmente, Internet y las redes sociales. El relato que difundió el Estado Islámico, el Dáesh, adquirió proporciones paraestatales con la publicación de varias revistas en idiomas distintos, manuales y programas de noticias que servían de base al reclutamiento, formación, motivación y financiación de sus actividades. Su estructura organizativa en el aspecto mediático incluía profesionales altamente cualificados.

El foco mediático que la prensa suele colocar en los asuntos más escabrosos, pornográficos y llamativos de la actualidad magnifica también el relato de estos grupos criminales dándole una visibilidad desproporcionada y creando la sensación de amenaza sistémica donde, en realidad, no hay más que un intento de subversión del orden establecido para mantenerlo a medio plazo cambiando a los actores.

Todas estas narrativas apelan constantemente a los sentimientos, a los afectos, mucho más que a la razón, a la que dejan de lado apelando a los miedos irracionales, a los sesgos y prejuicios, y a los hábitos poco recomendables que se alojan en los rincones más inconfesables de nuestras mentes. Las puertas abiertas que dejan estas debilidades cognitivas permiten acceder directamente a sentimientos de reacción inmediata que actúan impulsivamente.

Mientras que los estudios militares de hace apenas una década apelaban a la generación de efectos militares en las operaciones, es decir, a las consecuencias operacio-

nales de las acciones cinéticas más que a los efectos físicos tácticos que tenían lugar sobre el terreno, debemos plantearnos unas operaciones basadas en afectos.

Las operaciones basadas en afectos buscarían alterar los sentimientos, los afectos, de las audiencias propia y adversaria en base a la repercusión mediática y empática que tengan las actuaciones cinéticas. No persiguen tanto una traslación directa de los resultados sobre las estructuras o infraestructuras en ventaja militar sobre el terreno como un desgaste emocional del enemigo al tiempo que se responde a las expectativas o se refuerzan las creencias o la legitimidad entre las audiencias propias.

Acciones de castigo, como algunos bombardeos selectivos que tuvieron lugar en el teatro de operaciones de Siria, destrucciones simbólicas, como la de los Budas de Abiyán por parte de los talibán o la del puente de la ciudad bosnia de Mostar, y otras muchas más, persiguen dividir o multiplicar efectos en el ámbito afectivo y emocional, dentro y fuera del campo de batalla.

La desinformación, las falsas noticias entre otras, contribuyen a la construcción de esas narrativas y a la creación de esos afectos manipulados. Su difusión tiene mucho que ver con la capacidad concreta del creador de la noticia para darle la difusión adecuada, con la viralización que alcancen los contenidos, el tipo de base que se emplea para difundirlos (suelen ser mucho más eficaces aquellos que se basan en contenidos gráficos) y la actualidad de la noticia que se aborda.

También es de particular importancia la adecuación de los mensajes al canal de comunicación que emplee preferentemente la audiencia objetivo de los mismos. Cada segmento generacional tiene sus propias vías para compartir información, aquellas que mayor confianza les ofrecen y las que mayor flexibilidad permiten a su actividad. Las audiencias, como se ha apuntado más arriba, no pueden ya segmentarse de partida, pero sí se puede condicionar grandemente el impacto que va a tener cada envío de información en función de todas las características enunciadas.

Podemos concluir de todo lo anterior que la libertad de expresión contribuye muy positivamente al conocimiento al aplicar diferentes puntos de vista y enriquecer el debate. A su vez, este conocimiento se convierte en la base de la verdad aceptada que, a su vez, resulta ser el punto de partida para poder ejercer nuestra libertad.

No obstante, esa misma libertad de expresión introduce mucha distorsión en el sistema, ruido en algunos casos, manipulación en otros. La línea que separa la higiene informativa de la censura es tremendamente delgada e interpretable. El entorno informativo digitalizado del siglo XXI obliga a los medios a aplicar una disciplina mayor en el control de los contenidos, no con el objeto de limitar las opiniones sino de establecer el grado de veracidad y objetividad de los mismos. Una opinión, una pieza de publicidad o propaganda, es un instrumento perfectamente lícito, pero debe estar etiquetado adecuadamente para que sea identificado como tal y no como información propiamente dicha.

En segundo lugar, las audiencias adquieren una responsabilidad adicional derivada de la hiperconectividad que describo en *Mundo Orwell. Manual de supervivencia para un*

mundo hiperconectado, publicado por la editorial Ariel. La conexión directa de cada nodo, de cada individuo, con todos los demás, dificulta la intermediación y permite el acceso directo por lo que también la protección, la seguridad, debe individualizarse. Los lectores y oyentes somos responsables de contextualizar la información que recibimos y determinar su grado de fiabilidad.

Finalmente, las instituciones deben llevar a cabo su labor regulatoria para no dejar completamente en manos de emisor y receptor toda la carga de la determinación de qué es lícito o permisible. El gran poder que tienen las redes implica también una gran responsabilidad, pero si los Estados quieren seguir siendo relevantes tendrán que seguir asumiendo también la suya en tiempo y forma digital.

MESA REDONDA
El concepto de lo híbrido: de las amenazas híbridas a la zona gris

EL CONCEPTO DE LO HÍBRIDO: DE LAS ESTRATEGIAS HÍBRIDAS A LA ZONA GRIS

D. BONIFACIO GUTIÉRREZ DE LEÓN
Coronel subdirector de Investigación y Lecciones Aprendidas del MADOC

EL CONCEPTO DE LO HÍBRIDO: DE LAS ESTRATEGIAS HÍBRIDAS A LA ZONA GRIS

D. BONIFACIO GUTIÉRREZ DE LEÓN
Coronel subdirector de Investigación y Lecciones Aprendidas del MADOC

ANTECEDENTES

Aunque la expresión *Hybrid warfare* (HW)[1] se empleó por primera vez en 1998 para referirse a un modo de hacer la guerra combinando elementos de diferente naturaleza, no fue hasta 2005 cuando se la dotó de cierto contenido teórico con el artículo «La forma futura de hacer la guerra: el nacimiento de las guerras híbridas»[2]. Mattis y Hoffman afirmaban que las amenazas híbridas incorporaban un abanico completo de diferentes modos de hacer la guerra que incluye las capacidades convencionales, organización y tácticas irregulares, actos terroristas que incluían la violencia indiscriminada y la coacción, y el desorden criminal. Decían que las guerras híbridas se podían llevar a cabo tanto por estados como por una serie de actores no estatales diversos. También alertaban de que la superioridad tecnológica de los EE. UU. crearía una lógica que impulsaría a actores estatales y no estatales a evolucionar, a abandonar el modo tradicional de hacer la guerra y buscar capacidades o formas inesperadas de combinar tecnología y táctica para conseguir ventaja sobre su adversario. Aconsejaban abandonar la rigidez de pensamiento, preparar respuestas adecuadas a este tipo de amenaza y contemplarlas en su estrategia de seguridad nacional.

Sin embargo, este concepto no es nuevo. A través de la historia, las formas y métodos «híbridos» de diferente índole han sido utilizados en muchos conflictos y batallas desde la antigüedad. No obstante, los medios de lucha empleados han sido diferentes, dependiendo de las características sociales, del desarrollo tecnológico y del ingenio propio de cada época. Es por ello que, aunque muchas de sus características son reconocibles en

---

[1] WALKER, Lt. Robert G. «(Hybrid force for hybrid wars). The United States Marine Corps and Special Operations». Dec. 1998.

[2] MATTIS, lieutenant general James N. USMC, and HOFFMAN, lieutenant colonel Frank. «USMCR, Future Warfare: The rise of Hybrid Wars». Nov. 2005.

los enfrentamientos del pasado, su aplicación generalizada y con resultados decisivos en los conflictos más recientes ha propiciado un amplio debate doctrinal y académico, aún no resuelto, para determinar si «lo híbrido» supone en sí mismo una innovación en la forma de desarrollar los conflictos o si, por el contrario, es simplemente una variante en la forma de aplicar conceptos ya existentes (conflicto asimétrico, insurgencia…).

Este modo de hacer la guerra suele ser consecuencia de una relación asimétrica entre actores, en la que uno de ellos goza *a priori* de una ventaja militar convencional. El actor que se encuentra inicialmente en desventaja buscará soluciones alternativas de naturaleza híbrida para alcanzar una situación más equilibrada o ventajosa respecto a su adversario. Pero lo más significativo es que las amenazas híbridas tratarán inicialmente, por diferentes razones (economía de medios, mantenimiento del *status* internacional,…), de evitar un conflicto armado generalizado.

En su sentido actual, el término «guerra híbrida» se hizo muy popular para referirse a los métodos empleados por Hezbolá en 2006 para enfrentarse a Israel. Posteriormente, a partir de 2014, acontecimientos como la aparición del Dáesh, la intervención de Rusia en Ucrania o la construcción de islotes artificiales de China en el mar de China Meridional, han favorecido una evolución del término «híbrido», que «se ha ido ampliando, abarcando múltiples aspectos del panorama de la seguridad internacional»[3] y que tanto la OTAN como la Unión Europea o España hayan identificado a las amenazas híbridas como uno de los principales riesgos para la seguridad internacional y nacional (de cada estado).

El carácter innovador de este término se podría asociar, más bien, a dos factores principales:

- Las amenazas híbridas pueden estar presentes en todas las regiones del espectro del conflicto y demandar la actuación de los instrumentos de poder del estado atacado en situaciones por debajo del umbral del conflicto armado, en lo que denominamos «zona gris» (las fuerzas armadas no tienen un papel principal en el desarrollo del conflicto).
- El empleo imaginativo de las nuevas tecnologías por parte de la amenaza híbrida le permite integrar, con eficacia y de modo convergente, sistemático y creativo, formas y medios de actuación convencionales y no convencionales, ejercidos oportunamente en diferentes «espacios de batalla», (físico, político, económico, informativo, ciber). Entre ellos, destacan la utilización del ciberespacio como principal escenario de confrontación y el uso de los medios de comunicación de masas y sociales para manipular y moldear la información.

DEFINICIÓN DEL CONCEPTO

El modelo híbrido hace referencia a una forma ambigua de confrontación, en que unos actores estatales o no estatales son capaces de combinar acciones militares con-

[3] JORDÁN, Javier. «Guerra híbrida, un concepto *atrápalo-todo*». *GESI*. http://seguridadinternacional.es/?q=es/content/guerra-h%C3%ADbrida-un-conceptoatr%C3%A1palo-todo.

vencionales y no convencionales con acciones no militares basadas en una estrategia de desestabilización del adversario mediante el uso de acciones diversas, complementarias y sin restricciones, que integran todos los instrumentos de poder disponibles [diplomático, militar, económico, social y de información (DMESI)]. Con esta estrategia se trata de explotar las debilidades y vulnerabilidades de las sociedades occidentales en todos sus aspectos. Sus objetivos generales pretenden, sobre todo, influir en la dirección política y en la opinión pública (tanto la propia, la neutral o internacional, como la del adversario), para debilitar a sus adversarios y terminar provocando su desistimiento parcial o incluso su abandono del conflicto. La voluntad de la población es un objetivo prioritario.

Las amenazas híbridas adaptan los modos y los medios a las nuevas realidades estratégicas, que son en gran medida consecuencia de la globalización, de la redistribución del poder dentro de la comunidad internacional, de los avances tecnológicos y de los desarrollos sociológicos (opinión pública occidental, instrumentalización de las religiones e ideologías, papel dominante de los medios de comunicación, de Internet, de redes sociales, etc.).

> Los aspectos esenciales de estas estrategias (modos) son la ambigüedad, la combinación sincronizada de acciones convencionales con otras irregulares con objeto de conseguir una ventaja que permita a un actor imponer su voluntad y la supresión *de facto* de las restricciones jurídicas o éticas que podrían imponer límites a las acciones aceptables en la región del espectro en la que se desarrolla el conflicto. Cuando les convenga para obtener una ventaja, el adversario rebasará los límites de la diplomacia y del derecho internacional, sin someterse a los principios de buena fe en las relaciones internacionales ni a las leyes y usos de la guerra[4]. Por la misma razón, sus operaciones incluirán potentes campañas de propaganda y de desinformación que contribuyan a justificar sus acciones o, al menos, a sembrar la duda en la opinión pública nacional e internacional.
>
> De esta forma, las estrategias híbridas pueden contemplar y aplicar medidas de presión política, diplomática o económica; propaganda; acciones de naturaleza subversiva (terrorismo, delincuencia organizada, ciberataques, movilización de masas, escudos humanos, etc.) con un grado de violencia controlado, que implican generalmente la participación de actores no estatales; operaciones militares encubiertas y, en último caso, operaciones militares convencionales.

CONTRARESTAR A LA AMENAZAS HÍBRIDAS

La diversidad en la naturaleza de los actores y de las acciones que se llevan a cabo, hace que la respuesta a una estrategia híbrida sea de gran complejidad y con tendencia a prolongarse en el tiempo sin obtener resultados decisivos.

Para ello, además de que cada país identifique y fortalezca sus objetivos generales de seguridad nacional, que como, por ejemplo identifica, la *Estrategia de Seguridad Nacional de 2017* (avanzar en un modelo integral de gestión de crisis, promover una

[4] Lo que se vulnera es más la «bona fide» propia de las relaciones internacionales, que la ley en sí misma.

cultura de seguridad nacional, favorecer el buen uso de los espacios comunes globales, impulsar la dimensión de seguridad en el desarrollo tecnológico y fortalecer la proyección internacional de España) es necesario que cada estado desarrolle una estrategia frente a las amenazas híbridas que, inicialmente, debería:

- Realizar una autoevaluación de las funciones críticas de todos los sectores.
- Aumentar la tradicional evaluación de la amenaza para incluir herramientas y capacidades no convencionales, políticas, económicas, civil y de la información.
- Definir un organismo y establecer un proceso capaz de contrarrestar las estrategias híbridas.

El proceso podría ser el siguiente:

- Establecer objetivos estratégicos realistas.
- Identificar el umbral apropiado para emprender acciones, lo que se entiende como establecer las líneas rojas que desencadenan acciones de disuasión y/o respuestas.
- Diseñar y llevar a cabo una estrategia basada en los tres componentes de detección, disuasión y respuesta.
    - Detección: el tradicional análisis de amenaza centrado en el enemigo no es adecuado para detectar ataques híbridos, por lo que hay que articular métodos alternativos para establecer el conocimiento de la situación. Una forma de considerar la inteligencia de alerta es diferenciar los posibles ataques futuros en dos categorías: «incógnitas conocidas» e «incógnitas desconocidas».
    - Disuasión: es quizás la herramienta más importante para contrarrestar una estrategia híbrida, simplemente porque puede prevenir ataques antes de que se produzcan. Sin embargo, sus características complican el cálculo de la disuasión tradicional y requieren la actualización de los enfoques tradicionales para disuadir las amenazas híbridas modernas. Los pilares de la disuasión serán: credibilidad, capacidad y comunicación.
    - Respuesta: el dilema inicial a la respuesta a un ataque hibrido es precisamente si se responde. Una vez que se decide que la respuesta es necesaria, los «fines» (qué resultado debe lograr o contribuir a lograr la respuesta) se establecen de acuerdo con los objetivos estratégicos y los umbrales específicos para la acción del actor que responde.
- Desarrollar la maquinaria institucional para implementar estas medidas a través de los gobiernos nacionales y las instituciones multinacionales para asegurarse de que sea adecuado para su propósito.

LA CONSTRUCCIÓN DE LA ZONA GRIS

D. JOSEP BAQUÉS QUESADA
Doctor en Ciencias Políticas y profesor
de la Universidad de Barcelona

LA CONSTRUCCIÓN DE LA ZONA GRIS

D. JOSEP BAQUÉS QUESADA
Doctor en Ciencias Políticas y profesor de la Universidad de Barcelona

INTRODUCCIÓN

El capítulo que nos ocupa trata de mostrar, de un modo ágil, pero riguroso en términos académicos, las funciones que desarrollan las zonas grises, en el marco más amplio de los conflictos híbridos. Para ello, tras realizar algunas aclaraciones previas, indispensables a fin de hacerse con un cuadro más amplio del estado del debate (epígrafe 2), pasaremos a analizar por separado, tanto los fines u objetivos de la zona gris (epígrafe 3), como los medios o herramientas que le son propios[1] (epígrafe 4), para terminar haciendo una breve reflexión final, a modo de conclusión (epígrafe 5).

ACLARACIONES PRELIMINARES

Cuando se afronta la relación entre la zona gris y el concepto de los conflictos híbridos, es preciso hacer unas aclaraciones preliminares. La primera, referente a la relación que mantiene con el magma de lo híbrido; la segunda, relativa a los actores que suelen, o al menos, que pueden emplear este recurso. A saber:

- Por una parte, la zona gris encaja perfectamente en lo que damos en llamar amenazas híbridas (Chambers, 2016, p. 22), e incluso en las estrategias híbridas, en la medida en que el énfasis se pone en la explotación de todos los recursos de que dispone una nación, incluyendo los económicos, los diplomáticos, los culturales, etc, siendo lo militar apenas una pequeña parte del total de recursos empleados

[1] Vaya por delante, en todo caso, que en un concepto como el de la zona gris, los medios empleados son tan relevantes, que forman parte de la propia definición.

para afrontar un conflicto internacional. Sin embargo, la zona gris encaja mal —o, simplemente, no encaja— en la noción de guerra híbrida, en la medida en que esta incluye, por definición, la participación activa, en la zona de conflicto, de fuerzas militares, incluso dotadas con armas convencionales (Hoffman, 2012, p. 3). Esto conduce a aclarar que la zona gris no es un tipo de guerra, sino un tipo de paz. Ciertamente, se trata de una paz polemológica, conflictual, que atenta de modo intencionado contra las reglas de la buena fe que deberían presidir las relaciones internacionales, precisamente, en tiempos de paz. Ahora bien, lo que se pretende con una zona gris es, precisamente, no tener que iniciar una guerra para alcanzar los objetivos trazados.

- Por otra parte, aunque el resto de este capítulo versará sobre las razones y las herramientas que los Estados despliegan a la hora de desarrollar una estrategia de zona gris, conviene tener en cuenta que los Estados no son los únicos actores capaces de generar zonas grises. También pueden intentarlo con visos de éxito otros actores que, dada su naturaleza, ocupan o aspiran a ocupar territorio, si además cuentan con lo que podríamos denominar estructuras de Estado. Pensemos en los *warlords* que, *de facto*, hacen las veces de Estado (aunque sin reconocimiento internacional, ni, normalmente, nacional), dotándose de fuentes de ingresos propios (irregulares, no, puesto que lo primero no es incompatible con la zona gris), y de buena parte de los servicios —incluyendo los de seguridad— de los que hacen gala los Estados. Por razones parecidas, también las administraciones subestatales (estados federados, por ejemplo) podrían desarrollar esas habilidades. E incluso podrían hacerlo algunos grupos terroristas —caso del Dáesh, pero también de Hezbollah— cuya vocación es el control del territorio sobre el que se asientan. No solo, por lo tanto, su desestabilización (Kapusta, 2015, p. 20).

LOS FINES DE LA ZONA GRIS

¿Quién asume esta estrategia?

Lo primero que hay que acotar es el tipo de actor que, con más probabilidad, puede optar por el establecimiento de zonas grises. En el elenco de Estados que componen el sistema mundial, son proclives aquellos que podemos catalogar como moderadamente revisionistas. Los dos lexemas son relevantes. Son revisionistas porque se sienten incómodos con el *status quo* internacional. Pero lo son moderadamente, porque siguen siendo capaces de cubrir algunos de sus objetivos más elementales (seguridad, viabilidad económica, canales de expresión diplomática, etc.) dentro del orden que denostan. Quizá esto se entienda más y mejor a contraluz: ¿por qué Japón atacó Pearl Harbour en 1941? La razón estriba en que el embargo de crudo decretado en su contra por los EE. UU. en el verano de ese mismo año, condenaba al país del sol naciente a paralizar su ya de por sí inconclusa revolución industrial, devolviendo a los nipones a una situación decimonónica. Por lo tanto, no cabía estrategia gradualista alguna: el tiempo corría en contra de Japón y la guerra fue considerada como el único mecanismo que podría asegurarles el crudo indonesio y, quizá, en la mejor de las hipótesis, una renegociación de los términos de ese embargo con los propios EE. UU.

Por el contrario, los Estados que suelen ser citados en la bibliografía al uso entre los más activos a la hora de emplear zonas grises (China, Rusia e Irán), aunque manifiestan distintos niveles de insatisfacción con el actual liderazgo de los EE. UU., así como con las organizaciones internacionales más emblemáticas (caso de la OTAN) son actores que pese a esos condicionamientos (que están ahí) pueden seguir desarrollando aspectos fundamentales de sus respectivas agendas. Por ese motivo, pueden plantearse el empleo de un mecanismo, como el que ahora nos ocupa, que normalmente rinde dividendos geopolíticos a medio y largo plazo (Mazarr, 2015, pp. 58-60)[2].

¿Para qué se sigue esta estrategia?

La zona gris es útil para alcanzar fines similares a los que, en condiciones normales, exigirían una guerra. Son lo que algunos actores definen como *warlike aims* (Freier, 2016, p. 33). Es decir, hablamos de objetivos de gran valor geopolítico. Entre esos objetivos suele citarse, sobre todo, provocar la independencia de una parte de otro Estado, cuando ese Estado es un rival geopolítico del que establece la zona gris; o bien, provocar la anexión —en todo o en parte— de otro Estado, hasta entonces independiente; o bien, provocar un cambio de régimen, aunque se admite como caso de zona gris que el cambio lo sea tan solo de gobierno, a condición de que eso traiga consigo un impacto relevante en la distribución de poder, ora sea mundial, otrora regional.

Podrían emplearse algunos ejemplos históricos que permiten hacernos una idea del potencial de esas zonas grises. En el primero de los supuestos planteados, recordemos el apoyo de Francia a la independencia de las trece colonias británicas que, con el tiempo, serían el embrión de los EE. UU.: los galos apoyaron esa causa con una narrativa apropiada al caso (derivada de la Ilustración y del discurso revolucionario que ya se había larvado allende la corte de Versalles), con dinero susceptible de ser empleado para armar a los colonos norteamericanos, o garantizando la continuidad del comercio entre Europa y las colonias díscolas.

En el segundo de los escenarios propuestos, pensemos en el *Anschluss* austríaco, de 1938. Los alemanes lograron incorporar a Austria, mediante… ¡un referéndum de autodeterminación convocado por Hitler! Pero lo hicieron a renglón seguido, no de una guerra, sino de medidas como la propaganda en las calles del partido nazi austríaco, como una narrativa de corte racial —que enfatizaba el carácter esencialmente ario de los austríacos—, o como diversas medidas de presión económica, todo ello aderezado con un empleo limitado de la violencia política interna que, en todo caso, no era perpetrada por alemanes.

En el tercero de los casos indicados, recordemos la insistencia rusa en que el presidente checo, Zeman, se mantuviera en el cargo, cuando poco antes de la celebración

---

[2] Se suele aludir al caso de la intervención rusa en Crimea, en 2014, como un caso de zona gris desarrollada en un tiempo récord. En realidad, lo allí ocurrido tiene otra explicación compatible con las que aquí se ofrecen, pero necesitada de un matiz. Se trata de que, dadas las circunstancias que envuelven la historia reciente de esa península, los rusos tenían buena parte del trabajo hecho, de antemano: sustitución de la población tártara por la rusa (que no ucraniana), presencia de importantes bases militares rusas (de acuerdo con Ucrania) con la consiguiente presencia de las familias de esos militares y de las infraestructuras de todo tipo necesarias para su acomodo; así como las conexiones económicas que todo ello implicaba, entre Rusia y Crimea.

de las elecciones del año 2018, había sospechas razonables de que podían perderlas frente a un candidato claramente pro-UE y pro-OTAN. En cambio, Zeman ha prometido un «brexit checo», que afectaría, a través de referéndums, a la continuidad de Chequia en ambas organizaciones.

¿Por qué esta estrategia, y no otras alternativas?

Sobre todo, porque las demás opciones para alcanzar los objetivos pergeñados pueden activar una escalada bélica. En realidad, quienes emplean la zona gris, temen la posible reacción militar de los defensores del *status quo*. Saben que, si optan por una guerra híbrida, o, directamente, por una invasión ejecutada por fuerzas convencionales, se eleva exponencialmente la probabilidad de que otros Estados reaccionen del mismo modo a fin de restaurar la legalidad internacional. Y, dado lo que ya hemos comentado acerca de su moderado revisionismo, el precio a pagar sería demasiado elevado. Por lo tanto, quienes proponen una zona gris, lo hacen, precisamente, para no generar un *casus belli*. En ese sentido, procuran no cruzar determinadas líneas rojas. De este modo, además, logran que, de darse una escalada, la sociedad internacional pueda responsabilizar de la misma a los defensores del *status quo*.

Esas líneas rojas son de dos tipos. Puede hablarse de un doble filtro. Quienes generan una zona gris tienen en cuenta tanto los parámetros del derecho internacional (a-51 CNU), como la práctica de las principales potencias, analizadas desde un punto de vista empírico (Echevarría, 2016). Es lógico que así sea, puesto que, en ocasiones, aunque el derecho internacional demande una intervención, otros criterios, de prudencia política, dificultan o inhiben esa opción. Pensemos en el caso de la invasión de Hungría por parte de la URSS, en 1956. La OTAN no se planteó una respuesta armada, debido a que eso podría dar pie a una tercera guerra mundial. Pero antecedentes como este muestran a los generadores de zonas grises que su margen de maniobra puede ser algo más generoso del que da a entender el derecho vigente, especialmente si su poder relativo es grande, como lo es el de China, Rusia (siguen siendo potencias nucleares) y, aunque a otra escala, Irán.

¿La zona gris es siempre un fin en sí, o puede ser un medio para conseguir otras cosas?

Lo cierto es que las dos opciones son factibles. Idealmente, la zona gris debería cubrir sus objetivos sin dar pie a guerra alguna. Ni siquiera híbrida. Hemos citado algunos ejemplos en ese sentido. Pero, en caso de no lograrlo, el trabajo desempeñado para generarla, podría ser aprovechable en una hipotética escalada ulterior. E incluso podría planificar el comienzo de una guerra híbrida a partir del previo establecimiento de una zona gris (Mazarr, 2015, p. 58). Hay que tener en cuenta que, para una potencia revisionista, dispuesta a generar zonas grises, el escenario previo y el posterior al establecimiento de las mismas, cambia por completo. Lo hace de acuerdo con aspectos nucleares como el que Clausewitz integra en su trinidad: si la construcción de una zona gris es efectiva, es más probable que, en el lugar en el que se implementa, dichas potencias revisionistas

logren que crezcan sus apoyos entre la población civil local, al mismo tiempo que se deteriora la imagen del gobierno local.

Eso significa que, a partir de cierto momento, las potencias revisionistas sí que podrían tener incentivos para provocar una escalada, asumiendo más riesgos. En el ejemplo antes propuesto, la influencia francesa en las colonias británicas, a finales del siglo XVIII, no fue suficiente para decantar la situación en beneficio de los independentistas, pero contribuyó decisivamente a que la ulterior guerra híbrida o guerra compuesta, diera la victoria de las huestes de George Washington sobre la Corona británica. Las experiencias de Crimea y del Donbas también son emblemáticas, ya que en el primer caso no hubo necesidad de escalada, mientras que el segundo derivó a una guerra híbrida, pero con el resultado de que el gobierno de Kiev ha sido incapaz de impedir el establecimiento de sendas repúblicas que, de facto y pese a la virtual ausencia de reconocimiento internacional, constituyen una suerte de protectorados de Rusia.

LOS MEDIOS DE LA ZONA GRIS

La generación de un relato y su divulgación

El primero y principal de los medios a emplear es la generación de una narrativa que apoye las pretensiones de la potencia revisionista. No suele tratarse de un discurso riguroso, desde el punto de vista histórico, si bien suele tener anclajes en la realidad, a fin de resultar verosímil ante propios y extraños. La escuela social-constructivista ha demostrado la capacidad de ciertos actores para modular de ese modo, no solamente el comportamiento, sino incluso la personalidad, de grandes masas de gente, llegando al extremo de «crear» naciones allí donde no existían (Deutsch, 1969). El objetivo de estos relatos es doble: defender la propia causa, al mismo tiempo que erosionan la legitimidad del Estado en cuyo seno se instaura la zona gris.

Pero ninguna narrativa es eficaz sin los medios adecuados para difundirla. Deutsch alude al sistema educativo, a los *mass-media*, así como a las entidades o redes de entidades de la sociedad civil, que apoyen esa causa. Aunque, en la actualidad, habría que añadir, como mínimo, el papel de Internet (*webs* y *think-tanks*) así como el de las redes sociales. En algunos casos, también es útil una política de concesión de becas a estudiantes extranjeros, para que acudan a las universidades del Estado que genera la zona gris, pero con la mirada puesta en que regresen a su país de origen como estiletes de quien los acogió de ese modo. Algo así es lo que habría estado haciendo Turquía en diversos Estados de Asia Central, a tenor de lo comentado por algunos expertos (Huntington, 1997).

Protagonismo para los civiles

En segundo lugar, la zona gris, por su propia naturaleza, se basa en la movilización de civiles, que son quienes ostentan el protagonismo, a modo de resorte que permita alcanzar los objetivos trazados. Objetivos que son, según hemos visto, «agresivos» por

su propia naturaleza, pero que, precisamente por ello, deben ser modulados en lo que concierne al modo en que se implementan (Brands, 2016). Las movilizaciones subsiguientes suelen ser pacíficas, perfectamente compatibles con el Estado de derecho (manifestaciones masivas). En algunos casos, pueden estar al límite de la legalidad penal (ocupación permanente —o *sine die*— de calles y plazas), o pueden vulnerarla, sin incurrir en grandes dosis de violencia física (rodear sedes parlamentarias). Pero en otros casos, los ilícitos pueden ser flagrantes (las vanguardias de esas masas pueden realizar acciones de *kale borroka*, o bien actos de sabotaje contra infraestructuras, o bien atentados terroristas, o una combinación de esas acciones). Ahora bien, en todos esos casos, las vulneraciones de las normas en las que se incurre suelen subsumirse en el derecho penal interno, sin que lleguen a constituir ningún *casus belli* de acuerdo con el derecho internacional. Esa es la clave.

En otros casos, los actores preponderantes en una zona gris no serán grandes masas, sino que se tratará de funcionarios públicos, pero también dotados de un estatuto civil. Puede tratarse de miembros de fuerzas y cuerpos de seguridad, servicios de guardacostas (o asimilados), personal científico asignado a explotaciones, prospecciones o servicios hidrográficos, etc. Aunque también se pueden dar escenarios mixtos. O se puede incitar la colaboración de pesqueros de modo que, de hecho, siguen estando formalmente al margen de los órganos y/o estructuras militares de cada Estado. Sea como fuere, se evita la necesidad de que el peso de las operaciones lo lleven los militares. Es el modo en el que China viene operando en el mar homónimo, con especial inquina a partir del año 2012 (Baqués, 2018). De hecho, se minimiza su intervención, que quedaría circunscrita a los casos indicados en el punto 4.4. de este capítulo.

Las presiones económicas

Las zonas grises suelen integrar mecanismos de «guerrilla» económica. Las medidas aplicadas pueden ser formalmente legales, como las subvenciones. Pero en estos casos distan de satisfacer el interés público. Más bien se trata de potenciar a quienes están dispuestos a colaborar en la construcción de la zona gris, y de marginar intencionadamente al resto de protagonistas. Lo mismo sucede, si bien de manera todavía más directa, con los boicots a ciertos productos, o a ciertas empresas, con el objetivo de que el defensor del *status quo* integre en su función de costes dicho perjuicio. Por ejemplo, cuando estalló el conflicto sino-japonés en las Senkaku, en otoño de 2012, los chinos orquestaron una campaña contra los negocios japoneses existentes en el continente, y alimentaron la amenaza de que eso se extendiera a las importaciones de productos procedentes del archipiélago.

De hecho, la «guerrilla» económica puede suponer la puesta en marcha de medidas más contundentes, como las *gas wars,* a las que hemos asistido en Europa del Este a lo largo de los últimos años. En el fondo, se trata de embargos encubiertos, que Rusia ha ido modulando en función de los posicionamientos de algunos de los Estados que dependen de ese suministro (Freier, 2016, p. 41). Por ejemplo, cuando Chequia se aprestaba a recibir sistemas de radar asociados al escudo antimisiles promovido por los EE. UU., los problemas de suministro afloraban con la excusa de la aparición de problemas técnicos. Pero la correlación entre ambos hechos era evidente.

El papel de las FFAA

Por último, hay que tener en cuenta que, incluso en la generación de zonas grises, las fuerzas armadas pueden desempeñar algunos roles relevantes. Por un lado, ante la posibilidad de que miembros de sus servicios de inteligencia, o de operaciones especiales, realicen operaciones encubiertas, o incluso secretas, en el territorio en el que se despliega esa zona gris. Su función sería la de supervisar, reforzar o reconducir algunas de las acciones contempladas en los tres primeros apartados de este punto 4, aunque con especial énfasis en el 4.2. Pero, a fin de cumplir con lo previsto en el punto 3.3. las acciones más contundentes, susceptibles de generar situaciones rayanas con un *casus belli*, deberían ser ejecutadas por ciudadanos del territorio en el que se ha establecido esa zona gris.

El otro rol fundamental de las fuerzas armadas consiste en movilizar sus fuerzas convencionales a fin de generar presión contra el Estado que soporta el establecimiento de una zona gris. Pero sin que crucen la frontera. Se trata de mecanismos disuasorios, cuyo objetivo es impedir o limitar las acciones más contundentes que pueda tratar de desarrollar el Estado perjudicado por una zona gris. A decir de algunos expertos, esta situación en la que actualmente se vive en Polonia, en relación con Rusia, a partir de maniobras como las *Zapad*, que implican la movilización de decenas de miles de militares rusos en suelo Bielorruso. Pero podríamos añadir la presión ejercida por los aviones de la fuerza aérea rusa en los Estados bálticos, en los que existen minorías rusas, capaces de apoyar, llegado el caso, alguna tentativa comprendida entre las citadas en el punto 3.2. de este análisis[3].

CONCLUSIONES

La zona gris responde a una estrategia en la que la guerra abierta es descartada, debido principalmente a las capacidades de respuesta militar que mantienen las potencias defensoras del *status quo* internacional. Por lo tanto, se trata de un modo de alcanzar objetivos de gran relevancia estratégica, sin necesidad de generar ningún *casus belli*. Se trata de una de las razones que convierte en plausible la hipótesis según la cual este tipo de conflictos, de muy baja intensidad, están llamados a proliferar en los próximos años.

La principal ventaja de esta política radica en la ecuación coste-beneficio que genera en favor del Estado que emplea estos escenarios. Porque, en caso de que la zona gris consiga desplegar todos los efectos previstos, puede causar cambios relevantes en el sistema político global, con poco o nulo desgaste por parte de quien la genera. Pero, ante la presumible falta de respuesta ajena, incluso cuando esos objetivos no se cubran, la zona gris deteriora a terceros Estados, e incluso a organizaciones internacionales en las que estos se integran, poniendo en duda la credibilidad de esas alianzas, así como, finalmente, la de las potencias que las lideran.

---

[3] E incluso los ciberataques sufridos en Estonia, en 2007, a partir de un hecho secundario, al menos en apariencia (la retirada de una estatua conmemorativa del sacrificio de los soldados soviéticos en la 2.ª Guerra Mundial). Hay que tener en cuenta de que Rusia ha repartido pasaportes entre los ciudadanos residentes en diversos Estados de su extranjero próximo, con la esperanza de que apoyen su causa en caso de conflicto en el interior de esas zonas grises.

Por otra parte, la zona gris confiere la iniciativa estratégica al Estado que la despliega, ya que los demás actores son obligados a diseñar mecanismos de respuesta que, dadas las características del reto planteado, suelen autolimitarse, para evitar tener que pasar como los agresores. En este sentido, es esperable que la expansión de las zonas grises, opere incluso a modo de un test (*probing behavior*) cuya utilidad sería la de comprobar tanto el grado de celo, como la agilidad, de que hacen gala los Estados rivales a la hora de proceder a la defensa de sus intereses. El problema, en ese sentido, estriba en que las zonas grises terminen siendo no una alternativa, sino un acicate —o incluso una preparación— para el estallido de guerras futuras. Mientras que deslindar ambas posibilidades (zona gris como fin en sí misma, o como medio para escalar en mejores condiciones, y en el momento idóneo) no resulta fácil en la práctica. Razón de más para estar atentos a la evolución, conceptual y empírica, de un fenómeno que va a ir creciendo en importancia en los próximos tiempos.

BIBLIOGRAFÍA

– BAQUÉS, Josep. «La versión china de la zona gris». *Revista General de Marina*, 275 (1). 2018, pp. 557-564.

– BRAND, Hal. «Paradoxes of the Gray Zone». Philadelphia: Foreign Policy Research Institute. 2016.

– CHAMBERS, John. *Countering Gray Zone-Hybrid Threats*. West Point (NY). Modern War Institute, 2016.

– DEUTSCH, Karl. *Nationalism and Social Comunication —An Inquiry into the Foundation of Nationality.* Cambridge (MA) & Londres: MIT Press, 1969 [1953].

– ECHEVARRÍA, Antulio. *Operating in the Gray Zone: an Alternative Paradigm for US Military Strategy*. Carlisle Barracks: US Army War College, 2016.

– FREIER, Nathan. *Outplayed: Regaining Strategic Initiative in the Gray Zone*. Carlisle Barracks: Strategic Studies Institute, 2016.

– HOFFMANN, Frank G. *Future Hybrid Threats: An Update*. Washington DC: Center for Strategic Research, Institute for National Strategic Studies, 2012.

– HUNTINGTON, Samuel. *El choque de las civilizaciones y la reconfiguración del orden mundial.* Barcelona: Paidós, 1997.

– KAPUSTA, Philip. «The Gray Zone». *Special Warfare*, 28 (4). 2015, pp. 18-25.

– MAZARR, Michael J. *Mastering the Gray Zone: Understanding a Changing Era of Conflict.* Carlisle Barracks: US Army War College, 2015.

PONENCIAS DEL ÁREA 2
Amenaza híbrida y ciberdefensa

CHINA Y RUSIA EN LAS ZONAS GRISES DEL CIBERESPACIO

D. GUILLEM COLOM PIELLA
Profesor de Ciencia Política en la Universidad Pablo de Olavide y codirector de THIBER

CHINA Y RUSIA EN LAS ZONAS GRISES DEL CIBERESPACIO

D. GUILLEM COLOM PIELLA
Profesor de Ciencia Política en la Universidad Pablo de Olavide y codirector de THIBER

INTRODUCCIÓN

Conceptos como amenaza híbrida —que constituye el tema central de este XXVII Curso Internacional de Defensa— o zona gris se han popularizado para definir las actividades ambiguas que realizan países como Rusia, China, Irán o Corea del Norte para proyectar su influencia en el exterior, negando de forma plausible su responsabilidad y evitando cruzar el umbral de un conflicto que difícilmente podrían ganar.

La zona gris, definida como la franja que separa la paz de la guerra abierta es, por naturaleza, ambigua. Esta ambigüedad es la que permite a potencias revisionistas como las arriba mencionadas proyectar su poder más allá de sus fronteras sabiendo que, si sus actividades pueden ser negadas de forma plausible y no afectan intereses vitales, difícilmente tendrán una respuesta clara y efectiva. En otras palabras, observadas de forma aislada, estas acciones que podrán orientarse contra toda la sociedad difícilmente constituirán un *casus belli* porque siempre intentarán situarse bajo el umbral del conflicto. Sin embargo, su efecto agregado a largo plazo mediante la «táctica del salami»[1] sí podría alterar las correlaciones de fuerzas existentes[2].

Aunque muchas de estas actividades se realizan en el mundo físico (las tradicionales incursiones de pesqueros chinos en islas en disputa con Japón o los recientes ataques

---

[1] HADDICK, Robert. «Salami Slicing in the South China Sea: China's slow, patient approach to dominating Asia». *Foreign Policy*. 3 de agosto de 2012 [en línea]. https://foreignpolicy.com/2012/08/03/salami-slicing-in-the-south-china-sea/.

[2] JORDÁN, Javier. «El conflicto internacional en la zona gris: una propuesta teórica desde la perspectiva del realismo ofensivo». *Revista Española de Ciencia Política*, n.º 48. Noviembre 2018, pp. 129-151.

sobre petroleros saudíes en el Golfo Pérsico), cada vez más se realizan también en el mundo virtual. Ello se debe a la ambigüedad, anonimidad, asimetría, economía y ubicuidad propias del ciberespacio. Estas características permiten a muchos actores proyectar su poder de manera asimétrica dificultando la atribución de sus acciones, impidiendo la asignación de responsabilidades legales, imposibilitando cualquier represalia contra ellos y comprometiendo la credibilidad de las herramientas disuasorias del actor que ha sido atacado. Inicialmente, sucesos como los ciberataques rusos sobre Estonia (2007) y Georgia (2008) o el ciberespionaje chino [que culminó con la famosa atribución de la amenaza persistente avanzada 1 (APT-1) en 2013][3], motivaron que el foco de atención estratégico se centrara en las actividades de explotación y los potenciales efectos disruptivos que podría tener un ciberataque contra servicios, sistemas o redes. De ahí el interés de la comunidad internacional en determinar qué tipo de ciberataque podría constituir un *casus belli* y en plantear un enfoque «clásico» a la disuasión por negación y castigo. Sin embargo, la expansión del califato islámico en Iraq, Irán o Yemen, la ocupación de Crimea, la invasión del este de Ucrania o las operaciones de influencia en los pasados comicios presidenciales estadounidenses demostraron que el entorno *online* también posibilitaba otras actividades de mucho menor perfil, pero igualmente susceptibles de afectar la seguridad nacional. La propaganda multicanal, el perfilado de usuarios para reforzar su filtro burbuja, la viralización de noticias falsas o la filtración de información personal comprometida, también podían servir para explotar las divisiones existentes en las sociedades e influir sobre sus opiniones públicas. Además, las campañas rusas en Crimea, Ucrania o Siria no solo volvieron a poner de manifiesto la relevancia de la guerra electrónica en los conflictos modernos, sino también demostraron el potencial empleo del espacio radioeléctrico para realizar actividades en la zona gris, desde interferir comunicaciones, degradar sistemas de defensa aérea, suplantar las señales de GPS, hasta obstaculizar actividades de inteligencia[4].

¿Qué tienen en común las ciberoperaciones de explotación, defensa o ataque, las operaciones de influencia en el ciberespacio o las actividades en el espacio radioeléctrico? Todas ellas se ejecutan en el espacio informativo, que engloba el ciberespacio y cuyos efectos se pueden observar en el ámbito lógico, físico y cognitivo. Aunque el espacio informativo como nuevo dominio de la guerra se popularizó con el auge de la revolución en los asuntos militares (RMA) a principios de la década de 1990[5], con el paso a la transformación a finales de la década fue reemplazado —quizás por la penetración global de Internet, su impacto en la economía mundial o la creciente dependencia sobre los

---

[3] MANDIANT. *APT-1. Exposing one of China's Cyber Espionage Units*. Alexandria: Mandiant, 2013 [en línea]. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

[4] Descuidada desde el fin de la Guerra Fría, la guerra electrónica no solo ha experimentado un renacimiento a raíz de las actividades rusas en Crimea, Ucrania o Siria, sino que la digitalización de las comunicaciones ha motivado una creciente convergencia entre el espacio cibernético y el radioeléctrico. Ello ha llevado al desarrollo de las cyberspace electromagnetic activities (CEMA).

[5] Condicionada por los efectos revolucionarios de la aplicación de las tecnologías de la información en el ámbito militar, la RMA popularizó el concepto de guerra informativa. Se asumía que esta forma de conflicto propia de la Era de la Información permitiría dañar, degradar o destruir los sistemas de información del adversario para paralizar o confundir su ciclo de toma de decisiones o paralizar su capacidad para combatir. Esta idea culminó en el concepto de guerra de mando y control, que utilizaría guerra electrónica, operaciones psicológicas, seguridad operativa y engaño para degradar los procesos de toma de decisiones del adversario (COLOM, Guillem. *Entre Ares y Atenea, el debate sobre la Revolución en los Asuntos Militares*. Madrid: IUGM-UNED, 2008).

servicios e infraestructuras que lo posibilitaban— por el ciberespacio como un dominio eminentemente técnico y como quinto dominio de la guerra…al menos para Occidente[6].

Debido principalmente a su herencia histórica y política, tanto Rusia como China entienden que la información es una relevante herramienta para la proyección del poder nacional y uno de los pilares de la soberanía nacional, sino también uno de los principales activos a proteger para mantener su estabilidad política, social o moral frente a influencias nocivas externas. Estas concepciones que priman la protección del espacio informativo nacional y la proyección de la influencia exterior —algo que tradicionalmente se realizaba vía propaganda política— son anteriores a la llegada de Internet. Sin embargo, en la década de 1990 ambos países alertaron de que las nuevas tecnologías y las posibilidades de que la población obtuviera distintas fuentes de información no solo constituían una amenaza a la seguridad por su potencial desestabilizador, sino también por la dependencia tecnológica y debilidad estratégica que se generaba con Estados Unidos. En consecuencia, no solo consideraron necesario restringir el acceso a Internet e intentar que la comunidad internacional apoyara su control y regulación para proteger la seguridad nacional, sino también crear un ecosistema cibernético propio y potencialmente aislado del resto del mundo[7]. Paralelamente, sus estrategas militares entendieron que la información —y no las armas de precisión o los sensores tal y como inicialmente asumía Occidente en plena euforia revolucionaria— podía ser el pilar de esta RMA que prometía transformar la guerra[8]. En consecuencia, asumieron que la guerra informativa sería uno de los pilares de sus transformaciones militares, el fundamento de los conflictos futuros y el marco general donde no solo se emplaza el ciberespacio, sino el entorno donde se ejecuta cualquier actividad física, lógica y cognitiva vinculada con el uso de la información como vector, objetivo o medio. Además, ambos países —cuyas concepciones de la guerra informativa tienen importantes similitudes pero también significativas diferencias[9]— han integrado con gran éxito las actividades informativas en estrategias multidimensionales al proyectar el poder y los intereses nacionales en la zona gris del conflicto. Teniendo en cuenta estos elementos, a continuación se explicará brevemente cómo Rusia y China conciben la guerra informativa y cómo la utilizan en la zona gris del conflicto.

LA GUERRA INFORMATIVA RUSA

Rusia considera la guerra informativa (*informatsionnaya voyna*) como uno de los pilares de las «guerras de nueva generación» y el fundamento de los conflictos futuros[10].

---

6 Sin embargo, las doctrinas aliadas de operaciones de información —más restringidas que la guerra informativa planteada en la década de 1990— contemplan las ciberoperaciones como uno de sus componentes.

7 BENDETT, Samuel y KANIA, Elsa. *A new Sino-Russian high-tech partnership. Authoritarian innovation in an era of great-power rivalry*. Camberra: Australian Strategic Policy Institute, 2019.

8 Para el caso ruso, GAREEV, Makhmut. *If War Comes Tomorrow? The Contours of Future Armed Conflict*. Londres: Frank Cass, 1998; y para el caso chino, LIANG, Qiao y XIANGSUI, Wang. *Unrestricted warfare: China's master plan to destroy America*. Nueva York: Filament Books, 2004.

9 WALLIS, Jake. «China and Russia aren't the same when it comes to information warfare». *The Strategist*. 25 de septiembre de 2019 [en línea]. https://www.aspistrategist.org.au/china-and-russia-arent-the-same-when-it-comes-to-information-warfare/.

10 CHEKINOV, Sergei y BOGDANOV, Sergei. «The Nature and Content of a New-Generation War», *Military Thought* (edición inglesa), n.º 4. Invierno 2013, pp. 12-22.

Fundamentada en varias tradiciones —desde la *maskirovka* militar, las medidas activas soviéticas[11], la subversión comunista o las teorías sobre el control reflexivo— y desarrollada en el marco de la RMA, la guerra informativa rusa es objeto de acalorados debates tanto dentro como fuera del país. Aunque existen varias fuentes oficiales que se refieren al concepto y la doctrina básica de las fuerzas armadas resalta su importancia, la doctrina específica permanece clasificada y su guerra informativa continúa rodeada de un halo de misterio.

Entre múltiples definiciones más o menos oficiales que pueden hallarse, la más popular la considera como «…un conflicto entre dos o más estados en el espacio informativo con la finalidad de dañar los sistemas, procesos, recursos o estructuras informativas, erosionar los sistemas políticos, económicos y sociales, llevar a cabo campañas psicológicas masivas contra la población del estado para desestabilizar la sociedad y el gobierno o forzar al estado para que tome decisiones en el interés de sus oponentes[12]». Calificada por muchos estrategas del país como el componente de una confrontación informativa global en la que Occidente quiere imponer su voluntad sin recurrir al enfrentamiento militar directo, la guerra informativa es una herramienta «híbrida» que va mucho más allá de la desinformación, las noticias falsas o los ciberataques.

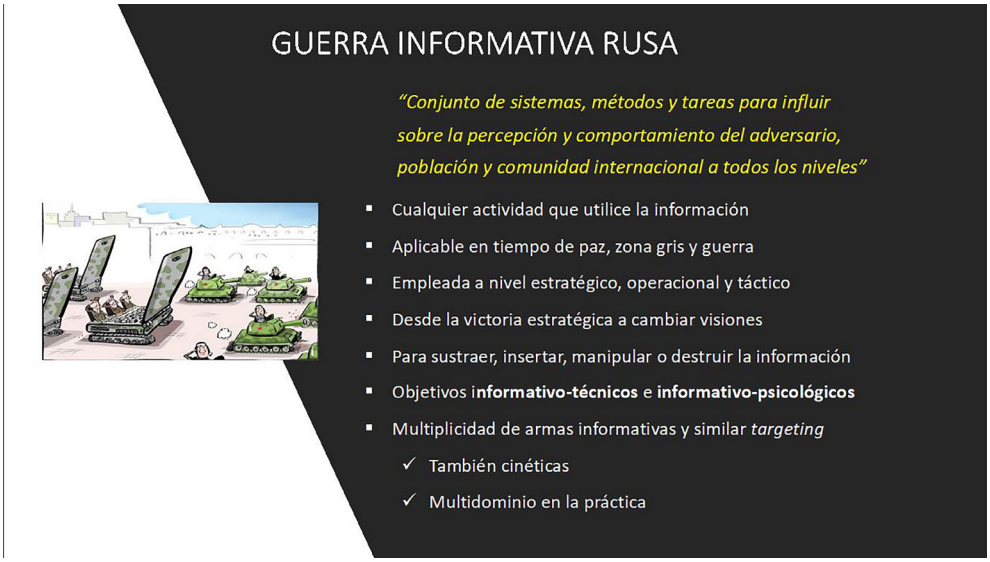


Figura 1: los rasgos definitorios de la guerra informativa rusa. FUENTE: elaboración propia (presentación de la ponencia).

[11] En términos generales, estas actividades subversivas combinaban desinformación con propaganda, manipulación de medios y fabricación de información. También podían incluir el uso de medios de comunicación clandestinos para diseminar información falsa, *proxies* (partidos, sindicatos o asociaciones con acreditados vínculos con Moscú), organizaciones pantalla (entidades científicas, culturales o pacifistas sin aparente relación con la Unión Soviética), agentes de influencia (que usarían su posición pública para apoyar secretamente al Kremlin), manipulación económica, chantaje o colaboradores que apoyarían la narrativa soviética. Las nuevas tecnologías han permitido adaptar estas viejas herramientas al entorno *online* y ampliar enormemente el alcance y efectividad de las medidas activas.

[12] MINISTERIO DE DEFENSA RUSO. *Conceptual Views regarding the Activities of the Armed Forces of the Russian Federation in Information Space*. Moscú: Ministerio de Defensa, Moscú, 2011, art. 1.

Las crónicas occidentales subrayan su empleo como arma asimétrica en la zona gris del conflicto mientras destacan técnicas como el control reflexivo (o la manipulación del proceso de toma de decisiones), la manipulación de la opinión pública para que esta acepte las acciones rusas o las tradicionales actividades de subversión o desestabilización. Sin embargo, Moscú entiende que la guerra informativa puede servir tanto para alcanzar los objetivos políticos sin la necesidad de utilizar la fuerza armada con una amplia gama de actividades no-militares en los dominios físico, lógico y cognitivo para negar, sabotear o manipular la información[13], como para contribuir a la conducción —modelando la opinión pública, apoyando a las unidades terrestres, navales o aéreas o batiendo objetivos informativos— de las operaciones militares[14]. Susceptible de utilizarse en tiempo de paz, escalada y conflicto abierto en los niveles estratégico, operacional y táctico, la guerra informativa posee una vertiente ofensiva, enfocada al logro de la superioridad informativa sobre el adversario, y defensiva, para garantizar la seguridad informativa del país y así contribuir a la estabilidad estratégica[15].

Además, entendiendo que el entorno informativo comprende todo lo relacionado con la información y que cualquier soporte, canal, medio o vector físico, radioeléctrico, digital o cognitivo puede ser destruido, degradado, alterado o corrompido, cualquier tecnología, medio o actividad que posea una dimensión informativa puede convertirse en un arma informativa. En consecuencia, la paralización de un sistema de defensa antiaérea, la destrucción de una estación de comunicaciones, la suplantación de una señal de GPS, la interferencia de las transmisiones de radiotelevisión, la denegación de un servicio web, la exfiltración de información personal, la eliminación de un periodista, una declaración oficial, una cadena de bulos en *Whatsapp*, una imagen alterada digitalmente en *Instagram* o un meme en *Twitter* son algunas de las armas que pueden utilizarse para combatir en el espectro informativo. Combinadas, estas se orientarán al logro de efectos informativo-técnicos sobre las infraestructuras y sistemas enemigos e informativo-psicológicos sobre sus percepciones. Para ello, se estima que Rusia puede utilizar una amplia variedad de herramientas, algunas de las cuales similares a las usadas en la doctrina occidental (guerra electrónica, operaciones psicológicas, inteligencia, engaño o ciberoperaciones[16]) y otras vinculadas con las tradicionales medidas activas (control social, desinformación, manipulación de información, chantaje, extorsión o presión en medios de comunicación y en redes sociales)[17]. Dependiendo de si Rusia se halla en periodo de paz, zona gris o guerra, el Kremlin usará distintos vectores de forma más o me-

---

13 Fundamentada en la interpretación rusa de los conceptos de guerra híbrida, no-letal o no-convencional occidentales, esta idea ha motivado que muchos cronistas occidentales hayan definido erróneamente la guerra informativa rusa como guerra híbrida (COLOM, Guillem. «La amenaza híbrida: mitos, leyendas y realidades». *Documento de opinión del IEEE*, n.º 24. Marzo 2019, [en línea]. http://www.ieee.es/Galerias/fichero/docs_opinion/2019/DIEEEO24_2019GUICOL-hibrida.pdf.

14 KJELLÈN, Jonas. *Russian Electronic Warfare. The role of Electronic Warfare in the Russian Armed Forces*. Estocolmo: FOI, 2018.

15 SAIFETDINOV, Charis. «Informatsionnoe protivoborstvo v voennoi sfere». *Voennaia mysl,* núm. 7. 2014, pp. 38-41.

16 Sin embargo, téngase en cuenta que la doctrina rusa no distingue las ciberoperaciones defensivas, de explotación o ataque —denominadas por muchos como guerra tecnoesférica— de otras actividades que utilicen el ciberespacio como vector. De la misma manera, tampoco distingue el ciberespacio del entorno informativo.

17 FRANKE, Ulrik. *War by non-military means. Understanding Russian Information Warfare*. Estocolmo: FOI, 2015.

nos abierta para garantizar su seguridad informativa, mantener el equilibrio estratégico, modelar la opinión pública, debilitar la voluntad del oponente o alcanzar la superioridad informativa con todos los medios posibles.

En conclusión, Moscú entiende que la guerra informativa es un elemento fundamental de la confrontación geopolítica global y una actividad integral que requiere la participación de una amplia gama de actores y de medios. Aunque es el componente principal de las guerras de nueva generación rusas y puede utilizarse en todo el espectro del conflicto, quizás es en la zona gris donde esta puede —combinando actividades de influencia, desestabilización y subversión en el mundo *online* con labores de explotación y ataque de sistemas informáticos o la degradación de señales radioeléctricas— desarrollar todo su potencial, enmascarando su procedencia, dificultando su atribución y apoyando el logro de sus objetivos de política exterior sin que ello pueda motivar escaladas militares de imprevisibles consecuencias.

LA GUERRA INFORMATIVA CHINA

Al igual que Rusia, China también considera la guerra informativa (*xinxi zhan*) como uno de los pilares de los conflictos posmodernos, un componente trasversal de las «tres» guerras futuras (sin contacto, no-linear y asimétrica) y una de las competencias que debe dominar el Ejército de Liberación Popular. Basada inicialmente en la emulación de los conceptos estadounidenses[18], la guerra informativa china se ha ido configurando desde la década de 1990. Teniendo como principal punto de partida la identificación de las lecciones de la guerra del Golfo de 1991 y el auge de la RMA, su desarrollo se ha producido siguiendo los debates occidentales sobre la transformación de la guerra y dialogando con su cultura estratégica.

Asumiendo que en la Era de la Información el poder nacional se mide en términos informativos, los líderes chinos concluyeron hace un cuarto de siglo que el auge y caída de las potencias estaría determinado por la capacidad para generar, obtener, transmitir, analizar y explotar la información. En consecuencia, China debía adaptarse a la Era de la Información apoyando el desarrollo nacional (legitimando así el Partido Comunista Chino), creando su propio ecosistema de innovación tecnológica, y preparando al Ejército de Liberación Popular para la guerra informatizada (*xinxihua zhanzheng*). Esta transformación cuyos pilares fueron establecidos por el premier Yang Zemin tras la espectacular victoria de la coalición liderada por Estados Unidos en la Operación Tormenta del Desierto, se lograría reduciendo la entidad de sus fuerzas, mecanizando sus unidades e informatizando sus procesos. Ello permitiría al país combatir eficazmente en «guerras locales en ambientes de alta tecnología» y, posteriormente, en «guerras locales en ambientes informatizados»[19].

---

[18] Sin embargo, es posible hallar una obra china de 1985 que ya vinculaba la revolución de la información con el surgimiento de la guerra informativa (MULVENON, James. «The PLA and Information Warfare», en: MULVENON, James y YANG, Richard (eds.). *The People's Liberation Army in the Information Age*. Washington DC: RAND Corporation, 1999, p. 177).

[19] Para comprender estos cambios en la concepción estratégica china, es muy recommendable la lectura de la siguiente obra: MCREYNOLDS, Joe (ed.). *China's Evolving Military Strategy*. Washington DC: The Jamestown Foundation, 2017.

Fundamentada en varias tradiciones —desde la guerra informatizada que la enmarca, la guerra política que la permea, la guerra revolucionaria que todavía la inspira o enseñanzas de Sun Tzu y de Mao Tse-Tung que la integran en su cultura estratégica[20]— y desarrollada en el marco de la RMA con características chinas[21], la guerra informativa china es objeto de importantes debates fuera del país. Aunque existe abundante literatura extranjera y varias fuentes tanto oficiales como oficiosas del país vienen haciendo referencia al concepto desde los noventa, la doctrina militar se mantiene clasificada y su guerra informativa continúa siendo una incógnita para los estrategas occidentales. Muchos de ellos centran su interés en las ciberoperaciones —que China define como guerra en redes (*wangluo zhan*)—, las operaciones psicológicas o las actividades de denegación y engaño, subrayar su carácter asimétrico y discutir sobre si esta permitiría triunfar en conflictos sin la necesidad de combatir cuerpo a cuerpo[22]. Sin embargo, la guerra informativa china es más compleja y amplia.

El diccionario terminológico militar del Ejército de Liberación Popular define la guerra informativa como aquellas «…actividades realizadas por los contendientes en el dominio informativo. Incluye la protección de los recursos informativos, el logro de la iniciativa en la producción, transmisión y gestión de la información o la disrupción de la capacidad del adversario para transmitir la información con el objeto de establecer las condiciones necesarias para disuadir, combatir y ganar conflictos[23]». Ello requiere la ejecución de una amplia gama de actividades físicas, lógicas y cognitivas en el plano político (librando las llamadas tres guerras: de opinión pública, psicológica y legal)[24] y militar (mediante guerra electrónica, guerra en redes o ciberguerra, guerra psicológica, guerra de mando y control y guerra de inteligencia) para lograr la supremacía informativa[25]. Mientras el planeamiento de las primeras recae en la Comisión Militar Central del Partido Comunista Chino, la ejecución de las segundas es realizada por la Fuerza de Apoyo Estratégico del Ejército de Liberación Popular, encargada de las actividades espaciales, ciberespaciales, electrónicas y psicológicas.

---

20 FERGUSON, Robyn. *Information Warfare with Chinese Characteristics: China's Future of Information Warfare and Strategic Culture*. Forth Leavenworth: U.S. Army Command and General Staff College, 2011.

21 NEWMYER, Jacqueline. «The Revolution in Military Affairs with Chinese Characteristics». *Journal of Strategic Studies*, vol. 33, n.º 4. Invierno 2010, pp. 483-504. De hecho, el general Wang Pufeng, considerado el «padre» de la guerra informativa china, vinculó ambas ideas en la obra seminal «Guerra informativa y revolución en los asuntos militares» de 1995 (PUFENG, Wang. *Xinxi zhanzheng yu junshi geming*. Pekín: Junshi Kexueyuan, 1995).

22 YOSHINARA, Toshi. *Chinese Information Warfare. A phantom menace of emerging threat?*. Carlisle Barracks: Strategic Studies Institute, 2001.

23 ACADEMIA DE CIENCIAS MILITARES DEL EJÉRCITO DE LIBERACIÓN POPULAR. *Chinese People's Liberation Army Military Terminology*. Pekín: AMS Publishing House, 1997, pp. 764-766.

24 Como bien resume Dean Cheng, el autor de uno de los mejores trabajos publicados sobre guerra informativa china, estas actividades de guerra política «…strive to shake the enemy's will, question their motives, induce divides and splits within the enemy's ranks, and constrain their activities […] erode an adversary's will and thus reduce the ability to sustain any resistance to more kinetic operations». (CHENG, Dean. *Cyber dragon: Inside China's information warfare and cyber operations*. Santa Barbara: Praeger, 2017, p. 42).

25 Recuérdese, no obstante, que la guerra informativa apoya a las operaciones integradas que, desde una perspectiva informatizada, integran distintas fuerzas, dominios y actividades, siendo las armas de precisión de largo alcance un elemento muy relevante de apoyo para lograr el dominio informativo.

Figura 2: los fundamentos de la guerra informativa china. FUENTE: elaboración propia (presentación de la ponencia).

Sin embargo, la misma naturaleza, ubicuidad, interconexión, globalidad y variedad de actores que interactúan en el espacio informativo obliga a que estas acciones deban realizarse tanto en tiempo de paz como en periodo de guerra, y tanto contra objetivos militares como civiles[26]. En consecuencia, los estrategas chinos entienden que actividades como las operaciones psicológicas, la propaganda política, la guerra legal o la penetración en las redes adversarias para detectar vulnerabilidades deben realizarse contra toda la sociedad tanto en tiempo de paz como antes del arranque de las hostilidades. En otras palabras, al difuminar la frontera entre la paz y la guerra mediante el establecimiento —al menos para nuestra concepción— de una amplia zona gris que se solapa con la competición pacífica, China considera legítimo emplear múltiples actividades psicológicas, propagandísticas, electrónicas o cibernéticas que no solo apoyen la consecución de la ventaja informativa en caso de crisis o conflicto, sino también apoyar —utilizando su propio enfoque integral— el desarrollo nacional en todas sus dimensiones[27].

Para llevar a cabo estos cometidos, la guerra informativa china combina una amplia gama de actividades ofensivas, defensivas y de explotación[28] junto con la protección

[26] A modo de ejemplo, aunque podrían relacionarse muchas actividades informativas en la zona gris, la decisión china de crear una zona de identificación de defensa aérea (ADIZ) que cubría las islas Diaoyu/Senkaku (cuya soberanía está disputada por Japón, China y Taiwán) y se solapaba con zonas económicas exclusivas reclamadas por China, Japón y Corea del Sur, combinaba guerra legal con guerra psicológica y guerra informativa (WORTZEL, Larry. *The Chinese People's Liberation Army and Information Warfare*. Carlisle Barracks: Strategic Studies Institute, 2014).

[27] En consecuencia, el popular ciberespionaje industrial chino —realizado mayoritariamente por unidades vinculadas con el Ejército de Liberación Popular— no solo debe interpretarse como un medio para la obtención de información relevante para el desarrollo nacional, sino también como una herramienta para conocer al potencial adversario (JOHNSON, Derek. «How China uses cyber theft and information warfare». *Federal Computer Week*. 6 de mayo de 2019 [en línea]. https://fcw.com/articles/2019/05/06/china-information-warfare-dod-report.aspx.

[28] Más concretamente se refieren a operaciones de información de reconocimiento, ofensivas y defensivas (recuérdese que la doctrina occidental tiende actualmente a integrarlas dentro de las ciberoperaciones), ope-

de sus propios recursos informativos (que también supone la protección de su población frente a injerencias externas que puedan degradar la legitimidad del Partido Comunista Chino)[29] y la disuasión informativa. Enmarcada dentro de la concepción china (*weishe*) que combina disuasión, persuasión y coerción, esta se vale de la dependencia global de Internet para demostrar su ventaja informativa y los potenciales efectos de una potencial escalada. Además, aunque las actividades informativas chinas en redes sociales son, por lo general, menos activas, sofisticadas y estratégicas que las operaciones rusas al centrarse en las vertientes psicológica, propagandística, legal y de opinión pública, no debe olvidarse que son especialmente activas tanto en el interior del país como en su área de influencia directa[30]. No obstante, no puede descartarse que las lecciones aprendidas por el Kremlin tanto en las campañas militares de Crimea, Ucrania, Siria y de las actividades de influencia en procesos políticos extranjeros sirvan para que China amplíe sus capacidades en esta materia y plantee un enfoque más global.

CONCLUSIONES

Tal y como se ha explicado en las páginas anteriores, la zona gris es, por su propia naturaleza, ambigua. Esta ambigüedad es la que está facilitando que actores como Rusia o China adopten estrategias multidimensionales —popularizadas como «amenazas híbridas»— para proyectar su poder negando de forma plausible su autoría, degradando la disuasión y reforzando su posición relativa en el mundo del siglo XXI. Aunque muchas de estas actividades se realizan en el plano físico, muchas se realizan en el plano virtual buscando efectos en las dimensiones física, lógica o cognitiva.

Aunque las concepciones informativas china y rusa tienen numerosas similitudes (desde sus tradiciones vinculadas con el control de la información, su interpretación sobre el impacto de la RMA en los conflictos futuros, una concepción del espacio informativo mucho menos tecnocéntrica que occidente o la consideración del ciberespacio como un componente de la guerra informativa), también muestran significativas diferencias motivadas por su cultura estratégica, tradición política o capacidad técnica. En este sentido, la guerra informativa rusa en la parte baja de la zona gris parece adaptar las medidas activas soviéticas al entorno *online*, en la parte alta es la vertiente militar la que toma la iniciativa. Por otro lado, la guerra informativa china en la zona gris parece más centrada en la propaganda y la guerra legal para apoyar la guerra política, en las actividades de explotación mediante APT contra países extranjeros para apoyar el desarrollo nacional y actividades específicas de disuasión informativa —incluyendo, quizás, el *spoofing* del GPS de varios buques estadouniden-

raciones de salvaguarda de la operación y operaciones de disuasión informativa, integrando a su vez cada una de ellas una amplia gama de actividades físicas, lógicas, electrónicas y cognitivas.

[29] CHENG, *op. cit.*, pp. 53-78 y MAZARR, Michael *et al.* «Hostile Social Manipulation: Chinese Activities», en: *Hostile Social Manipulation. Present Realities and Emerging Trends*. Santa Barbara: RAND Corporation, 2019, pp. 105-166.

[30] MAZARR, *op cit.*, pp. 113-126, y para los aspectos más actuales vinculados con las protestas de Hong Kong, véase: UREN, Tom; THOMAS, Elise y WALLIS, Jacob. *Tweeting through the Great Firewall*. Canberra: International Cyber Policy Centre – Australian Strategic Policy Institute, 2019.

ses en el mar del Sur de la China[31]— para mostrar las capacidades chinas en este dominio.

En cualquier caso, ambos países entienden que la guerra informativa es más que la ciberguerra, que puede utilizarse en todo el espectro del conflicto, que puede integrarse en estrategias multidimensionales, que puede integrarse en tácticas híbridas y que es mucho más que la propaganda, la desinformación, los ciberataques o el empleo de *trolls* y *bots* en redes sociales.

[31] WOODY, Christopher. «The Navy's 4th accident this year is stirring concerns about hackers targeting US warships». *Business Insider*. 24 de agosto de 2017 [en línea]. https://www.businessinsider.com/hacking-and-gps-spoofing-involved-in-navy-accidents-2017-8?IR=T.

GUERRA HÍBRIDA Y CIBERESPACIO

D. ENRIQUE CUBEIRO CABELLO
CN. jefe de Estado Mayor del Mando Conjunto de Ciberdefensa

GUERRA HÍBRIDA Y CIBERESPACIO

D. ENRIQUE CUBEIRO CABELLO
CN. jefe de Estado Mayor del Mando Conjunto de Ciberdefensa

INTRODUCCIÓN

En los últimos años, se ha producido una grave distorsión del término amenaza híbrida, hasta el punto que el ciudadano medio asocia el término, casi de forma exclusiva, con las denominadas *fake news*, a las que en lo sucesivo me referiré como bulos, término que la Real Academia Española de la Lengua define como noticia falsa que se difunde, generalmente, con el fin de perjudicar a alguien.

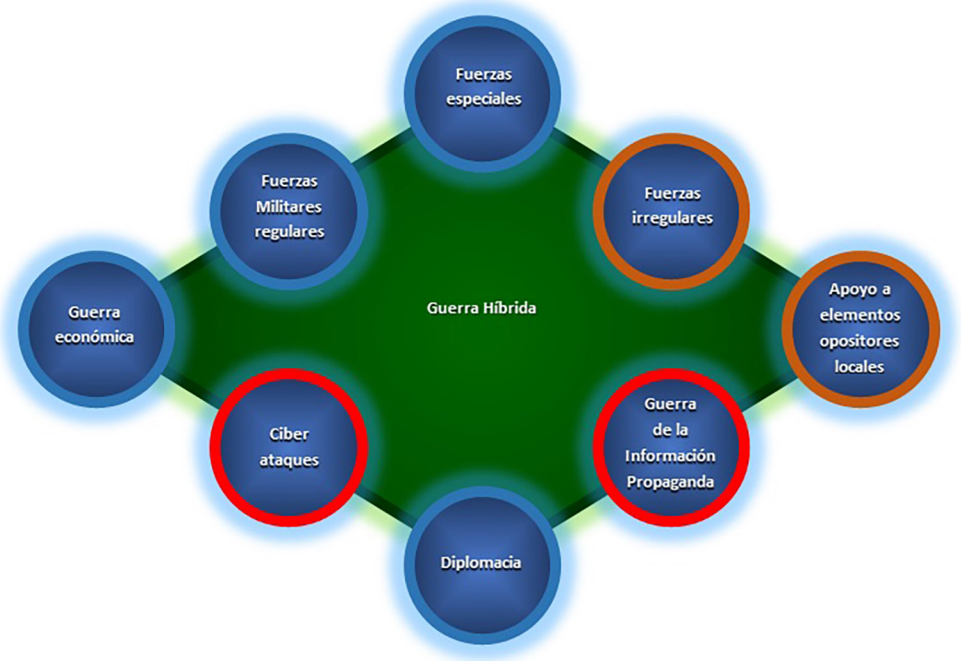
Es importante recordar que el término híbrido procede en sus orígenes de la naturaleza no solo militar de este tipo de contienda. Es decir, el término híbrido se aplicó en sus orígenes al empleo en el conflicto de otras formas de actuación más allá de las puramente militares.

Conceptualmente, la guerra híbrida se basa en el uso coordinado y sincronizado de una amplia gama de instrumentos contra el adversario, graduando su intensidad y evitando en lo posible la confrontación militar directa e, incluso, cualquier posible reacción del oponente.

A diferencia de una invasión militar a gran escala o una contienda bélica con frentes clásicos, la guerra híbrida combina el empleo de estrategias militares no convencionales

con operaciones hostiles de inteligencia, comunicación persuasiva o amenazas y presiones políticas y económicas que entran en el terreno de la guerra psicológica. Acciones que buscan como fin último derrotar, debilitar o someter la voluntad del adversario.

En realidad, no es un concepto nuevo, aunque ahora se nos presente bajo un nombre diferente. En esencia, sus planteamientos teóricos ya aparecen en los grandes clásicos de la estrategia, como Sun Tzu y von Clausewitz. Su única novedad es el salto cualitativo experimentado a raíz del empleo de las nuevas tecnologías y, fundamentalmente, de Internet.



De toda la panoplia de acciones propias de la amenaza híbrida, que es tan amplia como heterogénea, algunas de las más relevantes (ciberataques, desinformación o propaganda) se desarrollan fundamentalmente en o a través del ciberespacio. De ahí que en muchas ocasiones tienda a confundirse la parte con el todo.

Pues bien, de cómo se está empleando para ello el ciberespacio es sobre lo que versa esta conferencia.

GUERRA HÍBRIDA Y CIBERESPACIO

Uno de los motivos por los que el ciberespacio resulta el terreno idóneo para las acciones de la amenaza híbrida es lo difuso de la legislación que en él impera.

Ello da lugar a numerosas zonas grises ante las cuales son posibles dos planteamientos contrapuestos: autolimitando la actuación ante la duda o aprovechando esa indefini-

ción para actuar. Y, como en muchos otros casos, esta situación siempre favorece al que menos escrúpulos tiene. Y, también, a aquellos gobiernos, agencias u organizaciones que están menos sometidas al escrutinio y censura de la opinión pública.

Pero, además, tenemos que ser conscientes que cualquier acción en respuesta a una agresión requiere de cuatro condiciones previas, y esto es aplicable a cualquier entorno, incluido el ciberespacio.

La primera, obviamente, que la acción agresora sea detectada. La segunda, que esa acción se pueda categorizar y tipificar. La tercera, que exista trazabilidad, es decir, que sea posible reunir evidencias sobre la autoría de la acción que permitan atribuir esa acción a un actor concreto, que es la cuarta condición.

Pues bien, este proceso, que puede tener mayor o menor complejidad en el mundo físico, se torna prácticamente irrealizable en el ciberespacio, por la complicación que ya presentan cada una de las fases por separado.

Y en este contexto, nos encontramos con que las normas y la legislación acaban siendo anecdóticas. Y que el altísimo grado de impunidad que otorga el ciberespacio nos lleva a estos dos extremos: una comunidad dispuesta a aceptar esas normas y otra a la que le es absolutamente indiferente, resultando en la paradoja de que el desarrollo de normas y legislación aplicable al ciberespacio únicamente encorseta a los primeros.

Esta nueva forma de combatir da entrada a nuevas armas y campos de batalla, así como nuevos contendientes que ya no se circunscriben a las fuerzas regulares sino que engloban a todo tipo de actores. Uno de esos nuevos escenarios es Internet, en cuya consideración de campo de batalla ha tenido mucho que ver el salto cualitativo que ha supuesto su evolución a la web 2.0 primero y 3.0 después.

LA WEB 3.0 Y LOS NUEVOS ACTORES

La web 3.0 fomenta la participación, la colaboración, la diversificación, la creatividad, la compartición, la interactividad, la comunicación, todo ello de forma inmediata y sin excesiva dependencia de la ubicación, siempre que exista una conexión a Internet. Ello ha traído consigo la democratización de los medios, haciendo que cualquier grupo, organismo o individuo tenga las mismas posibilidades de publicar —y, en consecuencia, de influir— que un medio tradicional. Lo que determinará su influencia será su capacidad de llegar a un público lo más amplio posible.

En este sentido, los *social media* aglutinan una serie de características que los convierten tanto en herramientas como en espacios ideales para la guerra híbrida: generalización, ubicuidad, inmediatez, interactividad, horizontalidad, descentralización, interinfluencia, automatización y excepcionales facilidades para el anonimato, la suplantación o la distorsión de los contenidos. Esta amalgama de características, debidamente explotadas, puede transformar los aparentemente inofensivos *social media* en auténticas «armas de persuasión masiva».

Se trata de un combate en el que las armas son los argumentos, símbolos e imágenes, contra los que el armamento convencional y el poder militar poco o nada pueden hacer. Es necesario, por tanto, combatir con las mismas armas. Produciendo argumentos, símbolos e imágenes que neutralicen las del adversario, con la mayor intensidad y lo más rápidamente posible.

En definitiva, nunca el ser humano ha tenido tan fácil el acceso a tanta información y, paradójicamente, nunca ha estado más desinformado ni ha sido tan vulnerable a la manipulación.

La web 2.0 ha traído también consigo la aparición de nuevos actores en el ecosistema, como son los *influncers,* los *trolls* o los *sockpuppets*, con implicaciones relevantes en el campo de la influencia y, por extensión, en el de la guerra híbrida.

El término ***influencer*** se ha generalizado en todo el mundo. Se denomina así a la persona u organización que tiene la capacidad de ejercer influencia sobre las actitudes y formas de pensar de otros individuos, a partir de que es percibido por estos como una autoridad o fuente confiable de información, por lo que sus opiniones y puntos de vista son tomados como modelo. Su capacidad de influencia puede sustentarse en causas muy diversas: prestigio, conocimiento contrastado en algún campo, atractivo personal, carisma, capacidad de liderazgo, etc. Si bien los *influencers* han existido desde siempre, la aparición de medios de comunicación masivos les ha otorgado un status impensable hace unos años. La web 2.0 y su nueva tipología —blogs, foros, redes sociales, páginas de análisis político, etc.— han permitido la extensión de las audiencias, sin los condicionantes geográficos o idiomáticos existentes hasta hace poco.

En la jerga de Internet, el término *troll* se asigna a aquella identidad digital que publica mensajes provocadores, irrelevantes, groseros o fuera de tema en una comunidad *onli-*

ne, con la principal intención de molestar o provocar una respuesta emocional negativa en los usuarios y lectores. Las motivaciones de estos comportamientos son muy variadas. En sus orígenes, los *trolls* parecían buscar simplemente diversión o notoriedad. En la actualidad, su número ha crecido de forma considerable y también su tipología. En el campo de la guerra híbrida, la importancia del *troll* radica en su potencialidad para provocar efectos negativos sobre un foro o comunidad: enfrentamientos, confusión, desunión, desinformación, etc.

Se conoce como *sockpuppets* (títeres, marionetas) a las identidades *online* creadas y utilizadas con fines de engaño. Originalmente, el término se aplicó a cualquier identidad falsa asumida por un miembro de una comunidad de Internet que fingía ser otra persona. El término ha ido evolucionando con el paso del tiempo, y ahora incluye otros usos maliciosos de las identidades *online*, como las creadas para elogiar, defender o apoyar a una persona u organización o para manipular la opinión pública, pudiendo en muchas ocasiones superponerse las condiciones de *troll* y *sockpuppet* en una misma identidad digital.

Actualmente existen cerca de mil quinientos millones de cuentas activas de Facebook en el mundo. Se estima que cerca de 200 millones corresponden a identidades falsas.

ACCIONES DE GUERRA HÍBRIDA EN EL CIBERESPACIO

Tras esta introducción, ya es momento de entrar en materia y veamos cómo puede utilizarse el ciberespacio en términos de guerra híbrida. Sin ánimo de ser exhaustivo, el posible uso del ciberespacio en términos de guerra híbrida cubre un amplio abanico de opciones, que se agrupan, en mi opinión, en cinco categorías principales:

- ataque a infraestructuras críticas y servicios esenciales,
- robo de información,
- denegación de servicio,
- alteración de la información y
- distribución de información,

cada una de las cuales da cabida a diversos tipos de actividades muy diferentes entre sí, siéndolo también sus efectos. Todas ellas pueden categorizarse como «ciberataques» o acciones de «guerra de la información», y, en algún caso, a ambas categorías simultáneamente. Además, cada una de las modalidades puede ser llevada a cabo empleando técnicas de anonimización o de suplantación de identidad (bandera falsa), lo que puede amplificar considerablemente sus efectos, al tiempo que se reducen las posibles consecuencias.

Vamos a ver esto en más detalle, para lo cual me apoyaré en algunos ejemplos ilustrativos.

Comencemos por el más grave, al menos potencialmente. «Ciberataques a infraestructuras críticas y servicios esenciales», de los cuales tenemos algún ejemplo reciente en el marco del conflicto Ucrania-Rusia. Como ya he dicho anteriormente, una caracte-

rística habitual de los ciberataques es su difícil trazabilidad y casi imposible atribución, de ahí su extraordinario valor en términos de guerra híbrida: esa enorme dificultad en la atribución limita, si es que no impide, cualquier posible reacción por parte de la víctima.

Por otra parte, la propia normativa internacional genera otras cuestiones no menos trascendentes, como es el propio tratamiento jurídico de este tipo de acciones. Así, mientras no existe ninguna duda de que un ataque cinético que destruyera una planta de producción de energía constituye un ataque armado y, por tanto, genera el derecho legítimo de autodefensa, un ciberataque que dejara esa misma central inoperativa plantea muchas dudas y controversia en cuanto a su categorización: ¿constituye una agresión?, ¿puede equipararse a un ataque armado? Esta indefinición condiciona enormemente las posibles acciones de respuesta por parte de la víctima.

Izquierda: central energética destruida por un ataque aéreo. Derecha: misma central energética inoperativa por infección de malware.

El «robo de información», habitualmente calificado como «ciberespionaje», es otro elemento básico del abanico de posibilidades de actuación en el ciberespacio en el campo de la guerra híbrida. A las ya mencionadas dificultades de trazabilidad y atribución se une una todavía más grave: la de la propia detección del hecho. El robo de información puede responder a objetivos muy variados y traducirse en múltiples beneficios para el atacante: conocer planes o intenciones de la víctima y así anticiparse a sus movimientos, conocer vulnerabilidades o puntos débiles, obtener información industrial o tecnológica de valor estratégico, … Así mismo, puede posibilitar otras acciones posteriores. Por ejemplo, exposición pública de información privada que puede dañar al adversario. Lo que se conoce como *doxing* y que trataré más adelante.

Existen múltiples ejemplos de campañas de ciberespionaje que se han mantenido sin ser detectados un buen número de años y que se atribuyen, aunque sin pruebas sólidas en la mayoría de los casos, a diferentes grupos APT, amenazas persistentes avanzadas,

muchos de ellos asociados a diferentes agencias gubernamentales de las grandes potencias. Tenemos también ejemplos muy recientes de cómo puede utilizarse el robo de información en términos de guerra híbrida, como el que afectó a la campaña del señor Macrom en mayo de 2017.

Pricipales grupos APT.

La «denegación de servicio» persigue que un servicio o recurso sea inaccesible a los usuarios legítimos, o que este acceso resulte degradado. Tradicionalmente se han utilizado para ello las conocidas *botnets* o redes de ordenadores zombis, pero últimamente están apareciendo nuevas técnicas mucho más eficientes basadas en la reflexión amplificada mediante las que ya es posible alcanzar picos de ataque de varios terabytes por segundo. En términos de guerra híbrida, puede generar confusión (o hasta caos, según su alcance y duración), pérdida de confianza, socavar la credibilidad de la víctima, etc.

Este tipo de ataque ha sido empleado con alguna de las finalidades anteriores en el marco de conflictos armados o situaciones de crisis. Algunos ejemplos notables son los ciberataques masivos sufridos por Estonia en el año 2007 y por Georgia y Kirguistán en los dos años siguientes. En el caso de Estonia, que es sin duda el más conocido, se simultanearon ataques de denegación de servicio, con el *defacement* de páginas gubernamentales y oficiales, ataques a servidores de nombres de dominio (DNS) y envíos masivos de correo spam.

Se denomina *defacement* a la alteración intencionada de una página web. Puede producir confusión, pérdida de credibilidad y daños a la reputación de la víctima. La eficacia del ataque reside en la reacción de los medios de comunicación, por lo que la divulgación del hecho es mucho más importante que el ataque en sí.

Muy relacionado con el anterior está la «alteración de contenidos», que puede tener muy diversas modalidades y finalidades. En este apartado se incluiría, por ejemplo, la

publicación de un falso comunicado en una cuenta oficial de una organización gubernamental como el llevado a cabo por el Syrian Electronic Army, en abril de 2013. Esta organización se atribuyó la autoría de un falso *tuit* según el cual el presidente Obama había resultado herido en un atentado a la Casa Blanca. La confusión que provocó tan solo duró unos minutos, pero provocó un fuerte pico de bajada en la Bolsa de Nueva York. Otro ejemplo curioso de alteración de contenidos es la Operación Cupcake. En el año 2011, la agencia británica de inteligencia MI6 llevó a cabo un ataque a la publicación *online Inspire Magazine* de Al-Qaeda, en la cual suplantó un contenido de 67 páginas titulado «Cómo fabricar una bomba en la cocina de tu madre» por recetas para hacer magdalenas.

Al hablar de «alteración de datos» en términos de guerra híbrida, posiblemente no haya un ejemplo más ilustrativo que el de la alteración de los resultados de unas elecciones. Mucho se ha hablado en los últimos meses de la participación de *hackers* en diversos procesos electorales. El más sonado, el que en el año 2017 llevó a Donald Trump a la presidencia de los EE. UU., candidato al que la mayoría de las encuestas daban como perdedor. Existen diversas fuentes que apuntan a la posible injerencia rusa en esas elecciones, si bien más en términos de apoyo al candidato republicano a través de las redes sociales, supuestamente de la mano de ejércitos de *trolls* a sueldo del Kremlin, asunto que trataré en unos minutos.

La «sobrecarga informativa», también conocida como «infoxicación», es un problema cada vez más extendido. El ciclo de toma de decisiones se ve afectado, pudiéndose alcanzar un estado que podríamos definir de «parálisis por el análisis». Obviamente, cualquier tipo de acción que intensifique alguno de los factores anteriores contribuye a agravar la situación. Así, por ejemplo, la inyección a través de los *social media* de información discordante sobre un asunto concreto puede generar ruido y contradicciones que, a su

vez, pueden significar la aparición de posiciones encontradas entre la población, división entre aliados, etc.

La «desinformación» puede desarrollarse de múltiples formas, como puede ser la difusión de bulos o de versiones contrapuestas sobre un hecho concreto. Muchas veces pueden ser reforzadas con el apoyo de falsos vídeos o fotografías. La redistribución interesada o irresponsable a través de redes sociales y medios de comunicación permiten extender la audiencia de forma exponencial. Un ejemplo reciente lo tenemos en la difusión de una falsa noticia en febrero de 2018 según la cual un grupo de soldados perteneciente a las fuerzas de la OTAN desplegado en una de las repúblicas bálticas habría violado a varias mujeres locales. Esta simple acción tuvo una muy rápida e intensa repercusión mediática y exigió a la OTAN un enorme esfuerzo de comunicación estratégica para rebatir su credibilidad y contrarrestar sus efectos negativos.


Made for minds.

NEWS

NATO: Russia targeted German army with fake news campaign

Emails accusing German soldiers stationed in Lithuania of rape were sent to local news outlets and the parliamentary president. NATO officials allege that Russia is targeting the military alliance.

El falso rescate de la pequeña Frida, que quizás recuerden de hace un par de años cuando México sufrió un grave terremoto, es un excelente ejemplo de cómo un simple bulo puede convertirse en una noticia de alcance mundial.

En España hemos aprendido mucho sobre bulos últimamente, en especial con motivo de los diversos acontecimientos relacionados con la crisis catalana. La constatación de la enorme importancia de este fenómeno es la principal causa de que el Gobierno creara hace dos años el cargo de embajadora en Misión Especial para las Amenazas Híbridas y la Ciberseguridad, coloquialmente conocida en los medios como «la embajadora de las *fake news*».

En esa misma época, el CNI afirmaba que «parece demostrada la presencia de activistas patrocinados por instituciones rusas en la expresión mediática del conflicto derivado de la situación creada en Cataluña durante 2017, como consecuencia del alejamiento de la legalidad constitucional vigente de ciertas instituciones autonómicas catalanas».

Y es que existen numerosas evidencias de que Rusia hace profuso empleo de la desinformación en apoyo a sus objetivos. Según el artículo que tienen en pantalla, el Kremlin confía plenamente en las plataformas digitales. No hay diferencia entre cadenas de televisión con escasa audiencia, como RT, o agencias de noticias. La idea es difundir y amplificar titulares que describan la descomposición del modelo de estado democrático occidental, con dos audiencias preferentes: los propios ciudadanos rusos y los grupos radicales de derecha o izquierda dentro de los países donde emiten, en esa estrategia de apoyo a los grupos opositores locales, con el fin de desestabilizar a los estados que considera adversarios.

La «transmisión de *e-flets*» (que podríamos traducir como panfletos electrónicos) es el equivalente en el ciberespacio a las tradicionales octavillas arrojadas por la aviación sobre las fuerzas enemigas. Su forma más habitual de ejecución es la emisión masiva de correos electrónicos o mensajes SMS. La ventaja de su realización por medios electrónicos es su inmediata propagación sin riesgo alguno. Como las octavillas, el objetivo de los *e-flets* es provocar el desasosiego, dudas y desmoralización sobre el adversario, quebrando ese elemento fundamental en el combate que se llama voluntad de vencer. Aquí tienen algunos ejemplos de SMS recibidos por los soldados ucranianos en el frente. «¿Quién te está robando la familia mientras tú recibes unos peniques a la espera de tu bala?» «Asesinos de las Fuerzas Armadas Ucranianas. ¡El Este no os perdonará y el Oeste no os recordará!».

naked security by SOPHOS

Soldiers sent hate-SMS messages from rogue base stations

12 MAY 2017

by John E Dunn

Somebody has been bombarding Ukrainian soldiers with SMS messages – and they aren't nice ones, either.

According to evidence collected by Associated Press (AP), soldiers fighting pro-Russian separatists in the east of the country have received a steady stream of mystery propaganda texts since 2014, around the time the conflict started.

Examples can be viewed in Cyrillic or in English. As a flavour from November 11 2015:

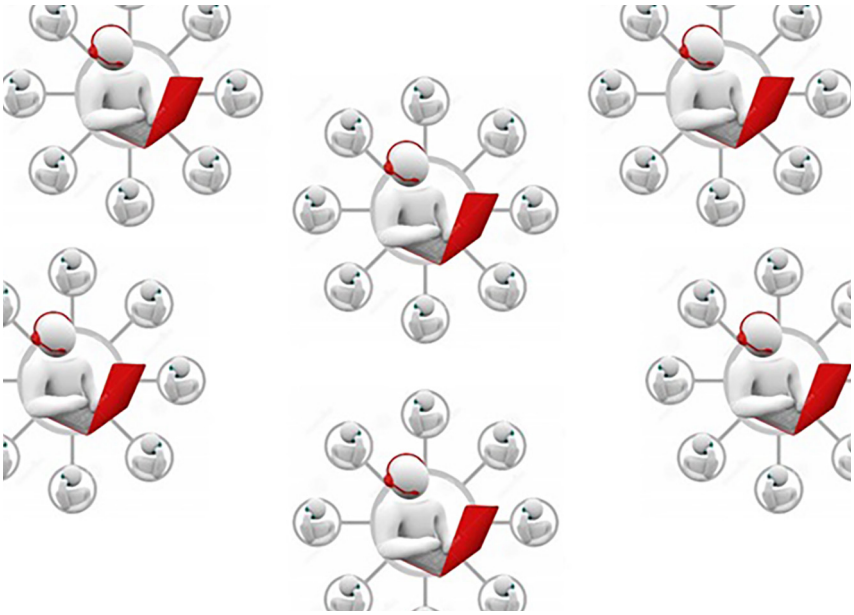
Who is robbing your family while you are paid pennies waiting for your bullet?

Or a few days later:

Murderer from the Ukrainian Armed Forces. The East won't forgive you and the West won't remember you!

El término *astroturfing* designa a aquellas campañas que pretenden dar a un movimiento o tendencia una impresión de espontaneidad, como nacido de una fuerte relación

con el entorno social, pero que realmente está organizada y se construye a partir de actos fingidos y cuidadosamente programados. Una técnica muy común en el *astroturfing on-line* es el uso de *sockpuppets*, donde una sola persona gestiona múltiples y falsas identidades *online* para dar la impresión de un apoyo de base. Existe *software* de gestión de identidades (*persona management software*) que posibilita que cada operador pueda manipular un elevado número de falsas identidades *online*. Este *software* permite disimular la antigüedad de las cuentas y hacer más convincente su autenticidad y está dotado con funcionalidades para facilitar la actividad de los operadores.



Estudios recientes denuncian que entre un 15 y un 20 por ciento de las cuentas en redes sociales son falsas. Y que muchos de los *likes*, *retuits* son generados por seguidores robot, siendo relativamente sencillo construir una red de seguidores robot aprovechando las propias funcionalidades de algunas redes sociales. Existen múltiples evidencias de que numerosos estados y organizaciones están utilizando *trolls*, *sockpuppets* y *bots*, de forma organizada, en apoyo a acciones de influencia. Los ejemplos más conocidos son el *Russia's Troll Army* o el *Water Army* chino, sobre los que existen infinidad de artículos en Internet. Del primero se conoce incluso su ubicación, en la ciudad de San Petersburgo, a partir de la información filtrada por exmiembros de la propia organización.

Pero no piensen ustedes que estas actividades se circunscriben a Rusia y China. Así, por ejemplo, la Operación Earnest Voice es una campaña de *astroturfing* supuestamente operada por el Mando Militar Central de los Estados Unidos (USCENTCOM). El objetivo de esta iniciativa es el empleo de *sockpuppets* para difundir propaganda proestadounidense en sitios de redes sociales basados fuera de los EE. UU. Como parte de la puesta en marcha de la operación, en el año 2011 la compañía californiana de seguridad web Ntrepid habría obtenido un contrato millonario con el USCENTCOM que incluía el desa-

rrollo de un *software* especializado y la infraestructura correspondiente que permitiera a agentes del gobierno publicar propaganda en sitios web en lengua extranjera.

Pero es que esta práctica está cada vez más generalizada. Así, un reciente estudio de la Universidad de Oxford demuestra que, al menos, 70 países llevaron a cabo campañas de manipulación de la opinión pública con fines políticos a través de RRSS en 2019 (56 de ellos a través de Facebook). Estos actores estarían haciendo uso de lo que se denomina propaganda computacional, mediante el empleo de algoritmos, herramientas de automatización y *big data*. Los estados más activos, según el estudio, serían China, India, Irán, Pakistán, Rusia, Arabia Saudí, y Venezuela.

Un reciente informe titulado «The Fake News Machine» publica los precios en el mercado de servicios de manipulación de la opinión pública, que resultan bastante asequibles para cualquier organización.

Existen también estudios sobre la actividad en redes sociales con ocasión de las elecciones a la presidencia de los EE. UU. en el año 2016. Según demuestra alguno de estos estudios, en los meses precedentes a la votación, la máxima actividad de las cuentas correspondió a las posiciones más extremas, siendo casi nula la de la parte intermedia. Esta situación implicó tanto una enorme polarización como una tremenda radicalización, como nunca había ocurrido en el electorado estadounidense, y que muchos analistas atribuyen en gran parte a la acción de las campañas de manipulación de la opinión llevadas a cabo por los ejércitos de *trolls*.

El mismo informe explica cómo los ejércitos de *trolls* atribuidos a Rusia exacerbaron esa polarización. En lugar de actuar sobre la corriente general, se dedicaron a actuar sobre infinidad de grupúsculos de ideología contraria, introduciendo en ellos cuentas falsas, pero dotadas de gran credibilidad. Los operadores que gestionaban estas cuentas se ganaban la confianza de la comunidad e iban provocando divisiones y moldeando la opinión de sus componentes, introduciendo nuevos puntos de vista, empleando de forma profusa la difamación y las falsas narrativas, siempre con un lenguaje adaptado a cada comunidad, alimentando sus particulares obsesiones y exacerbando sus fobias, en persecución de su objetivo final de encumbrar y ensalzar a un candidato y destruir la reputación del otro.

El resultado de todas estas acciones que hemos visto es una constante batalla por modelar las percepciones y voluntades de múltiples audiencias, con la particularidad de que la globalización ha roto la estanqueidad entre estas, que existía hasta hace poco.

Desde el punto de vista de las «operaciones militares», este es un factor que pasa a ser crítico a la hora del planeamiento y la conducción de operaciones, pues cualquier acción militar en el «teatro de operaciones» es objeto de un escrutinio sin precedentes, por lo que el término «teatro» debe entenderse ya no solo en su sentido geofísico, sino como un auténtico escenario en el que se actúa ante una audiencia, y en el que el público —como ocurría en el circo romano— puede influir en lo que ocurre en el escenario apuntando su pulgar hacia arriba o hacia abajo.

Siguiendo con las distintas técnicas, se denomina *doxing* a la práctica de revelar y dar a conocer información sobre una organización o un individuo con el fin de exponer, desacreditar o avergonzar públicamente a las víctimas. Las formas de obtención de la información utilizada pueden ser muy variadas (fuentes abiertas, intrusión, etc.). Este tipo de acción puede ser explotado de muy diversas formas, en función de la información obtenida: descrédito, mediante la publicación de datos que dañen la reputación de un individuo u organización rival, o debilitación de la confianza entre aliados (por ejemplo, filtrando documentos internos en los que una de las partes de una alianza critique, cuestione o desacredite a la otra).


El Confidencial

TRAS UN ATAQUE A LA WEB MUPOL.ES

Anonymous publica los datos personales de 5.400 funcionarios de Policía Nacional

Activistas asociados al colectivo Anonymous han 'hackeado' la web de la mutua de la Policía Nacional y filtrado los datos personales de más de 5.400 funcionarios policiales

M. A. MÉNDEZ 01.06.2016 – 11:23 H.

Otro de los posibles fines del *doxing* es provocar sensación de inseguridad, vulnerabilidad o desamparo en un individuo, grupo o comunidad; por ejemplo, mediante la filtración de información sobre la identidad y domicilio de personal militar adversario en

zona de operaciones o, como en el caso real ocurrido en junio de 2016, atribuido al grupo Anonymous, que publicó datos personales sobre funcionarios de la Policía Nacional.

Y para terminar, y no por ello menos importante, el «reclutamiento y adoctrinamiento» también encuentran su mejor terreno en Internet. Hoy en día, cualquier grupo terrorista o activista tiene presencia en la red. La utilización que ISIS hace de los medios sociales está fundamentalmente enfocada a la propaganda anti-occidental (especialmente, contra los EE. UU.), el adoctrinamiento y el reclutamiento. Al Qaeda cuenta con decenas de sitios web, algunos de ellos extremadamente sofisticados, en múltiples idiomas, e incluso con páginas dirigidas al público infantil.

Estos grupos usan Internet como medio principal para comunicar con la audiencia, utilizando los *social media* como intermediarios, «posteando» comunicados, declaraciones o amenazas. Es el medio a través del cual difunden mayoritariamente su narrativa y por medio del cual ejecutan una intensa contra-narrativa. Su destreza en el manejo de estos medios llega hasta el punto de adecuar su narrativa y su lenguaje (idioma incluido) a diferentes públicos objetivo (por tramos de edad, por nacionalidad de origen o de residencia,…). El fondo del mensaje es el mismo, pero la forma varía para adecuarse lo mejor posible a los distintos perfiles de la audiencia.

CIBERTERRORISMO Y HACKIVISMO

D. LUIS FERNANDO HERNÁNDEZ GARCÍA
Coronel jefe del Área Técnica de la Jefatura de Información de la Guardia Civil

CIBERTERRORISMO Y HACKIVISMO, SUBVERSIÓN Y DESESTABILIZACIÓN EN EL SIGLO XXI

D. LUIS FERNANDO HERNÁNDEZ GARCÍA
Coronel jefe del Área Técnica de la Jefatura de Información de la Guardia Civil

Ciberterrorismo y hacktivismo, dos términos no exentos de controversia; el primero, el *ciberterrorismo*, por la ausencia de una definición generalmente aceptada y por el hecho de que hasta la fecha no haya acontecido incidente que merezca tal calificación, ¿o quizás sí?, reflexionaremos sobre ello, y el *hacktivismo*, que unas veces por desconocimiento y otras por interés político se pretende confundir con el *ciberactivismo*, también reflexionaremos sobre ello.

Una reflexión previa, nuestra sociedad, soporte del individuo como ser social, es un ecosistema en constante mutación y evolución, y esta a lo largo del último cuarto de siglo ha experimentado cambios sin precedentes; la generalización del uso de las tecnologías de la información y las comunicaciones (TIC) ha propiciado un fenómeno sin precedentes y con profunda influencia en lo político, social y económico. El fenómeno de Internet ha traído consigo la mayor revolución tecnológica que ha vivido la humanidad; más allá de los aspectos meramente técnicos y productivos, ha tenido y sigue teniendo una significada repercusión en la forma de moldear nuevos hábitos y comportamientos sociales. La denominada «globalización» representa un marco de grandes oportunidades, pero lleva parejos riesgos, la mayoría a priori intangibles y por lo tanto de difícil percepción, y que en una imparable escalada, están llegando a tener trascendentales repercusiones. Internet ha pasado de ser un sueño de visionarios allá por los años 70 o un valioso instrumento de investigación en los 80, un insustituible elemento en el crecimiento económico en los 90, a irrumpir con fuerza de la mano del nuevo siglo para convertirse en el mayor fenómeno socio-económico y cultural conocido, con marcada influencia en lo cotidiano.

Resulta incuestionable que esta revolución tecnológico-social ha aportado aspectos muy positivos, como lo es la globalización del conocimiento y su acceso universal.

Con la extensión de la Red se ha proporcionado interoperabilidad a millones de usuarios de todo el mundo, en realidad miles de millones, a un abanico de servicios hasta ahora impensables —navegación y acceso a contenidos web tanto abiertos como restringidos, correo electrónico, redes sociales, información compartida, trasferencia y salvaguarda de datos tanto personales como profesionales, etc... y de forma casi instantánea; así pues, a través de la Red de redes, estamos siendo testigos de excepción de una total transformación de las relaciones humanas. Pero como ocurre con demasiada frecuencia, esta creación humana también ha sido y está siendo utilizado para satisfacer los ilícitos intereses de individuos y grupos faltos de escrúpulos que han visto en Internet una oportunidad para saciar sus oscuros e ilegítimos intereses. En este sentido cabe destacar los gravísimos incidentes a nivel mundial acontecidos a partir del ataque del *ransomware Wannacry* iniciado el 12 de mayo del 2017, declarado como el ciberataque más dañino ocurrido hasta la fecha, causando varios miles de millones de euros en pérdida de productividad de las empresas afectadas y revelando una vez más de la fragilidad de las infraestructuras vinculadas a las nuevas tecnologías. De esta forma términos tales como *ciberdelitos*, *ciberterrorismo*, *hacktivismo*, *ciberespionaje* o *ciberguerra* se están haciendo un hueco en lo cotidiano, hasta tal punto que los ciudadanos están aprendiendo a convivir con esta nueva realidad, ya que cada vez está siendo más frecuente hallar noticias sobre algún hecho ilícito que se ha producido a través de la Red. De igual manera, las relaciones entre Estados se están viendo profundamente distorsionadas y en algunos casos gravemente alteradas.

La Red es, de facto, un silencioso campo de batalla donde las potencias mundiales desarrollan su particular Guerra Fría; operaciones de influencia o CNO, en sus variantes ofensivas, de explotación o defensivas, operaciones psicológicas o PSYOPS, pruebas de ciberarmas enmascaradas en ciberataques anónimos, acciones enmarcadas en los conceptos de guerra asimétrica y amenaza híbrida, la desinformación difundida mediante una posverdad fruto de noticias falsas, o sencillamente acciones de falsa bandera se multiplican en el oscuro mundo que rodea al ciberespacio. Y es que debemos tener muy presente que el 80 % de los ciberincidentes realmente graves carecen de atribución conocida.

Los nuevos marcos de relación en lo social, cultural, económico, político y militar dependen cada vez en mayor medida de lo que acontece en el ciberespacio**,** y han hecho más que conveniente, necesario, articular un Sistema de Seguridad Nacional[1], vigente desde el 31 de mayo del 2013, cuando el Gobierno de España en su Estrategia de Segu-

[1] El año 2013 trajo consigo «aportaciones fundamentales» a la política de seguridad nacional en forma de nuevos documentos estratégicos y de una estructura integral orientada a la mejor organización del Sistema de Seguridad Nacional. En cuestión de meses, se aprobaron tres estrategias y se constituyeron órganos interministeriales con poder de decisión, coordinación y apoyo en materia de seguridad nacional.
La aprobación de dichos instrumentos vino precedida de cambios en la estructura de la Presidencia del Gobierno. Al comienzo de la presente legislatura se detectó la necesidad de dotar al Gabinete de la Presidencia del Gobierno de un órgano eficaz que sucediera al Departamento de Infraestructura y Seguimiento de Situaciones de Crisis (DISSC) en la función de prestar asesoramiento y apoyo técnico en materia de seguridad nacional a la Presidencia del Gobierno. Ello se materializó en «la creación del Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno (DSN)» mediante el Real Decreto 1119/2012, de 20 de julio, de modificación del Real Decreto 83/2012, de 13 de enero, por el que se reestructura la Presidencia del Gobierno... [Resulta recomendable la lectura del capítulo «El Sistema de Seguridad Nacional» del *Informe Anual de Seguridad Nacional 2013*].

ridad Nacional (ESN), dio carta de naturaleza al Departamento de Seguridad Nacional o DSN; estrategia revisada y actualizada con fecha 15 de diciembre del 2017. Ahondando y concretizando a través de las estrategias nacionales de ciberseguridad, seguridad marítima, seguridad energética, contra el terrorismo, contra el crimen organizado y la más reciente seguridad aeroespacial; en todas las «ciberamenazas» se presenta como la principal «amenaza trasversal» y que previsiblemente también estarán presentes en las que sean aprobadas en el futuro.

No existe una unidad de criterio a la hora de definir qué es o qué se entiende por ciberespacio, máxime cuando aún no está claro el alcance del mismo más allá de la descriptiva conformación de medios, tanto físicos como lógicos, que dan lugar a las denominadas infraestructuras TIC. Para el Departamento de Defensa de los Estados Unidos (DoD), el *ciberespacio* es:

> «Un dominio global dentro del entorno de la información que consiste en una red interdependiente de infraestructuras de tecnologías de la información, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos, procesadores empotrados y controladores»[2].

Si buscamos una definición «más actual» la escuchamos por boca del que fuera por muchos años nuestro representante nacional en la Agencia Europea de Seguridad de la Información (ENISA), el Prof. Manel Medina para el que:

> «El ciberespacio es una red etérea e intangible de infraestructuras tecnológicas, entre las que se encuentra Internet, las redes de telecomunicaciones, redes sociales y plataformas de mensajería, nubes de ordenadores y ordenadores incrustados en controladores de infraestructuras críticas[3]».

Los términos antagónicos «ciberamenaza vs ciberseguridad» son una realidad en permanente metamorfosis. A pesar de los constantes esfuerzos, tanto gubernamentales como del sector privado, cada día resulta más evidente que las acciones hostiles dirigidas contra los sistemas informáticos, especialmente aquellos vinculados de alguna manera a Internet, *son algo más que una amenaza y se han transformado en un riesgo emergente*. Esto es más evidente cuando se vinculan al concepto de *infraestructuras críticas* (IC) en general e *infraestructuras críticas de la información* (ICI) en particular.

Las TIC han coadyuvado al bienestar y progreso de las sociedades de forma que gran parte de las relaciones públicas y privadas no solo dependen de estas tecnologías, sino que ya no se conciben sin ellas. Con el tiempo y la evolución de las TIC, han aparecido

---

[2] María José Caro Bejarano en el capítulo segundo - «Alcance y ámbito de la Seguridad Nacional en el Ciberespacio» - recoge una serie de definiciones y realiza un amplio estudio del concepto ciberespacio. [Cuaderno de Estrategia n.º 149 del IEEE - *Ciberseguridad. Retos y Amenazas a la Seguridad Nacional* - diciembre 2010].

[3] El profesor Manel Medina es catedrático de la Universidad Politécnica de Cataluña (UPC) y hasta 2014 subdirector de Programas de la Agencia Europea de Seguridad de la Información (ENISA); su definición del ciberespacio está recogida en el libro *Cibercrimen - Aprende de víctimas, expertos y cibervigilantes.*

riesgos que hacen necesario gestionar de una forma lo más eficientemente posible su seguridad.

Inicialmente, la ciberseguridad se ocupó de proteger la información de una manera reactiva, pero ha evolucionado hacia una posición *proactiva* que identifica y gestiona los riesgos que amenazan el ciberespacio a través del ya referido sistema de seguridad nacional. Así se fomenta la integración de todos los actores e instrumentos, públicos o privados, para aprovechar las oportunidades de las nuevas tecnologías y hacer frente a los retos que presentan.

SEGURIDAD, TÉRMINO ANTIGUO, CONCEPTO NUEVO

El nuevo concepto de «seguridad» surge en la década de los ochenta del pasado siglo XX. Una vez que se hace realidad la distensión Este-Oeste, donde el empleo de la fuerza, incluida la nuclear, era el eje principal del concepto tradicional de la seguridad, emerge la realidad de considerar a la seguridad bajo un prisma más amplio que incardine entre otros a los riesgos económicos, medioambientales, delincuencia transnacional o que surgen de cuestiones de identidad social. Se ha pasado de un periodo de bipolaridad de la guerra fría a una multipolaridad. La globalización provocada por la revolución de la tecnología de la información ha invadido exponencialmente los espacios de todas las actividades humanas conformando un concepto de seguridad más heterogéneo de multipolaridad, que contrasta con la unipolaridad que ejerció Estados Unidos desde la distensión de la guerra fría hasta los atentados del 11 de septiembre de 2001 (11-S). Desde esa fecha tan fatídica se ha evidenciado, que el poder militar por sí solo, aunque siendo de un gran potencial, no es determinante para conseguir combatir adecuadamente ante los *conflictos asimétricos*. Los problemas globales de seguridad afectan a toda la comunidad internacional; el terrorismo yihadista, el tráfico encubierto de armas de destrucción masiva, la delincuencia internacional organizada (narcotráfico, tráfico clandestino de seres humanos o de armas, blanqueo de capitales, etc.) crecientes problemas medioambientales, pandemias, hambrunas, guerras y sus consecuentes éxodos de refugiados. Estos problemas, configuran un escenario de seguridad con un enfoque novedoso, donde el motivo no solo es el Estado, sino que el individuo es también un elemento fundamental en cuanto sujeto a proteger y como actor imprescindible para colaborar en la prevención y respuesta, concienciación.

Desde el 11-S y hasta la fecha, la barbarie y la sinrazón del terrorismo de corte islamista radical, personalizado primeramente en la organización terrorista Al Qaeda y en la actualidad en el Dáesh[4], ha experimentado un dramático recrudecimiento, sacudido los cinco continentes y golpeado a multitud de países, incluida España aquel fatídico 11 de

[4] «No recomiendo usar el término Estado Islámico porque desdibuja las líneas entre islam, musulmanes e islamistas», argumentó en septiembre de 2014 el ministro francés de exteriores Laurent Fabius.
También el Gobierno de España ha dejado de utilizar la autodenominación del grupo terrorista como «Estado Islámico» porque eso conllevaría, en opinión del Ejecutivo, «legimitar» su existencia y sus acciones como un país que rige la vida de sus ciudadanos. El secretario de Estado de Seguridad, Francisco Martínez, pidió públicamente «llamar a las cosas por su nombre», ya que el objetivo de que se autodenominen 'Estado Islámico' para que los demás les llamen así es el de «legitimar su organización como la única del territorio, la hegemónica y todopoderosa, separándose así del resto de formaciones terroristas».

marzo del 2004 en Madrid, con sus 191 víctimas mortales, convirtiéndose en el atentado más grave en suelo europeo hasta la fecha[5], y más recientemente con el doble atentado de Barcelona-Cambrils de los días 17 y 18 de agosto del 2017. Este nuevo escenario resulta aún más complejo que los anteriores, pues ya no hablamos de células más o menos autónomas pero con una dirección y organización directamente vinculados con el Dáesh y que potencialmente pueden ser rastreadas, sino de auténticos «lobos solitarios» que se autorradicalizan en muy poco tiempo y emplean cualquier método letal a su alcance, diferentes de armas y explosivos; evidentemente motivados por el llamamiento realizado por el Dáesh en un vídeo difundido por Internet en junio, que bajo el título «no soñarás estar seguro» advierte a los que denomina incrédulos de que «no dejaremos que se viva en paz», también hace un llamamiento a «todos los hermanos y hermanas musulmanes» que viven en las tierras de los infieles para advertirles que «no tiene sentido vivir una vida pacífica y lujosa cuando los judíos y cristianos atacan a nuestros hermanos y hermanas», e instándoles a escuchar al califa Abu Bakr al-Baghdadi y a seguir su mandato para «destruir al infiel», con mensajes tan explícitos como que «se les debe sacrificar por cualquier medio: atropellarles con el coche, envenenarles, apuñalarles con un cuchillo, con un punzón, o al menos escupirles».

Dáesh provocó intencionada y deliberadamente la crisis de los refugiados procedentes en su mayoría de las zonas en conflicto de Siria e Irák para debilitar a occidente y acrecentar las tensiones étnicas y religiosas en Europa y América del Norte; si bien la situación de los refugiados originó un movimiento de simpatía y solidaridad en occidente, este se está tornando en rechazo, a raíz de los atentados del 2016 en los que la participación de refugiados y demandantes de asilo fueron constatadas.

No se ha pretendido realizar un exhaustivo censo del terror, sino esbozar y contextualizar el grave problema al que se enfrenta la sociedad de nuestro tiempo. Aunque resulta

---

Un grupo de imanes británicos sugirieron al primer ministro británico, David Cameron, el uso de «Estado no islámico», pero esta idea no ha cuajado pese a que también la apoyó el secretario general de la ONU, Ban Ki-moon.

Tanto ISIS como ISIL son la traducción al inglés del acrónimo árabe «Islamic State of Irak and the Levant» (ISIL) o el más habitual «Islamic State of Irak and Syria» (ISIS). Es la más utilizada por la prensa anglosajona y la denominación más extendida en el mundo. La única diferencia con la denominación «Estado Islámico» es que añade la coletilla «de Irak y el Levante», que el grupo pidió eliminar el año pasado.

[5] Madrid 11 de marzo del 2004, con sus 191 víctimas mortales, convirtiéndose en el atentado más grave en suelo europeo hasta la fecha, Londres el 7 de julio del 2005 con 56 muertos, el 2 de octubre de ese mismo año en Bali-Indonesia o el 13 de septiembre del 2008 en Nueva Delhi, o el del Maratón de Boston EE. UU. el 15 de abril del 2013 con 3 muertos y 282 heridos; por recordar algunos de los más significados hasta llegar a los más recientes acaecidos a lo largo de los últimos 18 meses, como los de París de los días 7 y 8 de enero contra la redacción de la revista satírica Charlie Hebdo y una tienda de alimentación Kósher con gran eco mediático, más que por el número de víctimas mortales (ascendiendo estas a 17), y de la madrugada del 13 al 14 de noviembre del 2015 que causaron 130 víctimas mortales y más de 350 heridos (mayoritariamente en la sala de conciertos Bataclán), San Bernardino EE. UU. con 14 muertos y cerrando esta cronología del horror con los atentados del pasado año 2016, comenzando con el atentado del 22 de marzo en Bruselas capital de Bélgica con 35 víctimas mortales y más de 300 heridos, el 12 de junio el objetivo fue la discoteca de ambiente gay Pulse en la ciudad estadounidense de Orlando (Florida) causando 49 muertos y 53 heridos, el 14 de julio fue la turística ciudad francesa de Niza quien sufrió un atentado que costó la vida a 85 personas y dejó heridas a otras 303, en esta ocasión el «arma» fue un camión proyectado a gran velocidad contra los transeúntes, el mismo *modus operandi* fue utilizado el 19 de diciembre, esta vez en Berlín, provocando 12 muertos y 56 heridos. Cerrando esta breve y en modo alguno exhaustiva reseña con el doble atentado de Barcelona-Cambrils de los días 17 y 18 de agosto de 2017, con un saldo provisional de 14 muertos (13 en Barcelona y 1 en Cambrils), y más de 120 heridos de hasta 34 nacionalidades diferentes.

de justicia recordar otros muchos, casi ignorados o incluso olvidados, pero igualmente terribles, acontecidos en Siria, Irak, Turquía, Paquistán, Afganistán, Chechenia, Egipto, Yemen, Nigeria, Sudán, Kenia, y un largo etc…, porque si en algo se igualan todos ellos es en las víctimas, siempre inocentes y mayoritariamente anónimas, tanto mortales como heridos; no hay víctimas de primera o de segunda, el dolor de una madre, esposa o hijos al que le acaban de arrebatar un ser querido, de una forma brutal y sin sentido, es idéntico en Nueva York, Madrid, Londres, París o Barcelona que en la aldea más olvidada de Nigeria, y los dramas personales que acarrea toda acción terrorista son equivalentes en cualquier caso.

La amenaza del «terrorismo yihadista» (Dáesh, Boko Haram y Al Qaeda mayormente) supone el mayor reto para la convivencia a la que se enfrenta no solo la sociedad occidental, sino toda la sociedad y especialmente la musulmana, pues solo el 0,6 % de sus acciones se desarrollan en Europa, siendo Oriente Medio, norte y zona subsahariana de África y sur de Asia el epicentro de sus acciones[6]. Sin datos del 2019, reseñar que durante el 2018 se contabilizaron 1.571 actos terroristas, en 37 países diferentes y con un triste saldo de 10.598 víctimas mortales. El año 2015 está considerado como el más sangriento de la historia reciente, pues se calcula que este terrorismo segó la vida de más de 37.000 personas (mayoritariamente a manos del Dáesh y de Boko Haram, ambos de rama suni), de las cuales solo el 0,5 % eran occidentales (*kuffar*); o lo que es lo mismo que decir que la mayoría de las víctimas fueron musulmanes moderados (o «nominales» cuya vida se separa de la sunna —código de vida del Profeta), musulmanes chiíes (herejes) o no musulmanes residentes en territorios del islam (*dhimmies*). Estas cifras, dentro de la más absoluta irracionalidad, se explican en la realidad de que se calcula que en el mundo hay entre 1.700 y 1.900 millones de creyentes musulmanes, que de estos, unos 425 millones son fundamentalistas (o lo que es lo mismo, dan cobertura a los yihadistas o muyahidines) y que aproximadamente 75 millones de ellos son yihadistas con vocación terrorista[7].

Pero dicho esto, no debemos caer en el error de infravalorar o dejar en el olvido otras amenazas terroristas aún presentes en nuestra sociedad, el mal adjetivado por muchos como terrorismo «doméstico», en absoluto por ello menos brutal e irracional y que prostituyendo los más básicos principios de la democracia pretenden imponer —siempre desde una minoría sin representación alguna— su aberrante visión del mundo y la sociedad que les rodea, a una mayoría legítima, democrática y pacífica, por la imposición del terror; que en el caso de nuestra Nación y a lo largo de más de cuatro décadas ha cercenado la ilusión y el futuro a muchas familias españolas y que aún hoy sigue causando dolor y desasosiego a muchos conciudadanos; pues bien, muchas de sus tácticas y objetivos pueden ser perfectamente trasladables a la Red, como más adelante se concretará. Resultará evidente para el lector que la referencia hace especial mención a la organización terrorista *país vasco y liberta – euskadi ta as-*

[6] Información extraída de: Global Terrorism Database o GDT: https://www.start.umd.edu/research-projects/global-terrorism-database-gtd. Observatorio Internacional de Estudios sobre Terrorismo (OIET): https://observatorioterrorismo.com/.

[7] Datos estadísticos facilitados por Pew Research Center, Religion & Public Life of Washington 2015, recogidos por Eduardo Martín de Pozuelo, Jordi Bordas y Eduard Yitzutak en su libro *Objetivo: Califato Universal – Claves para entender el yihadismo*.

katasuna (ETA), en mayor medida; pero sin olvidarnos de otros tales como el *grupo de resistencia antifascista primero de octubre* (GRAPO), *frente revolucionario antifascista y patriótico* (FRAP), *ejército guerrillero del pueblo gallego libre – exército guerrilheiro do povo galego ceive* (EGDGC) o *tierra libre – terra lliure* (TERRA LLIURE). Con el triste saldo de 1.421 compatriotas fallecidos[8], la inmensa mayoría a manos de las precitadas organizaciones terroristas.

CIBERSEGURIDAD, LA SEGURIDAD EN EL CIBERESPACIO

Y es precisamente a raíz de los atentados del 11-S, cuando en los diferentes entes gubernamentales, tanto de los Estados Unidos como de los países occidentales, se generalizó la percepción de la amenaza desde el ciberespacio; inicialmente orientada hacia la potencial actuación de organizaciones terroristas, de ahí que tomara fuerza el concepto de ciberterrorismo como una amenaza global. Trascurrido ya más de un decenio, la realidad se ha mostrado muy diferente, ya que el concepto de ciberterrorismo se ha visto desplazado, del todo a una parte de un nuevo concepto globalizador, el de ciberamenaza, y frente a esta, como antagonista, el ya mencionado de la ciberseguridad.

Para entender este nuevo escenario y estar en condiciones de interactuar en él resulta fundamental adquirir una «conciencia de ciberseguridad», tanto en lo profesional como en lo personal, faceta esta que se convierte en vertebradora, ya que la seguridad es una percepción que permite al ser humano y a las organizaciones desarrollar de una forma armónica sus relaciones. Y es que las relaciones sociales se desarrollan en marcos conceptuales definidos, en los que la seguridad jurídica y el cumplimiento de la ley y de las normas establecidas permiten una ordenación estable, definida. Pero los espacios donde esas relaciones se desarrollan no están aún regulados, porque la velocidad de los cambios es significativamente superior al de su marco regulatorio de referencia, racionalmente establecido.

> «Existe un fenómeno creciente, el de los «nativos en Internet», con patrones de comportamiento e incluso patologías muy características, que les llevan con frecuencia a no encontrar razonables determinadas limitaciones que son reclamadas por aquellos que han visto el nacimiento de este nuevo modelo de interacción social. Las iniciativas sobre materias de ciberseguridad que están siendo desarrolladas en todos los países ante este entorno de cambio y en el ciberespacio configuran un reto de entendimiento de este «nuevo mundo». Un mundo que permite grandes oportunidades y presenta grandes retos, una experiencia fascinante para el investigador social donde, transformado en analista de inteligencia, debe interpretar los datos, ver más allá de lo evidente y concluir que, desde un punto de vista interpretativo y otro prospectivo, el papel que desarrollan los individuos, las empresas, las organizaciones públicas y los Estados está sometido a cambios y revisión»[9].

---

[8] http://www.interior.gob.es/fallecidos-por-terrorismo.

[9] «¿Por qué una conciencia nacional de ciberseguridad?». introducción a la Monografía del CESEDEN n.º137 - *Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario.* Abril 2013.

CIBERAMENAZAS, LAS NUEVAS AMENAZAS TRANSNACIONALES DEL S. XXI

Y es que las nuevas amenazas para nuestra seguridad, tanto individual como colectiva son múltiples, diversas y cambiantes, e *Internet y su tecnología asociada* están contribuyendo a ello, de una forma cada vez más determinante —ciberamenazas—; ya que están siendo utilizados con profusión como soporte para la ejecución de tradicionales acciones ilícitas pero con novedosos *modus operandi*; y no solo empleados por los grupos delincuenciales al uso —que se han adaptado y rápido a los nuevos tiempos— sino que lo están siendo también por otras formas de delincuencia grave y organizada, tales como grupos y organizaciones terroristas, colectivos antiglobalización y antisistema —preferentemente a través del denominado hacktivismo— o que tienen como fin último la desestabilización de un Estado en particular, atacando su estructura social, económica y política, sin olvidar organizaciones clandestinas, e incluso acciones encubiertas de las estructuras de inteligencia de algunos estados.

Un estudio del 2016, de la Universitat Internacional de Valencia, establece que el *hacktivismo* ya ha entrado en el podio de los mayores peligros para las grandes organizaciones, inmediatamente después del *espionaje industrial*; esto en una valoración cualitativa. Cuantitativamente hablando, el primer puesto lo siguen ocupando los *cibercriminales* (con un inalcanzable 44 %), el *hacktivismo* se alza con el segundo puesto con un 17 %, frente al *ciberterrorismo* (15 %), los *ataques gubernamentales* (12 %) y la competencia directa o *ciberespionaje* (11 %)[10].

Al hablar de delincuencia vinculada a organizaciones terroristas o afines, debemos contemplar Internet y las TIC desde una óptica amplia; verlo como parte de su «negocio», su forma de obtener ilícitos beneficios o saciar sus más depravados instintos; para ellos representa una oportunidad, sin precedentes, de organizarse, comunicarse y coordinarse, de compartir, de proclamar, intoxicar y difamar, de reclutar y financiarse, etc…, y todo ello con unas condiciones de seguridad y anonimato sin precedentes.

Desde que la organización terrorista Al Qaeda cometió los brutales atentados del 11-S, retransmitido en directo por los medios de comunicación audiovisuales, la percepción del mundo en el que vivimos ha cambiado drásticamente y muchas miradas se han vuelto hacia este entorno y han descubierto el sin fin de perversas posibilidades que ofrece a todos aquellos que optan por el terror como forma de vida, y una interferencia directa de todo ello son las nuevas ciberamenazas.

Ya la extinta Estrategia Española de Seguridad del 2011 (EES) abordaba cinco factores considerados como potenciadores de riesgo que «propician la propagación o transformación de las amenazas y riesgos e incrementan nuestra vulnerabilidad». Estos factores transnacionales eran: «Las disfunciones de la globalización, los desequilibrios demográficos, la pobreza y la desigualdad, el cambio climático, "los peligros tecnológicos", y las ideologías radicales y no democráticas». Estos peligros tecnológicos se han visto nuevamente reflejados y concretados en la vigente ESN de modo que se presentan

[10] *Informe de seguridad informática de la Universitat Internacional de Valencia 2016.*

como auténticos potenciadores de riesgo. En definitiva, la tecnología aparece como parte del problema y a la vez de la solución.

Como ya se esbozó en el preámbulo, podemos hablar de que las *nuevas ciberamenazas* comprenden cinco áreas fundamentales y perfectamente diferenciadas que si bien comparten técnicas y procedimientos, obedecen a motivos, fines u objetivos perfectamente diferenciados y premeditados, estas son: *ciberdelincuencia, ciberterrorismo, hacktivismo, ciberespionaje y ciberguerra*.

Quizás antes de continuar con la exposición resulte oportuno adelantar una de las posibles conclusiones de la misma, y es el hecho de considerar algunas de las ideas que a lo largo de este documento se exponen como parte de una visión fatalista y alejada de la realidad; es por ello *que se debe desmitificar pero no subestimar el riesgo creciente que supone Internet como medio e instrumento de materializar las referenciadas como ciberamenazas*.

Siempre se ha dicho que en el arte de la guerra es esencial el conocimiento de tu enemigo, sin el cual cualquier campaña está destinada al fracaso. En el campo de la ciberseguridad, el conocimiento de los «ciberenemigos o ciberatacantes» y de sus «técnicas y procedimientos de ataque» obviamente resulta así mismo fundamental.

Al hablar de *acciones hostiles en el ciberespacio*[11] en sus diferentes modalidades nos enfrentamos a un primer problema, que es el de la atribución. La atribución es la capacidad de poder identificar quién ha atacado un determinado objetivo y desde dónde. Se trata de un problema con trascendencia legal que plantea un fuerte reto técnico, ya que los orígenes de los ataques emplean medios y técnicas muy elaborados para ocultar sus huellas. A veces, es muy difícil incluso determinar el verdadero objetivo del ataque, debido al empleo de técnicas de decepción.

La Orden PCI/487/2019, de 26 de abril, por la que se publica la *Estrategia Nacional de Ciberseguridad 2019*, aprobada por el Consejo de Seguridad Nacional, en su capítulo 2.º indica que:

> «La cibercriminalidad, por su parte, es un problema de seguridad ciudadana de primer orden, representando una de las amenazas más extendidas y generalizadas, que se materializa de forma continua y que victimiza cada vez de manera más importante a miles de instituciones, empresas y ciudadanos. El término cibercriminalidad, hace referencia al conjunto de actividades ilícitas cometidas en el ciberespacio que tienen por objeto los elementos, sistemas informáticos o cualesquiera otros bienes jurídicos, siempre que en su planificación, desarrollo y ejecución resulte determinante la utilización de herramientas tecnológicas; en función de la naturaleza del hecho punible en sí, de la autoría, de su motivación, o de los daños infligidos, se podrá hablar así de ciberterrorismo, de ciberdelito, o en su caso, de hacktivismo**.**

[11] Fuente: José Manuel Roldán Tudela.

El empleo de nuevas modalidades de transacción financiera y económica, como las criptomonedas, para el tráfico y el comercio de bienes y prestación de servicios ilícitos o la extorsión, el fraude y la falsificación de medios de pago no monetarios, constituyen un serio desafío a la seguridad por su sofisticación y complejidad. Estos pueden ser utilizados en el blanqueo de capitales y la evasión de impuestos y representan una fuente de ingresos para el crimen organizado y por lo tanto son facilitadores de otras actividades como la financiación del terrorismo, que toma provecho de la dificultad de seguimiento que estas nuevas técnicas ofrecen.

Los ciberdelincuentes operan bajo esquemas de crimen organizado y continúan explorando de manera incesante técnicas sobre las que construir modelos de negocio lucrativo y de bajo riesgo, amparados por la difícil trazabilidad de sus acciones.

Los grupos terroristas tratan de aprovechar las vulnerabilidades del ciberespacio para realizar ciberataques o para actividades de radicalización de individuos y colectivos, financiación, divulgación de técnicas y herramientas para la comisión de atentados, y de reclutamiento, adiestramiento o propaganda. Íntimamente relacionado con ello, se halla la amenaza contra las infraestructuras críticas, con la posibilidad cierta de causar un colapso a través de las redes mediante una caída en cadena de los servicios esenciales.

Los grupos hacktivistas realizan ciberataques por razones ideológicas y, aprovechándose en ocasiones de productos, servicios y herramientas disponibles en el ciberespacio, buscan desarrollar ataques con un gran impacto mediático o social.

Tampoco se puede menospreciar la amenaza que entraña el incremento continuado de la contratación de servicios de cibercriminales, las organizaciones que buscan causar daño a sus competidores y los recursos tecnológicos y humanos internos que puedan resultar dañinos para las organizaciones, sin olvidar todas aquellas amenazas emergentes y las acciones resultantes de la falta de cultura de ciberseguridad.

Por otra parte, la información digital se ha convertido en un activo de alto valor añadido. El análisis de los datos personales que circulan en la red se aprovecha para múltiples fines que abarca desde estudios sociológicos hasta campañas comerciales. El empleo malintencionado de datos personales y las campañas de desinformación tienen un alto potencial desestabilizador en la sociedad, y la explotación de brechas en los datos personales supone una violación a la seguridad de dichos datos, que afecta a la privacidad de las personas y a la integridad y confidencialidad de sus datos.

En cuanto a las campañas de desinformación, hacen uso de elementos como las noticias falsas para influir en la opinión pública. Internet y las redes sociales amplifican el efecto y alcance de la información transmitida, con potencial aplicación en contra de objetivos como por ejemplo organizaciones internacionales, Estados, iniciativas políticas o personajes públicos o incluso a procesos electorales democráticos».

El ciberdelito / cibercrimen / delito informático

Para contextualizar, decir que la globalización de la delincuencia y la indeterminación del ámbito geográfico en el que viene actuando la delincuencia organizada trasnacional

en las últimas dos décadas, donde el lucro obtenido por el ciberdelito se estima supera los 600.000 millones de US dólares, o lo que es lo mismo el 0,8 % del PIB mundial. Según las estadísticas del Ministerio del Interior, durante el año 2018 se conocieron 110.613[12] infracciones penales relacionadas con la cibercriminalidad, con un crecimiento anual superior al 30 %

A comienzos del año 2013 se creó, en el seno de la organización de cooperación policial europea EUROPOL, el *Centro Europeo de la Lucha contra la Ciberdelincuencia* o EC3, como punto focal para el tratamiento de los ciberataques y constituyendo en su seno un CERT de ámbito europeo —CERT-EU—. Y en septiembre del 2014, conformada bajo el soporte estructural de Europol, pero con vocación de integrar estructuras ajenas a las meramente europeas (Estados Unidos, Canadá, Australia, Colombia o Japón entre otros), inició su andadura el Grupo de Acción contra el Cibercrimen —JCAT— (Joint Cybercrime Action Taskforce).

Resulta obligado hacer mención al concepto de cibercrimen como servicio (*Cybercrime As A Service*) que ha experimentado una penetración y profesionalización sin precedentes, permitiendo a delincuentes con escasos o sin conocimientos técnicos contratar «ciber-herramientas delictivas», valiéndose de la privacidad de los «mercados» desarrollados en la denominada *Deep Web*, y que indefectiblemente entrecruzará en un futuro los caminos de organizaciones criminales y grupos terroristas, si es que no lo ha hecho ya.

Ciberterrorismo

Retomando el concepto de ciberterrorismo y haciendo una interpretación extensiva del término, se vinculan este último al uso que de las TIC en general, y de Internet en particular, vienen haciendo las organizaciones terroristas y grupos afines, para la consecución de sus objetivos, siempre enmarcados en el uso de estas TIC como «medio o instrumento», más que como objetivo de la acción ilícita —momento en que en punibilidad sí nos encontraríamos ante una acción pura del denominado ciberterrorismo—. Por lo tanto, el ciberterrorismo, en su concepción estricta, estaría orientado a la realización de acciones ofensivas contra los sistemas de información y comunicaciones que sustentan el normal funcionamiento de las denominadas infraestructuras críticas (IC) y estratégicas, así como cualquier otro servicio esencial para la ciudadanía —lo que se denomina «Internet como objetivo»—.

El Consejo de Seguridad de las Naciones Unidas (ONU), en febrero del 2017, adoptó por unanimidad la «Resolución 2341» en la que subraya la necesidad de fortalecer la colaboración internacional para proteger las infraestructuras críticas frente a las amenazas físicas y cibernéticas del terrorismo.

Si miramos a otros actores nacionales e internacionales se evidencia la existencia de tantas definiciones válidas sobre el concepto ciberterrorismo como enfoques de análisis se planteen, desde conceptos simples, pero no por ello desatinados, como:

---

[12] https://estadisticasdecriminalidad.ses.mir.es/dynPx/inebase/index.htm?type=pcaxis&path=/Datos5/&file=pcaxis.

> «La convergencia del ciberespacio con el terrorismo[13]».

Acuñado en los EE. UU. en los años 80, y que ha evolucionado en sintonía con la transformación de la amenaza hacia conceptos tales como los siguientes:

> «El ciberterrorismo es el ataque premeditado y políticamente motivado contra información, sistemas, programas y datos informatizados no combatientes, por parte de grupos terroristas o agentes encubiertos de potencias extranjeras[14]».

Llegando a definiciones tan elaboradas como:

> «El ciberterrorismo es la ejecución de un ataque sorpresa por parte de un grupo (o persona) terrorista, extranjero subnacional, con objetivo político, utilizando tecnología informática e Internet para paralizar o desactivar las infraestructuras electrónicas y físicas de una nación, provocando de este modo la pérdida de servicios críticos, como energía eléctrica, sistemas de emergencia telefónica, servicio telefónico, sistemas bancarios, Internet y otros muchos... El objeto de un ataque ciberterrorista no es solo impactar sobre la economía de una región o país, sino amplificar los efectos de un ataque terrorista físico tradicional provocando confusión y pánico adicionales en la población en general... El ciberterrorismo existe porque es en el reino cibernético donde son más débiles la mayoría de las naciones industrializadas[15]».

En el seno de la Unión Europea ya en el año 2002 y a través de la DM 173/2002[16], al analizar la amenaza de ataques terroristas contra los sistemas de información vitales de la UE, se vislumbró la naturaleza del riesgo de ciberataques, empleando expresamente el término ciberterrorismo.

Pero como ya se ha dicho, los tiempos y los conceptos cambian, y recuperando nuevamente la reflexión sobre los conceptos antagónicos «ciberamenazas vs ciberseguridad», ya que las primeras pueden tener su origen no solo en organizaciones terroristas, sino en países o estados —tanto hostiles como «aliados»—, redes de delincuencia

---

13 Ciberterrorismo: La convergencia del ciberespacio con el terrorismo. COLLIN, Barry. Instituto de Inteligencia y Seguridad. California, USA: 1984.

14 Ciberterrorismo: El ciberterrorismo es el ataque premeditado y políticamente motivado contra información, sistemas, programas y datos informatizados no combatientes, por parte de grupos terroristas o agentes encubiertos de potencias extranjeras. POLLITT, Mark M. E.A.FBI – Proccedings of the 20th National Information Systems Security Conference, oct. 1997.

15 Ciberterrorismo: El ciberterrorismo es la ejecución de un ataque sorpresa por parte de un grupo (o persona) terrorista, extranjero subnacional, con objetivo político, utilizando tecnología informática e Internet para paralizar o desactivar las infraestructuras electrónicas y físicas de una nación, provocando de este modo la pérdida de servicios críticos, como energía eléctrica, sistemas de emergencia telefónica, servicio telefónico, sistemas bancarios, Internet y otros muchos ... El objeto de un ataque ciberterrorista no es solo impactar sobre la economía de una región o país, sino amplificar los efectos de un ataque terrorista físico tradicional provocando confusión y pánico adicionales en la población en general ... El ciberterrorismo existe porque es en el reino cibernético donde son más débiles la mayoría de las naciones industrializadas. Dan Verton – Periodista especializado en seguridad informática y ex oficial de inteligencia Naval de los Estados Unidos – Washington, D.C. 2003.

16 Decisión Marco del Consejo, Bruselas 19/04/2002 COM(2002)173 final 2002/0086 (CNS).

organizada, movimientos y colectivos reivindicativos de toda índole, *hackers*, etc. De hecho, los incidentes más serios que han acontecido en los últimos años se han centrado en acciones de *espionaje (económico, militar y político), sabotaje*, *desobediencia civil, e incluso guerra*. Por este motivo, bajo el denominador común del prefijo «ciber-», se están acuñando diversas acepciones, catalogadas y diversificadas por los fines cuya consecución se persigue, aunque compartiendo todas ellas las tecnologías de ataque y centrando sus objetivos en Internet, o más bien a través de esta.

Concretando aún más el concepto, se puede hablar del:

a ***Uso con fines terroristas***. Las diferentes organizaciones terroristas, vienen utilizando las TIC e Internet como instrumento[17] para la consecución de sus objetivos, y en este sentido, utilizan en su beneficio las posibilidades que las nuevas tecnologías les ofrecen para ocultar sus comunicaciones o blindar la información contenida en los ordenadores que les son incautados. De hecho, en los últimos años se ha realizado un gran esfuerzo para dotar humana y materialmente a los departamentos de informática forense, para poder dar respuesta al aumento, casi exponencial, tanto del número de dispositivos incautados como la de complejidad de análisis de los mismos. Así mismo, destacar el uso de Internet y las TIC como medio[18], a través de su utilización para el reclutamiento, financiación,

[17] Ante la cuestión de si se ha materializado de alguna manera la amenaza ciberterrorista, significar que del empleo de Internet y las TIC como instrumento existen pruebas evidentes de que las organizaciones terroristas vienen aprovechando las posibilidades que les ofrecen las TIC en su propio beneficio, así y a titulo de ejemplo destacar las comunicaciones vía e-mail, anonimizadores de correo, técnicas de buzón compartido, etc…, empleo de canales de chat privados mediante el empleo de protocolos de comunicación seguros, utilización de programas de encriptación, tales como PGP o Muhaedin Secret, establecimiento de sus propios servidores web con acceso restringido mediante autenticación y reforzados con el empleo de protocolos seguros enlace y acceso, unidos a técnicas de enmascaramiento y ocultación como la steganografía, la utilización de comunicaciones de la denominada «voz sobre IP» (uso de Internet como soporte a comunicaciones telefónicas) y el empleo de dispositivos móviles de conexión a través de puntos de acceso inalámbricos vulnerables o de libre acceso al público. Es una realidad que ya no existen operaciones contra cédulas, taldes o grupos terroristas en las que no se intervengan medios informáticos, es más, la presencia de estos ha experimentado un crecimiento exponencial, no tanto en el número sino en la capacidad de almacenamiento de los mismos, lo que nos ha obligado a afrontar nuevos retos en todo lo relativo a la informática forense; tanto por su complejidad con por los cada vez más sofisticados procedimientos y sistemas informáticos que den soporte a las necesidades de las unidades de lucha antiterrorista. En este sentido destacar el éxito obtenido con el modelo de informática forense-operativa, haciendo salir a los analistas forenses de sus laboratorios, transformar estos en elementos móviles y fusionar la actividad técnica con la operativa de obtención sobre el terrero, con más que notables resultados.

[18] Como medio reseñar que el empleo de las TIC les está reportando claros beneficios a la hora de facilitar las relaciones y colaboraciones entre diferentes organizaciones, grupos o células, favorece sus objetivos de guerra psicológica al posibilitar la desinformación y difusión de amenazas, posibilita e identifica canales de financiación, fomenta la recluta, sirve de base para todo su aparato de propaganda. En la memoria colectiva han quedado gravadas las horrendas imágenes de rehenes asesinados por decapitación, o acciones terroristas filmadas y posteriormente difundidas a través de la Red, que lógicamente se escapan de nuestra racional concepción de las cosas y escala de valores. Los vídeos con mensajes propagandísticos del propio Osama Bin Laden, o comunicados de la organización terrorista ETA; estas nuevas técnicas mejoran y optimizan la consecución de sus objetivos, ya que impiden la «censura y/o valoración» a que mayoritariamente son sometidos por los medios de comunicación en el momento de su difusión, amedrentan la moral de sus objetivos y víctimas y enaltecen la sinrazón de sus adeptos. Finalmente constituye una inestimable fuente de información de todo tipo sobre potenciales objetivos tanto personales como de infraestructuras. El programa de actos de un evento determinado, identificación de autoridades asistentes, horarios, fotografías personales, etc…, cuando no vistas aéreas o fotografías satélite de instalaciones, vías de comunicación, etc… y un sin fin de posibilidades más.

difusión de ideas, comunicados o reivindicaciones y localización de información esencial para la planificación de acciones contra potenciales objetivos; este uso resulta más evidente en la actividad de la *CiberYihad*.

Conscientes de la importancia de mantener una presencia activa en Internet y especialmente en las redes sociales, para la consecución de sus objetivos (en particular la captación, adoctrinamiento y el reclutamiento, la financiación y el proselitismo), las organizaciones terroristas como Al Qaeda y el Dáesh han multiplicado su presencia en la Red. Para ello, Al Qaeda creó *As Sahab*, dedicado a *desarrollar y ejecutar la estrategia de comunicación, propaganda y captación* de esta organización terrorista, apoyado por el «Global Islamic Media Front» como medio de difusión; y el Dáesh emplea con gran sofisticación los m.c.s. y las nuevas tecnologías para la consecución de sus objetivos, a través de «ALHAYAT MEDIA CENTER».

El 26 de febrero del 2016 ya tuvo lugar un incidente que no pasaría de ser una pura anécdota en un mar de relevantes incidentes si no fuera por dos motivos, la víctima y el alcance mediático. La cuenta de Twitter del conocido cantante *Justin Bieber* fue hackeada por seguidores del Daesh para publicar un vídeo titulado *Un mensaje al islam de Occidente*, de unos quince minutos, en el que se podía ver a los terroristas haciendo un llamamiento a sus fieles para que se unieran a la causa islámica, también se podía ver la ejecución de cuatro hombres. Además, usaron el hashtag #JustinBieber, para mandar mensajes. Más allá del hecho de que este cantante mostrara una actitud pública «beligerante» contra el Dáesh, a raíz de que uno de sus managers falleciera en la sala de conciertos Bataclán de París, es de destacar que esta acción le reportó a sus autores generosos titulares en los diferentes m.c.s. y lo que sin duda fue más importante para sus fines, un acceso «directo» a los más de 76 millones de jóvenes seguidores del cantante a través de la cuenta de Twitter hackeada.

La «presencia» del Dáesh en Internet en general y en las redes sociales en particular, donde su campaña de propaganda, financiación y en especial de captación y reclutamiento están alcanzando niveles nunca vistos, está obligando a los gobiernos occidentales a reaccionar, y no solo con campañas de contrapropaganda y sensibilización ante la problemática de la radicalización de algunos de sus nacionales; sino con medidas más directas contra la fuente del problema. En este sentido, EE. UU. anunció el 29 de febrero del 2016 a través de su secretario de Defensa, que «utilizamos herramientas informáticas para debilitar la capacidad del grupo terrorista Dáesh de operar y comunicarse en el campo de batalla virtual … se trata de hacerles perder confianza en sus redes, de sobrecargarlas para que no puedan funcionar, y hacer todo aquello que perturbe su capacidad para comandar sus fuerzas, y controlar su población y economía», apostillando el jefe del Estado Mayor de las Fuerzas Conjuntas que «estamos tratando a la vez físicamente y virtualmente de aislar al grupo Dáesh … pero no queremos que los terroristas sean capaces de notar la diferencia entre las perturbaciones vinculadas a las ciberarmas estadounidenses y otras perturbaciones».

A medida que el Dáesh perdió terreno físico en Siria e Irak decayó también la producción de su aparato propagandístico. Aun así, sacó fuerzas para abrir un par de canales

de comunicación en español, según señaló MEMRI el 30 de abril del 2017, un centro de investigación con sede en Washington que sigue de cerca la actividad mediática de los grupos terroristas. *Al Haqq Media Center*, que propaga la doctrina yihadista, ha inaugurado también en español un canal en Telegram, una cuenta en Twitter y una web que probablemente deberá ir cambiando de servidor a medida que se la vayan cerrando. Hasta ahora «Al Haqq» solo distribuía material en inglés.

Siguiendo con ejemplos significativos de la profusión en el uso de las TIC por parte de las organizaciones terroristas, y nuevamente hablando del Dáesh, a primeros de mayo del 2017, la conocida como *Electronic Horizons Foundation* (EHF), que tiene por finalidad:

> «La finalidad de este canal es ayudar a los miembros de Dáesh a cifrar sus mensajes para pasar inadvertidos y no ser detectados por las autoridades occidentales. La EHF se fundó como un esfuerzo conjunto de los mejores expertos en ciberseguridad de Dáesh y funciona como *help desk* para el cifrado de las comunicaciones entre miembros y seguidores del grupo terrorista».

La EHF encontrándose que la misma se constituye como un elemento de distribución de la información necesaria para dar conocimiento y orientación de distintas aplicaciones y servicios informáticos y su correcta utilización. Así la *Electronic Horizons Foundation* conocida también como *Horizons Foundation*, hace distintas publicaciones dando a conocer aplicaciones y servicios relacionados con la seguridad informática, creando en el año 2015 una «colección de seguridad informática para sistemas Windows» la cual contiene enlaces a tutoriales y manuales de distintos productos, aplicaciones y servicios relacionados con la seguridad informática tales como antivirus, aplicaciones de borrado seguro, servicios VPN, etc.

Y si Internet, y en especial las redes sociales, están jugando un papel fundamental en la recluta de «combatientes», también lo es para la de «cibercombatientes»; y en este sentido destacar que el 25 de mayo del 2017, en un canal de Telegram, el grupo hacker pro Dáesh, Fighter Moeslim Cyber Caliphate (FMCC), hizo una publicación en la cual indican que «han vuelto» y que «necesitan *hackers* musulmanes» para unirse a ellos y atacar a los infieles. Este grupo apoya al United Cyber Caliphate (UCC), también conocido como Caliphate Cyber Terrorims Army (CCTA)*, lo cual supone que un engrose en las filas del FMCC suponga al mismo tiempo un aumento de capacidades de manera indirecta del UCC/CCTA.

> **El nombre Caliphate Cyber Terrorims Army (CCTA) siembra dudas entre algunos analistas, por supuestamente auto denominarse terroristas, quizás estemos ante una ACCION DE FALSA BANDERA.*

Conscientes de la grave repercusión del adoctrinamiento y recluta que las organizaciones terroristas de corte yihadista, valiéndose de las oportunidades que las nuevas tecnologías les brindan, en especial redes sociales, la Comisión Europea, en marzo del 2018, adoptó una resolución obligando a las prestadoras de servicios (especialmente Facebook, Twitter y YouTube) a la retirada de contenidos, en un plazo máximo de una

hora desde que un cuerpo policial de un Estado miembro de la UE, o la propia EUROPOL, se lo comunique, y sin mediar acción judicial alguna, al considerar que estos contenidos resultan «especialmente dañinos en las primeras horas de su aparición en línea».

b. ***Internet como medio para llegar a objetivos tecnológicos u objeto directo de acciones hostiles***. Esta es la razón última del ciberterrorismo; y a la pregunta de cuáles serían los objetivos propios del terrorismo a través de Internet la respuesta resulta obvia, los mismos que ya lo son en la actualidad: *telecomunicaciones*, *infraestructuras*, *economía y empresa*, *servicios públicos en general y Administración y Estado*. En suma, aquellas que se encuadran en el concepto de infraestructura crítica, entendiendo como tal:

> «Instalaciones, redes, servicios, equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos». [COM (2004) 702 final, 20 octubre].

La debilidad de estas, las IC, además de su naturaleza intrínseca, viene amplificada por el hecho de la interconexión e interdependencia que existe entre ellas, propiciando efectos encadenados, también conocidos como «en cascada» o «dominó», que posibilitarían que la pérdida directa de uno de ellos conlleve a su vez la pérdida, inoperatividad o inaccesibilidad de otras. Esto provocaría no solo los consiguientes perjuicios y daños en servicios esenciales, sino también, y muy especialmente, efectos psicológicos en la población. *No perdamos de vista que nuestra cada vez mayor dependencia tecnológica nos hace más débiles y vulnerable*s[19].

> «La primera reivindicación de un presunto ataque ciberterrorista tuvo lugar el día 19 de febrero del 2004 cuando la autodenominada "brigada Abu-Nafsa" se atribuyó la autoría de un supuesto ciberataque contra la infraestructura energética de EE. UU. que derivó en el mayor apagón de su historia (verano del 2003); a este comunicado no se le dió credibilidad por lo extemporáneo, si bien la causa real del incidente sigue siendo un misterio[20]».

Realmente existen elementos tangibles de la amenaza. Aunque a nivel nacional aún no se podría hablar de proyección real de una amenaza concreta, a nivel internacional, y más concretamente de EE. UU., sí, toda vez que han obtenido evidencias reales de que algunos sistemas informáticos de administración remota de infraestructuras críticas

---

[19] La población mundial en general, o en particular los más jóvenes, cada vez es más dependiente del uso de la tecnología y consecuentemente vulnerable a su carencia. Psiquiatras surcoreanos ya han desarrollado el concepto de «demencia digital» y han identificado la sintomatología de este cuadro clínico de trastorno mental. Dr. Manfred Spitzer [Demencia Digit@l - El peligro de las nuevas tecnologías - editorial B grupo Zeta].

[20] Informe de Andrey Belousov del Centro de Investigación de Delitos Informáticos de los EE. UU. [Computer Crime Research Center].

están comprometidos, concretamente los denominados sistemas SCADA[21] o sistemas de control industrial (SCI):

> «Los ataques con éxito sobre los sistemas SCADA podrían producir terror a gran escala. En las cuevas de Afganistán, las tropas de EE. UU. encontraron planes de Al Qaeda para atacar esos sistemas[22]».

Sin duda son las denominadas infraestructuras críticas las que están en el ojo del huracán ya que cualquier interferencia grave en su normal funcionamiento acarrearían graves problemas a una sociedad cada vez más dependiente de la tecnología y de los servicios que esta sustenta; así mismo la actividad económica también es objetivo; de hecho, se estima que una acción ciberterrorista de gran calado no se materializaría de forma aislada sino que sería el complemento o refuerzo de otra acción terrorista convencional.

Vivimos en una sociedad cada vez más dependiente de las nuevas tecnologías y este hecho se va a ver, y se está viendo, multiplicado por fenómenos como el *Internet de las cosas (IoT), la inteligencia artificial o la conectividad 5G.*

Son numerosas y cuantiosas las ventajas y beneficios que este Internet de las cosas va a portar al desarrollo social, pero es indudable también que una gran cantidad de dispositivos conectados todos ellos a la Red puede suponer un aumento terrible de la superficie susceptible de ciberataques mediante por ejemplo los ya mencionados DDoS.

Como ejemplos muy recientes podemos destacar por un lado el ataque del pasado día 21 de octubre de 2016 a través de la *botnet Mirai*. Esta botnet, formada por miles de dispositivos conectados a Internet infectados, es capaz de dirigir a todos ellos para lanzar ciberataques masivos y coordinados, saturando los servidores a los que atacan para dejarlos sin servicio. Este DDoS dejó sin servicio a empresas tecnológicas tan importantes como Twitter y Spotify a través del ataque a los servidores de la empresa Dyn, imposibilitando el acceso a Internet a gran parte de la costa este de Estados Unidos y notándose sus efectos a nivel mundial. El segundo ataque más destacado y protagonizado por una variante de esta *botnet Mirai* es el acontecido el pasado mes de noviembre sobre los *routers* de la compañía tecnológica Deutsche Telekom**.** Este ataque provocó según los responsables de la propia compañía que unos aproximadamente 900.000 clientes experimentaran importantes problemas de conexión a la Red, con lo que se atenta directamente contra los derechos de todas estas personas al libre acceso a Internet.

Y llegados a este punto alguien de ustedes se estará preguntando si realmente los terroristas son conscientes de esta situación y pretenden aprovecharla o se está ante un mero ejercicio de informática-ficción; pues a modo de respuesta unas breves citas

---

[21] «Los ataques con éxito sobre los sistemas SCADA podrían producir terror a gran escala. En las cuevas de Afganistán, las tropas de EE. UU. encontraron planes de Al Qaeda para atacar esos sistemas». Cita de Mark Rasch – antiguo jefe de la Unidad de delitos informáticos del Departamento de Justicia de EE. UU.

[22] Cita de Mark Rasch – antiguo jefe de la Unidad de delitos informáticos del Departamento de Justicia de EE. UU.

cargadas de gran significación dada la naturaleza de las mismas, el contexto en el que se citan y sus autores:

> «Es muy importante concentrarnos en golpear a la economía de EE. UU. de todas las formas posibles... buscando los pilares clave de la economía de EE. UU. deberían golpearse los pilares clave del enemigo...».

Osama Bin Laden, entrevistado en un medio de difusión árabe el 27 de diciembre del 2001.

> «Dividid su nación, rompedla en pedazos, destruid su economía, quemad sus empresas, arruinad su bienestar, hundid sus barcos y matadlos en tierra, mar y aire...».
>
> Cita atribuida a Muhammad Atef, antiguo comandante militar de Al Qaeda.

> «... Salah había recibido cursos de programación, cifrado y otras técnicas de *hacking* y vigilancia electrónica realizadas con la inteligencia en una casa de huéspedes perteneciente a Osama Bin Laden en Hyatabad, un barrio de Peshawar, Pakistán...»
>
> *Testimonio de L'Houssaine Kherchtou ante un tribunal de Nueva York el 7 de febrero del 2001.*

> «El FBI cree que el ciberterrorismo, la utilización de ciberherramientas para parar, degradar o denegar el acceso a infraestructuras críticas nacionales, como la energía, el transporte, las comunicaciones o los servicios gubernamentales, con el propósito de coaccionar o intimidar a un gobierno o a la población civil, es claramente una amenaza emergente para la que debemos desarrollar habilidades de prevención, disuasión y respuesta».
>
> Louis Freeh – antiguo director del FBI en una declaración ante un Comité del Senado de los EE. UU., mayo 2001.

> «Aunque todavía no hemos visto a estos grupos emplear ciberherramientas como arma contra infraestructuras críticas, su dependencia de las tecnologías de la información y la adquisición de pericia informática son claros indicadores de alerta».
>
> *Leslie G Wiser, jefe de la Sección de Estrategia, Prospectiva y Formación del NIPC – FBI - Manifestaciones realizadas ante un Comité de la Cámara de Representantes sobre la investigación de Ramzi Yousef, cerebro del ataque con bomba al Wold Trade Center, agosto 2001.* El supuesto que se está planteando es *perfectamente viable,* ya que en la actualidad las TIC están diariamente comprometidas por la acción anónima de *hackers*, y organizaciones delictivas, algunas con bastante éxito por la relevancia de los sistemas comprometidos, el número de ordenadores afectados o incluso por los daños económicos causados. Pues bien, lo único que le faltaría a cual-

> quiera de estas acciones para convertirse en una acción ciberterrorista es la motivación o reivindicación por parte de una organización terrorista.

Y en esta línea, el 2 de febrero del 2012, el director de la Oficina Federal de Investigaciones de EE. UU. (FBI), Robert Mueller, aseguró que «el ciberterrorismo igualará o superará a las amenazas que suponen el modelo de terrorismo actual en un futuro no muy lejano», realizó tal afirmación durante su declaración en audiencia ante el Comité de Inteligencia del Senado estadounidense sobre las amenazas mundiales, advirtiendo que el FBI y las agencias de inteligencia deberían cambiar su estructura para hacer frente a este tipo de amenaza, cada vez más fuerte:

> «Es muy poco lo que hacemos hoy en día con los asuntos relacionados con Internet. El robo de propiedad intelectual, el robo de investigación y desarrollo, el robo de planes y programas empresariales para el futuro, todo ese tipo de asuntos son vulnerables de ser explotados por atacantes». En segundo lugar, señaló que las agencias de inteligencia «han de compartir información... tenemos que construir un colectivo para hacer frente a esa amenaza, de la misma manera que lo hicimos y rompimos las barreras tras el 11 de septiembre».

Sin lugar a dudas, un nuevo hito en la evolución o materialización de la amenaza ciberterrorista la encontramos en el ciberataque sufrido, en la madrugada del 8 al 9 de abril del 2015, por la cadena francesa TV5 Monde. El ataque, a manos del autodenominado *CyberKahilafah* (CiberCalifato), vinculado al Dáesh, bloqueó la emisión de la señal de televisión satélite de la cadena, su página web y perfiles en redes sociales. Esta acción supone un cambio cualitativo sin precedentes en la percepción de la amenaza y en la constatación de que la amenaza ya no es tal sino más bien una inquietante realidad. Este mismo grupo de *hackers* protagonizó un ciberataque contra la cuenta de Twitter del Mando Central de Estados Unidos (CENTCOM), el 13 de enero de ese mismo año. En octubre del 2016 la empresa de ciberseguridad FireEyes aseguró haber obtenido evidencias de que el atacante real había sido el grupo *hacker* conocido como Fancy Bear, vinculado con Rusia a través de la GRU, y si bien esas evidencias no se han hecho públicas, el hecho de que no se hayan reproducido acciones de tal complejidad técnica, atribuidas al CiberCalifato, hacer plausible esta acusación y con ello considerar ambos incidentes como ACCIONES DE FALSA BANDERA.

Según el informe oficial «Seguridad TIC en Alemania 2014», publicado el 26 de diciembre del 2014, elaborado por la Oficina Federal para la Seguridad de la Información (BSI), una planta siderúrgica no identificada en el país germano fue atacada por *hackers* que manipularon los sistemas de control de tal manera que un alto horno no pudo ser correctamente apagado, generando de este modo daños «masivos» (aunque no especificados). Los atacantes tuvieron acceso a la planta a través de la red corporativa de la misma, desde la que se abrieron paso hasta las redes de producción y los equipos de control. El método usado para infiltrarse en la red corporativa fue mediante un ataque *phishing*, enviando un *e-mail* diseñado para que aparentara proceder de una fuente fiable. Este incidente resucitó los «fantasmas» surgidos tras el incidente acaecido en 2010 en la Central Nuclear iraní de Bushehr y el Complejo Nuclear de Natanz, que sufrieron un ciberataque protagonizado por el *malware* tipo gusano bautizado como Stuxnet, que se replicaba, mutaba y adaptaba de forma desasistida (sin la presencia de un panel de

mando y control), infectando solo en Irán 63.000 ordenadores (significar que lo fueron 88.000 a nivel mundial, lo que da idea de lo «dirigido» que fue el ataque) sin causar daños en ninguno de ellos, hasta encontrar ese ordenador objetivo para el que había sido programado y sobre el que sí causó daños.

Pero el temor a las implicaciones de un ciberataque exitoso contra una IC es la esencia de toda amenaza ciberterrorista, pues garantizaría una rápida e inevitable degradación de servicios esenciales para el normal desarrollo de la actividad de nuestra sociedad, tal y como esta se concibe. Y es que la tecnología es el «talón de Aquiles» de las sociedades modernas, como tantas y tantas veces se ha constatado con ocasión de accidentes, sabotajes o desastres naturales. La dependencia de la tecnología cada vez es mayor y su pérdida o disrupción acarrea cada vez mayores problemas.

Sirva de ejemplo la problemática en torno a las infraestructuras de generación, transporte y distribución de energía eléctrica, que tan sensibles y críticas resultan. Lo que en el mundo anglosajón denominan el *blackout*, o gran apagón, supondría la rápida degradación o pérdida de servicios esenciales hasta alcanzar niveles «apocalípticos». Pues bien, lo que hasta ahora no ha sido más que un ejercicio de informática ficción o un recurrente guión del cine más catastrofista, parece estar más próximo a la vista de los inquietantes acontecimientos que han sucedido en los primeros meses del 2016. Por un lado, Ucrania: si ha sufrido o no un ciberataque a gran escala es una de las cuestiones que las agencias de inteligencia de la OTAN están estudiando. Lo que sí es cierto es que miles de familias pasaron unos días muy duros después de que la compañía energética Prykarpattyaoblenergo**,** prestadora del servicio de abastecimiento eléctrico a la región de Ivano-Frankisvk, al oeste del país, interrumpiera el suministro eléctrico el 23 de diciembre a cerca de 600.000 hogares tras sufrir una «interferencia» en sus sistemas de control. Pero aún el 20 de enero del 2016 la situación se repitió en otras regiones de Ucrania. Los ataques parecen tener una clara motivación política y materializarse desde la vecina Rusia. Pues bien, el pasado 27 de enero del 2016, Israel sufrió un grave ciberataque contra su red energética que afectó a varios de sus sistemas, en uno de los momentos de mayor demanda eléctrica por las bajas temperaturas. No ha trascendido mucho de los detalles del incidente, si bien el ministro de Energía israelí aseguró que tuvieron que parar algunos sistemas para poder solucionar el problema sobre su *Nation's Electrical Power Grid Authority's Network,* confirmado durante la celebración de la conferencia CyberTech 2016 que habían sufrido uno de los ciberataques más graves que han experimentado hasta el momento.

En muchos aspectos, los conceptos de ciberterrorismo y ciberguerra se entremezclan a través de una línea cada vez más difusa; evidentemente la motivación lo es todo y el actor o actores, que estén realmente detrás de cada acción, su elemento definitorio, pero este muchas veces se nos escapa.

En julio del 2015, se constituyó una nueva estructura en Europol, esta vez focalizada en la prevención y respuesta del fenómeno del ciberterrorismo, y bautizada Unidad de Referencia de Internet —IRU— (Internet Referral Unit).

Pero en marzo del 2016, se produjo un incidente que tuvo escasa repercusión en los m.c.s. pero que si se analiza resulta tremendamente inquietante. La web británica

The Register hizo público un informe de la empresa Verizon Security Solutions, relativo al incidente acaecido en la planta de potabilización de aguas de una localidad británica de 2,5 millones de habitantes, consistente en una intrusión en su sistema de mando y control y llegando a cambiar los niveles de sustancias químicas que se utilizan para tratar el agua del grifo en cuatro ocasiones; asimismo, los *hackers* obtuvieron acceso a los registros personales y financieros de más de 2 millones y medio de consumidores. Debido a la naturaleza sensible de estos datos no se revela el nombre de la planta ni el país donde está situada. La planta fue capaz de identificar y anular los cambios, el impacto a los clientes se redujo al mínimo y nadie se enfermó. «La infracción fue grave y fácilmente podría haber sido más crítica. Si los responsables de la amenaza hubieran tenido un poco más de tiempo y más conocimiento del sistema ICS/SCADA, la empresa y la comunidad local podrían haber sufrido graves consecuencias», según escribieron en el informe los investigadores de Verizon. Las autoridades británicas, un grupo «hacktivista» con vínculos con Siria comprometió las computadoras de Kemuri Water Company después de explotar las vulnerabilidades del portal web de pago de clientes. Hasta ahí la versión oficial, pero si la analizamos con detalle observaremos que el ataque perseguía modificar parámetros físicos, potencialmente dañinos y que el propio informe califica como grave; a mi juicio no nos encontramos ante un acto de hacktivismo sino de ciberterrorismo.

Hacktivismo

El año 2015 nos trajo un nuevo término asociado al ciberterrorismo, pues el Centro Nacional de Inteligencia comenzó a emplear en sus informes ciberyihadismo[23],

> «… Que usando métodos, procedimientos y herramientas del terrorismo, el hacktivismo y la ciberguerra constituye una realidad incipiente y supone una de las mayores amenazas con las que se enfrentarán las sociedades occidentales en los próximos años. Las importantes vías de financiación de estos grupos, al socaire de Dáesh, hacen posible que puedan llegar a adquirir los conocimientos y las herramientas precisas para el desarrollo de ciberataques o la contratación de los mismos. Hasta el momento sus ciberataques se han limitado a la desfiguración de páginas web, ataques DDoS a pequeña escala o, más comúnmente al uso de Internet y de las redes sociales para la diseminación de propaganda o el reclutamiento y la radicalización, actividades que no exigen grandes conocimientos o infraestructuras. LAS CAPACIDADES DEL CIBERYIHADISMO NO HAN HECHO SINO EMPEZAR A MOSTRARSE. ES DE ESPERAR CIBERATAQUES MÁS NUMEROSOS, MÁS SOFISTICADOS Y MÁS DESTRUCTIVOS EN LOS PROXIMOS AÑOS, EN TANTO PERSISTA LA ACTUAL SITUACIÓN EN TORNO AL DÁESH».

Detallan los especialistas del CNI-CCN que durante 2015 estas tramas terroristas llegaron a utilizar «códigos dañinos» en Siria para «obtener datos sobre posiciones de los objetivos locales».

---

[23] Ciberyihadismo, terminología y reflexiones acuñadas por el Centro Criptológico Nacional. Véase CCN-CERT IA-09/16 CIBERAMENAZAS 2015 / TENDENCIAS 2016 [RESUMEN EJECUTIVO].

En la actualidad existen diferentes grupos yihadistas pro Dáesh que se mueven en el entorno cibernético y desarrollan actividad propia de los denominados grupos hactivistas, parte de los cuales se señalan a continuación: Al-Qaeda Electronic, Team System DZ, Islamic State Hacking Division, Middle East Cyber Army, Moujahidin Team, Islamic Cyber Army, Ghost Caliphate (grupo surgido de la unión de Anon ghost y Cyber Caliphate) y el más activo United Cyber Caliphate (grupo creado a partir de la unión de los siguientes grupos: Caliphate Cyber Army, Ghost Caliphate Section, Sons Caliphate Army, Kalachnikv E-Security Team, Cyber Kahilafah, Al Khansaa Kateeba, Fighter Muslim Cyber Caliphate (FMCC) y Anon Terror Team o Shadow Caliphate Anon Terror). También existen grupos afines al régimen sirio: Syrian Electronic Army (SEA) y Syrian Cyber Army (SCA). Por último están los grupos hactivistas, de la órbita del movimiento Anonymous, que se enfrentan a los anteriores en una incruenta guerra conocida como #OpISIS, incruenta pues hablamos de actividad hactivista, pero a la vez ilícita, siendo estos: GhostSec, Ghost Security Group, Controlling Section y Ghost Squad Hackers.

Los hacktivistas combinan la habilidad de los hackers con la «tenacidad» de los activistas; sus objetivos suelen ser empresas, gobiernos, servicios secretos, etc… en definitiva, todos aquellos que consideran responsables del modelo social imperante, para ellos injusto y corrupto. Nos encontramos ante los individuos y grupos más radicales de entre los denominados activistas (colectivos anti-sistema, grupos anti-globalización, anarquistas, okupas y otros movimientos de izquierda radical). Pero en este caso estamos ante individuos que están dispuestos a trasgredir las leyes y convertirse en cibercriminales, pues lo consideran legítimo y justificado para la consecución de sus objetivos.

Este movimiento nace a principios de los 90 fruto del grupo Cult of the Dead Cow. Sus creadores la definen como «hacer *hacking* o crear tecnología en pos de un objetivo político o social». La primera acción de esas características fue el gusano Wank que penetró en el sistema del Departamento de Energía Americano en protesta contra la energía nuclear en 1989. Estados Unidos se mantiene en el foco de las críticas del hacktivismo, focalizándose en sus servicios de inteligencia y especialmente la Agencia de Seguridad Nacional (NSA) los estamentos contra los que más se rebelan. El exponente principal de esa lucha es el extrabajador de esa agencia, Edward Snowden. «Uno de los valientes que se la ha jugado para demostrar al mundo que el Gran Hermano existe».

A finales del año 2011, Anonymous y LulzSec publicaron un comunicado en el que hacían un llamamiento a sus simpatizantes la cancelación de sus cuentas en PayPal (entonces parte de la empresa eBay) por el bloqueo de esta a tramitar las donaciones a la organización Wikileaks. Esta acción fue la «puesta de largo» del movimiento Anonymous pues se cerraron más de 30.000 cuentas en PayPal, lo que sin duda contribuyó a que el valor de las acciones de eBay en el índice tecnológico cayera algo más de un 3 %. Una caída que supuso para la compañía pérdidas por valor de 1.000 millones de dólares.

En nuestro país la actividad de estos grupos es escasa y las acciones desarrolladas han sido puntuales y de escasa repercusión. El objetivo preferido de los seguidores españoles de Anonymous ha sido el Gobierno de la Nación, las Administraciones públicas y los partidos políticos tradicionales. El 3 de febrero del 2016, el autodenominado La9 de Anon (el grupo nacional más activo y afín al movimiento Anonymous), logró extraer in-

formación y hacerla pública, de los servidores de acceso a la compañía que gestiona los patrocinios de la empresa El Corte Inglés; dichos documentos se refieren a los gastos de los últimos seis ejercicios (de 2011 a 2016). Fuentes de la propia compañía reconocieron que se produjo en fechas recientes un robo de información, aunque no validaron la totalidad de los números que aparecen en la base de datos, que consta de cerca de 18.000 registros de transferencias, talones, pagos en especie y otro tipo de gastos; la relación de gastos asciende a más de 53 millones de euros.

En agosto del 2015, la División Cibernética del FBI no dudó en considerar, cuantitativamente, el hactivismo como la mayor amenaza para los EE. UU., por encima incluso del ciberdelito.

Para cerrar este capítulo, destacar que desde septiembre del 2017, en nuestro país, se vienen sucediendo una serie de acciones hactivistas de baja intensidad y escasa eficacia, protagonizados por aquellos que han abrazado la causa del secesionismo en Cataluña y que bajo las denominadas #OpCatalunya, #FreeCatalonia u #Op21Dec, entre otras, pretenden alterar el normal funcionamiento o exfiltar datos de aquellas páginas web o dominios, preferentemente de organismos de las Administraciones públicas aunque tambien de entidades privadas, que consideran «españolistas». Una vez más, al frente de estas acciones nos encontramos a la ya citada «La9 de Anom».

Ciberespionaje

Pero los ciberataques de motivación esencialmente económica, mediante la sustracción de información, campañas de desinformación o sencillamente alterando la normal continuidad de negocio, que afecten gravemente la capacidad competitiva de nuestras empresas, y más en unos momentos de crisis económica, pueden acarrear una pérdida de soberanía nacional real.

Y es que encontramos en el ciberespionaje, un elemento perturbador y desestabilizador en el legítimo desarrollo económico de las sociedades modernas, los incidentes de esta naturaleza —orientados sobre objetivos económicos— han experimentado un crecimiento viral, afectando a la práctica totalidad del tejido productivo de los países occidentales. Los daños patrimoniales infligidos por esta ciberamenaza se estimaba que ocasionaron unas pérdidas anuales superiores a los 300.000 mill. de euros, en los últimos años, cifras estas que escandalizaban y preocupaban, si bien ya se puede hablar de que han quedado obsoletas. No existiendo una cuantificación o estadística fiable a nivel nacional, tomaremos como referencia los de otros países de nuestro entorno y así, por ejemplo, en el 2013 estos daños en el Reino Unido han sido cuantificados en 27.000 mill. de libras y en la República Federal de Alemania en 45.000 millones de euros.

En 2015 el Centro Criptológico Nacional dependiente del Centro Nacional de Inteligencia (CNI-CCN) no dudó en calificar el ciberespionaje[24] (político o industrial) como la

[24] Ciberespionaje, reflexiones del Centro Criptológico Nacional. Véase CCN-CERT IA-09/16 CIBERAMENAZAS 2015 / TENDENCIAS 2016 [RESUMEN EJECUTIVO].

mayor amenaza a la que se enfrentan las sociedades o estados modernos, categorización que se ha mantenido hasta la actualidad.

Ciberguerra

A diferencia de las cuatro anteriores, esta es la única modalidad de ciberamenaza que por sí misma no constituye una acción ciberdelictiva y que no estaría regulada por cumplimiento de la legislación penal de los estados, ni de los convenios internacionales sobre cibercriminalidad, sino por el Derecho Internacional de Guerra de las Naciones Unidas. Pero en realidad tiene una implicación muy directa con todas las anteriores, máxime si se aplican conceptos como el de guerra híbrida y guerra asimétrica, o la conjunción de ambas, donde el «arte de la guerra» tradicional se combina con todo tipo de acciones en el ciberespacio, la mayoría de ellas aprovechándose de las malas artes del ciberdelito en general.

En julio del 2016 la Unión Europea (UE) y la Organización del Tratado del Atlántico Norte (OTAN) se comprometieron a intensificar su cooperación en materia de ciberdefensa en una declaración conjunta, motivada en los «desafíos sin precedentes» que comparten sus fronteras exteriores. El nuevo pacto se fundamenta en el desarrollo de capacidades de defensa complementarias e interoperables y la realización de proyectos conjuntos en las áreas de la ciberseguridad, amenazas híbridas, comunicaciones estratégicas y formación de fuerzas de seguridad, siendo la primera vez que ambas instituciones firman un acuerdo de tal alcance.

Dicho acuerdo llega tras el reconocimiento oficial de la OTAN del ciberespacio como un dominio más de la guerra, lo que implica que ciertos ataques llevados a cabo en este contexto podrían desencadenar como respuesta las acciones recogidas en el artículo 5 del Tratado del Atlántico Norte; o lo que es lo mismo, respuesta militar ante ciertos ciberataques.

Sirva de ejemplo ilustrativo, que a su vez supuso el inicio de la espiral de recelo entre estados y alianzas militares, el grave incidente acaecido en Estonia en la primavera del 2007 supuso el punto de inflexión entre la especulación a la constatación de una realidad, por primera vez se producía un ciberataque «a gran escala», y con éxito, contra un Estado, inutilizando o colapsando una parte más que considerable de sus infraestructuras TIC. Internet había sido algo más que el medio, había sido el objetivo de las acciones ilícitas. Este incidente obligó a la OTAN a replantear toda su estrategia de ciberseguridad y ciberrespuesta, o más bien a definirla, concretándose en dos hechos de evidente relevancia: por un lado, la creación del Centro de Excelencia de Ciberdefensa Cooperativa (CCD CoE) en Tallín, capital de Estonia, y por otro la nueva Estructura de la Alianza surgida de la Cumbre de Lisboa en octubre del 2010.

Igualmente resulta muy significativa la constitución, por parte del DoD, del denominado Mando de Defensa Cibernética (CYBERCOM ó USCMBERCOM) el año 2010. En analogía al anterior, y clara inspiración en este, el día 26 de febrero del 2013 y mediante la Orden Ministerial 10/2013 vio la luz en el seno de las Fuerzas Armadas españolas del Mando Conjunto en Ciberdefensa (MCCD).

Recapitulando

Alcanzado este punto, resulta obligado hacer una reflexión que plantee la problemática real de las nuevas ciberamenazas, mayoritariamente cibercriminalidad (ciberdelincuencia, ciberterrorismo y hacktivismo) aunque sin olvidad el ciberespionaje, planteándolas como un conjunto múltiple de técnicas y vulnerabilidades que en manos de la delincuencia tradicional, transforman el ciberespacio y todo lo que este «alberga» como objetivos potenciales de la acción ilícita.

No existen barreras ni líneas divisorias que nos permitan compartimentar ni acciones (entendiendo como tales los delitos en sí mismos) ni aun menos agentes (ciberdelincuentes, independientemente de la motivación que les lleven a delinquir). Tanto las acciones como los actores se «desplazan» trasversalmente por todas ellas, según convenga a sus intereses y facilite la consecución de sus fines.

A continuación, se exponen dos escenarios reales que pretenden ilustrar estas ideas y que pretenden llamar a la reflexión:

1.º) La modalidad de extorsión mediante *software* malicioso conocida genéricamente por *ransomware*, que está ocasionando ingentes perjuicios a empresas y particulares, tanto por la extorsión en sí misma, como especialmente por los daños ocasionados y con ello el lucro cesante, hasta tal punto que una estimación del FBI cifra el lucro obtenido por los «cibercriminales» durante el 2016, en no menos de los 1.000 millones de dólares, y se estima que está creciendo desde entonces a un ritmo no inferior al 200 % anual.

El 12 de mayo del 2017 aconteció el incidente, de mayor impacto a nivel mundial, de esta modalidad delictiva, conocido como Wannacry; se estimó en más de 230.000 las infecciones en todo el mundo, durante sus primeras 72 horas de actuación, y por las diferentes variantes de este virus en un total de 179 países (fuente Europol). Según el INCIBE, en nuestro país, primero que sufrió y detectó el ataque, hubo 1.200 infecciones conocidas. La extorsión, para los presuntos cibercriminales, resultó un rotundo fracaso, pues solo consiguieron pagos de las víctimas por importe de 52,19 unidades de la moneda virtual (Bitcoin), equivalentes al cambio a 120.291 euros[25]. Sin embargo, los

[25] Los responsables del virus WannaCry se cobran los 120.000 euros que consiguieron en rescates (3 AGO. 2017)
Un total de 52,19 «bitcoins» procedentes de tres monederos virtuales que los responsables del ciberataque protagonizado por WannaCry habían habilitado para rescates de ficheros encriptados por el *ransomware* han sido retirados este jueves en siete partidas. Los movimientos han sido detectados por un *bot* de Twitter creado para informar del estado y actividad de las cuentas vinculadas a este ciberataque.
Las 52,19 unidades de la moneda virtual, equivalentes al cambio a 120.291 euros, habían sido acumulados en tres monederos *online* a los que se transferían los pagos solicitados por WannaCry para liberar los archivos secuestrados. El *bot* de Twitter Actual Ransom, creado por el periodista de Quartz Keith Collins, ha detectado y publicado siete retiradas de dinero entre las 05:10 y las 05:25 horas de este jueves que han dejado vacías estas cuentas, según ha recogido BBC.
El informe de Actual Ransom previo a esta retirada de dinero había registrado un total de 338 pagos, el último de ellos recibido el pasado 24 de julio. Al encriptar los archivos, el *ransomware* solicita a sus víctimas rescates en «bitcoins» equivalentes a cifras de entre 300 y 600 dólares —252 y 505 euros aproximadamente, al cambio—. A finales del pasado mes de julio, la compañía de control de movimientos de «bitcoins» Elliptic había detectado la retirada de parte de los ingresos de WannaCry.

daños estimados ascienden a 3.600 millones de euros, de los que tan solo 5 millones correspondieron a nuestro país, que se repartieron de la siguiente forma: la pérdida de información (39 %), la interrupción de actividades (36 %), la pérdida de ingresos (20 %) y el daño a los equipos (4 %). Ante la magnitud del ataque, se activaron la práctica totalidad de las estructuras de ciberseguridad-ciberdefensa del mundo, civiles y militares, públicas y privadas; y se inició una investigación coordinada al máximo nivel (en nuestro caso en Europol, y a nivel nacional la Fiscalía Especial en Delincuencia Informática abrió diligencias informativas con el auxilio de los dos cuerpos de policía del Estado (Guardia Civil y Policía Nacional). En diciembre de ese mismo año las autoridades estadounidenses responsabilizaron de la autoría del mismo al Régimen Norcoreano, pero la pregunta que aún queda en el aire es ¿qué pretendían realmente los atacantes? Parece que el móvil económico, si hubiera sido este, resultaría decepcionante para los ciberdelincuentes; pero, ¿y si no fuera el móvil económico el que se perseguía, sino más bien obligar a los países occidentales a dar visibilidad a sus capacidades de ciber-respuesta?

El 27 de mayo, se detectó que uno de los grupos integrantes del United Cyber Caliphate (UCC), más concretamente el autodenominado Fighter Moeslim Cyber Caliphate (FMCC), había variado su estrategia ampliando su amenaza con ataques mediante *ransomware* y extorsión en bitcoins. Esta nueva vía de estrategia podría verse impulsada por el empuje mediático que en fechas recientes ha tenido este tipo de ataques (*wannacray*) y en la posibilidad de búsquedas alternativas de financiación. CyberSPhreak, alias de uno de los *hackers* del FMCC con más repercusión, es quien parece estar desarrollando actualmente la mayoría de los ataques, y liderando por ahora los ataques *ransomware*. Tampoco pasó desapercivido a los analistas que sus primeras acciones coincidieron con el inicio del ramadam, para darle mayor «legitimidad moral» a esta forma de financiación de la organización terrorista Dáesh.

También en 2017, y más concretamente el 27 de junio, se produjo un segundo incidente a gran escala, esta vez el *maleare* fue bautizado como Petya, por su similitud con un *ransomware* anterior, aunque algunos analistas lo desmintieron y renombraron como NoPetya. Su novedoso mecanismo de propagación le confería mayor agresividad y sofisticación que su predecesor Wannacry. Con un ratio de infección menor, se contabilizaron unas 2.000 organizaciones infectadas procedentes de 64 países, si bien el más afectado y potencial origen de la infección a otros se ubicó en Ucrania (60 % de las infecciones). Los presuntos cibercriminales no obtuvieron lucro conocido y los daños reales se desconocen, pero quedó en evidencia que el objetivo era Ucrania como Estado y sus infraestructuras (algunas de ellas críticas) las víctimas. A título de ejemplo, y para entender la magnitud del ataque, la naviera danesa Maersk ha cuantificado en un máximo de 255 millones de euros —entre 200 y 300 millones de dólares— los daños. Una vez

---

Expertos consultados por el medio público británico han explicado que los 'bitcoins' retirados podrían haber sido colocados en un 'mezclador', nombre con el que se conoce a un sistema a través del que el dinero es transferido y mezclado con una gran lista de pagos para dificultar su seguimiento. Sin embargo, las fuentes consultadas por la BBC han reconocido no saber la razón del movimiento de este dinero, que podría ser empleado para pagar servicios de la 'dark web'.

El ciberataque global protagonizado por el 'ransomware' WannaCry comenzó el pasado mes de mayo y afectó a particulares, instituciones y empresas de más de un centenar de países. El virus exige a las víctimas el pago de un rescate para desbloquear los archivos encriptados en el ataque, forzando a los propietarios a abonar la cantidad exigida mediante una cuenta atrás.

más seguimos sin autor conocido. En febrero del 2018 el Reino Unido acusó públicamente a la Federación Rusa de estar detrás del incidente, que además había evidenciado que el objetivo del mismo fueros IC ucranianas y más concretamente la destrucción de la información digital; ¿podríamos por tanto hablar claramente de sabotaje o incluso de ciberguerra?

Resulta evidente que estamos hablando de *ransomware,* una de las formas más novedosas de ciberdelito, pero a la pregunta de si es empleada exclusivamente por ciberdelincuentes al uso, esto es, aquellos que actúan motivados exclusivamente por lucro económico personal, la respuesta es que evidentemente no. Se han presentado tres escenarios muy graves, acaecidos en un espacio temporal escaso (6 semanas) y que tienen como único denominador común, a parte del obvio uso de una misma «técnica informática», que en ninguno de ellos la autoría parece corresponder al perfil de ciberdelincuente descrito anteriormente. En el caso de Wannacry, numerosas fuentes de investigación, tanto gubernamentales como privadas, coinciden en señalar al grupo *hacker* Lazarus, directamente vinculado con el Gobierno de Corea del Norte; que por otra parte ha protagonizado otros ataques relevantes, en especial contra el sistema interbancario SWIFT, para financiar al régimen norcoreano. En el caso del FMCC tenemos un nuevo escenario de financiación del terrorismo, por parte de un grupo hacktivista que ha jurado lealtad al Dáesh y que se integra en el denominado cibercalifato; tampoco es nuevo, en su día se descubrió una red de estafadores de tarjetas de crédito por Internet que lo hacían para financiar a Al Qaeda. Por último Petya, nuevamente por boca de diversas fuentes de investigación, tanto gubernamentales como privadas, atribuye la autoría a Rusia, sin concretar si es el Estado ruso o los denominados *hackers* patrióticos, pero claramente como un episodio más del conflicto de Ucrania.

2.º) El ciberespacio, ese ente abstracto que aglutina tecnología, servicios y usuarios, se ha convertido en el elemento de mayor expansión social, política y económica de las últimas dos décadas. Las sociedades modernas se han vuelto tecnoadictas y nuestros bienes y servicios tecnodependientes.

En 2007 se produjo el grave incidente conocido como «caso Estonia» que supuso el primer ciberataque a gran escala contra una Nación, esta pequeña república báltica sufrió durante dos semanas el azote de lo que oficialmente fue un ataque de «*hackers* patrióticos rusos», demostrando que ni siquiera toda la capacidad de ciberrespuesta de la OTAN, la UE ni los EE. UU., resultaba adecuada ni suficiente (tras este incidente, en la Cumbre de Lisboa, la OTAN modificó drásticamente la visión y tratamiento que le concedía al ciberespacio).

En 2010 el incidente conocido como «Stuxnet» supuso el primer cibersabotaje contra una infraestructura tecnológica (en este caso el Complejo Nuclear de Natanz, que alberga entre otras instalaciones la Central Nuclear de Bushehr, de la República Islámica de Irán); lo que hizo a este ciberataque único fue el utilizar un «vector de ataque desasistido» que rastreó durante tres años el camino a su único objetivo, llegando a infectar, pero no dañar, más de 96.000 ordenadores. Sin autoría reconocida, se cree que detrás del incidente estuvo el conocido Grupo Equation, división tecnológica de la SNA estadounidense.

En 2013 se vivió una grave crisis diplomática entre los EE. UU. y la República Popular China, tras descubrirse una masiva campaña de ciberespionaje conocido como «Informe Mandiant», procedente de esta última, y que tuvo como principal objetivo secretos militares de alto valor estratégico (como el desarrollo del avión de combate F-35 y que facilitó el desarrollo de su homólogo chino, el J-21). Sin autoría reconocida, diversos estudios y análisis apuntan hacia los grupos *hackers* APT1, directamente vinculados con el Gobierno de la República Popular China.

En el año 2016 se han sucedido diversos y graves incidentes que han afectado tanto a centros de producción/transformación de energía como a las redes de distribución de EE. UU., Alemania, Ucrania, Corea del Sur e Israel. Sin autoría reconocida, diversos estudios y análisis apuntan hacia los grupos *hackers* APT27 y APT28, directamente vinculados con el Gobierno de la Federación Rusa.

Nuevamente resulta evidente que técnicas y procedimientos propias del denominado «ciberdelito», son empleadas por múltiples agentes, que nada tienen que ver con ciberdelincuentes (pues no hay lucro directo), ciberterroristas (pues no hay reivindicación), ni hacktivistas (pues no hay publicidad); forzosamente tenemos que pensar en agentes de inteligencia de Estados o de grandes corporaciones empresariales. Podríamos estar ante las nuevas formas del arte de la guerra, que difieren mucho de las tradicionales, incorporando elementos como guerra asimétrica, guerra híbrida, guerra de información, desinformación e infoxicación, etc.

TIPOS PENALES RECOGIDOS EN EL VIGENTE CÓDIGO PENAL

La cibercriminalidad, en sus múltiples modalidades ya expuestas en el epígrafe anterior, conforma cuatro de los cinco bloques temáticos de las ya mentadas ciberamenazas del siglo XXI, ciberdelito, ciberterrorismo, hacktivismo y ciberespionaje, exceptuando por ello el concepto de ciberguerra.

De entre todas las definiciones de delito informático o cibercrimen, la que goza de mayor aceptación, por el consenso alcanzado, ha sido la realizada por el Consejo de Europa a través de su Convenio de Ciberdelincuencia. Este, fue promulgado a la firma, el 23 de noviembre del 2001 en Budapest, y ratificado por España en el año 2010[26]. Posteriormente, en enero de 2003, se añadió al Convenio un Protocolo Adicional para criminalizar los actos de racismo y xenofobia cometidos a través de sistemas informáticos.

El Convenio de Budapest es, sin lugar a duda, un acuerdo nacido con vocación universal, que supuso y sigue siendo el máximo referente para la lucha contra la ciberdelinciencia, y sigue siendo el único tratado que tiene por objeto la armonización normativa del derecho penal de las naciones o Estados que lo ratifican. Nuestro país lo ratificó en el año 2010 y se unió así a los restantes Estados miembros de la UE que lo han ratificado —23 países— y a través de la Estrategia de Ciberseguridad de la UE se ha solicitado a los cinco Estados que aún no lo han ratificado que así lo hagan e

[26] https://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf.

incorporen al ordenamiento jurídico de propio —Grecia, Irlanda, Luxemburgo, Polonia y Suecia— buscando con ello la homogeneización normativa o su universalización cuando menos en el espacio común europeo. Pero no olvidemos que tiene un alcance «limitado», puesto que solo contempla delitos contra la confidencialidad y disponibilidad de los datos y sistemas informáticos, delitos de falsificación y fraude informáticos, delitos de contenidos vinculados con la pornografía infantil y finalmente infracciones a la propiedad intelectual y derechos afines.

Pero la cambiante perspectiva que nos arroja esta nueva realidad ha obligado a adaptar nuestro ordenamiento jurídico, incorporando modificaciones sustanciales y relevantes bien estableciendo nuevas modalidades o subtipos de figuras específicas ya existentes, bien introduciendo y creando nuevos tipos penales como figuras específicas y autónomas, hasta entonces inexistentes (tales como el *sexting*, *sexteo*, *stalking*, *phishing* desde el año 2010 el llamado *grooming*). La culminación de este proceso de adaptación la encontramos en la reforma del Código Penal tras la Leyes Orgánica 1/2015 y 2/2015, ambas de 30 de marzo.

Se haya gestado toda una nueva categoría de nuevos ciberdelitos**,** bautizados como «delitos informáticos»**,** que tienen como punto en común las nuevas tecnologías (como medio, objeto o bien jurídico protegido). En numerosas ocasiones, estas reformas han venido impulsadas por la normativa europea, como la Decisión Marco 2005/222 del Consejo, de 24 de febrero de 2005, relativa a ataques contra los sistemas de información, que ya fue sustituida por la Directiva Europea 2013/40/UE del Parlamento Europeo de 12 de agosto de 2013.

Aunque dispersos en el articulado del CP y sin una ordenación sistemática común y homogénea, encontramos «otros delitos informáticos», algunos de los cuales no son más que subtipos o submodalidades de delitos ya existentes (como las amenazas, injurias, calumnias) cuya comisión se produce valiéndose de las TIC; igualmente sucede con el delito de terrorismo. En definitiva, los delitos recogidos en el Convenio de Budapest son solo una fracción de los ciberdelitos recogidos en el vigente Código Penal[27]. A continuación, se detalle de los tipos penales recogidos en el vigente Código Penal:

---

[27] El magistrado Eloy Velasco explica los 16 ciberdelitos del nuevo Código Penal que se pueden cometer con la tecnología.
El magistrado de la Audiencia Nacional, Eloy Velasco, es conocido con el apodo del «ciberjuez» por sus conocimientos y asesoramiento para elaborar el articulado «ciber» del nuevo Código Penal —en vigor desde finales de 2015—. Se trata de una de las grandes pasiones de este magistrado que, entre otros, instruye la operación Púnica, entre otros muchos casos conocidos.
Viernes 27 de mayo de 2016.
El magistrado de la Audiencia Nacional Eloy Velasco ha participado en la jornada dedicada al cibercrimen de la compañía española Segure&IT —presentada por su director general, Francisco Valencia— para resumir, de forma magistral, los cambios que ya se están aplicando a los delitos informáticos y relacionados con datos en el nuevo Código Penal. Así ha explicado que hay tres tipos de delitos en este campo. En primer lugar están los del cibercriminal que roba dinero —que son el 85% de los casos».
1.-Es importante destacar el protagonismo que adquiere en el mundo «ciber» la estafa, que ha pasado del mundo físico al digital y que se materializa en todo tipo de timos incluyendo el conocido como «virus de Correos» —que secuestra tu ordenador a cambio de un pago que generalmente no sirve de nada—. Mucha gente lo conoce y no paga… pero «de cada 100 personas que los sufre siempre hay dos que pagan por lo que resulta muy rentable para los criminales».

Dentro de este tipo de delitos también está el robo de datos, tipificado en el artículo 248 del nuevo Código Penal. No se trata de la clonación o uso de tarjetas de forma fraudulenta. Aquí lo que se castiga es la suplantación de identidad, por ejemplo, para comprar en nuestro nombre. El Código Penal también castiga «la defraudación, derivada del concepto de fraude. Por ejemplo, cuando alguien te 'roba' la wifi que pagas tu. Ahora es considerado delito en cualquier forma que se cometa, porque ya no existen en el Código Penal las faltas —que se limitaban a infracciones hasta 400 euros—, pasando a ser un delito como tal».

2.-Son importantes los delitos que tienen que ver con hurto de tiempo. Consiste en utilizar un dispositivo, como un ordenador de la empresa para causar un perjuicio. Se trata de una falta importante aunque «considero que no debe ser penalmente perseguible, creo que hay que apostar por la vida laboral».

3.-«Se castiga el llamado delito de 'craking' dentro del que están los que tienen que ver con la interrupción de un servicio —los llamados ataques de denegación de servicio—. Con ello, por primera vez, se protegen, de forma penal, los ataques contra infraestructuras críticas —entre las que hay desde bancos a sistemas de gestión del tráfico—. De hecho, este tipo de ataques son considerados un agravante en el artículo 264 del Código Penal».

4.-El nuevo Código Penal incluye el delito de plagio de toda la vida —se copia un libro y se edita como si fuera de otro— al que añade los delitos de referenciación. Con este concepto se castiga a quien facilite el acceso a contenidos protegidos o cuya difusión no ha sido autorizada por ese medio. «Es algo importante porque va contra la piratería», también, cotra sistemas técnicos que vayan contra quien difunde contenidos de forma ilegal. «En este punto es muy importante tener en cuenta y leer la sentencia Svensson, de 2014, que aclaró cómo interpretar la Ley cuando alguien difunde contenidos sin permiso de su autor».

5.-La ciberdelincuencia intrusiva está en el nuevo Código Penal y es un delito importante, ya que supone el 14 % de los casos que nos llegan a la Sala. «Es el más delecnable de los delitos, ya que en él está incluida la difusión de material pornográfico de menores, añadiendo nuevas modalidades. Así, por primera vez, ver pornografía infantil por Internet es delito. Pero solo si se ve a partir de dispositivos técnicos. O sea verlo en real no está penado pero lo segundo sí. Además, se castiga la pornografía virtual que creo que es un tema sobre el que hay que hablar ya que se pena ficciones e imágenes y puede terminar castigando películas convencionales con mucha violencia o caricaturas». «El *sexting* también está penado ya que se castiga los actos que el cibercriminal hace para embaucar a menores desde los 13 años para obligarle a través de la extorsión a facilitarle imágenes pornográficas».

6.-«El acoso, en el artículo 172.3, está tipificado también cuando se realiza en modalidades a través del ciberespacio. Se trata de penar cualquier alteración normal a la vida cotidiana: obligándote a dejar de ir a los sitios a los que ibas, a cambiar de móvil… un delito que no es de coacción ni amenaza pero que ya ha sido incluido. Además, del acoso de violencia de género esto permite perseguir el acoso vecinal o el acoso que sufren personas por el fenómeno fan. Esto está tipificado ya».

7.-Por primera vez, se tipifica no cambiar las pilas a dispositivos como las pulseras antiviolencia de género, ya que ello impide su funcionamiento «y se castiga cualquier acción que la inutilice o perturbe su funcionamiento».

8.-Continúa en el Código Penal «el delito de descubrimiento y revelación de secretos —concepto que internacionalmente se llama *hacking*. Creo que es un hito. Por fin se ha cambiado la interpretación del Tribunal Supremo sobre este tema. Creo que el pecado no es enterarte del secreto del otro sino inmiscuirte en el «sacrosanto sitio» donde tenemos los secretos, el móvil. Así que igual que entrar en una casa es un delito entrar en un dispositivo tecnológico es también un delito. Con ello se protege la vida privada —en el artículo 197— y se castiga el mero allanamiento en el dispositivo. Si además robas información el delito también es de robo de información».

9.-«Como curiosidad, también se tipifica —en el artículo 197 bis— el robo de información privada en los diálogos entre máquinas y la difusión de contenidos privados sin consentimiento —por ejemplo, si alguien a quien hemos enviado un vídeo de contenido íntimo lo difunde sin nuestro permiso, como pasó en el 'caso Hormigos'—».

10.-«Las calumnias e injurias por Internet tienen una importancia nueva en el Código Penal aunque continúa planteando una pregunta: ¿cuándo es delito y cuándo no? Hay jueces que piensan que te llamen puta no pasa nada pero creo que es importante clarificarlo y ahora el Código Penal, que ha eliminado la falta de 'injurias y calumnias' sí explica en su artículo 215 será delito cuando la expresión sea considerada en el concepto público por grave, con lo que se deja esta pena a criterio del juez».

11.-«Se pena cualquier atentado contra el orden público a través de medios tecnológicos, así como la incitación al odio y la violencia contra quien es diferente también es importante y se ha tipificado como delito».

12.-Por último, se contempla el ciberterrorismo, aunque es un tema muy extenso que no está considerado cibercriminalidad por lo que daría pie a otro foro.

13.-Más control sobre los delitos tecnológicos. «Tras casi un año desde que se aprobara el nuevo Código Penal —que entró en vigor en diciembre—, es importante destacar que frente al desasosiego que produce en los programadores destaca por proponer una medida importante: adelanta la barrera de protección de los datos. O dicho de otra forma si se hace alguna acción de tentativa se castiga. Esto es un punto polémico, aunque ya existía antes castigando a alguien que tenía *software*, que se puede usar para estafar. Pero ahora la reforma del Código Penal castiga las tentativas como consumación —aunque con menor pena—. Y se añade en el 197

1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.

   – Del descubrimiento y revelación de secretos (arts. 197, 197bis, 197ter, 197 quater, 197 quinquies, 198, 199, 200 y 201).
   – De los delitos relativos al mercado y a los consumidores (descubrimiento de secreto de empresa) (arts. y 279).
   – De sabotaje informatico (art. 263).
   – De los daños (art. 264).
   – De las defraudaciones de fluido (arts. 255 y 256).

2. Delitos informáticos.

   – De los delitos relativos a las falsedades documentales (arts. 390, 392, 395 y 400).
   – De las estafas (fraude informático) (arts. 248 y 249).

3. Delitos relacionados con el contenido.

   – De los delitos relativos a la prostitución y la corrupción de menores (arts. 187 y 189).
   – De los abusos sexuales (art. 181).
   – De los delitos de exhibicionismo y provocación sexual (art. 186).
   – Induccion a la prostitucion de menores (art. 187).
   – Produccion, venta, distribucion, exhibicion o posesión de material pornográfico en cuya elaboración hayan intervenido o sido utilizados menores de edad o incapaces (art. 189).

---

al *hacking* y al *cracking*, así que se pena el que adquiera contraseñas o código de acceso a sistemas ajenos y al que compre *software* para dañar o para acceder de forma ilegal a un dispositivo.

14.-Por primera vez en la historia se contemplan medidas restrictivas a través del Código Penal. Está claro que hay que castigar al «malo» pero, a mí, más que castigar me gusta prevenir. Por ejemplo, si alguien utiliza un *software* en la Red para hacer un *phising* —suplantación de una web para obtener datos ajenos— es mejor actuar, retirar ese programa y detenerle al momento. Muchos consideran que si quitas el «reclamo» no podrás detener al estafador que lo ha creado, pero creo que es importante esta medida de retirada de contenido de Internet con la colaboración de las empresas servidoras.

15.-«Ahora también se pueden retirar enlaces por orden judicial. Así, con este Código Penal, no puede pasar lo que ha ocurrido con Apple que se ha negado a dar el acceso al FBI a un dispositivo de un terrorista. Aquí no hay sugerencias, se trabaja con una orden judicial. Con ello se puede también bloquear el acceso a los contenidos e interrupción del sistema informático que los ofrece. Unas medidas que se permite en el artículo 273 contra la propiedad intelectual, contra la pornografía infantil, contra el terrorismo yihadista —artículos 578 y 579— y también la difusión de consignas terroristas».

16.-«La transformación que está motivando el Código Penal en el ámbito de la empresa es enorme». En el nuevo texto se considera que una compañía puede cometer 26 tipos de delitos tecnológicos entre los que están desde el de estafa hasta de daños informáticos, denegación de servicio, contra la propiedad intelectual, espionaje, falsificación de tarjetas, blanqueo de capitales, pornografía infantil, *hacking* y, por supuesto, el descubrimiento de secretos o difusión de material sobre el que no tiene permiso la empresa —o sus empleados—. Muy importante: ¿Cómo puede evitar una empresa que la inculpen por algo que han hecho sus ejecutivos o empleados? Las empresas obran a través de personas físicas. Así que lo que hace el legislador es darle calidad de persona jurídica. Es cierto que las empresas como tal no puede cometer delitos pero sí sus ejecutivos o subordinados. Unos delitos que pueden conllevar sanciones de hasta nueve millones de euros e, incluso, la disolución de la empresa por una orden judicial. Para evitarlo, la empresa tiene que demostrar que ha puesto en marcha todo tipo de planes de prevención para evitar estas conductas.

- De las amenazas (arts.169 y 171).
- De las coacciones (art.172).
- De la calumnia (arts. 205 y 206).
- De la injuria (arts. 208 y 209).
- De los delitos contra la comunidad internacional (apología del racismo y la xenofobia) (art. 607).

4. Delitos relacionados con infracciones de la propiedad intelectual y derechos afines.

   - De los delitos relativos a la propiedad intelectual (art. 270).
   - De los delitos relativos a la propiedad industrial (arts. 273 y 274).

5. Delitos de terrorismo.

   - Captacion, adoctrinamiento, formacion u otros a traves de Internet (art. 576).
   - Trafico de armas y explosivos a traves de Internet (art. 577).
   - Enaltecimiento, apología y ultraje a las víctimas (arts. 578 y 579).

6. Responsabilidad civil (arts. 109, 110 y 120).

REFLEXIÓN FINAL

Para concluir, indicar que en el seno de la Guardia Civil, la Jefatura de Información**,** también conocida por su denominación histórica de SIGC (Servicio de Información de la Guardia Civil), tiene la responsabilidad de combatir las amenazas del ciberterrorismo y hactivismo, como tipologías delincuenciales que buscan subvertir el ordenamiento constitucional y alterar gravemente la paz social, contando para ello con las unidades y despliegue adecuados. La Jefatura tiene como misión de organizar, dirigir y gestionar la obtención, recepción, tratamiento, análisis y difusión de la información de interés para el orden y la seguridad pública en el ámbito de las funciones propias de la Guardia Civil, y la utilización operativa de la información, especialmente en materia antiterrorista, en el ámbito nacional e internacional (art. 4.6.c. del Real Decreto 952/2018, de 27 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior).

El SIGC por tanto se configura como una verdadera policial judicial antiterrorista y contra el crimen organizado de carácter desestabilizador, manteniendo una serie de elementos diferenciadores frente al de unidades de policía judicial, incluso en áreas de solape como puede ser la del crimen organizado, siendo las más significativas las siguientes:

- Enfoque proactivo vs. enfoque reactivo: Mientras que las unidades de policía judicial por lo general «reaccionan» ante la comisión de uno o varios delitos para esclarecerlo, el enfoque de las unidades de información es más parecido al de un servicio de inteligencia, en el sentido de que se trata de hacer un seguimiento de un determinado fenómeno con la finalidad de obtener información y generar inteligencia que permita luchar contra el fenómeno en toda su extensión.

- El SIGC se sitúa de esta manera a medio camino entre un servicio de inteligencia y un servicio policial, formando parte de la «comunidad de inteligencia» nacional, poniendo énfasis en la prevención para la evitación, o en su caso, la desactivación anticipada, en toda su extensión, de la materialización de las amenazas que configuran las responsabilidades informativas asignadas, más que en el esclarecimiento de los delitos en que aquellas puedan materializarse.
- En general, el SIGC realiza una labor continuada y mantenida en el tiempo de forma discreta para preservar tanto la información obtenida en sí misma, como los procedimientos de obtención propiamente dichos, debido a las repercusiones y trascendencia de las responsabilidades asignadas al SIGC, que garanticen la adopción de la decisión más adecuada de la forma más oportuna, rigurosa y segura posible, o en su caso, la reevaluación correspondiente de la misma para reorientar esfuerzos y misiones informativas.

Por todo lo anteriormente expuesto, para la Jefatura de Información de la Guardia Civil, el ciberterrorismo es una amenaza emergente, de baja probabilidad, pero alto impacto.

PONENCIAS DEL ÁREA 3
Amenaza híbrida y posverdad

POSVERDAD. DE LA FABRICACIÓN DEL CONSENSO A LA PRODUCCIÓN (DELIBERADA) DE IGNORANCIA

D. EMILIO ANDREU JIMÉNEZ
Corresponsal para asuntos de defensa de los Servicios Informativos de Radio Nacional de España. Presidente de la Asociación de Periodistas de Defensa

POSVERDAD. DE LA FABRICACIÓN DEL CONSENSO A LA PRODUCCIÓN (DELIBERADA) DE IGNORANCIA

D. EMILIO ANDREU JIMÉNEZ
Corresponsal para asuntos de defensa de los Servicios Informativos de Radio Nacional de España. Presidente de la Asociación de Periodistas de Defensa

Sabemos, por Picasso, que el arte es una mentira que nos hace ver la verdad. Al menos, cuando la verdad significaba algo para nuestra construcción como seres humanos. No solo porque nos fuera a hacer libres sino porque, sobre todo, nos acercaba al principio de realidad.

Pero a punto de entrar en la tercera década del siglo XXI, y a tenor de los escrutinios con los que han salido de las urnas una pléyade de líderes en todo el mundo, ya no parece tan seguro que las sociedades en su conjunto quieran afrontar los hechos.

Unos comicios —la victoria de Trump— y dos referendos —el del Bréxit y el de los Acuerdos de Paz en Colombia— son considerados el tridente de la posverdad, de última hora. Las tres consultas tuvieron lugar en el mismo año de 2016. Por ejemplo, el NO que tumbó el pacto entre el Gobierno y las FARC, se centró en las emociones negativas. Su estrategia dejó de explicar los acuerdos para focalizarse en un mensaje simple: el de la indignación. Y, a tenor de su victoria, funcionó.

Antes de entrar en las definiciones, les propondré otros dos ejemplos de posverdad. Primero. La invasión de la península de Crimea, en febrero de 2014, por unos autoproclamados «grupos de autodefensa» ucranianos que —¡casualidad!— vestían uniformes rusos verde oliva sin emblemas ni insignias identificativas. Vestimenta que, según Putin, habrían adquirido en tiendas locales de equipamiento. «Una falsa narrativa» que, a juicio del Gobierno de Barack Obama, «Rusia había hecho circular para justificar sus acciones ilegales en Ucrania».

El segundo caso nos lleva a la reciente gran depresión. Nueve de los grandes bancos que fueron rescatados con el dinero de los contribuyentes siguieron regando con

primas millonarias a sus directivos. Un botón de muestra. El Citigroup que había recibido 45.000 millones de dólares de los fondos de rescate —tras haber perdido 18.000 en 2008—, repartió bonus por un total de 5.300 millones de dólares. 124 altos ejecutivos recibieron tres millones de dólares cada uno. Tengo para mí que los ejecutivos de marras ya vivían hace 10 años en la posverdad.

«Emociones negativas» (referéndum Colombia) y «narrativa falsa» (invasión de Crimea) configuran el alma de la posverdad. Este neologismo, aceptado por la RAE a finales de 2017, saltó a la palestra mediática cuando, como todos ustedes ya saben, fue elegida palabra del año 2016 por el Diccionario de Inglés Oxford. La razón aducida por sus editores fue que su empleo mediático y académico se había incrementado un 2.000 por ciento.

Según el Oxford English Dictionary, *post-truth* (con «t» en el prefijo separada del sustantivo truth) es un adjetivo que «califica aquellas circunstancias en la que los hechos objetivos son menos influyentes en la formación de la opinión pública que las apelaciones a las emociones y a las creencias personales».

Sin salir del Reino Unido. El diccionario de su otra famosa Universidad, la de Cambridge, define ese neologismo también como un adjetivo que determina «situaciones en las que las personas son más propensas a aceptar un argumento basado en sus propias emociones y creencias, que otro que esté basada en hechos».

A diferencia del idioma inglés, en el nuestro, la Academia de la Lengua optó por una sola palabra para la acepción de posverdad, sin «t» en el prefijo post ni guión ilativo. Tampoco es un adjetivo sino un sustantivo. Se refiere a la «distorsión deliberada de una realidad, que manipula creencias y emociones con el fin de influir en la opinión pública y en actitudes sociales. Los demagogos son maestros de la posverdad».

Frente a posverdad, en Alemania se ha optado por «post-fáctico» (*postfaktisch*). Este término, sin ser común, no es inhabitual. De hecho, en castellano, la Fundéu, acepta posfactual como alternativa a posverdad.

Pero la posverdad y la mentira ¿no son lo mismo? Es una pregunta necesaria. Porque invariablemente se vincula a otro extranjerismo, innecesario en nuestro idioma, como es el de *fake-news*. Las noticias falsas, fraudulentas, siempre han sido los bulos, las difamaciones, los libelos y otras patrañas de la familia de la mendacidad.

La comisión Hutchins, que reunió a un grupo de académicos norteamericanos, en 1947, ya advirtió de los peligros de publicar artículos «factualmente correctos, pero sustancialmente falsos», como, por ejemplo, hacer hincapié en la raza o la etnia, pero prescindiendo del contexto, ya que así «se reforzaban los estereotipos». Según su diagnóstico, ya no bastaba con reproducir los hechos sino que era «necesario informar de la verdad que encerraban los hechos». En este compromiso abunda el Código Internacional de Ética Periodística de la UNESCO, de 1983, cuando apela a una «adhesión honesta a la realidad objetiva». Pero la veracidad es irrelevante para las sociedades de posverdad.

En la revista *Política Exterior*, de marzo/abril, de 2017, el joven historiador Diego Rubio sostiene que «la verdad no se opone a la mentira, sino a otra verdades, que compiten entre ellas, consideradas de igual validez». En esa pugna de verdades, para Joaquín Muller-Thysen, antiguo director de la Fundéu, «la gran diferencia de la posverdad con respecto a la mentira radica en la disponibilidad del individuo a aceptar el engaño». Considera que esto es así «quizá porque hoy la realidad es tan compleja que nos cuesta entenderla y somos más proclives a dejarnos convencer». Sin embargo, a juicio de Rubio «no existe ninguna evidencia empírica que demuestre, como sugieren algunas élites despechadas, que al ciudadano de hoy no le importe ser engañado o que esté dispuesto a apoyar discursos basados en datos que ellos mismos consideran falsos».

Pero en tengamos en cuenta que solo el 0,7 por ciento de los habitantes de los 35 países más desarrollados, englobados en la OCDE, son capaces de entender textos que impliquen «contrastar ideas o puntos de vista, o evaluar argumentos basados en evidencias». En números absolutos, esas siete décimas serían 9 millones de personas sobre un total de 1.300 millones de individuos.

Si el Brexit ganó el referéndum fue porque los partidarios de abandonar la Unión Europea crearon una posverdad, un estado de opinión alternativo, prometiendo desviar a la sanidad pública de ese país los 350 millones de libras que supuestamente se aportaban al presupuesto de los 28 en Bruselas. El populista Farage admitió a posteriori que había mentido.

Todos los estudios coinciden en datar en 1992 el nacimiento de la posverdad como concepto. Un término creado por el dramaturgo de origen serbio Steve Tesich en una entrevista con The Nation, una veterana publicación de la izquierda norteamericana.

Al criticar los escándalos del Watergate, 20 años antes, con Nixon, y en la época en la que habla, los del Irán-Contra, llamado entonces Irangate, con Reagan, y la primera guerra del Golfo, con Bush, padre, Tesich aseguraba que era innecesario ya suprimir la verdad como habían hecho todos los dictadores, porque «se había adquirido un mecanismo espiritual que desnudaba la verdad de cualquier significado». «De modo muy fundamental, nosotros, como un pueblo libre (el norteamericano se sobreentiende) hemos decidido libremente que queremos vivir en algún mundo de posverdad».

Sustantivo o adjetivo, posverdad no hace referencia a un fenómeno temporal, posterior a una supuesta época dorada de la verdad, que habría existido con anterioridad, sino que nos conduce al estadio filosófico de cosa superada, por dejar algo de ser relevante, en nuestro caso, los hechos, la realidad que queda desplazada del núcleo incandescente del pensamiento.

Desde que Tesich pergeñó la idea de un mundo de posverdad transcurrieron 12 años hasta que su idea se fundamentó en un libro. En 2004, el sociólogo Ralph Keyes publicó *La era de la posverdad: Deshonestidad y desinformación en la vida contemporánea*. Sostiene el autor que la posverdad se refugia en un territorio, Euphemasia, donde se evita nombrar los hechos de la realidad, así para el vocablo mentira, tenemos verdad

poética, verdad paralela, verdad imaginativa, casi verdad. Podríamos añadir, cosecha del castellano, mentirijilla o mentira piadosa. Y para los escándalos económicos acuñamos la «contabilidad creativa».

Sucede que quien define las palabras tiene el garrote, según Lewis Carroll. En 1871, publicó *A través del espejo y lo que Alicia encontró allí*. ¿Un antecedente de la posverdad? Repasemos este breve colofón a un diálogo entre Alicia y Humty Dumpty, el personaje en forma de huevo que se encontraba subido a una tapia:

> Cuando yo uso una palabra —insistió Hunty Dumpty, con tono de voz más bien desdeñoso— quiere decir lo que yo quiero que diga… Ni más ni menos.
>
> – La cuestión —insistió Alicia— es si se puede hacer que las palabras signifiquen tantas cosas diferentes.
> – La cuestión —zanjó Humty Dumty— es saber quién es el que manda; eso es todo.

Y hasta hoy, eso se sabía a través de los medios de comunicación de masas. Una de sus funciones había sido —conforme a la teoría de Walter Lippman, hace casi un siglo—, la fabricación del consenso. Esta clave de bóveda de la sociedad de masas comenzó a desquebrajarse con la fragmentación de las audiencias que tuvo lugar al final de los años ochenta y principios de los noventa. Con las redes sociales, que aglutinan a unos 2.000 millones de seres humanos, esa cohesión social se ha hecho añicos. Cualquier trozo de cristal puede encerrar una verdad, si nos la creemos y la creen nuestras contrapartes.

Esto así porque caemos en una serie de sesgos cognitivos. Un exceso de confianza hace que sobreestimemos nuestros conocimientos, cuando vivimos, a mi juicio, un retorno a la agnosia medieval. Una ilusión de control nos lleva a que enfaticemos nuestra influencia en los demás. Interpretamos la información recibida como aldabonazo a nuestros estereotipos o ideas preconcebidas. Solo se buscan los *inputs* que nos ratifican. Para su anclaje existe una predisposición a dar más peso a la información obtenida en primer lugar, aunque sea falsa, que a una información nueva, verdadera, que la contradiga. Conforme al principio de autoridad, se tiende a creer las opiniones de determinadas personas, medios o redes sociales a las que se confiere una verdad absoluta, sin someterlas a un enjuiciamiento crítico. A esto coadyuva el gregarismo. Se siguen la corriente principal, la más fuerte, el *mainstream*. El calor del rebaño da una falsa seguridad.

¿Existe algún antídoto contra la posverdad? Robert Proctor, profesor de Historia de la Ciencia en la Universidad de Stanford, cree que sí. Propone la agnotología. Así tituló su libro, publicado en 2008, donde sostiene que la ignorancia se está inoculando de manera deliberada en las sociedades del siglo XXI. Agnosia que es la transliteración de la palabra dada por los griegos para la ignorancia. De esa raíz se deriva agnóstico, en castellano. Si la epistemología estudia el conocimiento filosófico, la agnotología, propuesta por Proctor, se centra en la ignorancia, entendida no solo como una ausencia de conocimiento.

La posverdad sería una manifestación epidérmica de esa agnosia, que como causa de la causa sería la causa del mal causado. Y el mal causado no es otro que la deslegitimación de todas las instituciones que entiban los estados democráticos como los gobiernos o las fuerzas armadas o la escuela o el profesorado o la universidad o la medicina o la intelectualidad o el sindicalismo. Pero no solo. También se cuestiona el conocimiento científico, y por tanto universal, siempre respetado como Faro de Alejandría.

La hierba institucional no vuelve a crecer por donde pasa desbocado el caballo del populismo. Además, si esa posverdad se afana en provocar un «efecto halo», enjuiciará a esas instituciones sobre la base de una única tacha, que ensombrecerá todas las demás cualidades positivas.

De ahí que me surja el temor a un reverdecimiento de las masas de acoso como definió Elías Canetti, Premio Nobel de Literatura 1981, a las camadas de fanáticos asilvestrados o verdugos voluntarios que camparon por la Europa de entreguerras hasta el final de la segunda contienda mundial. Sin soslayar las más cercanas guerras de los Balcanes, en los años 90, o Ruanda, con las matanzas entre hutus y tutsis.

Y no olvidemos que con las masas de acoso surgen las masas de fuga, que huyen de las primeras. Pero estas casi nunca encuentran un refugio como el Bosque de los Lectores Solitarios, donde se aprendían de memoria los libros, antes de que ardieran a 451 grados Fahrenheit. El fuego, como metáfora. Porque Ray Bradbury en su distópico libro nos alerta sobre todo lo que abrase, aun sin llamas, la sabiduría encerrada en los libros. Al respecto, Kevin Kelly, fundador de la revista *Wired* (la «Rolling Stone» de los cibernautas) afirma que ya no necesitamos a los autores porque todas las ideas del mundo que se reunían en los libros, se pueden ahora combinar en un solo libro global.

La posverdad es una herramienta de la demagogia contemporánea. Porque los hechos ya no importan. «Esto es el oeste, señor, cuando una leyenda se convierte en un hecho, escribimos la leyenda» afirma con cinismo el director de un periódico mientras rompe las notas que había tomado sobre el verdadero «hombre que mató a Liberty Valance». John Ford en las escenas finales de esta película, de 1962, nos describe, conscientemente, lo que siempre ha sido la posverdad así llamada: la ficción, el cuento o los cantares de gesta.

Hoy, el imaginario de lo político, no necesariamente veraz, se forja con una narración colectiva sobre un mismo hecho. No es nada nuevo. Es la técnica que empleó Wilkie Collins en su aclamada como primera novela de suspense de la literatura universal *La piedra lunar*, de 1868. El lector debe inferir quién robó la piedra lunar, una joya de la India, a través de las declaraciones de cada una de las personas que se encontraban en una mansión de la campiña inglesa durante la sustracción. Cada testigo ofrece una versión, su posverdad. A pesar de esa maraña de percepciones sobre la realidad, solo la inteligencia del sargento Cuff, policía encargado de la investigación, será capaz de presentar el cargo de culpabilidad.

Los escritores son quizá quienes mejor han comprendido el declive de la realidad como paradigma de la certeza. En 1921, Ryunosuke Akutagawa, escribió el cuento

breve *En un bosquecillo*, donde un comisario mayor escucha las versiones sobre el asesinato de un hombre y la violación de su esposa. Todas difieren. Y resulta imposible discernir lo que ha ocurrido en realidad. Si son cinéfilos, habrán reconocido que se trata del argumento de «Rashomon», que dirigió Akira Kurosawa en 1950.

En definitiva. Si se retuercen los hechos, la realidad confesará los que queramos (en eso consiste la posverdad).

LA ÉTICA MILITAR EN LOS CONFLICTOS DEL SIGLO XXI

D. JUAN ANTONIO MOLINER GONZÁLEZ
GD (reserva) subdirector del Instituto Universitario «General Gutiérrez Mellado»

LA ÉTICA MILITAR EN LOS CONFLICTOS DEL SIGLO XXI

D. JUAN ANTONIO MOLINER GONZÁLEZ
GD (reserva) subdirector del Instituto Universitario «General Gutiérrez Mellado»

INTRODUCCIÓN

En la Institución militar tratamos a menudo los asuntos relativos a los valores y la moral que consideramos más apropiada para el militar. Debatimos y escribimos sobre el honor, la disciplina y otros principios de larga tradición y bien asentados en lo que llamamos *ethos* militar.

En el caso de España, los profesionales de la milicia se forman en academias y centros recibiendo enseñanzas que buscan curtir y forjar el carácter, así como se estimula un comportamiento en el que ambos, carácter y conducta, se deben acomodar a nuestro código moral: las Reales Ordenanzas para las Fuerzas Armadas de 2009.

Ese conjunto de conceptos: valores, moral, comportamiento profesional, son propios de la ética militar, aplicación de la ética a la profesión concreta del militar, responsable del uso de la fuerza legal y legítima delegada por la sociedad a través del Estado.

Algunas de las cuestiones que se pueden plantear en relación con esa ética militar, entre otras, son: ¿se ha reflexionado suficiente y correctamente sobre lo que es y la importancia que tienen?, ¿se da una formación adecuada de los profesionales de la milicia para cumplir sus tareas en paz y, sobre todo, en guerra?

Las siguientes ideas que se van a tratar pretender dar respuestas a esas y otras preguntas directamente asociadas. Para ello se analizará en primer lugar el significado otorgado a diversos conceptos como la relación entre ética, moral y derecho, las nociones de guerra y paz, tan difusas en estos comienzos de siglo XXI, o la importancia del derecho internacional humanitario y su sentido para el ejercicio de la profesión de las armas.

A continuación se describirá, apoyándonos en ejemplos concretos, cómo las conductas militares no éticas, que pueden llegar a ser verdaderas atrocidades, tienen importantes consecuencias legales, éticas y estratégicas.

Finalmente se abordarán los desafíos que se plantean a la ética militar por las nuevas tecnologías y avances científicos que se incorporan, como ha ocurrido siempre, al repertorio de armamentos que se ponen a disposición del militar cuando tiene que utilizar la fuerza. Drones, las ciberoperaciones, la robótica y la inteligencia artificial (IA) se utilizan como ejemplos de casos que exigen profundizar, desde la ética militar, para que el combatiente, el soldado, siga mostrando lo que de él espera la sociedad que confía en sus capacidades militares y éticas.

GUERRA Y EXIGENCIAS HUMANITARIAS

Clausewitz, al estudiar la guerra, nos aclara la diferencia entre su naturaleza y sus características. Aquella, la naturaleza, es inmutable al ser un fenómeno social y humano, que implica el uso de la violencia letal y que está subordinado a la política. Por el contrario, sus características varían constantemente en formas, medios, procedimientos, etc.

En nuestros días esa mutación permanente de las características de los conflictos bélicos se observa en que se han difuminado los límites entre la paz y la guerra; no se declaran los conflictos, híbridos y asimétricos, incluso cuando tienen la condición de interestatales; al tiempo, el militar debe ampliar sus funciones y cometidos profesionales en operaciones de mantenimiento de la paz, que incluyen intervenciones humanitarias, tareas policiales o actuar en catástrofes y emergencias, llegando incluso a constituir unidades especializadas de las que la Unidad Militar de Emergencias (UME) de España es un magnífico ejemplo.

Por otro lado, la guerra es sometida a una creciente regulación jurídica, lo que ha creado el concepto de *lawfare* (uso de la ley como arma de guerra); surgen nuevos combatientes que tradicionalmente han sido las victimas principales, como mujeres y niños; incluso las empresas privadas hacen su aparición en escenarios bélicos generando conflictos legales y presentando problemas éticos sobre su condición y utilización como combatientes.

Respecto a las nuevas tecnologías que se incorporan a los arsenales militares se ha generado un especial interés por la inteligencia artificial, considerada como el cerebro rector que dirige y toma decisiones para el empleo de sistemas de armas letales. Estos tienen, o pueden llegar a tener, la capacidad de operar como sistemas autónomos y si esta cualidad es totalmente independiente de las personas el gravísimo problema ético presentado es que la máquina tomaría decisiones sobre vida y muerte, algo hasta ahora exclusivo del ser humano. Quizá por esto el subsecretario de Defensa USA Robert Work llegó a decir en 2017 que con las nuevas tecnologías y la IA la naturaleza de la guerra ya había cambiado.

Aunque no se comparte esa opinión, sí es una realidad que las nuevas tecnologías siempre han estado ahí y se han utilizado para hacer la guerra. Ejemplos históricos son

la ballesta, prohibida por la Iglesia católica en el siglo xi, la artillería de la que Cervantes dijo que era una invención diabólica, o los submarinos alemanes *U-Boat* que fueron objeto de reuniones internacionales para prohibir su desarrollo a comienzos del siglo xx. Hoy día es la IA liderando otras tecnologías en sistemas de armas letales.

Los avances científicos están aquí para quedarse, lo que no es óbice para considerar los problemas legales y morales que la ética militar debe afrontar y resolver. Exigencia moral para el combatiente a lo largo de todas las épocas ha sido el respeto por el principio de humanidad que, junto al desarrollo actual de los derechos humanos, nos lleva a plantearnos las exigencias éticas en el uso de la fuerza.

Se argumenta que esos derechos humanos son relativos y están «contaminados», al responder a una concepción mediada por valores occidentales. Es cierto que nacen en el marco del sistema occidental de principios que impulsa la creación de Naciones Unidas tras el fin de la Segunda Guerra Mundial, pero su vocación es indudablemente universal, para todos los pueblos y para todos los seres humanos.

Y es así porque ha habido un progreso moral de la humanidad, un desarrollo que en el ámbito jurídico ha conducido a la aceptación global de un derecho internacional humanitario que se plasma en los conceptos del *ius ad bellum*, *ius in bello* y *ius post bellum*. Un progreso que avanza en la concepción ética de la igualdad esencial de todas las personas, pues idéntica es la igualdad de todos los seres humanos en su dignidad de seres libres y racionales. Progreso, en fin, que encuentra su menos imperfecta expresión política en la democracia liberal occidental, con su primacía de la justicia y la libertad, la transparencia y la exigencia de responsabilidad social, y que no puede relativizar la ausencia de valor ético en comportamientos inaceptables desde la ética humana como la lapidación por adulterio o el cortar la mano por robar.

ÉTICA, MORAL Y DERECHO

Para profundizar en nuestro objetivo: la ética militar, es necesario tener una idea bien fundada de lo que es la ética y de las diferencias que tiene con conceptos como la moral o el derecho.

La ética es una parte de la filosofía que se ocupa de ideas tales como el bien y el mal, de lo que es correcto e incorrecto, de lo justo o injusto en relación con el desempeño del ser humano, de la valoración de sus acciones en cuanto ser libre y racional, de la adecuación de las mismas a determinados valores o virtudes. Como actividad teórica que es, la ética no establece preceptos ni reglas, aunque los códigos morales derivan de ella.

La moral, por el contrario, es algo práctico. Es la acción concreta que se produce y sobre la que se puede reflexionar éticamente dándole una calificación de apropiada o inapropiada, de si cumple un determinado deber o no, de si es conforme a una virtud. La moral suele seguir o encuadrarse en un código o conjunto de reglas y normas. Para los militares españoles, el código moral por excelencia son las Reales Ordenanzas para las Fuerzas Armadas (ROFAS).

Creo que es relevante analizar la relación entre ética y derecho desde la perspectiva del militar que se prepara, y llegado el caso, hacer la guerra. Desde tiempos inmemoriales, han existido unas costumbres y usos de la guerra (lo que no quiere decir que se hayan observado siempre y no siquiera a menudo).

Desde el imperio romano se empezaron a dictar una serie de normas y disposiciones que, ampliadas y reformuladas, se plasmaron en la Edad Media en la Teoría de la Guerra Justa, en la que tanta influencia tuvieron jurisconsultos españoles como Suárez o Vitoria. Está basada en el principio de humanidad y en la determinación de unas reglas morales para ordenar los usos de la guerra y evitar que se convierta en una barbarie inhumana y ausente de la dignidad que caracteriza al hombre como especie.

Aunque no de forma lineal y sí con avances y retrocesos, la humanidad ha avanzado éticamente y, en este sentido, podemos considerar que la ética va por delante del derecho, siendo este el que trasforma en leyes positivas y normas jurídicas, prescripciones éticas desarrolladas y consensuadas previamente en el cuerpo social. Así, se ha establecido un derecho internacional humanitario (DIH), o un derecho de los derechos humanos que han llegado a nosotros con una profunda influencia en el origen y desarrollo de conflictos y guerras.

CONCEPTO Y NATURALEZA DE LA ÉTICA MILITAR

Desde Clausewitz está comúnmente aceptado que la guerra es un acto de fuerza destinado a obligar al enemigo a hacer nuestra voluntad. En esa lucha de voluntades el medio que se emplea es la fuerza, que produce violencia, muerte de seres humanos y destrucción de bienes materiales. Por tanto, «es intrínseco al concepto mismo de guerra el que todo lo que ocurre debe originalmente derivarse del combate».

El combate militar se convierte de esta forma en el elemento crucial de la guerra, que es tanto como decir la función primigenia para la que existe la profesión de las armas y sus profesionales, los militares.

En nuestros días se habla poco de la guerra a pesar de que por un lado el empleo del término se recorta[1] y por otro se hace un abundante uso retórico del mismo (guerra contra el terrorismo, guerra contra las drogas, guerra meteorológica, etc.). Parece lógico que así sea, pues en nuestras sociedades occidentales se han producido notables avances para evitar que ocurran y sus catastróficas consecuencias.

Todo esto es lógico y puede considerarse norma en la sociedad civil, pero para el militar el combate sigue siendo, si inevitablemente se llega a la lucha militar, la función principal de las Fuerzas Armadas (FAS). A modo de ejemplo, en un seminario sobre «Liderazgo y Ética», celebrado en el Centro Superior de Estudios de la Defensa Nacional en 2014, de

[1] En la Constitución española de 1978 se utiliza el termino guerra (artículos 15, 63 y 169), pero no se hace en las Reales Ordenanzas para las Fuerzas Armadas de 2009 y en el Código Penal Militar de 2015 se recoge en el Preámbulo que la locución «tiempos de guerra» es sustituida por «conflictos bélicos».

los más de una decena de ponentes, solo uno mencionó el combate en su exposición y la mayoría optó por centrarse en el ejemplo ético dado por los militares en tiempo de paz.

Sin despreciar ni minusvalorar la fuerza de las ideas pacifistas en nuestras sociedades, los ciudadanos siguen manteniendo unas instituciones armadas, dados los diversos riesgos y amenazas que tienen que afrontar y para apoyar a la población en casos de catástrofes y emergencias (UME), así como la cooperación internacional para colaborar en llevar la paz y la seguridad a los pueblos que padecen los conflictos (operaciones de mantenimiento de la paz). Pero también, y sobre todo, los componentes de las Fuerzas Armadas deben prepararse y formarse para llevar a cabo operaciones militares con el objetivo primordial de cumplir su misión, que es la legítima defensa de la soberanía nacional y sus intereses vitales.

Asumidos estos principios, en esa tarea al militar se le exige que la lleve a cabo bajo unos elevados estándares de legalidad y, sobre todo, legitimidad. Esta es la que proporciona la ética militar al marcar los parámetros de una actuación que implica poner en riesgo la propia vida y estar capacitado para tomar vidas ajenas.

Las guerras son fenómenos humanos y sociales que enfrentan a grupos y sociedades con consecuencias siempre indeseables. Para reducir los excesos que conducen a la barbarie y avanzar, incluso en esas situaciones extremas, manteniendo los estándares de humanidad más exigentes, tenemos a la ética militar.

Se propugna una concepción de la ética militar como ética aplicada apoyada en una construcción teórica que tiene tres pilares. El primero es la ética de la virtud, de raíz aristotélica, que contribuye a formar el carácter del guerrero en los valores y principios que forman el *ethos* militar. La segunda base conceptual de la ética militar es el cumplimiento del deber, de inspiración kantiana, que se presenta en una ética deontológica que impone códigos profesionales de comportamiento. La tercera es una ética utilitarista, representada en nuestros días por Michael Walzer, que debe tener en cuenta las consecuencias de las acciones militares como un mal, eso sí, como el mal menor, pero inevitable.

Adquirir una competencia elevada en ética militar, al lado de otras capacidades tácticas, técnicas, logísticas o estratégicas, es un deber para el militar que así logrará desarrollar un juicio moral adecuado para afrontar esa suprema situación de la guerra que es el combate.

ALGUNAS CONSECUENCIAS DE LA AUSENCIA DE ÉTICA MILITAR

La situación de estrés inducida por el combate es reconocida por la psicología social como una de las más graves y difíciles de controlar. En ella inciden tres factores:

– La situación, que se caracteriza por una serie de factores que van desde el ambiente sucio y maloliente (cuando no nauseabundo), emociones excitadas y descontroladas que facilitan la oportunidad de desarrollar comportamientos sin ninguna restricción ética.

– El grupo, que altera las percepciones individuales y la capacidad de toma de decisiones, así como el desvanecimiento de la responsabilidad moral dentro del anonimato que proporciona.
– El individuo, que por muy normal que sea ve cómo la presión ambiental acaba por pervertirlo al tiempo que en él se produce una autojustificación moral de conductas inadecuadas, para lo cual se apoya en valores distorsionados, siendo muy intensa la deshumanización del enemigo.

En esas circunstancias, la comisión de atrocidades, obviamente prohibidas por el derecho internacional humanitario y la inmensa mayoría de los códigos militares, acaba produciéndose con las nefastas consecuencias para el individuo, el grupo militar, la institución y la propia nación.

Atrocidades cometidas por individuos (My Lai, Vietnam; Abu Graib, Irak) o incluso por un régimen político (Pol Pot, Camboya), son conocidas y buen ejemplo para analizar y sacar conclusiones de las consecuencias que tiene la ausencia de una ética militar adecuada a nivel individual y colectivo.

EL *ETHOS* MILITAR

Se entiende por *ethos* militar el conjunto de valores, actitudes y hábitos, muchos de ellos demostrados no solo como válidos sino como imprescindibles a lo largo de la historia para la eficacia operativa, que están arraigados en las fuerzas armadas y han mostrado su necesidad y utilidad en la función militar, a modo de predisposiciones para actuar de acuerdo con determinados valores.

Íntimamente asociado a ese concepto que abarca valores y principios está la necesidad para el militar de estar convencido de la justicia de la causa que le sumerge en el conflicto, de la causa justa que legitima el uso de la fuerza y que en el plano individual sostiene la disposición del soldado a entregar su vida; en el plano institucional sustenta a las Fuerzas Armadas para defender a la sociedad y al Estado de derecho con lealtad al poder político, y en el plano social respalda el sacrificio de la sociedad que ha delegado su soberanía en las instituciones democráticas y otorgado la responsabilidad a las FAS para usar la fuerza letal.

También relacionado con el *ethos* militar y desde una posición más controvertida está el tema de la obediencia debida y sus límites. Se ha dicho que la exclusión de la obediencia debida a la ejecución de órdenes contrarias a la ética militar forma parte intangible de los valores militares (GD Jorge Ortega), pero ya José Almirante en el siglo XIX y en su *Diccionario militar* se refería a ella.

Asumimos que la simple legalidad de una orden no la convierte en moral y en cualquier caso se puede renunciar a su cumplimiento cuando, como dicen las Reales Ordenanzas, es manifiestamente ilegal (a lo que se debería añadir y patentemente inmoral), y asumiendo siempre las consecuencias de la acción u omisión.

Para concluir estas breves notas sobre el *ethos* militar parece oportuno remarcar el decisivo papel que el mando militar, como un auténtico líder, tiene en el desempeño ético de sus subordinados. Desarrollar un liderazgo ético que haga del líder militar la brújula moral de los combatientes a sus órdenes, que conozca a su grupo y a los individuos que lo forman, que impulse la lealtad a los comportamientos morales como señas de identidad grupal y que tenga la capacidad de controlar y encauzar las emociones en las terribles situaciones del combate donde el militar empeña su vida y usa la fuerza letal para cumplir su misión.

LA ÉTICA MILITAR EN ESPAÑA

Ya se ha expresado que la ética militar va más allá de los códigos morales militares, siendo estos como muestran las Reales Ordenanzas para las Fuerzas Armadas los códigos deontológicos esenciales para guiar el desempeño de los profesionales en paz y en guerra.

Sin embargo, debe aclararse que las ROFAS aprobadas en 2009, con sus hermosos antecedentes de 1768 y 1978, constituyen el cuerpo doctrinal en que se sustenta la ética militar en España, pero no son los únicos documentos que forman sus referencias morales.

Dentro del conjunto de normativas internas, sin hacer una ordenación jerárquica desde la perspectiva ética o legal, se pueden describir cronológicamente aquellas disposiciones que forman parte de la ética militar profesional y aplicada de los componentes de las FAS. Así, nos encontramos con la Constitución española de 1978, la Ley Orgánica de la Defensa Nacional de 2005, la Ley de la Carrera Militar de 2007 y la Ley de Derechos y Deberes de los miembros de las FAS de 2011, además de las leyes orgánicas relativas al Régimen Disciplinario (2014) y al Código Penal Militar (2015).

En el plano internacional, la Carta de Naciones Unidas de 1945 y la Declaración Universal de Derechos Humanos de 1948, además de todos los protocolos, tratados y convenios que constituyen el derecho internacional humanitario y que como todos los tratados internacionales suscritos por España forman parte de nuestro ordenamiento jurídico.

Ahora bien, las vigentes ROFAS tienen un papel instrumental como código deontológico y compendio de los principios éticos y reglas de comportamiento del militar español, además de ser una síntesis del espíritu militar y la forma de entender y operar los mandos de las FAS españolas. Aunque se han oído algunas críticas sobre la limitación dada al combate en las mismas, las ROFAS tienen un capítulo titulado «De la ética en las operaciones» en donde se sintetizan las reglas, usos y costumbres de la guerra que forman parte de la tradición española.

DESAFÍOS ÉTICOS DE LAS NUEVAS TECNOLOGÍAS EN SU UTILIZACIÓN MILITAR

Pasamos ahora a un campo en el que también la ética militar debe entrar de lleno y no puede permanecer indiferente, por lo que los militares deben abordar desde esa moral

profesional los desafíos, riesgos y problemas éticos que presentan el uso de máquinas, tecnologías y desarrollos científicos generando nuevos sistemas de armas para llevar a cabo su esencial función de utilización de la fuerza.

También la teoría de la guerra justa, ya mencionada, debe iluminar esos desafíos y a ellos, desde el principio, deben ajustarse los nuevos avances en el desarrollo y el uso de la fuerza militar. De igual forma que deben regirse por una serie de principios éticos que se recogen a continuación.

El principio de humanidad. Es la dignidad esencial del ser humano y su integridad moral, que nos iguala a todos los habitantes de este planeta y que se apoya en la antropología para justificar su aplicación a todas las sociedades y no solo a Occidente. Confiere primacía a la ética para analizar, interpretar y valorar la conducta que es justa y la que no.

El principio de prevención, que exige a los científicos que desarrollan las nuevas tecnologías que desde el principio de sus investigaciones tengan en cuenta las consideraciones éticas para prevenir efectos indeseados. De hecho, se han generado importantes movimientos académicos y de organismos no gubernamentales en demanda de controles y prohibiciones que eviten el uso y la integración de la IA en sistemas de armas, así como la necesidad de crear normativas sancionadas internacionalmente que prevengan una carrera de armamentos sobre la base de la IA.

El principio de reducción del riesgo innecesario a los combatientes propios. Todo comandante de una fuerza militar empeñada en combate tiene como exigencia ética el esfuerzo por reducir el riesgo y la posibilidad de bajas a que va a someter a sus subordinados en la guerra.

Este principio apoya a determinadas tendencias que lo utilizan para justificar la utilización de máquinas en combate, pues cometen menos errores y son, en principio, más fiables incluso para evitar bajas colaterales. En la misma línea, el alejamiento del combatiente del campo de batalla (pilotos de drones en salas de control ubicadas a miles de kilómetros de distancia) contribuye a reducir ese riesgo del soldado.

El problema que esto plantea es que al considerar que serán menos las bajas propias, aquellos que tienen la obligación y la capacidad de decidir sobre el uso de la fuerza, puedan reducir su contención dando lugar a una proliferación de conflictos, pues el recibir militares fallecidos supone un coste político y social que actúa como restricción en el recurso a la fuerza para resolver los problemas que se dan en las relaciones internacionales.

Se desarrollan a continuación otros principios que son esenciales para el DIH, mencionando en primer lugar al principio de proporcionalidad, que exige utilizar y responder con medios, entre los que se deben incluir los nuevos desarrollos tecnológicos, ajustados a los objetivos a conseguir y en especial teniendo en cuenta las víctimas que se pueden causar. En torno a este principio se desarrolla habitualmente la discusión sobre el arma nuclear.

Otro es el principio de necesidad en el uso e intensidad de la fuerza militar para lograr los objetivos militares y que debe tener especialmente en cuenta las consideraciones de legítima defensa y las consecuencias de los daños previsibles.

Finalmente mencionamos el principio de discriminación tan necesario para diferenciar entre combatientes y no combatientes. Importante en este sentido y desde la perspectiva de las nuevas tecnologías y la IA es considerar que los nuevos sistemas de armas apoyados en la misma pueden tener mayor y mejor discriminación que la que pueden ofrecer los sistemas operados por humanos.

Como reflexión final de estos desafíos éticos que presentan las nuevas tecnologías y conocedores de las complejas órdenes a dar en el combate, hay que resaltar que en la guerra se toman decisiones sobre la vida y la muerte y en ellas los seres humanos implican también a su conciencia, emociones y sentido común, algo imprescindible para generar comportamientos éticos y hoy por hoy ajenos a las capacidades a desarrollar por los sistemas de armas impulsados por la IA.

La responsabilidad en el uso de la fuerza letal no se puede dejar a las maquinas ni a su IA y es el ser humano quien debe asumirla en toda su plenitud.

ALGUNAS CONSIDERACIONES SOBRE DRONES

Los drones, denominados de diversas maneras: vehículos o sistemas no pilotados, vehículos o sistemas pilotados remotamente (creemos la más precisa), etc., son una muestra de las nuevas tecnologías que más se ha desarrollado y que presenta un impresionante inventario de productos que ya están facilitando a la sociedad tareas en múltiples campos, civiles y militares, y en el que trabajan y se empeñan miles de empleos que generan un enorme volumen económico.

Vamos a considerar algunos aspectos de su utilización en el ámbito militar desde el análisis de determinados principios mencionados en el apartado anterior.

A partir de la exigencia de reducción del riesgo a las fuerzas propias, con el uso de los drones, en ocasiones a miles de kilómetros de distancia, es claro que se produce una discriminación notable del riesgo del piloto que los dirige, con menos estrés, cansancio o miedo, o sea que hay una merma del coraje, del valor en la asunción del peligro para defender a un compañero. Por otro lado, hay factores militares que apoyan la utilización de drones como la mayor fiabilidad de sus sensores, o la mayor precisión en sus ataques.

Podríamos resumir que la operación militar es más cómoda, fácil y barata. La consideración ética que se desprende es que estas ventajas podrían llevar a una menor restricción en el uso de la fuerza, a una mayor «ligereza» en afrontar crisis y conflictos, como nos han mostrado los incidentes en el estrecho de Ormuz en el verano de 2019 entre Estados Unidos e Irán. Los drones abatidos, supuestamente uno de cada país, ¿lo hubieran sido si se tratara de aviones pilotados por humanos?

Además, al aumentar la distancia física entre pilotos y dron se produce un despegue emocional, la llamada mentalidad *play station* con la que se ha criticado a los pilotos de drones, con calificaciones incluso de «guerra de cobardes». Sin embargo, se ha argumentado en sentido contrario, que los pilotos de drones mantienen un alto nivel ético a la hora de tomar decisiones, y consideran cuidadosamente la distinción combatiente-no combatiente, analizando con rigor extremo los posibles daños colaterales y llegando a tener un conocimiento detallado de sus objetivos y todas las circunstancias legales y éticas a tener en cuenta.

En este contexto, en el que entran en consideración los aspectos relacionados con el principio de discriminación, es importante reseñar el «tiempo de latencia», ese que trascurre desde el momento en que se pulsa el botón de la intervención hasta que se impacta en el objetivo por la posibilidad de que en ese intervalo se introduzcan personas que podrían ser civiles no implicados.

En resumen, debemos considerar que con la utilización de drones en los conflictos sí existe el riesgo de una deshumanización en el combate, al poderse producir una liberación consciente o inconsciente de la responsabilidad de matar. Más cuando ganar las guerras en el siglo XXI demanda una paz duradera y estable, algo que se ha asociado reiteradamente a la necesidad de ganar no solo sobre el terreno militar, sino en esa nueva dimensión cognitiva que supone el ganar las mentes y los corazones.

CIBERDEFENSA Y CIBERATAQUE

A los tradicionales dominios terrestre, marítimo y aéreo se les han unido los dominios espacial, cibernético, cognitivo y de la información. Es sobre el cibernético en el que se centran las siguientes reflexiones desde la ética militar.

El *ius ad bellum* exige una serie de condiciones legales y legítimas para el uso de la fuerza militar. Desde esta exigencia nos podemos plantear si los ciberataques e intrusiones que cada jornada se llevan a cabo, algunas de ellas sobre los dispositivos de defensa y seguridad, que intentan afectar y modificar disruptivamente nuestras infraestructuras críticas, o tratan de conocer datos de sistemas, industrias, entidades económicas y financieras, o alterar el funcionamiento de instituciones básicas de los Estados, están violando nuestra soberanía o afectando a nuestros intereses vitales y constituyendo una injerencia intolerable, todos ellos motivo de *causus belli* que legitiman una respuesta armada.

El primer aspecto que analizamos es el problema de la atribución. Esta, aunque posible, es difícil de determinar dado el anonimato que permiten las redes, la interposición de sistemas y servidores ubicados en terceros países en los ataques cibernéticos e incluso la negación del Estado desde cuyo territorio se tiene constancia que partieron las agresiones, argumentando que desconocían las mismas y fueron realizadas por particulares. A esto se debe añadir el efecto diferido en el tiempo, pues desde el inicio de la agresión cibernética pueden pasar días, semanas o meses, como ocurre por ejemplo con las bombas lógicas.

En nuestra época la dificultad de distinguir entre la situación de guerra y la de paz, esa zona gris, encuentra en los ataques llevados a cabo en el dominio cibernético un campo abonado. Recuérdese a este respecto que la OTAN en su concepto estratégico considera a las amenazas cibernéticas causa de invocación del artículo 5 de la defensa colectiva.

Con los «algoritmos de guerra», con la IA sirviendo a los ciberataques y diseñando sus propios códigos se pierde la posibilidad de rastrear y controlar el origen del ataque cibernético.

La cuestión siguiente se refiere al cómo respondemos, al *ius in bello* del uso de la fuerza. La respuesta ante un ciberataque exige al Estado que la ha sufrido tener presente una serie de condiciones legales y éticas. Así, desde los principios de necesidad, discriminación y proporcionalidad hay que evaluar los posibles efectos colaterales de las respuestas cibernéticas, con los resultados que se pueden causar en objetivos civiles, lo que por otro lado nos recuerda las *fake news* y la intromisión e interferencia grave incluso en el sistema electoral y el devenir político de un país.

Otro aspecto a considerar es el empleo de civiles para el ciberataque o la ciberdefensa y las dudas que se plantean sobre su consideración de combatientes y posibles objetivos militares.

Concluimos esta parte reconociendo que la cibernética también está sometida al derecho internacional humanitario y a la ética militar, que exigen la necesidad de convicción y justificación legal concluyente de la causa justa y la atribución de responsabilidad para responder a un ataque que puede provenir de un individuo o un grupo, civil o estatal, y cuya gravedad puede afectar seriamente a un Estado que trata de defenderse del mismo.

Sin duda, los conflictos cibernéticos son unos de los que ponen en cuestión a Clausewitz en su consideración de la inmutabilidad de la naturaleza de la guerra.

INTELIGENCIA ARTIFICIAL, ROBOTS Y SISTEMAS AUTÓNOMOS

Cuando hablamos de inteligencia artificial y su aplicación al ámbito militar como un extraordinario desarrollo científico, nos estamos refiriendo en realidad a un conjunto de tecnologías que se complementan y estructuran de forma práctica. Van desde la biogenética a las telecomunicaciones, pasando por la cibernética y la robótica y todas ellas, al final, dirigidas por la inteligencia artificial.

Esta, la IA, es la clave de bóveda de un futuro que ya está aquí, pues como recoge la Estrategia sobre Sistemas Robóticos y Autónomos del Ejército de EE. UU., publicada en 2017, contempla la integración de los mismos en unidades militares.

Estos sistemas, al ser considerados desde la ética militar, presentan ventajas e inconvenientes que pasamos a analizar. Entre las primeras hay que mencionar que con la

utilización de robots en misiones de alto riesgo (desactivadores de explosivos) se evitan y reducen las pérdidas humanas; su coste es mucho más reducido y la precisión mucho mayor; al carecer de emociones como el miedo o del instinto de supervivencia sus acciones son más estables cometiendo menso errores y alcanzando más eficacia.

Respecto a los inconvenientes hay que reseñar la enorme dificultad o imposibilidad de dotarles de códigos éticos, dado que la ética es por y para humanos, los cuales son los únicos a los que se les puede y debe exigir responsabilidad legal y ética por sus acciones, algo que no tienen los robots, aunque ya se han alzado voces demandando que se les dote de una identidad legal y jurídica.

El problema que subyace está referido a la autonomía de la máquina y la dificultad de determinar ante sus acciones quién es el responsable, o imputable, o incriminable por las decisiones que pudieran tomar en el campo de batalla. Y sobre todo se plantea la cuestión profundamente ética: ¿se puede dar a una máquina autonomía para decidir la utilización de la fuerza letal, para tomar decisiones sobre la vida o la muerte?

Nos estamos refiriendo, principalmente, a los sistemas de armas autónomos letales (SALAS en español y LAWS en inglés), para cuyo control se han constituido desde hace varios años y dentro de la «Convención sobre las Prohibiciones o Restricciones en el Uso de Ciertas Armas Convencionales» de Naciones Unidas, un grupo de expertos gubernamentales sobre tecnologías emergentes en el área de los SALAS. A sus trabajos asisten no solo los representantes gubernamentales, sino también organismos civiles no gubernamentales que tienen la oportunidad de expresar sus ideas y preocupaciones, algunas de las cuales son defendidas ante los que se ha dado en llamar «robots asesinos».

Sobre el trascendental problema de la autonomía de las máquinas ya ha habido pronunciamientos como el del Comité Internacional de la Cruz Roja que exige, como imperativa, la existencia de un control humano significativo y la necesidad de que ese requisito sea planteado y resuelto en una norma legal de carácter internacional, empezando por lograr una mayor precisión y consenso en los conceptos de «autonomía», «autonomía de las armas» y «armas autónomas».

El dejar plena autonomía a la máquina podría llevarnos a esa situación que corrientes como el «Transhumanismo» ofrece cuando postula que se avanza hacia una fusión entre la IA y la humana que abre el campo a la creación de organismos mixtos (¿militares?) conformados por humanos y robots gracias a la biotecnología, nanogenética y otras disciplinas similares.

Sin embargo, es necesario dejar constancia de que existen científicos que defienden la posibilidad de una «ética robótica» que conduciría a que las máquinas pudiesen llegar a ser tan éticas, incluso más que los humanos, en el uso de la fuerza letal.

Esa ética robótica es necesaria, dicen sus defensores, dadas las importantes implicaciones éticas de la tecnología robótica en la sociedad así como la urgencia de dar respuestas a los retos para establecer una guía ética de colaboración entre la máquina y el ser humano. El objetivo final sería crear la capacidad de que las máquinas dispusie-

ran de pautas y capacidad ética para que tomen decisiones de forma completamente autónoma.

Desde la ética militar se exige partir del principio de prevención, que exige a los científicos empeñados en el desarrollo de sistemas autónomos para ser utilizados en las guerras que desde el inicio de sus diseños tengan en cuenta y adopten medidas (en sus algoritmos) que prevengan los efectos perniciosos que pueden producir los sistemas, particularmente cuando las decisiones impliquen la posibilidad de causar heridos o bajas humanas en combate.

Que esta cuestión parece que se toma en serio lo ejemplifica la noticia conocida hace unos días a través del diario *The Guardian,* por la que los responsables del Pentágono están buscando expertos en ética para el desarrollo conjunto, desde el inicio, de los sistemas de armas apoyados en la IA.

Para finalizar con estas consideraciones de la ética militar sobre la IA, reseñemos el grave asunto de la responsabilidad a asignar a los SALAS que pudieran ser utilizados militarmente. La exigencia ética (y legal) de la proporcionalidad de un ataque a ejecutar con un sistema de armas autónomo, por ejemplo con drones dirigidos por la IA, implica una serie de requisitos que debe cumplir respecto a la selección y ataque a objetivos. Así, se diferencia entre:

- Sistemas militares *human in the loop*: sistemas semiautónomos en los que el hombre decide qué objetivos se van a seleccionar y atacar y el sistema ejecuta la acción con completa autonomía. Las municiones guiadas o los misiles *fire and forget* podrían encajar en esta categoría.
- Sistemas militares *human on the loop*: sistemas en los que el hombre no decide los objetivos a seleccionar y enfrentar, tarea que lleva a cabo el sistema de forma independiente, pero aquel puede intervenir en la máquina y modificar su funcionamiento o pararla completamente en cualquier momento que observe un fallo o malfunción. Son también semiautónomos. Los sistemas Aegis y Patriot, entre otros, pertenecerían a esta categoría.
- Sistemas militares *human out of the loop*: sistemas capaces de operar sin intervención de un operador. El hombre no decide los objetivos a seleccionar y enfrentar y el sistema lleva a cabo con plena autonomía esas funciones sin que aquel pueda intervenir en ningún momento, aunque lo considere necesario. La gran mayoría de estos sistemas se emplean en misiones defensivas y la *loitering munition* («munición merodeante») como el sistema israelí Harpy 2 sería un ejemplo.

Es claro que en todos los casos anteriores hay un control humano inicial en el diseño y programación. Con la IA aplicada a los drones, al problema del error o mal funcionamiento se le añade el de la autoprogramación que el sistema autónomo pueda llevar a cabo gracias al aprendizaje automático, escapando aún más al control y la necesidad de responsabilidad humana.

En la ya mencionada Estrategia de Sistemas Robóticos y Autónomos del Ejército de Tierra americano se plantea que «El Ejército pretende mantener el control huma-

no sobre todos los sistemas autónomos. Se conseguirá este objetivo manteniendo a los humanos *in the loop* u *on the loop* de los actuales y futuros sistemas robóticos y autónomos».

CONCLUSIONES

Las guerras del siglo XXI no han sido convencionales como las vividas en el siglo anterior. Afganistán e Irak nos muestran cómo son mucho más difíciles de ganar en el campo político. La percepción social de la terrible capacidad destructora de las armas, el papel que ejercen los medios de comunicación, el desarrollo de las redes sociales y otros factores, han producido una mayor concienciación y sensibilización de las sociedades occidentales ante la violencia y la crueldad de la guerra.

Por otro lado, las amenazas se han hecho globales, lo que impulsa la cooperación internacional, y la victoria militar se ha demostrado insuficiente para lograr una paz estable y duradera, lo que impulsa los esfuerzos en ganar las mentes y los corazones de las poblaciones más que el dominio del territorio que habitan.

La naturaleza inmutable de la guerra, de la que nos hablaba Clausewitz, continúa teniendo plena vigencia y en el combate bélico se produce destrucción y muerte. Esta circunstancia es lo que hace de la guerra un fenómeno humano terrible que exige al militar, que ha hecho de la preparación para la misma su profesión, desarrollar unas profundas convicciones que ajusten su conducta a unos elevados estándares éticos y morales.

A pesar de lo terrible de la guerra, para no caer en la barbarie, el uso de la fuerza debe responder a criterios de legalidad y, además y sobre todo, de legitimidad. Si la legalidad encuentra su fundamento en la causa justa —*ius ad bellum*— y en el derecho internacional humanitario —*ius in bello*—, es la necesidad de iniciar y mantener la legitimidad moral del uso de la fuerza donde adquiere plena justificación la ética militar como el marco teórico y cuerpo doctrinal no solo de interés, sino de auténtica necesidad para el profesional de la milicia.

Incluso avanzan las consideraciones legales y éticas en relación con las condiciones auténticamente justas que se deben mantener cuando cesa el conflicto y llega la paz. Es el *ius post bellum* que se ha desarrollado en sus criterios y planteamientos en las últimas décadas.

La restricción y contención que impone la ética siguen siendo principios exigidos por las sociedades auténticamente democráticas ante los conflictos bélicos. En estos comienzos del siglo XXI cambian y se introducen nuevas, y a veces profundamente disruptivas, características en las guerras y por ello es más exigible la formación y capacitación de los miembros de las Fuerzas Armadas en la ética militar.

También la ética militar debe afrontar los cambios que se introducen en estrategias, tácticas, procedimientos y medios con las nuevas tecnologías y en las que la inteligencia artificial desempeña un papel de auténtico liderazgo y control. Los nuevos sistemas de

armas que se desarrollan gracias a la ciencia y la tecnología desempeñarán un papel fundamental en los conflictos del presente siglo.

La ética militar, con sus exigencias y restricciones morales debe seguir desempeñando en relevante papel y por ello es muy necesaria la formación en la misma de los militares, depositarios legales y legítimos del uso de la fuerza en nuestras sociedades democráticas.

Es imprescindible que el ser humano mantenga un «control humano significativo» sobre los nuevos sistemas de armas, que le siga otorgando esa imprescindible capacidad de ser el último responsable de las decisiones que implican el uso de la violencia letal. Solo así la guerra seguirá siendo un fenómeno social y humano que forma parte de la naturaleza inmutable del conflicto.

Si no fuera de ese modo, la guerra podría convertirse en un asunto a resolver y decidir por las máquinas. Entonces sí que podríamos decir que ha cambiado la naturaleza de la guerra y se ha transformado en algo efectivamente inhumano.

CÓMO AFRONTAN LOS MEDIOS DE COMUNICACIÓN LAS FAKE NEWS

D. MANUEL CAMPO VIDAL
Periodista y doctor en Sociología.
Presidente de Next Educación

CÓMO AFRONTAN LOS MEDIOS DE COMUNICACIÓN LAS FAKE NEWS

D. MANUEL CAMPO VIDAL
Periodista y doctor en Sociología. Presidente de Next Educación

Vamos a hablar de un asunto muy importante: el desafío de la desinformación. En cuestiones semánticas, algunos consideran llamarles «noticias falsas» y no desinformación. Es como España vacía o España vaciada. Ya sabemos de qué hablamos, los problemas que tenemos ahí.

Estamos acostumbrados los periodistas más veteranos a ver que hemos aprendido a trabajar con medios convecionales: (prensa, radio y televisión), pero la revolución tecnológica nos ha traído otros medios y debemos convivir con ellos.

Cuando llegó la radio, se dijo que estaba muerta la prensa. Cuando llegó la televisión se dijo que estaba muerta la prensa y la radio. Cuando han llegado las redes sociales, siguen vivos todos los medios, no solo los convencionales sino también las redes sociales.

Desde una paronámica histórica, Kennedy es a la televisión lo mismo que fue antes el presidente Roosevelt en los años 30 respecto a la radio y lo que sería a partir de 2008 Obama con relación a las redes sociales.

Los emisores y los receptores son los mismos en todos estos medios. Pero, hay un grifo más para repartir el caudal y fragmentar audiencia de radio y televisión y los medios que nacen en la red. El problema es cuando, en relación con los medios convencionales, en las redes sociales se incorporan elementos que adulteran el proceso y aparecen, por ejemplo, las famosas granjas de *bots* que supuestamente se ubican en San Peterburgo o quizás en Macedonia o en Venezuela, o pueden estar en Estados Unidos o en otros países.

Un ejemplo muy claro: un *tweet* muy agresivo en defensa de la independencia de Cataluña de Julián Assange; y al día siguiente había 72.000 *retuis*. Luego se probó que ha-

bían entrado en acción los robots (*bots*), que son perfiles falsos en los que se distribuye la información con alguna variable. Se sugirió que la investigación y Julián Assange había sido contratado por la Generalitat de Cataluña a través de una agencia norteamericana de relaciones públicas.

Por tanto, no solo tenemos medios convencionales y redes sociales, también tenemos la adulteración por velocidades, en este caso, o cosas peores que han sucedido en el Brexit. Todo esto nos conduce al fenómeno de la POSVERDAD y esto supera a lo de «una mentira repetida mil veces es una verdad» porque apela a sentimientos emocionales que hace que realmente se produzca la convicción de que aquello es cierto cuando no lo es.

Las características de una noticia falsa son que:

– Se difunde con voluntad deliberada de engañar.
– Tiene un objetivo claro.
– Apariencia de noticia real.

Esto es lo que les hace especialmente peligrosas porque uno cree que está ante una noticia real y no es así, además se distribuyen las noticias falsas 7 veces más rápidamente que las noticias verdaderas.

Los objetivos de las noticias falsas pueden ser:

– Económicos (clicks, visitas, desprestigio comercial).
– Ideológicos: influir en el pensamiento.
– Alterar el relato objetivo de los hechos para crear uno alternativo para:

    1. Desestabilizar, debilitar y desacreditar democracias.
    2. Sembrar dudas.

Otro tema es la diferencia entre propaganda y noticias falsas. La propaganda pretende convencer y unificar a la sociedad entorno a un ideario, mientras que las noticias falsas pretenden alterar la verdad desestabilizando.

Son cosas distintas. Una cosa es cuando se quiere hacer propaganda, dando mucha difusión de la noticia que sea y otra es cuando se alteran las bases y se modifica la verdad para producir una alteración de los estados emocionales. Y eso se produce siempre saliendo beneficiados los extremos de un lado o del otro.

Es muy difícil ser moderado, o cauto, y hay que esforzarse para serlo. Es muy difícil estar en el centro, aunque el centro no existe, no tanto desde el punto de vista de la cordura, de la sensatez y se debe intentar dar la razón al que se cree que la tiene, pero es mucho más fácil militar en un extremo o en el otro. Desgraciadamente los «instrumentos tecnológicos» que llevamos en el bolsillo están ayudando que esto se produzca así porque hay unos niveles de concentración y de segmentación de tal modo que los algoritmos te relacionan en las redes con personas que normalmente piensan como

tú. Lo mismo les sucede a los otros y hay muy poca conexión entre distintos mundos. Estamos todos relacionados con ese grupo y eso es enormemente peligroso porque rompe el concepto de comunidad y la conversación necesaria en la que está sustentada la democracia y, en última instancia, la convivencia.

Naturalmente, esto preocupa a todos: a los gobiernos, a los parlamentos, a las empresas, al ejército, a la sociedad civil, a los jóvenes, a los mayores, a los periodistas… etc.

¿Qué puede preocuparnos a los periodistas? Hay que hablar muy claro de dónde estamos, de cuál es nuestra responsabilidad, cuáles son los errores que cometemos y con un tono autocrítico tenemos que relacionar cuál es considerar, analizar el ejercicio de la responsabilidad social básica que tenemos las personas que estamos en los medios de comunicación.

Según estadísticas, las noticias falsas preocupan a 8 de cada 10 españoles (Edelman Trust Barometer 2019). El 86 % no son capaces de diferenciar entre una noticia falsa y una verdadera (I Estudio sobre el impacto de las *fakenews* en España). El 60 % dice que sí que cree saber detectarlas y el 14 % asegura poder diferenciarlas.

Por suerte, están apareciendo en el escenario del ecosistema informativo en el que vivimos, tanto en España como en otros países, algunas organizaciones que normalmente son de periodistas, investigadores… que ayudan a combatir las noticias falsas.

En España, tenemos básicamente dos: Maldito Bulo y Newtral. En Next Educación hemos llegado a un acuerdo para suministrar talleres para aprender a detectar y combatir las noticias falsas. Newtral está mucho más centrado en combatir las noticias falsas en la televisión. Si fuéramos a México encontramos una organización más o menos similar «Verificado 18». Todos combaten las noticias falsas. Estas empresas luchan contra los bulos y hacen de «policía» en la red. Por lo tanto, es muy importante que se sepa que hay organizaciones con capacidad para detectar noticias falsas.

Un ejemplo de todo esto, son unas imágenes que aparecieron en 2018 de un hombre que pegaba a un médico en un pasillo. La noticia era que un inmigrante le pega a un médico en un hospital español. Esta noticia la estudió Maldito Bulo que con una búsqueda inversa, buscando en Internet hacia atrás, aparecieron esas mismas imágenes que habían sido utilizadas unos meses antes en Francia con la noticia de un argelino que pegaba a un médico en un hospital francés. También era noticia falsa. Siguió la búsqueda hacia atrás y se llegó a la fotografía correcta. La noticia verdadera era que esa agresión se había producido por parte de un borracho contra un médico en un hospital ruso.

Otro ejemplo: en la campaña electoral brasileña en la candidatura de Bolsonaro, que ganó las elecciones, un grupo de empresarios dio un montón de dinero para tener un grupo que se dedicara todo el día a producir noticias falsas, aparentemente con visos de ser ciertas, para alterar el clima político.

En definitiva, ¿por qué se generan las noticias falsas?:

- Casi el 90 %: «para perjudicar la imagen y la reputación de personas u organizaciones».
- Más del 75 %: «porque quien las genera cree que puede sacar un beneficio personal o para el colectivo al que pertenece».

Todo esto, según Estudio de Comunicación y Servimedia: «influencia de las noticias falsas en la opinión pública».

Según este estudio, a la pregunta: ¿Difunden *fakes* los medios de comunicación? El tanto por ciento que cree «probable o muy probable» encontrar una noticia falsa en sus informaciones es:

- Prensa impresa: 30,5 %.
- Prensa *online*: más del 75 %.
- Televisión: 50,3 %.
- Radio: 38,1 %.
- Webs oficiales: 20,7 %.
- Agencias de noticias: 30,85%.

También, dentro de este estudio, a la pregunta ¿somos creadores y difusores de noticias falsas? Respondieron:

- El 4 % reconoce haberlas creado en alguna ocasión.
- La mitad de ellos la han difundido.
- 56 % dice hacerlo por razones sentimentales como «frustración» y «desconfianza».

Los ciudadanos podemos ser difusores de noticias falsas y se recomienda no enviar cualquier noticia que nos llegue antes de comprobar que es verdadera. Podemos ser difusores y se recomienda no enviarlas porque podemos ser cooperadores necesarios, según denominación del Código Penal. Hay jurisprudencia sobre el asunto y ha habido multas y se han exigido responsabilidades, concretamente en el Reino Unido a personas que han difundido una noticia falsa. Hay que tener mucho cuidado con las noticias, no solamente con las noticias falsas, sino también con lo que se escribe en las redes. A veces con eliminar los mensajes ofensivos o agresivos no exime para incurrir en falta o delito, pues no se han borrado estos mensajes y se pueden recuperar. Además, puede afectar incluso para encontrar trabajo, que en la entrevista se puede investigar al demandante de empleo cómo se comporta en las redes sociales en *Reputación.com*. De todo lo que se escribe, de todo lo que se dice en redes sociales queda rastro.

En otro orden de cosas, según una investigación sobre noticias falsas del Instituto de Tecnología de Masachusetts (MIT):

- Las noticias falsas se retuitean un 70 % más que las ciertas de media.
- Las ciertas tardan seis veces más en llegar por Twitter hasta 1.500 personas.
- Es un riesgo para el funcionamiento de las democracias.
- «Si solo fueran *bots*, necesitaríamos una solución tecnológica».

Nos referimos a un *bot* como la supuesta red de injerencia rusa. Hay varias informaciones publicadas por La Vanguardia por la cual los creadores de las noticias falsas

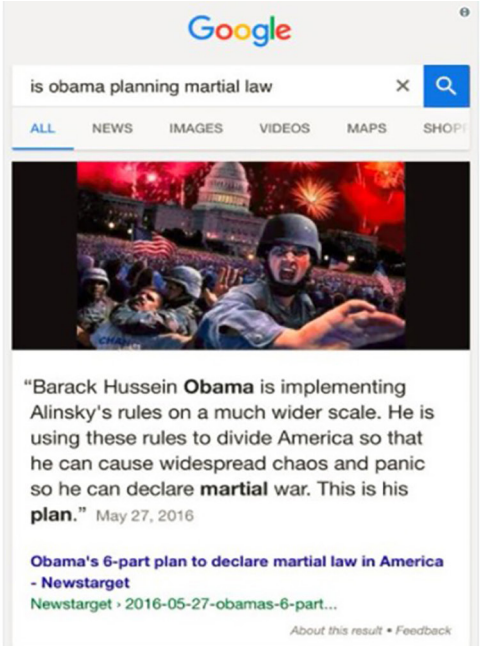
podrían ser activistas engañados, cuentas religiosas falsas, partidos suplantados… que contratan a personas como Julián Assange en el caso de Cataluña. ¿Hasta qué punto nos puede manipular un bot? Supuesta injerencia rusa: la fábrica de noticias falsas.

¿Cómo se puede contrarrestar la difusión de noticias falsas?

Según la declaración de Jens Stoltenberg, secretario general de la OTAN, en *El País* (26/01/2018):

«Debemos estar atentos a reforzar nuestra capacidad de respuesta, pero no creo que la mejor manera de responder a la propaganda sea con propaganda. Lo mejor es facilitar la verdad. Necesitamos prensa libre e independiente, periodistas que hagan preguntas incómodas». Esto es una manera de decir que es una forma de combatir la falsedad.

En Estados Unidos, en 2011 Trump personalmente lanzó una campaña para demostrar que Obama había nacido en Kenia y no en Estados Unidos. Si hubiera sido keniano no hubiera podido ser presidente de los EE. UU. porque la Constitución lo impide. Fueron 6 meses de tortura, pero con las partidas de nacimiento, el testimonio de la matrona al final quedó claro. Pero, Trump ensució la campaña con esta noticia falsa. Obama hizo público el certificado de nacimiento y por declaraciones de Trump: «Una fuente extremadamente creíble ha llamado a mi oficina y me dijo que el certificado de nacimiento de Barack Obama era un fraude». Hay que defenderse contra la desfachatez de todo este tipo de campañas, que no es la única, como ha pasado con la noticia falsa de que Obama prepara un golpe de Estado. Esto es lo que aparecía si lo buscabas en Google:



Aquí está la responsabilidad de los dueños de las plataformas: no se puede difundir cualquier cosa antes de comprobar que es una noticia falsa. En Next Educación se está trabajando en este momento, concretamente en Facebook, unas 30.000 personas limpiando cosas, como textos e imágenes relacionadas con la pederastia, textos e imágenes relacionadas con el terrorismo… pero aun así se cuelan muchísimas cosas.

Además, las redes sociales tienen datos que se van quedando de los usuarios, que se puede entrar sobre ellos. Esto es muy grave porque en el caso concreto de Cambridge Analítica autorizaron a que se pudiera dar publicidad determinada a los amigos de Facebook. Eso permitió que por esa segmentación 100 millones de norteamericanos leyeran noticias falsas como que el Papa apoyaba a Donald Trump. Pero, si además esta noticia se dirige a un determinado grupo de personas en esa comunidad se crea el fenómeno de la posverdad y se da por hecho de que esto es cierto.

Otro ejemplo, el caso del Brexit. Una situación como esta (se cuestionaba en las redes) nos coloca en el cuestionamiento de las encuestas que estamos manejando para este caso. Las encuestas del domingo anterior a la celebración del referéndum del Brexit decían que ganaban «no salimos de Europa»; las del sábado decían que sí.

Es importante cómo funcionaba la supuesta trama rusa en este caso: El FBI probó que Rusia usó 419 cuentas falsas de Twitter para interferir en la campaña del Brexit. Estas cuentas difundieron casi 3.500 *tuits* que a su vez fueron difundidas por millones de personas.

La investigación de Twitter demuestra que 13.000 *bots* interfirieron en el Brexit, pero solo un 1 % eran rusos. Estas cuentas falsas rusas publicaron 942 *tuits* que recibieron 637 «me gusta» y 461 *retuits*.

En Cataluña, pasó algo parecido y la «combinación», instrumento de la guerra de la información en Cataluña, que plantea el Real Instituto Elcano en su investigación integra:

- Ciberguerra.
- Ciberinteligencia.
- Desinformación.
- Propaganda.
- Colaboración con actores hostiles a los valores de la democracia liberal.

La trama rusa con más de 400 cuentas de Twitter falsas de Rusia en Cataluña, como la cuenta de Julián Assange que de cada 5.000 seguidores, casi el 60 % eran falsos, consiguiendo más de 2 mil *retuits* en una hora.

Esta imagen se difundió el día 1 de octubre de 2017, por Lagarder Danciu, activista con más de 24 mil seguidores en Twitter. Pero esta foto no es de ese día. La foto real es de Javier Bauluz, tomada el 12 de julio de 2012, durante una carga policial en una marcha minera.

Esta imagen corresponde en realidad al 14 de noviembre de 2012 y no al 1-O. El menor, de 13 años, resultó entonces herido y cuatro personas imputadas en una carga policial de los Mossos d´Esquadra ante El Corte Inglés de Tarragona.

Esta foto utilizada desde Valls (Tarragona) por la CUP para su campaña del referéndum del 1 de octubre, en realidad es obra del periodista Joan Socies y sirvió para ilustrar en enero de 2012 una protesta contra el entonces presidente del Govern balear, José Ramón Bauzá.

Esta imagen es de un grupo de ciudadanos forcejeando con uno de la Guardia Civil a la que se añadió digitalmente una bandera independentista. Esta foto fue compartida por Josep María Mainat, miembro de La Trinca, que tiene 74.400 seguidores en Twitter.

Esta imagen, empleada en perfiles de Twitter y Facebook, sobre todo extranjeros, como la italiana Veneto Award, fue empleada para resaltar la supuesta brutalidad policial en el referéndum. En realidad esta foto correspondía a mayo de 2011 y está alojada en el perfil de Flickr de Acampadabcnfoto. Esto es un fotomontaje.

Esto es una imagen real.

Esto también ocurrió el 1-O.

Esto es real y estas fotos pertenecen al 1 de octubre de 2017.

Ante todo esto, las redes sociales se han comprometido a luchar contra las noticias falsas.

Facebook se une a los medios para ofrecer una selección diaria de informaciones de calidad. (El País, The Washington Post, Buzz Feed, Fox News y Bild).

Se crea *Facebook Journalism Project*, proyecto contra las noticias falsas, con noticias elaboradas y editadas por periodistas y apostando por el periodismo de calidad.

Otra herramienta utilizada por esta red social contra las noticias falsas es el *Fact-checking*: colaboración con la Red Internacional de Verificación de los Hechos (IFCN) y Fact-Check-EU, impulsado por la Unión Europea.

También se ataca utilizando, y esto es muy importante, una jerarquización del contenido, entendida como cambio en el algoritmo para promocionar la información verificada.

Google también utiliza herramientas para el ataque y detección de las noticias falsas, con la colaboración con la International Fact-Checking Network para etiquetar las noticias de Google News verificadas y con el programa educativo «Be Internet Awesome» que ayuda a los niños en la toma de decisiones en línea.

También se compromete Twitter en esta lucha con la suspensión de cuentas que violen las políticas de Twitter, como *bots* y usuarios falsos, con la aplicación que los

usuarios pueden informar de las noticias sospechosas a revisar y con la suspensión de 130 cuentas falsas a principios de 2019 asociadas al independentismo.

Conclusiones: lo que se quiere plantear desde el mundo del periodismo es que todo esto es muy preocupante, lo es también para Next Educación, para los periodistas individualmente, y para los medios de comunicación. Es una oportunidad extraordinaria para reforzar la credibilidad de los periodistas que ponen su nombre asociado a una noticia, para reforzar la credibilidad de las cabeceras, marcar una diferencia frente a los que están planteando noticias falsas.

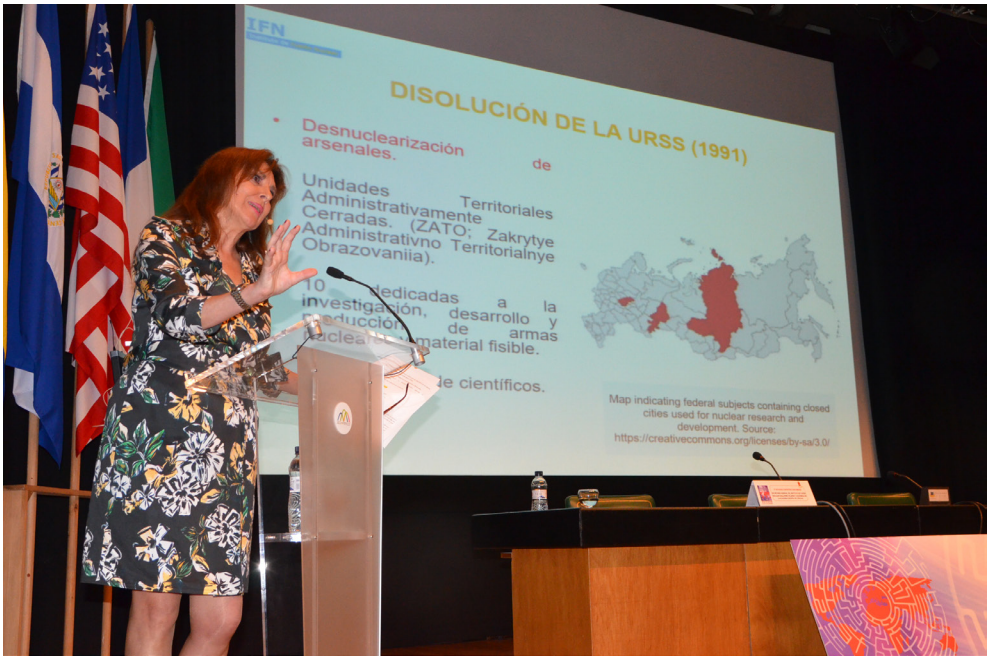
El mundo del periodismo tiene que estar necesariamente reforzando sus condiciones de credibilidad. El capital del periodista es su credibilidad. Si no se tiene credibilidad no tienes ningún valor. Así pues, el capital de una institución es que su personal es creíble. Si hay errores, pediremos disculpas a partir de ese momento.

Estamos en ese debate, en ese trabajo y me gustaría invitarles a ustedes a que cada uno en su espacio tenga y llame a la responsabilidad a la hora de dar un click, que ayude a todas esas plataformas que están haciendo ese trabajo de combatir las noticias falsas, como Maldito Bulo, Newtral… etc.

A pesar de todo esto sigue la red llena de noticias falsas. Noticias falsas ha habido siempre, pero lo que no ha habido siempre es el instrumental tecnológico que nos permite esta alteración y esta aceleración de las noticias. Y, es aquí, donde tenemos todos la responsabilidad de trabajar sobre esta cuestión.

PONENCIAS DEL ÁREA 4
Otras amenazas híbridas

RIESGOS NUCLEARES



Dª NATIVIDAD CARPINTERO SANTAMARÍA
Secretaria general del Instituto de Fusión Nuclear Guillermo Velarde y académica de la Academia Europea de Ciencias

RIESGOS NUCLEARES

Dª NATIVIDAD CARPINTERO SANTAMARÍA
Secretaria general del Instituto de Fusión Nuclear Guillermo Velarde y académica de la Academia Europea de Ciencias

«The fact that there has never been a major terrorist attack involving nuclear or radioactive material should not blind us to the severity of the threat».
Yukiya Amano – Director general del OIEA (2015)

Resumen

La seguridad física nuclear se ha convertido en una cuestión de máxima prioridad, tanto para evitar la proliferación nuclear, como para impedir que materiales radiactivos pudieran caer en manos de grupos terroristas que hasta la fecha han demostrado interés en la adquisición de agentes o materiales nucleares, radiológicos, biológicos y químicos (NRBQ), bien a través del contrabando, el robo o la fabricación propia. Los atentados del 11 de septiembre de 2001 en los Estados Unidos inauguraron un terrorismo de carácter estratégico, diferente del terrorismo táctico de épocas anteriores. Este terrorismo estratégico tiene distintos objetivos: intención de causar un alto número de muertos y heridos; causar un gran impacto psicosocial que vendría acompañado de miedo y pánico masivo y, por último, originar daños económicos de gran envergadura. Naciones Unidas y Organismo Internacional de Energía Atómica, OTAN e INTERPOL, entre otros, han desarrollado programas de prevención, respuesta y mitigación ante este tipo de amenaza, siendo prioritarios entre otros aspectos, combatir el tráfico ilícito de materiales radiactivos.

Key words: proliferación nuclear – tráfico ilícito – terrorismo radiológico.

INTRODUCCIÓN

A raíz de la explosión de la primera bomba atómica soviética el 29 de agosto de 1949 en Semipalatinsk, en las estepas de Kazajistán, los Estados Unidos y la URSS iniciaron una carrera para la producción de armas atómicas y termonucleares que alcanzaría cifras espectaculares de producción y desarrollo. Según datos publicados,

en 1967 Estados Unidos llegó a tener un arsenal de 31.233 cabezas nucleares y en 1986 la URSS alcanzó el récord histórico de 45.000 cabezas nucleares[1]. En medio de este desarrollo armamentista y de no pocas tensiones diplomáticas, en octubre de 1962 Estados Unidos descubrió que se estaban desplegando en Cuba plataformas para misiles de corto y medio alcance susceptibles de cargar cabezas nucleares. La alta tensión política derivada de este episodio, ocurrido a solo unas millas de distancia de las costas norteamericanas, hizo temer a millones de ciudadanos en los Estados Unidos, en la Unión Soviética y en el resto del mundo que una guerra nuclear sería inminente. Tras días intensos de conversaciones y alertas y de sopesar distintas estrategias, ambos gobiernos desde la Casa Blanca y el Kremlin llegaron a un pacto mediante el cual la URSS retiraría sus plataformas de lanzamiento de misiles de Cuba y los Estados Unidos retirarían sus misiles de medio alcance ubicados en Turquía, país miembro de la OTAN, y que estaban instalados a lo largo de la frontera soviética. Uno de los acuerdos fue que no se daría publicidad a este último hecho. Según información publicada por la Agencia de Seguridad Nacional de los Estados Unidos, las Fuerzas Estratégicas Soviéticas entraron en alerta en tres ocasiones en los meses de septiembre y octubre de 1962.

Durante aquellos días de octubre de 1962, la inminencia de una guerra nuclear fue tan alarmantemente real que el ataque se esperaba de un momento a otro, tanto en Washington como en Moscú. La experiencia del científico español Guillermo Velarde que vivió, hora a hora, aquellos dramáticos días resulta un testimonio muy valioso de cómo se desarrolló la situación: «Nunca olvidaré aquellos días en que me encontraba trabajando en Atomics International, en Canoga Park, cerca de Los Ángeles. Al llegar una mañana, nos dieron a todos unos folletos en los que se indicaba que la guerra nuclear era inminente y que no había tiempo para construir refugios que protegiesen a la población frente a la onda térmica y la onda de choque. Por esta razón nos dijeron que en pocas horas teníamos que adecuar una habitación para protegernos de la lluvia radiactiva. Las normas eran claras: escoger una habitación provista de sanitario, cubrir las ventanas con paneles de madera y tapar sus rendijas con masilla. También teníamos que taponar las juntas de esta habitación con la masilla y hacer un orificio en la puerta tapado con papel de filtro. Debíamos almacenar agua para 15 días y durante ese tiempo procurar alimentarnos con pastillas de proteínas, vitaminas, etc, tratando de evitar en lo posible ingerir alimentos perecederos. Debíamos tener asimismo una radio con pilas suficientes para ir recibiendo las instrucciones del Mando de Protección Civil que nos confirmaría en qué momento preciso podríamos abandonar las habitaciones y alejarnos de la zona. Me llamó especialmente la atención la reacción de gran serenidad y disciplina por parte de la gente, factores claves en aquellos momentos, sobre todo porque sabíamos que las personas que no muriesen por la onda térmica y la onda de choque, sobrevivirían si cumplían las instrucciones. Era primordial que cuando sonase la alarma se fuese cada uno de forma inmediata a las habitaciones que se habían escogido como refugio, bien en el sitio de trabajo, en los colegios, en la casa, donde fuera. Se prohibió terminantemente que los padres fueran a buscar a sus hijos al colegio o los familiares ir a reunirse unos con otros.

[1] NORRIS, R. S. and KRISTENSEN, H. M. «Global Nuclear Stockpiles, 1945-2006 . Nuclear Notebook prepared by the Natural Resources Research Council». *The Bulletin of Atomic Scientists*. July/August 2006, pp. 64-67

Desde luego, las instrucciones que nos dieron eran las más sencillas y adecuadas que se podían dar[2]».

La crisis de los misiles de Cuba demostró a las naciones que su existencia estuvo a punto de desaparecer y que, por tanto, había llegado el momento de poner un freno a la producción de armas nucleares. El 10 de octubre de 1963, teniendo en cuenta que los diversos ensayos de bombas nucleares podían alcanzar niveles preocupantes en cuanto a contaminación ambiental, se suscribió un acuerdo internacional que prohibía las pruebas nucleares en la atmósfera, bajo el agua y en el espacio exterior. Se llamó Limited Test Ban Treaty (LTBT) que se firmó el 10 de octubre de 1963 y al que se unieron inicialmente los EE. UU., la URSS y el Reino Unido. Posteriormente lo firmarían otros 110 países.

En 1 de julio de 1968 se abrió para la firma el Tratado de No Proliferación de Armas Nucleares (TNP) en Washington, Londres y Moscú y que entraría en vigor el 5 de marzo de 1970. El Tratado de No Proliferación nacía con la intención de crear obstáculos a la proliferación de armas nucleares y establecía tres tipos de países: 1) Países nucleares en 1967, que habían sido victoriosos tras la Segunda Guerra Mundial y eran miembros permanentes del Consejo de Seguridad de Naciones Unidas: Estados Unidos, la URSS, China, Francia y el Reino Unido. Estos países se comprometían a no transferir tecnología de armas nucleares a otras naciones. 2) Países no nucleares en 1967, que se comprometían a no desarrollar armas nucleares y aceptaban el sistema de salvaguardias del Organismo Internacional de Energía Atómica (OIEA) y a utilizar la tecnología nuclear exclusivamente para usos civiles. 3) Países no nucleares en 1967 que declinaron unirse y ratificar el TNP y mantuvieron su derecho de fabricar armas nucleares: España, India, Israel, Pakistán y Sudáfrica no suscribieron el Tratado. De ellos, Sudáfrica se adhirió al TNP en julio de 1990 y es, a fecha de hoy, el único país que lo ha cumplido estrictamente procediendo a un desarme unilateral. Corea del Norte anunció su retirada efectiva en enero de 2003. España firmó el TNP en 1987. Lo ratificó en 1995 y ha suscrito los Protocolos Adicionales en 1998 y 2004.

DOCTRINAS ESTRATÉGICAS

Desde los años 50 se desarrollaron una serie de doctrinas militares estratégicas basadas en los principios de disuasión y contención. En 1954, Estados Unidos adoptó la conocida como represalia masiva (Massive Retaliation) por la que este país se reservaba la opción de lanzar una represalia instantánea en caso de ser atacado, atacando por su parte lugares que considerase y con los medios que considerase. Esta doctrina se mantuvo a lo largo de la Administración Eisenhower que confiaba en el arsenal nuclear americano como la base de su defensa principal en el caso de agresión por parte de la URSS. Este último país ensayó su primera bomba termonuclear en 1955. La doctrina de la represalia masiva fue evolucionando con la puesta a punto de armas nucleares tácticas a finales de los años 50 y la evolución de las fuerzas convencionales de la OTAN. En los

[2] CARPINTERO SANTAMARÍA, N. La bomba atómica: El factor humano en la Segunda Guerra Mundial. Madrid, España: Ediciones Díaz de Santos, 2007, pp. 263-386.

años 60 se estableció la doctrina conocida como de respuesta flexible (Flexible Response) que aumentaba el poder disuasorio de la política americana y establecía que las armas nucleares solo se utilizarían si Occidente hubiera hecho frente a una derrota efectiva de fuerzas convencionales. Sin embargo, la paridad nuclear a la que se llegó paulatinamente por parte de los Estados Unidos y de la URSS llevaría a la doctrina nuclear estratégica más extrema de todas ellas: La destrucción mutua asegurada (Mutual Assured Destruction). Esta doctrina llevaba implícito el hecho de que el país que hubiese atacado primero habría tenido las mayores probabilidades de ser masivamente destruido.

A 70 años de distancia de aquella época, se puede afirmar que ni la URSS ni los Estados Unidos hubieran desencadenado primero un ataque nuclear en el que habrían tenido las mayores probabilidades de ser destruidos masivamente, por lo que puede decirse que la probabilidad de una guerra nuclear entre ambas potencias fue prácticamente nula. Otro escenario que hubiera podido darse es el de que, si como consecuencia de un grave enfrentamiento internacional, la URSS hubiera atacado nuclearmente a una nación perteneciente a la zona de influencia de los Estados Unidos, a pesar de cuantos acuerdos de defensa hubiera tenido establecidos con esta nación, los Estados Unidos no hubieran podido contraatacar nuclearmente a la URSS porque, en el mejor de los casos, se habrían destruido mutuamente. Así pues ni los Estados Unidos ni la URSS podían garantizar una cobertura nuclear sobre otra nación, independientemente de los pactos de defensa mutua que tuvieran establecidos con ella[3]. Acertadamente el teniente general Manuel Díez Alegría en su discurso de entrada como académico de número de la Real Academia de Ciencias Morales y Políticas dijo «Paradójicamente podría afirmarse que en una guerra nuclear sin restricciones entre los Estados Unidos y Rusia, el vencedor sería Australia»[4].

En noviembre de 1989, la caída del muro de Berlín se convertía en el símbolo de una situación irreversible, a través de la cual la URSS entraba en un proceso de camino sin retorno que tanto afectaría a las estructuras de la seguridad internacional. Nadie podía imaginar en aquellos momentos que tan solo dos años más tarde, el 8 de diciembre de 1991, la Unión Soviética iba a dejar de existir como entidad jurídica y como realidad geopolítica, dando paso al nacimiento de la Comunidad de Estados Independientes (CEI).

La disolución de la Unión Soviética produjo una gran alarma internacional por la preocupación suscitada ante la vulnerabilidad a la que se vieron expuestas sus instalaciones para el diseño y fabricación de armas nucleares, biológicas y químicas (NBQ), también llamadas armas de destrucción masiva (ADM). Estas instalaciones estaban insertas en un vasto complejo de ciudades, asentamientos y bases militares conocidas como unidades administrativas territorialmente cerradas (ZATO, Zakrytye Administrativno Territorialnye).

En el año 2001, la nueva Constitución de la Federación Rusa reconoció la existencia de 47 de estas ciudades cerradas, aunque posiblemente nunca se sabrá la cifra exacta de cuántas hubo y qué número de habitantes tuvieron. De las 47, diez de ellas estaban

---

[3] VELARDE, G. «Evaluación de las probabilidades de una guerra nuclear entre los Estados Unidos y la Unión Soviética. Consideraciones sobre el caso de España». Monografías de la Junta de Energía Nuclear. Madrid, España: 1977.

[4] DÍEZ ALEGRÍA, M. *Ciencia y Sociedad*. Madrid, España: Alianza Editorial, 1976.

dedicadas a la investigación, desarrollo y producción de material fisible y al montaje de las armas nucleares: Arzamas-16, Cheliabinsk-65, Cheliabinsk-70, Krasnoyarsk-26, Krasnoyarsk-45, Penza-19, Sverdlovsk-44, Sverdlosk-45, Tomsk-7 y Zlatoust-36, que se encontraban bajo la autoridad del Ministerio de Energía Atómica (MINATOM). Aunque la mayoría de las instalaciones de armas NBQ se encontraban en territorio ruso, repúblicas de la nueva Comunidad de Estados Independientes (CEI) como Kazajistán, Bielorrusia y Ucrania, tenían almacenados un alto número de armas nucleares tanto tácticas como estratégicas y misiles balísticos intercontinentales (Intercontinental Ballistic Missiles, ICBM) SS-18, SS-24 y SS-25. Tras una serie de complejas reuniones y acuerdos, finalmente se pudo llevar a cabo la desnuclearización de estas tres repúblicas que devolvieron a la Federación Rusa las armas nucleares y los ICBM desplegados en su territorio. Devolución que en algunos casos se hizo peligrosa y complicada al tener que atravesar los convoyes cargados con estas armas por territorios que, como Chechenia, presentaban grandes problemas para su seguridad durante el transporte.

Estados Unidos y la Federación Rusa firmaron y ratificaron en diciembre de 2010 y enero del 2011, el New Start Treaty que establece un máximo de:

1) 1.550 cabezas nucleares en ICBM, SLBM y bombarderos. 2) 800 ICBM, SLBM y bombarderos, operativos o no y 3) 700 ICBM, SLBM y bombarderos, todos operativos.

Solo nos cabe esperar que este tipo de armamento continúe siendo exclusivamente una fuerza de disuasión donde las lecciones aprendidas de la Guerra Fría y del final de la misma contribuyan a fortalecer la seguridad internacional.

TRÁFICO ILÍCITO DE MATERIALES RADIACTIVOS

Tras la disolución de la URSS surgieron rumores sobre posibles actos de contrabando o de venta de armas nucleares tácticas en el mercado negro procedentes de arsenales soviéticos que crearon verdadera preocupación. Uno de estos rumores se derivó de las declaraciones que en su día realizara el general Alexander Lebed, secretario del Consejo de Seguridad Nacional del presidente Boris Yeltsin. El general Lebed había sido elegido asimismo gobernador de la región siberiana de Krasnoyarsk, pero en octubre de 1996 fue depuesto creando su propio Partido Nacional Republicano. En 1997, el general Lebed, fallecido en un accidente de helicóptero en Abakan (Siberia) en 2002, hizo unas declaraciones a un periódico norteamericano en las que dijo que «más de 100 [bombas nucleares] del supuesto número de 250 no están bajo el control de las Fuerzas Armadas rusas. No sé dónde están. No sé si han sido destruidas, si han sido almacenadas o si se han vendido o robado[5]». El general Lebed, sin aportar prueba de sus declaraciones, se refería a una serie de bombas nucleares tácticas que habían sido fabricadas durante años por la URSS, transportables en maletas de reducido tamaño y que no tendrían incorporado el sistema electrónico de detonación. Por su parte, el Ministerio de Defensa de la Federación Rusa ha declarado en repetidas ocasiones que su arsenal nuclear no sufrió ninguna alteración delictiva.

[5] ALLISON, G. *Nuclear Terrorism. The Ultimate Preventable Catastrophe*. New York: Owl Books, 2005, pp. 44-45.

A principios de la década de los años 90 comenzaron a producirse una serie de delitos de contrabando de fuentes radiactivas que alcanzaron su máximo nivel entre 1994 y 1995. El uso de las fuentes radiológicas ionizantes (fuentes radiactivas) abarca diferentes áreas en los campos de la industria, medicina, biología, recursos hídricos, producción de energía, agricultura, investigación etc., lo que supone el uso de una gran cantidad de estas fuentes de manera cotidiana y en un amplio radio geográfico internacional. Unos 10 millones de envíos de material radiactivo circulan anualmente a nivel mundial, de los cuales un 95 % son pequeñas cantidades destinadas mayoritariamente para diagnóstico y tratamiento médico, agricultura, industria e investigación avanzada.

El creciente número de incidentes condujo al Organismo Internacional de Energía Atómica (OIEA) de Naciones Unidas a generar una base de datos conocida como Incident and Trafficking Database (ITDB) que incluyese los incidentes que sobre uso o adquisición ilegal, robo, posesión no autorizada, transferencia, deshecho y tráfico de materiales radiactivos fuesen comunicados oficialmente por los países miembros del OIEA. Entre otros, la ITDB tiene como objetivos orientar prioridades en cuestiones de seguridad y ser una fuente de información solvente sobre este tipo de actividades. Durante el periodo 1993-2018, se informó a la OIEA de 3.497 incidentes, de los cuales, 285 relacionados con uso malicioso[6].

Asimismo y con el objetivo de combatir esta amenaza, en 2006 se puso en marcha la Iniciativa Global para Combatir el Terrorismo Nuclear que tiene como observadores oficiales el OIEA, la UE, INTERPOL y la Oficina para Drogas y Delitos de Naciones Unidas. Entre los objetivos de esta Iniciativa se encuentran los siguientes:

1) Incrementar la seguridad en las instalaciones nucleares. 2) Mejorar los sistemas de detección de materiales radiactivos con objeto de evitar su contrabando. 3) Desarrollar técnicas de detección de estos materiales que pudieran ser utilizados en un atentado terrorista. 4) Poner en marcha medidas que eviten la financiación de grupos terroristas que intenten adquirir o utilizar armas nucleares.

TERRORISMO RADIOLÓGICO

La Estrategia Europea de Seguridad adoptada por el Consejo de la Unión Europea de 12 de diciembre de 2003 indica: «Estamos entrando actualmente en un nuevo y peligroso periodo en que surge la posibilidad de una carrera armamentística centrada en las armas de destrucción masiva, sobre todo en Oriente Próximo. […] Los atentados con sustancias químicas y radiológicas también son una posibilidad verosimil. […] La adquisición de armas de destrucción masiva por grupos terroristas constituye el escenario más temible. Si se produjera, un grupo pequeño podría causar daños de una magnitud que antes solo estaba al alcance de los Estados y los ejércitos[7]».

---

6 IAEA ITDB (Fact Sheet 2019).

7 *Estrategia Europea de Seguridad.* 2003, pp. 3-4.

Este terrorismo estratégico, caracterizado por un terror gráfico sin precedentes, tiene distintos objetivos: intención de causar un alto número de muertos y heridos; causar un gran impacto psicosocial que vendría acompañado de miedo y pánico masivo y, por último, causar daños económicos de gran envergadura.

Del mismo modo que el terrorismo químico y biológico puede ser considerado como una aplicación perversa de las ciencias químicas y biológicas, el terrorismo radiológico puede ser considerado como una aplicación perversa de la ciencia nuclear. Los dispositivos de dispersión radiológica, comúnmente llamados *bombas sucias* o radiactivas, son bombas de explosivo químico convencional que tienen adosadas un recipiente con materiales radiactivos que podrían obtenerse de fábricas de esterilización de alimentos, unidades de medicina nuclear de hospitales, laboratorios de investigación, etc. Al explosionar el explosivo convencional, la onda de choque producida dispersaría los materiales radiactivos contaminando una zona cuya extensión dependería de la cantidad de explosivo convencional utilizado, de la clase de materiales radiactivos, si están en estado sólido o líquido, del viento local, de la disposición de las edificaciones, de la orografía del terreno, etc., por lo que el cálculo de los efectos dependería de una considerable cantidad de variables. Las bombas sucias serían empleadas para producir una situación de pánico y caos entre la población no previamente advertida[8 y 9].

COOPERACIÓN INTERNACIONAL

Uno de los programas para la detección de materiales radiactivos a nivel internacional es el desarrollado por el Departamento de Energía de los Estados Unidos, llamado Programa de Segunda Línea de Defensa (SLD) que, a su vez, está estructurado en dos programas: Core y la Iniciativa de Megapuertos. El SLD fue establecido en el año 2007 con objeto de disuadir, detectar y prohibir que los materiales nucleares y radiactivos pudieran caer en manos de grupos terroristas, especialmente aquellas substancias que fueran susceptibles de utilizarse para la fabricación de bombas sucias. El otro programa dentro del SLD es la Iniciativa de Megapuertos.

El tráfico ilícito de materiales radiactivos a través del mar es uno de los grandes desafíos que existen en la actualidad debido a los millones de contenedores (Twenty Foot Equivalent Unit, TEU) que navegan anualmente en todo el mundo. La misión del SLD se lleva a cabo a través del escaneo de contenedores en puertos de gran volumen de tránsito[10]. En 2003 España firmó una Declaración de Intenciones entre el Servicio de Aduanas de los Estados Unidos y el Departamento de Aduanas de España, en el contexto de la Iniciativa de Contenedores Seguros. Y en 2004, el Gobierno español a través de la Agencia Estatal de Administración Tributaria (AEAT), suscribió con el Departamento de Energía norteamericano el Memorando de entendimiento sobre cooperación para la prevención

---

8 CARPINTERO-SANTAMARÍA, N. «A Holistic Approach to Radiological Terrorism». In APIKYAN, S. and DIAMOND, D. (eds). *Nuclear Threats and Security Challenges*. Springer: 2015.

9 CARPINTERO-SANTAMARIA, N. «Radiological Terrorism: Mental and Health Effects». http://www.cbrneportal.com/radiological-terrorism-mental-and-physiological-health-effects-prof-natividad-carpintero-santamaria/.

10 The White House, Fact Sheet: The Global Initiative to Combat Nuclear Terrorism, Office of the Press Secretary, July 15, 2007.

del tráfico ilícito de material nuclear y radiactivo, que tenía como objetivo principal el escaneo de los contenedores con destino a los Estados Unidos. Este acuerdo es especialmente relevante, pues para hacernos una idea del gran volumen de tránsito TEU en nuestro país, desde enero a abril de 2016, 1.235.369 contenedores pasaron a través de los principales puertos españoles de Valencia, Bahía de Algeciras, Barcelona, Las Palmas y Bilbao[11]. España participa asimismo en la Iniciativa de Seguridad en los Contenedores y cuenta con portales de monitorización radiológica en los puertos de Bahía de Algeciras, Barcelona, Valencia, Las Palmas, Bilbao y Vigo, considerados entre los cien puertos más importantes del mundo.

CONCLUSIONES

Desde el 11 de septiembre de 2001, los esfuerzos internacionales han tenido como uno de sus objetivos prioritarios mejorar la seguridad con el fin de evitar que grupos terroristas pudieran adquirir materiales o agentes NRBQ, teniendo en cuenta que actualmente cualquier escenario es plausible dentro de un terrorismo estratégico. La problemática del tráfico ilícito de materiales radiactivos es una cuestión compleja, ardua, y difícil de calibrar por lo que la colaboración y cooperación internacional son esenciales para poder hacer frente a una de las amenazas asimétricas trasnacionales más perturbadoras en el siglo XXI.

BIBLIOGRAFÍA

– ALLISON, G. *Nuclear Terrorism. The Ultimate Preventable Catastrophe*. New York: Owl Books, 2005.

– CARPINTERO SANTAMARÍA, N. *La bomba atómica: El factor humano en la Segunda Guerra Mundial*. Madrid, España: Ediciones Díaz de Santos, 2007.

– CARPINTERO-SANTAMARÍA, N. «A Holistic Approach to Radiological Terrorism». In APIKYAN, S. and DIAMOND, D. (eds). *Nuclear Threats and Security Challenges*. Springer: 2015.

– CARPINTERO-SANTAMARIA, N. «Radiological Terrorism: Mental and Health Effects». http://www.cbrneportal.com/radiological-terrorism-mental-and-physiological-health-effects-prof-natividad-carpintero-santamaria/.

– DÍEZ ALEGRÍA, M. *Ciencia y Sociedad*. Madrid, España: Editorial Alianza, 1976.

– Estrategia Europea de Seguridad. 2003. https://www.consilium.europa.eu/media/30808/qc7809568esc.pdf.

[11] www.puertos.es.

– IAEA ITDB (Fact Sheet 2019). https://www.iaea.org/sites/default/files/19/04/itdb-factsheet-2019.pdf.

– NORRIS, R. S. and KRISTENSEN, H. M. «Global Nuclear Stockpiles, 1945-2006 . Nuclear Notebook prepared by the Natural Resources Research Council». *The Bulletin of Atomic Scientists*. July/August, 2006.

– The White House, Fact Sheet: The Global Initiative to Combat Nuclear Terrorism, Office of the Press Secretary, July 15, 2007. https://2001-2009.state.gov/t/isn/c18406.htm.

– VELARDE, G. «Evaluación de las probabilidades de una guerra nuclear entre los Estados Unidos y la Unión Soviética. Consideraciones sobre el caso de España». Monografías de la Junta de Energía Nuclear. Madrid, España: 1977.

AMENAZAS ECONÓMICAS

D. VALENTÍN MARTÍNEZ VALERO
GD (retirado) ex director del Centro de Inteligencia de las Fuerzas Armadas (CIFAS)
(Texto no facilitado)

LA GEOPOLÍTICA DE LOS RECURSOS ENERGÉTICOS

D. IVÁN MARTÉN ULIARTE
Senior Fellow de ESADEGeo and Senior Partner Emeritus de BCG
(Texto no facilitado)

PONENCIAS DEL ÁREA 5
Europa, España y seguridad

MESA REDONDA
Situación geopolítica. Entorno europeo

MEDITERRÁNEO. UNA VUELTA AL HORIZONTE

D. JUAN A. MORA TEBAS
Coronel (reserva) analista asociado
del Instituto Español de Estudios Estratégicos

MEDITERRÁNEO. UNA VUELTA AL HORIZONTE

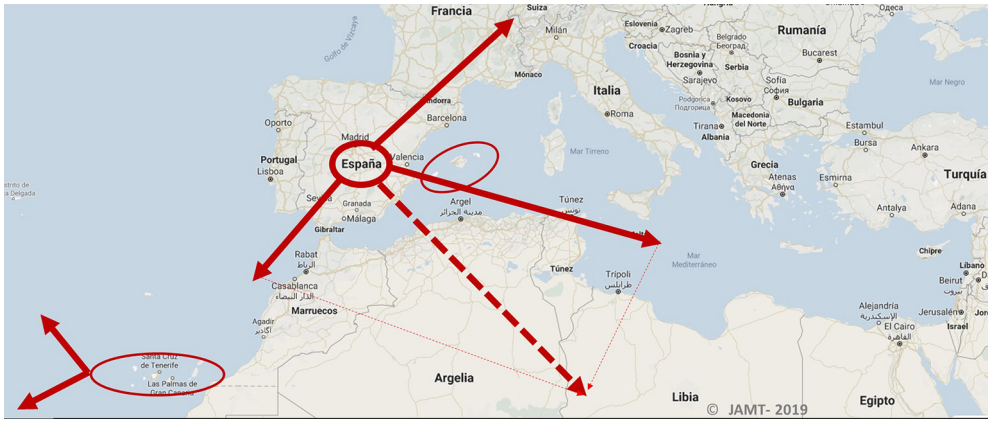
D. JUAN A. MORA TEBAS
Coronel (reserva) analista asociado del Instituto Español de Estudios Estratégicos

«Estoy convencido de que la Tierra es muy grande y que no habitamos en ella más que esta parte que se extiende desde Fasis[1] hasta las Columnas de Hércules, repartidos alrededor del mar como las hormigas y las ranas alrededor de un estanque».

***Fedón: Capítulo* LVIII**
Platón (428 av.J.C.– 348 av.J.C.)

INTRODUCCIÓN

Según la Estrategia de Seguridad Nacional (ESN) de 2017, la seguridad nacional de España está condicionada por su singular posición geoestratégica. Sus condiciones europeas, mediterráneas y atlánticas determinan la importancia de estas regiones para su seguridad, estabilidad y prosperidad[2]. A ello habría que añadir la componente resultante, es decir, la vocación magrebosaheliana.

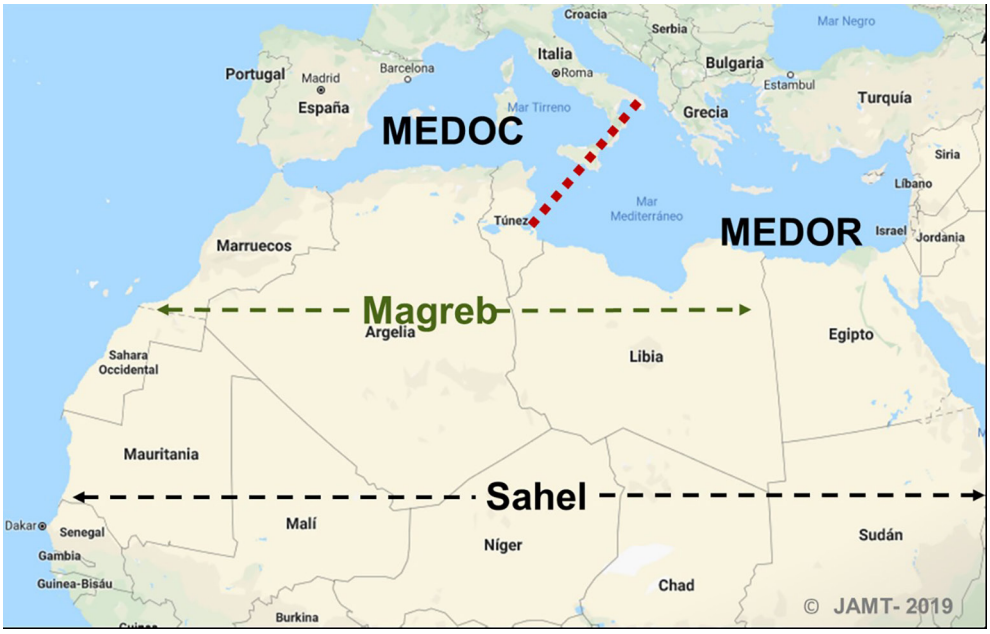


[1] Río del Cáucaso que desemboca en el mar Negro y que marcaba el límite entre Europa y Asia. Actualmente se denomina río Rión.

[2] *Estrategia de Seguridad Nacional (ESN) 2017*. P. 9.

Se trata de un tema muy extenso por lo que en este artículo, tras ver la importancia del Mediterráneo para España, tal y como lo relata la Estrategia de Seguridad Nacional (ESN), se enumerarán los principales problemas, centrándose en los más novedosos y tratando de identificar los focos de crisis y conflictos, recordando las ambiciones geopolíticas presentes en la región, para finalizar con un breve ejercicio de prospectiva.

LA REGIÓN DEL MEDITERRÁNEO EN LA ESTRATEGIA DE SEGURIDAD NACIONAL (ESN)



Con solo dos accesos, uno natural (estrecho de Gibraltar) y otro artificial (Canal de Suez desde 1869), el Mediterráneo ha actuado durante siglos como un espacio de frontera al mismo tiempo que de unión. En la actualidad, la novedad es que ya no solo sus orillas son relevantes, sino también los espacios del interior que se han incorporado a este espacio geopolítico singular y secular que es el Mediterráneo y que acoge a 25 países ribereños[3].

Actualmente, la fragmentación del Mediterráneo en Mediterráneo Oriental -MEDOR y Mediterráneo Occidental - MEDOC, complica la tarea de España frente a esta prioridad estratégica, que es el foco de tantos desafíos potenciales para la seguridad nacional[4].

[3] España, Francia, Italia, Malta, Croacia, Bosnia y Herzegovina (BiH), Montenegro, Albania, Grecia, Bulgaria, Rumania, Ucrania, Rusia, Georgia, Turquía, Chipre, Siria, Líbano, Israel, Egipto, Libia, Túnez, Argelia, Marruecos y Reino Unido.

[4] *ESN (2017)*. Pp. 38-39.

España, como un jugador clave en el área del Mediterráneo, propugna:

- Un mayor papel de la OTAN en el sur, iniciativa que se ha visto respaldada a través del refuerzo de la capacidad de la Alianza en el Mediterráneo.
- Continuar contribuyendo a los esfuerzos internacionales para hacer de Libia un lugar seguro[5].

PRINCIPALES PROBLEMAS Y DESAFÍOS

Como ya dijo en 2008 Bernard Kouchner, ministro de Asuntos Exteriores francés:

> «El Mediterráneo está en el corazón de todos los principales problemas de este cambio de siglo. Desarrollo, migración, paz, diálogo de civilizaciones, acceso al agua y la energía, medio ambiente, cambio climático: es en el sur de Europa donde se juega nuestro futuro[6]».

A finales del siglo XX, el Mediterráneo vivió su periodo más tranquilo y más cercano a una cierta unidad de los últimos dos milenios denominado por ello «Lago OTAN». Sin embargo, el comienzo del tercer milenio contrasta con su «dinamismo» y las intensas rivalidades políticas, militares y económicas que concurren en el área mediterránea. Hasta hace poco, ningún actor podía competir o amenazar seriamente el monopolio de Estados Unidos y la OTAN en el acceso a los recursos mediterráneos. Por el contrario, el surgimiento del fundamentalismo islámico, especialmente desde el 11 de septiembre, y el ciclo de eventos resultantes, lamentablemente muy conocidos, han tendido a reavivar las fracturas culturales y religiosas de la cuenca mediterránea (relacionadas con la visión del choque de civilizaciones sugerido por Huntington[7]). Fracturas relativamente debilitadas y cerradas con la colonización de la costa sur por el norte en el siglo XIX (y una homogeneización, aunque relativa pero existente, de las culturas que le siguieron). El declive y posterior extinción del Imperio otomano, consagraron la victoria, al menos simbólica, del norte.

---

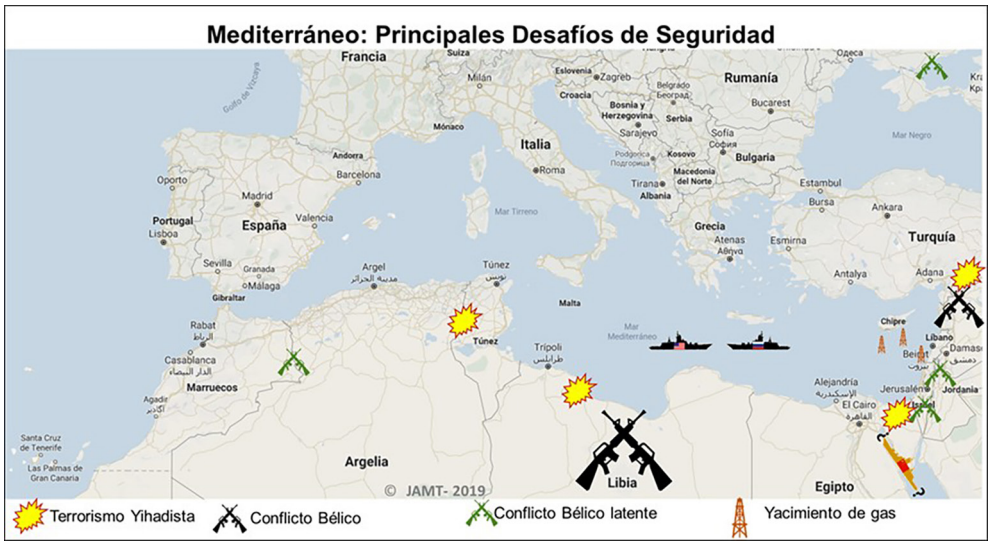
5 Ibídem, p. 46.

6 KOUCHNER, Bernard. «Europe : l'avenir passe par la Méditerranée». *Le Monde*. 10 de julio de 2008.

7 HUNTINGTON, Samuel. «The Clash of Civilizations?». *Foreign Affairs*, vol. 72, n.º 3. 1993.

Actualmente, el Mediterráneo, especialmente con la crisis migratoria, las revueltas árabes, la guerra civil siria, el impulso de los partidos identitarios en ambas orillas *(Golden Dawn* en Grecia o *MS5* en Italia, partidos islamistas del sur, como *Ennadha* en Túnez o el supuesto giro antisecular de Erdogan en Turquía) y los ataques islamistas en Europa occidental, se ha (re) convertido en la principal expresión de estas pasiones y divisiones[8].

PRINCIPALES DESAFÍOS ECONÓMICOS Y DE SEGURIDAD



Ruta marítima clave para la Unión Europea

El mar Mediterráneo sigue siendo un espacio comercial de primera clase, un verdadero cordón umbilical económico entre Occidente y Oriente. De hecho, concentra el 25 % del tráfico mundial del comercio marítimo, aunque constituye solo el 1 % de la superficie de los mares.

Reservas de combustibles fósiles

Desde 2009, la actividad de exploración de hidrocarburos en alta mar en el Mediterráneo Oriental (MEDOR) ha llevado al descubrimiento de varios yacimientos de gas natural, y de continuas campañas de nuevas exploraciones. Por otro lado, entrar en producción depende de la rentabilidad financiera esperada y, en particular, de las posibilidades de transportar gas a mercados de consumo atractivos. Las relaciones entre los diferen-

[8] CELERIER-DAVRIL, Maxime. «La Méditerranée est-elle le premier des théâtres géopolitiques ?» *Antenne International Security and Defense*. 6 de febrero de 2018. http://www.isd.sorbonneonu.fr/blog/la-mediterranee-est-elle-le-premier-des-theatres-geopolitiques/.

tes países involucrados en la producción y el transporte (Egipto, Israel y, posiblemente Chipre, Líbano, Turquía y Grecia) plantean desafíos para el perfecto desarrollo de este sector[9].

La explotación y exportación de recursos de gas en el Mediterráneo Oriental (MEDOR) presenta muchos desafíos de seguridad relacionados con las relaciones políticas inestables entre los países de la región y los riesgos de acciones terroristas. La ubicación de ciertos campos podría revivir disputas preexistentes sobre la delimitación de límites marítimos y zonas económicas exclusivas (ZEE), particularmente con respecto al límite marítimo entre Líbano e Israel, que nunca ha sido aprobado formalmente. Tampoco se pueden descartar disputas sobre la delineación de las estructuras geológicas de los campos de gas, particularmente cuando están cerca de los límites de la ZEE, ya que podrían superponerse. En el caso de bolsas subterráneas que se extienden entre diferentes ZEE, se debe considerar la explotación conjunta del campo, pero también cabe esperar tensiones entre los países en cuestión. Un caso particularmente complejo se refiere a Turquía, la República de Chipre (CR) y la República Turca del Norte de Chipre (TRNC[10]). Ankara se opone más generalmente a cualquier actividad de investigación y producción siempre que no se encuentre un acuerdo entre ambas repúblicas. Turquía y la TRNC creen que cualquier ingreso proveniente de la producción de hidrocarburos debe ser compartido entre toda la población de la isla de Chipre, lo que implica una resolución del conflicto entre la RC y la TRNC. La situación de Israel también es especial. Los conflictos persistentes entre Israel y sus vecinos (un estado de guerra formal con el Líbano, el antagonismo con Hezbolá, las tensiones con los palestinos y la inestabilidad en Siria) exponen las instalaciones de gas al riesgo de ataques militares o terroristas. Estos mismos riesgos de ataques terroristas también pesan sobre las instalaciones de energía en Egipto, un país que sufre regularmente ataques dirigidos por grupos islamistas, presentes principalmente en el Sinaí (región a través de la cual pasa el oleoducto de *East Mediterranean Gas* -EMG[11]).

En general, la proliferación de plataformas de extracción, tuberías, barcos e incluso terminales de gas natural licuado (GNL) implica una proliferación de objetivos sensibles y mayores necesidades de vigilancia. El descubrimiento y la explotación de hidrocarburos será un elemento importante del futuro de los países del Mediterráneo Oriental. Podrían actuar como un factor de cooperación regional, al mismo tiempo que puede alimentar enfrentamientos y agregar fricción a una región ya de por sí volátil. En este contexto, la UE tiene el máximo interés en promover todas las formas posibles de cooperación regional y en defender su interés desde los puntos de vista energético, económico y político. Con respecto a la energía, el gas del Mediterráneo Oriental puede mejorar su seguridad y diversificar el suministro para varios Estados miembros, particularmente en Europa sudoriental y Europa central, regiones que hoy dependen casi exclusivamente del gas ruso.

---

9 BACCARINI, Luca. «Enjeux économiques et sécuritaires de la production de gaz naturel en Méditerranée orientale». *Analyses*. Institut de Relations Internationales et Stratégiques (IRIS). 14 de junio de 2019.

10 TRNC: *Turkish Republic of Northern Cyprus*.

11 La venta de gas natural israelí a Egipto para los próximos diez años, estimada en 15.000 millones de dólares, refuerza la relación entre Israel y el primer país árabe con el que firmó la paz en 1979.
EMERGUI, Sal. «El gas consolida la alianza entre Israel y Egipto». *El Mundo*. 20 de febrero de 2018.

Económicamente, las empresas europeas son las más activas en exploración y producción en la región (incluidas el ENI italiano, la francesa Total y la angloholandesa Shell y sería legítimo defender sus intereses si fuera necesario. Finalmente, desde un punto de vista político, la República de Chipre es miembro de la Unión Europea y el desarrollo de sus reservas de gas representaría un activo poderoso para el desarrollo.

El Mediterráneo Oriental es testigo de los mayores descubrimientos de gas natural en alta mar de este milenio, con perspectivas de importantes hallazgos adicionales. Sin embargo, este beneficio potencial para la región se ve ensombrecido por el hecho de que muchos actores regionales tienen reclamaciones territoriales y compiten por estos valiosos recursos, lo que aumenta las tensiones ya existentes y aumenta el riesgo de conflicto.

La crisis migratoria

En 2018, según el alto comisionado de las Naciones Unidas para los Refugiados (ACNUR/UNHCR) el Mediterráneo Occidental (MEDOC) se convirtió en la ruta más utilizada por los migrantes para acceder a Europa, duplicándose por segundo año consecutivo el volumen, hasta alcanzar la cifra récord de 57.034 personas.

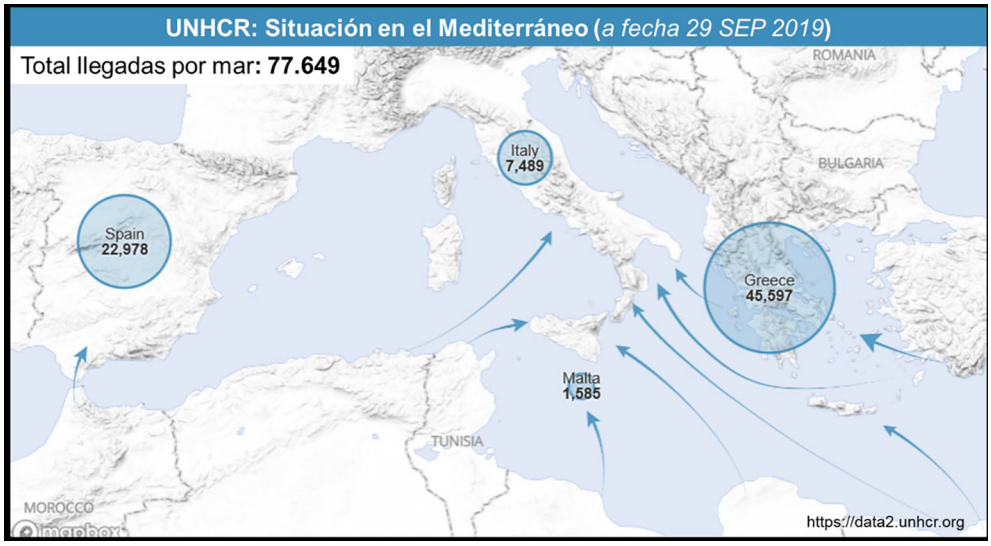


Figura 1: rutas migratorias en el Mediterráneo (fuente UNHCR/ACNUR).

Marruecos fue el principal punto de partida hacia Europa para los migrantes irregulares. La mayor parte de la presión migratoria registrada en esta ruta estaba vinculada a los migrantes procedentes de países subsaharianos. Sin embargo, hacia finales de 2018, el número de inmigrantes marroquíes sufrió un importante aumento. Los migrantes que afirman ser menores representaron el 9 % de las llegadas en esta ruta. En gene-

ral, tanto en rutas terrestres como marítimas, los marroquíes fueron la nacionalidad más detectada, seguidos por los guineanos, malienses y argelinos[12].

En los últimos años, el número de migrantes irregulares detectados en la ruta del MEDOC, que se extiende a través del mar entre España y Marruecos, ha aumentado significativamente. Esta vía ha sido la ruta principal utilizada por las redes criminales para contrabandear drogas en Europa.

El supuesto giro antisecular de Erdogan en Turquía

Un catalizador importante de posibles conflictos, es la transformación de Turquía bajo el presidente Recep Tayyip Erdogan. Ya no es un miembro confiable de la OTAN, es cada vez más autoritario e impredecible en desacuerdo con sus antiguos socios, no solo con los Estados Unidos y Europa, sino también con Israel y Egipto. La adquisición del sistema de defensa aérea avanzada S-400 a Rusia puede ser el mejor indicio del abandono de Turquía de su papel tradicional como baluarte del sur de la OTAN[13].

Presencia de varias flotas de guerra:¿riesgo de conflicto naval?

En el MEDOR, Rusia ha consolidado un centro logístico en Tartus (N de Siria) donde ha basado dos submarinos clásicos y, por lo tanto, ya no tiene que sufrir el control de los estrechos turcos para poder acceder a los mares cálidos. Su flota «mediterránea» puede ahora proyectarse mucho más allá de la costa siria. Los rusos han ganado un espacio real de maniobras que ahora se extiende al sur de Creta[14].

La concentración de fuerzas navales rusas, turcas, israelíes y occidentales en el MEDOR, puede llegar a favorecer malentendidos tácticos que podrían provocar el aumento de la «tensión estratégica» que lleve a una escalada peligrosa en esta región. El derribo del avión ruso *Ilyushin* Il-20 con 15 militares a bordo por la defensa aérea siria el 17 de septiembre de 2018 es un buen ejemplo de ello.

La decisión de Turquía de operar sistemas de defensa antiaérea rusos ha debilitado la estrategia de proteger los flancos del sur de Europa. Esta decisión se ha unido a la potenciación de su flota de guerra y la aplicación de la «diplomacia de las cañoneras» amenazan a Grecia, Chipre, Israel y Egipto, que ha realizado avances en cuestiones de energía y seguridad. Por otro lado, el riesgo de un gran conflicto entre Israel e Irán sobre el Líbano, Siria e incluso más lejos, sigue siendo alto. La proliferación de vehículos sub-

---

12 FRONTEX. «Migratory Routes». Disponible en https://frontex.europa.eu/along-eu-borders/migratory-routes/western-mediterranean-route/. Consultado el 1 de octubre de 2019.

13 EDELMAN, Eric & WALD, Charles. «A Return to Geopolitics in the Mediterranean». *The National Interest Magazine*. 3 de agosto de 2019.

14 LA FAVERIE DU CHÈ, Charles-Henri. «La Méditerranée stratégique-Laboratoire de la mondialisation». *Revue de Défense Nationale* n.° 822. Été 2019, pp. 7-9.

marinos autónomos y no tripulados baratos intensificaría los efectos desestabilizadores de esta carrera armamentista[15].

Entre las armadas europeas, solo Francia despliega permanentemente buques lejos de sus bases. La mayoría de las otras marinas reflejan mejor sus enfoques, a pesar de algunas actividades rutinarias en apoyo de la cooperación multilateral o proyectos de apoyo a la exportación. La suspensión del componente marítimo de la operación *Sophia* de la Unión Europea constituye un ejemplo emblemático de esta precaución.

La OTAN también sufre sus disensiones internas en el Mediterráneo. La postura ambivalente turca en MEDOR cuestiona, en particular, una organización en busca de cohesión. Mientras que las fuerzas navales permanentes de la OTAN navegan y participan en ejercicios importantes que son muy beneficiosos para la preparación de la fuerza, la Alianza ofrece un marco teórico para enfrentamientos de alta intensidad[16].

Al mismo tiempo, las flotas de las orillas sur y este del Mediterráneo se están armando. En 2021, Turquía adquirirá un portaaviones; Marruecos, Argelia y Egipto renovaran sus flotas y compiten en una carrera por el dominio bajo el mar. Este crecimiento de la capacidad lleva mensajes dirigidos a los vecinos regionales: Turquía a Grecia y Chipre, Egipto a Turquía, Marruecos a Argelia y viceversa.

...y todo este «nuevo juego mediterráneo» se desarrolla bajo la atenta mirada de la armada china en plena afirmación de poder: las escalas de los buques chinos en Toulon (Francia) han pasado a ser anuales.

Reanudación de la rivalidad de grandes potencias

Identificada por la estrategia de seguridad y defensa nacional de Estados Unidos como la principal amenaza a la que enfrenta el país, la reanudación de esta rivalidad es otro importante impulsor del incremento de la tensión. Aunque más comúnmente asociada con Europa del Este y el Pacífico Occidental, Rusia e Irán también están actuando en el Mediterráneo Oriental, normalmente a través de terceros (*proxys*). Así, por ejemplo, Teherán tiene una línea recta de influencia política y militar que va a través de Irak y Siria hacia el Líbano y el Mediterráneo, incluidos los misiles avanzados de Hezbolá capaces de actuar sobre el tráfico marítimo, puertos e infraestructura energética[17].

Del mismo modo, Moscú está más involucrado que nunca, incluida la actividad renovada de su flota y una formidable cobertura de defensa aérea que abarca gran parte de la región. Todo ello, en un momento en el que la presencia regional de EE. UU. ha dis-

---

15 EDELMAN, Eric & WALD, Charles. «A Return to Geopolitics in the Mediterranean». *The National Interest Magazine*. 3 de agosto de 2019.

16 https://www.franceculture.fr/emissions/cultures-monde/mer-mediterranee-mare-nostrum-24-batailles-navales-le-nouveau-grand-jeu.

17 EDELMAN, Eric & WALD, Charles. «A Return to Geopolitics in the Mediterranean». *The National Interest Magazine*. 3 de agosto de 2019.

minuido, los planificadores estadounidenses por primera vez en décadas ya no pueden asumir que el Mediterráneo Oriental es un entorno operativo incontestable.

CONTRIBUCIÓN DE ESPAÑA: MULTILATERAL (ONU, EU, NATO)

España quiere estar, y está, presente en los esfuerzos colectivos para garantizar la paz y la seguridad en el Mediterráneo. De hecho es la zona del mundo donde tiene unos 1.150 militares desplegados en el área mediterránea, el 40,6 % del total del contingente que despliega en misiones internacionales[18]:

Fuerza Interina de Naciones Unidas en el Líbano (FINUL)

España despliega unos 600 militares y 12 guardias civiles, distribuidos entre la Brigada Multinacional Este que lidera y el Cuartel General de FINUL en Naqoura (al SO del Líbano).

Esta misión se encuentra en una fase de estabilización, orientada a lograr que el Ejército libanés pueda hacerse cargo de la situación en la línea de separación con Israel establecida por la ONU, la *Blue Line,* sin necesitar para ello a las tropas internacionales.

[18] https://www.defensa.gob.es/Galerias/gabinete/red/2019/10/Infografiamisionesexterior.pdf.

Operación «Sea Guardian»

La seguridad marítima es una de las principales prioridades de la OTAN. En noviembre de 2016, la OTAN lanzó una operación de seguridad marítima, llamada *Sea Guardian*, que puede realizar una amplia gama de tareas relacionadas con las operaciones de seguridad marítima:

– conciencia de la situación marítima,
– preservación de la libertad de navegación,
– interdicción marítima,
– lucha contra la proliferación de armas de destrucción masiva,
– protección de infraestructuras críticas,
– lucha contra el terrorismo,
– desarrollo de capacidades de seguridad marítima.

Actualmente, de acuerdo con las decisiones del Consejo del Atlántico Norte, esta operación se implementa en el Mediterráneo, donde realiza tres de esas tareas: contribuye al conocimiento de la situación marítima, la lucha contra el terrorismo y participa en la construcción de capacidades de seguridad marítima.

La operación tiene como objetivo desarrollar un conocimiento sólido del entorno marítimo, combinando redes basadas en sensores y no basadas en sensores, con un intercambio de información confiable y conectividad entre aliados y todas las agencias relacionadas con el entorno marítimo.

De esta forma, la OTAN contribuye a mantener un entorno marítimo seguro y protegido, al tiempo que contribuye a las tres tareas centrales de la Alianza: defensa colectiva, gestión de crisis y seguridad cooperativa. La Operación *Sea Guardian* informa a la Sede

del Mando Marítimo Aliado (MARCOM HQ) en Northwood, Reino Unido, y las fuerzas se generan a partir de capacidades nacionales.

España lideró esta operación (del 12 de febrero al 14 de marzo de 2018), al frente del grupo formado por la fragata italiana *Eolo* y la belga *Louise-Marie,* estuvo la fragata *Navarra* (F-85). Cartagena fue el punto de encuentro de estas unidades[19].

Operación OTAN de apoyo a Turquia «Active Fence»

http://www.defensa.gob.es/Galerias/gabinete/red/2017/

Durante el año 2012 la situación de guerra civil en Siria, trajo como consecuencia una situación de inestabilidad en el flanco sur de la OTAN y la posible amenaza de un uso incontrolado de misiles balísticos en las fronteras de Turquía. Ello llevó al Gobierno turco a solicitar a la Alianza la adopción de medidas de refuerzo de su defensa aérea, lo que motivó el despliegue a principios de 2013, en el marco del Plan Permanente de Defensa Aérea *Active Fence* del territorio aliado, de unidades PATRIOT de EE. UU., Alemania y Países Bajos en territorio turco.

En agosto de 2014, el Mando de la OTAN solicitó a España que valorara la posibilidad de relevar en 2015 a alguna de las citadas unidades PATRIOT, para poder mantener el esfuerzo de la Alianza. España anunció su intención de atender a lo solicitado y de esta forma, una unidad PATRIOT española inició su misión en el mes de enero de 2015 para la protección del aeropuerto y ciudad de Adana. El contingente español se compone aproximadamente de 150 militares.

[19] http://www.defensa.gob.es/misiones/en_exterior/actuales/listado/otan-sea-guardian.html.

La unidad formada por una batería de misiles PATRIOT ha sido generada por el Ejército de Tierra y procede del Regimiento de Artillería Antiaérea número 74, ubicado en Dos Hermanas (Sevilla) y San Roque (Cádiz).

Con la participación en esta misión, España realiza una nueva aportación a la seguridad y estabilidad internacional, confirmando su compromiso con las operaciones de la Alianza, en un momento en que la estabilidad regional en el flanco sur se ve afectada por un conflicto en la frontera de la Alianza. Esta contribución nacional se enmarca además en la misión permanente de defensa aérea del territorio y poblaciones de la Alianza, y se orienta hacia uno de los escenarios en los que la Alianza se enfrenta en mayor medida a retos y amenazas en la región de Oriente Medio y África del Norte (MENA)[20].

2.º Grupo de la Fuerza Naval Permanente de Reacción de la OTAN (SNMCMG2)

La OTAN tiene fuerzas navales permanentes (SNF[21]) que le permiten proporcionar una presencia naval continua. Estas fuerzas disuasorias multinacionales responden a un imperativo marítimo de la Alianza. Llevan a cabo un programa preestablecido de ejercicios, maniobras y escalas, y pueden desplegarse rápidamente en tiempos de crisis o tensión.

Las fuerzas navales permanentes de la OTAN se dividen en cuatro grupos:

– 2 grupos marítimos permanentes (SNMG1 y SNMG2[22]).
– 2 grupos permanentes de acción contra las minas (SNMCMG1 y SNMCMG2[23]).

20 http://www.defensa.gob.es/Galerias/gabinete/red/2017/red-336-misiones.pdf.

21 SNF: Standing Naval Forces.

22 SNMG: Standing NATO Maritime Group.

23 SNMCMG: Standing NATO Mine Countermeasures Group.

Estos cuatro grupos son parte de la fuerza de reacción rápida de la Alianza, la Fuerza de Respuesta de la OTAN (NRF).

SNMG1 y SNMG2, los grupos marítimos permanentes de la OTAN, son una fuerza marítima multinacional compuesta por barcos de diferentes países de la Alianza. Estas naves están permanentemente disponibles para la OTAN para realizar diversas tareas, desde ejercicios hasta misiones operativas. También sirven para establecer la presencia y la solidaridad de la Alianza, realizar visitas diplomáticas de rutina a diferentes países, apoyar el compromiso con los socios y proporcionar una gama de capacidades militares, disponible para misiones actuales. Operan de acuerdo con las necesidades operativas de la Alianza, lo que ayuda a mantener una flexibilidad óptima. Su composición varía, y generalmente cuentan de dos a seis barcos proporcionados por la mayor cantidad de países miembros de la Alianza.

> SNMG1 y SNMG2 son responsabilidad del Comando Marítimo Aliado (MARCOM) con sede en Northwood, Reino Unido, desde su inauguración (DIC 2012), como centro operativo para todas las operaciones marítimas de la Alianza.
> Como parte de la Fuerza de Respuesta de la OTAN, las Fuerzas Navales Permanentes de la OTAN proporcionan a la Alianza una presencia constante en el mar. Estas fuerzas multinacionales, que realizan regularmente: patrullas, ejercicios y escalas para trabajar con sus socios, se puede activar rápidamente en momentos de tensión o crisis. Además, apoyan el despliegue de la Alianza en el mar Egeo, ayudando así a cortar las rutas de migración ilegal entre Turquía y Grecia.
> El Grupo Marítimo Permanente de la OTAN n.º2 es una fuerza naval multinacional de la OTAN dedicada a la Operación *Active Endeavour* en el Mediterráneo desde 2001. Hasta el 1 de enero de 2005, era conocida como la Fuerza Naval Permanente del Mediterráneo (STANAVFORMED[24]), consta de 3 a 8 fragatas o destructores y un buque de apoyo logístico. La fragata *Santa María* estuvo integrada en la SNMG2 desde el 2 de febrero al 5 de abril de 2019[25].

2º Grupo Permanente de Acción contra las Minas de la OTAN (SNMCMG1)

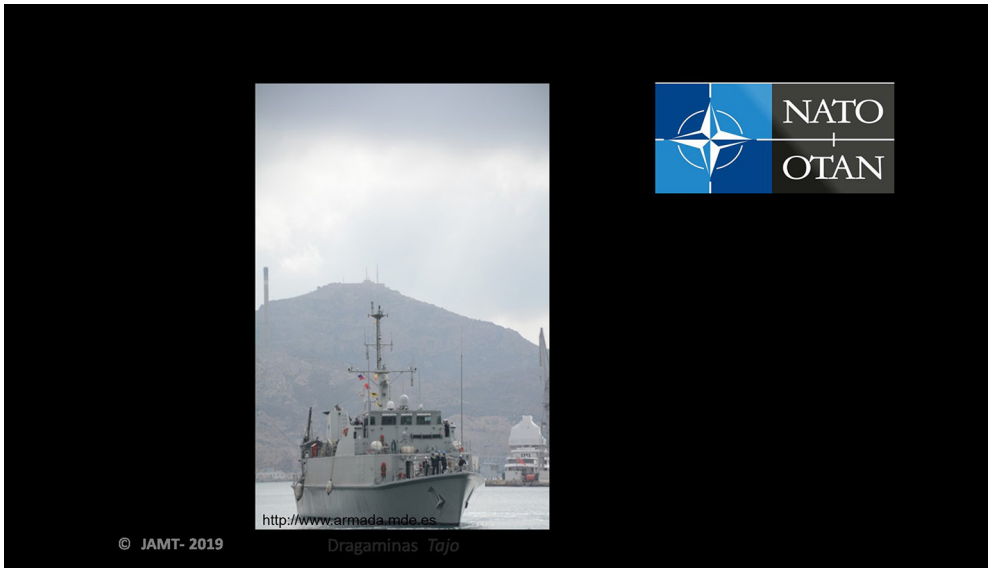
Los grupos permanentes de acción contra las minas de la OTAN (SNMCMG1 y SNMCMG2) son fuerzas multinacionales que participan principalmente en operaciones de búsqueda y eliminación de artefactos explosivos. SNMCMG2 también está llevando a cabo operaciones de eliminación de artefactos explosivos «históricos» para reducir la amenaza que representan las minas de la Segunda Guerra Mundial.

---

[24] STANAVFORMED/SNFM: Standing Naval Force Mediterranean.

[25] https://www.nato.int/cps/fr/natohq/topics_70759.htm http://www.defensa.gob.es/Galerias/defensadocs/misiones-internacionales.pdf.

Ambos SNMCMG son activos esenciales de la NRF, pudiendo realizar una amplia gama de funciones, desde misiones humanitarias hasta operaciones. Pueden desplegarse con poca antelación y, a menudo, son los primeros medios en ser enviados a un teatro de operaciones[26].



Operación EUNAVFOR MED – Sophia

Ante la situación provocada en el Mediterráneo central y meridional en relación con la inmigración irregular, alimentada por la inestabilidad en Libia, la Unión Europea decidió reforzar su presencia en el mar para luchar contra los traficantes, prevenir los flujos de migración ilegal y reforzar la solidaridad y la responsabilidad internas.

El 18 de mayo de 2015, el Consejo de Asuntos Exteriores de la Unión Europea aprobó la Decisión (PESC) 2015/778 que autorizaba el establecimiento de una operación militar de la UE en el Mediterráneo central meridional (EUNAVFOR MED[27]). El lanzamiento de la misión se aprobó el 22 de junio.

La misión tiene por objeto interrumpir el modelo de negocio de las redes de tráfico ilícito de personas en el Mediterráneo central y meridional, mediante esfuerzos sistemáticos para identificar, capturar y eliminar las embarcaciones y medios utilizados o que se sospeche son utilizados por los traficantes, de conformidad con el derecho internacional.

---

[26] Dossiers de l'OTAN. «Les activités maritimes de l'OTAN». 6 de agosto de 2019. https://www.nato.int.

[27] EUNAVFOR MED: European Union Naval Force- Mediterranean.

Para ello la operación se articula en varias fases:

- 1.ª Fase: Apoyo a la detección y seguimiento de las redes de migración a través de la recopilación de información y patrullas en alta mar.
- 2.ª Fase:

  a. Visita, registro, apresamiento y desvío en alta mar de las embarcaciones sospechosas de ser utilizadas para el tráfico ilícito o la trata de seres humanos conforme al derecho internacional aplicable.
  b. Visitar, registrar, apresar y desviar en alta mar, mar territorial o aguas interiores del mencionado Estado, las embarcaciones sospechosas de ser utilizadas para el tráfico ilícito o la trata de seres humanos, conforme a una resolución del Consejo de Seguridad de Naciones Unidas o el consentimiento del Estado ribereño concernido.

- 3.ª Fase: Adoptar todas las medidas necesarias contra una embarcación sospechosa y los medios relacionados, incluso deshacerse de ellos o inutilizarlos, de conformidad con una resolución del Consejo de Seguridad de Naciones Unidas o el consentimiento del Estado ribereño en cuestión.

Dado que el objetivo de la Unión Europea es proporcionar soluciones duraderas y estables a largo plazo, se establece que EUNAVFOR MED coopere con los Estados miembros relevantes, estableciéndose los mecanismos de coordinación apropiados con otras agencias y organismos, especialmente FRONTEX, EUROPOL, EUROJUST, la Oficina Europea de Apoyo al Asilo y las misiones PCSD relevantes.

España, como socio responsable de la UE, decidió participar en la operación ofertando diversos medios militares que fueron definidos por el Gobierno en el Acuerdo de Consejo de Ministros de 24 de julio de 2015.

Para la primera fase, España desplegará un avión de patrulla y reconocimiento marítimo en Sigonella (Sicilia), con una dotación de 50 personas con los correspondientes medios de apoyo y sostenimiento.

Además, aportará 12 efectivos del Ejército del Aire y la Armada que trabajarán en el Cuartel General del Mando de la operación en Roma y en el Cuartel del comandante de la Fuerza establecido en el portaaviones italiano *Cavour*.

Dependiendo de la evolución de la situación, se podría ampliar la participación española hasta un máximo de 250 efectivos.

En febrero de 2019, la fragata española Reina Sofía (F-84) completaba su rotación tras cuatro meses en el mar, durante los que verificó la identidad de 58 buques mercantes, para garantizar la tarea de controlar el embargo de armas contra Libia, la lucha contra el tráfico de petróleo y seres humanos[28].

El 26 de septiembre, la UE prorrogaba 6 meses más la operación Sophia contra las mafias migratorias en el Mediterráneo, hasta el 31 de marzo de 2020, pero sin barcos.

CONCLUSIONES

La cuenca mediterránea, sigue presentando una concentración de preocupaciones presentes y futuras a escala mundial. Es por eso que algunos autores la consideran un «laboratorio de globalización».

Es asombrosa la velocidad con la que ha cambiado la situación en el Mediterráneo a lo largo de estos últimos años, de forma que se están estableciendo nuevos equilibrios que sería muy importante conocer en profundidad. Valga como ejemplo, la alianza sin precedentes entre Egipto, Grecia, Chipre e Israel en torno a los campos de gas descubiertos en sus zonas económicas exclusivas (ZEE).

Las incógnitas que se plantean en esta región son numerosas:

– Evolución del conflicto israelo-palestino, siempre clave para la paz en Oriente Medio, pero que también ejerce su influencia en toda la región MEDOR, países del Magreb-Sahel incluidos.
– Tras las revueltas árabes (2011-2013), mal llamadas primaveras árabes, ¿cuál será el papel de la sociedad civil en Siria, Túnez y Egipto?

---

[28] http://www.defensa.gob.es/misiones/en_exterior/actuales/listado/eunavformed.html.
https://www.operationsophia.eu/media_category/assets/.
http://www.defensa.gob.es/Galerias/defensadocs/misiones-internacionales.pdf.

– No hay que desdeñar el papel de Rusia que, tras su anexión de Crimea, se ha visto reforzado por su gestión en la guerra de Siria y plantea una presencia cada vez mayor en África en general y en el norte de África (Argelia, Libia, Egipto) en particular, como ha quedado demostrado en la 1.ª Cumbre Rusia-África (Sochi 23-24 de octubre de 2019).
– Ni tampoco hay que desdeñar el papel de China, ya presente en los dos puntos de entrada del Mediterráneo: Port Said (Egipto) y Tánger-Med (Marruecos) y en otros puertos mediterráneos: El Pireo (Grecia) Marsaxlokk (Malta), Estambul (Turquía), Venecia y Chioggia (Italia), Valencia (España), Marsella (Francia).
– La «diferencia de potencial demográfico» entre África y Europa que acabará transformando gradualmente el Mediterráneo hasta convertirse en un espacio de paso continuo.
– La Unión Europea debería reescribir, incluso reinventar, sus relaciones con los países mediterráneos, más allá de temas como la migración y la ayuda humanitaria, en estrecha colaboración con la OTAN.
– Los persistentes desafíos de seguridad en el Mediterráneo requieren la consolidación de la cooperación de la Organización del Tratado del Atlántico Norte (OTAN) con la orilla sur, que no debe verse solo como una fuente de amenazas, sino también como una fuente de cambio, progreso y de desarrollo económico.
– La débil extensión de las zonas marítimas de los Estados de la orilla sur del Mediterráneo, agravada por la no posesión de territorio insular, queda reflejada en la aparición de rivalidades geopolíticas cuando se trata de prospectar y explotar los grandes depósitos de hidrocarburos.

Como afirman algunos autores, el Mediterráneo ha pasado de ser el centro («ombligo») del mundo, a un laboratorio de la globalización[29] exportable a «otros mediterráneos», es decir constituirá el tablero donde se jugarán algunas de las más importantes «partidas» por el liderazgo mundial.

En cuanto a España, continuará estando presente a corto y mediano plazo y cooperará, principalmente, en las áreas de desarrollo, ayuda humanitaria y gestión de crisis. Al mismo tiempo, está comprometida en redactar documentos de la OTAN para que se considere al Magreb no solo como un área de interés prioritaria, sino también como un escenario diferenciado en la región MENA (Oriente Medio y norte de África) y abogará por un mayor papel para los países de esta región a la hora de evaluar los riesgos y amenazas, y encontrar soluciones.

Por último, no podemos estar más de acuerdo con el geógrafo francés Albert Demangeon, que hace justo un siglo ya anunciaba un resurgir del Pacífico, que se convertiría en un «nuevo Mediterráneo». La visión del mundo a partir de ahora deja de ser «mediterraneocéntrica» para volverse «pacificocéntrica» o quizás debiéramos decir «chinocéntrica».

> «El océano Pacífico, durante mucho tiempo excéntrico en relación con los grandes focos comerciales, después llamado a la vida por los navegantes y comerciantes de Europa, se despierta a una vida independiente; sus dos orillas, que durante un siglo se orientaron una hacia el oeste y la otra hacia el este, se vuelven la una hacia la otra y se convierten en el litoral de un nuevo Mediterráneo».

[29] CÉLÉRIER-DAVRIL, Maxime.«La Méditerranée est-elle le premier des théâtres géopolitiques ?». 6 de febrero de 2019.

TRÁFICOS ILÍCITOS Y REDES CRIMINALES

Dª SONIA ALDA MEJÍAS
Investigadora principal. Directora del Observatorio de Tráficos Ilícitos y Redes Criminales del Real Instituto Elcano
(Texto no facilitado)

INCERTIDUMBRES Y CERTEZAS, EN EL FUTURO DE LAS FUERZAS ARMADAS

D. FERNANDO ALEJANDRE MARTÍNEZ
General de ejército jefe de Estado Mayor de la Defensa (JEMAD)
(Texto no facilitado)

COMUNICACIONES

LA AMENAZA HÍBRIDA: UN CONCEPTO COMODÍN

GUILLEM COLOM PIELLA
Profesor de Ciencia Política en la Unversidad Pablo de Olavide y codirector de THIBER

Resumen

El trabajo repasa la evolución del concepto «híbrido» desde sus orígenes militares hasta hoy en día. Se exponen las relaciones entre lo híbrido y la guerra política, las actividades de subversión, desestabilización y operaciones de información, contraponiendo la interpretación rusa y occidental de las actividades híbridas.

Palabras clave

Amenaza híbrida – subversión – desestabilización – guerra política – guerra informativa – zona gris.

COMUNICACIÓN

Introducción

Las «cosas» híbridas se han convertido en uno de los *hype* informativos del momento por méritos propios. Aunque la guerra o amenaza híbrida tiene un extenso y controvertido recorrido en el ámbito estratégico-militar para definir la integración de elementos convencionales e irregulares, actualmente lo híbrido está siendo utilizado por muchos *think tanks*, periodistas, académicos y políticos para describir, de forma casi exclusiva, las actividades que realiza el Kremlin para proyectar su influencia exterior.

Aunque las invasiones de Crimea y del este de Ucrania entran dentro de las definiciones ya «clásicas» de guerra híbrida[1], otras actividades consideradas híbridas se relacionan con las tácticas de subversión y desestabilización soviéticas, y otras se encuadran en el concepto de guerra política, donde un estado emplea todos los instrumentos a su disposición para debilitar y desmoralizar política, militar, económica o socialmente al adversario. Sin embargo, lo híbrido que más atención está recibiendo se relaciona con el otro *hype* del momento: la desinformación, obviando tanto la larga tradición soviética de «medidas activas» como los grandes desarrollos realizados en la concepción rusa de guerra informativa desde la década de 1990 y centrales en su estrategia militar[2].

En cualquier caso, algunas crónicas afirman que Moscú ha inventado la guerra híbrida y otras argumentan que el Kremlin está llevando a cabo una guerra híbrida contra Occidente, pareciendo olvidar que lo híbrido puede ser utilizado por cualquier actor, tanto para ampliar su capacidad en el campo de batalla posmoderno como –utilizando una definición extensiva– para proyectar su influencia en el mundo físico, psicológico, perceptivo o virtual.

Paradójicamente, Moscú también sostiene algo similar: asumiendo su papel civilizador, percibiéndose amenazada y preparando mentalmente a su población para la guerra, también declara estar siendo objeto de una guerra híbrida conducida por Occidente. Definida como cualquier acción militar, política, cultural, diplomática, económica, informativa o medioambiental[3] y fundamentada en el empleo de ONG y organizaciones civiles, el apoyo a movimientos sociales u opositores políticos, el control de internet, la penetración cultural o la propaganda en medios de comunicación, esta guerra híbrida promovida por Estados Unidos pretende explotar el potencial de protesta popular para facilitar cambios de régimen[4]. Esta percepción de amenaza y su inferioridad militar en el plano convencional con la Alianza Atlántica le permite justificar sus actividades de subversión y desestabilización, sus operaciones informativas o sus acciones militares en su área de influencia más directa.

---

[1] Moscú lo consideraría como guerra de nueva generación (THOMAS, Timothy. *Thinking like a Russian Officer: Basic Factors and Contemporary Thinking on the Nature of War*. Fort Leavenworth: FMSO, 2016).

[2] GERASIMOV, Valeri. «Vektory razvitija voennoj strategii». *Krasnaja zvezda*. 4 de marzo de 2019. En esta misma crónica, el jefe de estado mayor de la defensa rusa argumenta que las medidas no-militares o híbridas pueden apoyar la consecución de los objetivos militares, influir en el desarrollo de las operaciones y facilitar el empleo de la fuerza militar convencional, pero que las confrontaciones en «otras esferas» son distintas al utilizar sus propias lógicas y estrategias, siendo lo militar uno de los componentes que las conforman.

[3] Estas ideas han sido ampliamente debatidas en la comunidad estratégica rusa desde la década de los noventa, primero vinculadas con la necesidad de blindar su espacio informativo frente a cualquier injerencia externa y posteriormente relacionadas tanto con el poder blando como forma de influencia política como con las ideas de guerra híbrida.

[4] En este sentido, obsérvese lo que comenta Valeri Gerasimov: «…las medidas políticas, económicas, informativas, humanitarias y no-militares se han empleado junto con el potencial de protesta popular. Todo ello ha sido apoyado por medios militares de carácter clandestino realizando actividades informativas y operaciones especiales. El empleo abierto de unidades militares –a menudo bajo la apariencia de fuerzas de mantenimiento de la paz y gestión de crisis– se ha realizado en cierto momento con el objetivo de contribuir al logro de la situación deseada en el conflicto». GERASIMOV, Valeri. «Cennost' nauki v predvidenii». *Voenno-promyšlennyj kur'er*. Febrero 2013, vol. 8, n.º 476, s.n. De hecho, los sucesos de Venezuela están siendo considerados como una guerra híbrida conducida por Occidente, especialmente si se produjera un intervencionismo humanitario, algo que choca completamente con el principio de soberanía clásico. Para encuadrar las ideas de Gerasimov, véase: COLOM, Guillem. «La Doctrina Gerasimov y el pensamiento estratégico ruso contemporáneo». *Ejército*. Diciembre 2018, n.º 933, pp. 30-37.

El viaje conceptual de lo híbrido

Cualquier interesado en lo híbrido conoce el largo viaje conceptual que ha experimentado esta idea desde 2006 hasta 2019. Hoy en día, las concepciones abarcan desde cualquier actividad informativa, cibernética, subversiva o cinética realizada bajo el umbral del conflicto armado o cualquier manifestación de guerra política que entrañe el empleo de medios diplomáticos, informativos, militares, económicos, financieros, legales o de inteligencia en tiempo de paz, crisis o guerra[5]. Sin embargo, esta idea que siempre ha mantenido una calculada ambigüedad por sus limitaciones inherentes, se ha estirado tanto que cualquier actividad extraña –desde un *tweet* a la suplantación o *spoofing* de la señal del GPS de un avión[6]– puede ser considerada como algo constitutivo de lo híbrido.

Sin embargo, quizás la referencia más gráfica de la concepción actual de lo híbrido procede del secretario general de la Alianza Atlántica cuando declaró que «…lo híbrido es el lado oscuro de nuestro Enfoque Integral»[7], por lo que cualquier respuesta debería combinar todos los instrumentos del estado y de la comunidad internacional: diplomáticos, informativos, militares, económicos, financieros, de inteligencia o legales.

Paradójicamente, mientras muchos comentaristas utilizan lo híbrido como sinónimo de desinformación o «ciberataque» (refiriéndose a actividades de (ciber)inteligencia, hackeo de dispositivos o servicios, *hack&leak*, uso de *trolls* o *bots* para amplificar mensajes o propaganda computacional), las definiciones oficiales continúan recogiendo como rasgo distintivo el elemento militar convencional[8]. Este puede ser el caso de la Alianza Atlántica, que define las amenazas híbridas como «…la integración de medios convencionales y no-convencionales, medidas militares abiertas y encubiertas, paramilitares y civiles por parte de actores estatales y no-estatales para lograr sus objetivos»[9], o la Unión Europea, que más que definir el concepto y acotarlo, enumera un conjunto de características que podrían definir lo híbrido:

> «Las amenazas híbridas combinan actividades militares y no-militares convencionales y no-convencionales que pueden ser utilizadas de manera coordinada por actores estatales y no-estatales para lograr sus objetivos políticos. Las campañas híbridas son multidimensionales, combinando medidas coercitivas y subversivas, utilizando herramientas y tácticas tanto convencionales como no-convencionales.

---

[5] Ello permitiría describir muchas de las actividades –a pesar de que muchos analistas centran su atención en las amenazas persistentes avanzadas debido a su difícil atribución– que actores como Rusia, China, Irán, Arabia Saudita o Corea del Norte, por poner algunos ejemplos, están llevando a cabo en la actualidad.

[6] El lector especializado habrá observado que ambas acciones tienen mucho más en común de lo que parece: son dos ejemplos de guerra informativa, el primero orientado a los efectos informativo-psicológicos y el segundo a los informativo-técnicos. Para conocer estos asuntos con más detalle, véase: HEICKERO, Roland. *Emerging cyber threats and Russian Views on Information Warfare and Information Operations*. Estocolmo: FOI.

[7] Discurso del secretario general Jens Stoltenberg en la apertura del Seminario de Transformación de la OTAN (25 de marzo de 2015). Esta misma idea también es utilizada por muchos teóricos militares rusos, que consideran el Enfoque Integral como el habilitador de la guerra híbrida.

[8] La concepción rusa subraya el papel de los ejércitos convencionales en la consecución de los objetivos estratégicos (KORYBKO, Andrew. *Hybrid Wars: The Indirect Adaptive Approach to Regime Change*. Moscú: People's Friendship University of Russia, 2015).

[9] Declaración final de la Cumbre de Varsovia (9 julio 2016), para. 72.

> Han sido diseñadas para ser difíciles de detectar y atribuir. Estas amenazas apuntan a vulnerabilidades críticas y pretenden generar confusión para dificultar la toma de decisiones rápida y efectiva. Las amenazas híbridas pueden abarcar desde ataques cibernéticos a sistemas de información críticos, pasando por la interrupción de servicios críticos como el suministro energético o servicios financieros, hasta el debilitamiento de la confianza pública en las instituciones gubernamentales o la profundización de las divisiones sociales. Como la atribución es difícil, estos desafíos requieren medidas específicas y coordinadas para contrarrestarlos»[10].

Con independencia de los largos debates que pueden realizarse sobre la conveniencia de hablar de guerra, adjetivarla como híbrida, considerar si se trata de algo novedoso, si deben utilizarse ideas alternativas (ambigua, irregular, asimétrica, política, no-lineal…) o aparcar este concepto, lo cierto es que lo híbrido es atractivo y posee fuerza expresiva para que el público no especializado comprenda la multidimensionalidad de la amenaza[11]. Sin embargo, al ampliar tanto el objeto de análisis, estirando tanto el concepto y manteniéndolo tan ambiguo, lo híbrido corre el riesgo de convertirse en un concepto comodín, vacío de contenido, usado principalmente para definir las acciones rusas en el exterior o describir un amplio abanico de actividades que escapan a la lógica «convencional». En cualquier caso, si se asume esta visión expansiva, cualquier respuesta debería plantearse en el marco de un Enfoque Integral internacional o un Enfoque Gubernamental a escala nacional, algo que escapa al objeto de esta comunicación.

De hecho, en un plano más militar muchos consideran que no existen razones suficientes para emplear otro concepto que solo añade confusión al análisis estratégico, varios sostienen que lo híbrido es el producto natural de la adaptación de la guerra irregular y asimétrica al mundo globalizado y a la era de la información. Otros subrayan que el concepto no está consolidado ni tampoco existe ninguna definición aceptada que vaya más allá del mínimo común denominador de la combinación de medios, procedimientos y tácticas convencionales e irregulares. Finalmente, a raíz de la expansión del concepto, muchos expertos argumentan que debería dividirse en sus distintas vertientes (subversión, desestabilización, operaciones informativas, fuerza militar…) mientras alertan que lo híbrido corre el riesgo de perder su valor explicativo al haberse popularizado para definir cualquier actividad situada por debajo del umbral del conflicto. Aisladas, estas actividades difícilmente pueden constituir un *casus belli*, pero su impacto agregado utilizando la «táctica del salami» sí puede alterar la correlación de fuerzas.

---

10 COMISIÓN EUROPEA. *A Europe that protects: Countering Hybrid Threats*. Bruselas: Unión Europea, 2018, p. 1.

11 Sin embargo, la fuerza expresiva de esta idea que ha experimentado este gran viaje conceptual tampoco es nueva. Antes de ser definido como la combinación de medios regulares e irregulares (HOFFMAN, Frank. *Conflict in the 21st Century: The rise of hybrid wars*. Arlington: Potomac Institute for Policy Studies, 2007) el término «guerra híbrida» fue empleado en un documento oficial estadounidense de 2005 para explicar la combinación de dos o más amenazas de tipo tradicional (convencional), irregular, catastrófico o disruptivo. Su uso pretendía concienciar al poder político sobre la dificultad intrínseca de planear la defensa en un mundo menos previsible que el bipolar (Department of Defense: *National Defense Strategy of the United States of America*. Washington DC: Government Printing Office, 2005). Sobre estas ideas, véase: COLOM, Guillem. «El nuevo rostro de la guerra, los conflictos híbridos», en REQUENA, Miguel (ed.). *Luces y sombras de la seguridad internacional en los albores del siglo XX*. Madrid: IUGM, 2010, pp. 55-64.

A raíz de la expansión del concepto, el énfasis de lo híbrido ha pasado del elemento militar a toda la gama de actividades que pueden producirse en la zona gris de forma más o menos encubierta para preparar el teatro de operaciones, desestabilizar y desmoralizar el adversario o lograr la situación final deseada sin emplear la fuerza militar de forma abierta. Sin embargo, si finalmente se cruza el umbral del conflicto y se utilizan medidas abiertas o el actor carece de los medios para preparar informativamente el campo de batalla, lo híbrido intentará explotar las limitaciones del estilo occidentalizado de combatir, fundamentado este en la supremacía tecnológico-militar y en el cumplimiento de las leyes y costumbres de la guerra para lograr victorias rápidas, decisivas, contundentes y sin apenas bajas propias ni daños colaterales. En consecuencia, tal y como ha sucedido desde la antigüedad, ante la imposibilidad de medirse con un ejército más poderoso o la oportunidad de no hacerlo, el adversario usa tácticas asimétricas, se confunde entre la población, identifica como centro de gravedad la ciudadanía adversaria, actúa ajeno a los usos y costumbres de la guerra y aprovecha para sus intereses el derecho internacional e intenta que sus actividades tengan los mayores efectos estratégicos mediante una eficaz explotación informativa de sus actos físicos, lógicos e informativos. En otras palabras, lo híbrido explota las debilidades políticas, sociales, jurídicas, morales, económicas, demográficas o militares de adversarios más eficaces en el terreno convencional.

Las sociedades occidentales han abrazado los valores posmodernos y posmaterialistas. Además de facilitar las actividades de influencia por su relativismo y cuestionamiento de la realidad, estos valores impiden ver el mundo como algo complejo y peligroso, donde el poder, el interés y la ambición pueden provocar choques violentos y donde las controversias internacionales pueden resolverse pacíficamente con arreglo al derecho internacional. Es por esta razón que nuestras sociedades son cada vez más reacias a concebir el empleo de la fuerza o la amenaza de recurrir a ella como herramienta de política exterior para defender los intereses o la soberanía nacional. En este contexto, nuestro poder militar se convierte en irrelevante y nuestra capacidad disuasoria en inverosímil si carecemos de la voluntad de utilizar la fuerza o advertir de forma creíble que cualquier alteración del *statu quo*, por pequeña que sea, podrá motivar una respuesta clara y contundente. Junto con la desafección política, la explotación del juego democrático, la manipulación de las emociones o la explotación de los clivajes políticos, ideológicos o étnicos, esta falta de credibilidad de la disuasión está motivando la escalada de las actividades bajo el umbral del conflicto sin que Occidente pueda plantear ninguna réplica efectiva.

En el marco de las operaciones militares, la situación tampoco es mejor. La volubilidad de la opinión pública doméstica y la presión de la comunidad internacional, el pánico a las bajas propias y el temor a los daños colaterales, el sometimiento a unos usos y costumbres de la guerra restrictivos y anacrónicos, la ansiedad por los costes políticos y los efectos electorales de las operaciones, la exigencia de restringir su alcance, impacto y duración o la necesidad de emplear la fuerza de manera limitada y restrictiva son otros elementos que pueden ser explotados por los actores que se enfrentan contra un ejército occidental. La unión de todos estos factores ha contribuido a la construcción y popularización de lo híbrido.

Conclusiones

Lo híbrido ha experimentado un largo viaje conceptual desde sus orígenes hasta hoy en día. Heredera del concepto «guerra complejo-irregular», esta idea se popularizó tras el choque entre Israel y Hezbollah de 2006 para describir la integración de tácticas, técnicas y procedimientos a convencionales e irregulares, mezcladas con actos terroristas, propaganda y conexiones con el crimen organizado. Actualmente, lo híbrido es un concepto comodín que puede emplearse para explicar actividades encuadradas dentro de la tradicional concepción de guerra política, cualquier acción situada por debajo del umbral del conflicto e incluso para describir de forma interesada toda la gama de operaciones de influencia rusas en el exterior. A pesar de sus múltiples interpretaciones y la ampliación que ha experimentado el concepto, sí pueden establecerse continuidades en lo híbrido desde el nivel táctico al estratégico como forma de guerra política o en lo híbrido en todo el espectro del conflicto, desde la paz hasta la guerra abierta, con actividades de distinto perfil, huella o atribución.

Igualmente, gracias a su atractivo y fuerza expresiva, lo híbrido está permitiendo que el público no especializado comprenda la complejidad y multidimensionalidad de los riesgos y amenazas que pueden cernirse sobre sus sociedades. Muchas de ellas son de naturaleza difusa, difíciles de identificar, complejas de atribuir y buscan explotar las debilidades políticas, económicas, sociales o psicológicas del oponente. Sin embargo, la mayoría de estas amenazas ni son nuevas, ni tampoco lo son muchas de las tácticas, técnicas y procedimientos que emplean para lograr sus objetivos. En el siglo XXI lo que sí ha cambiado ha sido el área de exposición, las tecnologías, las debilidades, la capacidad de influencia o los vectores que pueden utilizarse para proyectar el poder, como puede ser el caso del ciberespacio, un nuevo dominio que permite maximizar el impacto informativo con un coste limitado y manteniendo una cierta denegabilidad.

No obstante, la calculada ambigüedad y el estiramiento conceptual que ha experimentado lo híbrido pueden comprometer su utilidad real hasta convertirlo en un concepto utilizado para describir cualquier actividad de influencia, de proyección del poder, de explotación social con vectores físicos, financieros, legales, informativos o psicológicos o la combinación de actividades militares regulares e irregulares. Tampoco debemos olvidar que lo híbrido no es propiedad del Kremlin, que lo híbrido es también consustancial en la cultura estratégica china y que cualquier actor –aliado, neutral o adversario– también puede hacer «cosas» híbridas para proyectar su influencia y mejorar su posición relativa en el mundo actual.

BIBLIOGRAFÍA

– COLOM, Guillem. «La Doctrina Gerasimov y el pensamiento estratégico ruso contemporáneo». *Ejército*. Diciembre 2018, n.º 933, pp. 30-37.

– COLOM, Guillem. «El nuevo rostro de la guerra, los conflictos híbridos», en REQUENA, Miguel (ed.). *Luces y sombras de la seguridad internacional en los albores del siglo xx*. Madrid: IUGM, 2010, pp, 55-64.

– COMISIÓN EUROPEA. *A Europe that protects: Countering Hybrid Threats*, Bruselas: UE, 2018.

– DEPARTMENT OF DEFENSE. *National Defense Strategy of the United States of America*. Washington DC: GPO, 2005.

– GERASIMOV, Valeri. «Cennost' nauki v predvidenii». *Voenno-promyšlennyj kur'er*. Febrero 2013, vol. 8, n.º 476, s.n.

– GERASIMOV, Valeri. «Vektory razvitija voennoj strategii». *Krasnaja zvezda*, 4 de marzo de 2019.

– HEICKERO, Roland. *Emerging cyber threats and Russian Views on Information Warfare and Information Operations*. Estocolmo: FOI.

– HOFFMAN, Frank. *Conflict in the 21st Century: The rise of hybrid wars*. Arlington: Potomac Institute for Policy Studies, 2007.

– KORYBKO, Andrew. *Hybrid Wars: The Indirect Adaptive Approach to Regime Change*. Moscú: People's Friendship University of Russia, 2015.

– THOMAS, Timothy. *Thinking like a Russian Officer: Basic Factors and Contemporary Thinking on the Nature of War*. Fort Leavenworth: FMSO, 2016.

IDENTIFICACIÓN MIGRANTES. APLICACIÓN ANTROPOLOGÍA FORENSE

MANUEL PARTIDO NAVADIJO
Criminólogo por la Universidad de Sevilla. Antropólogo y doctorando en Biomedicina por la Universidad de Granada

Resumen

En las últimas décadas, el fenómeno migratorio se ha visto agravado por la aparición de redes de tráfico de migrantes que se aprovechan de la desesperación de los migrantes por una vida mejor. En este sentido, un grave problema es la falta de identificación de estos migrantes, en muchos casos menores de edad que quedan solos en las calles hasta que son tutelados por la Administración, siendo necesaria una estimación de edad previa que determine su mayoría o minoría de edad. Otro grave problema derivado de esta falta de identificación es la imposibilidad de poder identificar a los migrantes fallecidos, imposibilitando por tanto su repatriación y devolución a sus familiares.

En este trabajo se exponen los métodos antropológicos utilizados para la estimación de la edad de menores extranjeros no acompañados, así como la utilidad de la antropología física y forense para la identificación de migrantes fallecidos, dadas las limitaciones de los métodos tradicionales de identificación en casos de cadáveres irreconocibles o en proceso de descomposición.

Palabras clave: migraciones, menores de edad, identificación, antropología forense.

Abstract

In the last decades, the migratory phenomenon has been aggravated by the appearance of networks of smuggling of migrants that take advantage of the desperation of these migrants for a better life. In this sense, a serious problem is the lack of identification of these migrants, in many cases, underage migrants that remain alone in the streets

until they are overseen by the Administration, being required a previous age estimation that determines their adulthood or underage status. Another serious problem derived from this lack of identification is the impossibility of identifying deceased migrants, thus precluding their repatriation and the delivery of the mortal remains to their families.

This work will expose the anthropological methods utilised for the age estimation of underage and unaccompanied migrants, as well as the utility of Physical and Forensic Anthropology for the identification of deceased migrants, given the limitations of the traditional identification methods in cases of unrecognizable corpses or in decomposition process.

Keywords: migrations, underage, identification, Forensic Anthropology.

INTRODUCCIÓN

Según el Diccionario de la Real Academia Española, podemos definir el concepto de «migración» como el «desplazamiento geográfico de individuos o grupos, generalmente por causas económicas o sociales» (Diccionario de la Real Academia Española: https://dle.rae.es/?id=PE38JXc Última consulta: 19/07/19). Como tal, dentro del concepto de migración, hemos de discernir dos conceptos diferentes:

Inmigración: tomando como referencia el país receptor de migrantes, llegada de migrantes a un nuevo destino.

Emigración: tomando como referencia el país emisor de migrantes, salida de migrantes hacia un nuevo destino.

Las causas de las migraciones son múltiples y complejas, pudiendo ser por motivos económicos, gobiernos, por falta de trabajo, por motivos bélicos, etc. Históricamente, las migraciones han sido y son una constante en la sociedad. Basta con retroceder hacia las primeras sociedades, originarias del ser humano, en las que las migraciones eran una condición natural de vida, dado su estatus de nómadas. Durante siglos, las personas han abandonado sus hogares en busca de una vida mejor. En la última década, el proceso de globalización ha conllevado un aumento sin precedentes de la migración de los países menos desarrollados de Asia, África, América Latina y Europa oriental hacia Europa occidental, Australia y Norteamérica [1].

Sin embargo, de igual manera que los flujos migratorios han ido en aumento, también lo han ido haciendo las redes de tráfico ilegal de migrantes, entendiéndose por tráfico de migrantes la «facilitación de la entrada ilegal de una persona en un Estado Parte del cual dicha persona no sea nacional o residente permanente con el fin de obtener, directa o indirectamente, un beneficio financiero u otro beneficio de orden material» [2]. De hecho, de acuerdo con información del Ministerio de Exteriores [3], en la Unión Europea, el número de ciudadanos no comunitarios legales supera los 25 millones, habiendo a su vez unos 10 millones de indocumentados. Según la misma fuente, la llegada de inmigrantes ilegales a las costas españolas en 2011 aumentó casi un 50 por ciento respecto a 2010 —de 3.562 a 5.443 personas—, lo que rompió la tendencia descendente que se venía produciendo desde hacía cuatro años [4] [5].

En este sentido, para tratar de combatir la lacra que supone el tráfico de migrantes y luchar contra ella, el 15 de noviembre de 2000 se creó en Nueva York el Protocolo contra el Tráfico Ilícito de Migrantes por tierra, mar y aire [2], ratificado por España el 25 de noviembre de 2003, con el objeto de prevenir y combatir efectivamente el tráfico ilícito de migrantes por tierra, mar y aire, con un enfoque amplio e internacional que conlleve la cooperación y el intercambio de información, dada la necesidad de dar un trato humano a los migrantes y de proteger plenamente sus derechos humanos ante la ausencia hasta el momento de un instrumento universal que aborde todos los aspectos del tráfico de migrantes.

Según el Departamento de Seguridad Nacional de España, en su «Informe Global de Tráfico de Migrantes 2018» [4], en 2016, el tráfico de migrantes afectó por lo menos a 2,5 millones de personas. Además, ninguna región del mundo estuvo a salvo de esa lucrativa violación de las leyes y los derechos de las personas, que generó ganancias de 7.000 millones de dólares para los traficantes, una cantidad equiparable a la suma de los presupuestos para ayuda humanitaria global de Estados Unidos y la Unión Europea durante el mismo año [3].

Asimismo, el primer Estudio Global sobre el Tráfico Ilícito de Migrantes de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) [6] muestra cómo las redes del tráfico de migrantes están desarrollando organizaciones con capacidades cada vez más sofisticadas y el uso de rutas más peligrosas para eludir los controles fronterizos, mientras aportan una mala información o desinforman a los migrantes sobre las condiciones de viaje.

Evidentemente, existe una gran cantidad de riesgos que corren los migrantes en manos de traficantes, detectándose en casi todas las rutas asesinatos, malos tratos, violaciones, extorsiones, etc. Asimismo, destacan los riesgos que afectan a su propia vida, como las muertes por ahogamiento, asfixia, accidentes o deshidratación. De acuerdo con la Organización Internacional para las Migraciones (OIM) [1], en la actualidad el Mediterráneo es la ruta donde se registran más fallecimientos con la mitad del total de muertes de migrantes. Ello ha convertido al Mediterráneo en un gran cementerio submarino, en ocasiones ante la impasibilidad de organizaciones gubernamentales internacionales.

A este problema se le suma el de la identificación: en la mayoría de los casos de inmigración ilegal, estos migrantes carecen de documentos de identidad, lo cual dificulta muchísimo las labores de identificación, especialmente en casos de inmigrantes fallecidos, y más aún cuando ha transcurrido un tiempo desde la muerte y los restos cadavéricos no se encuentran en condiciones de ser identificados por los métodos tradicionales, siendo necesario el auxilio de otros métodos [7].

INTERVENCIÓN CON MIGRANTES MENORES DE EDAD

Dentro del dramatismo que supone el tráfico de migrantes, esto se exacerba cuando hablamos de migrantes menores de edad. La definición de menor de edad no acompañado (conocidos popularmente como MENAS) aparece en la Resolución del Consejo de

Europa del 26 de junio de 1997, siendo la siguiente: «menores de 18 años, nacionales de terceros países, que llegan a territorio español sin ir acompañados de un adulto responsable de ellos, ya sea legalmente o con arreglo a los usos y costumbres, en tanto no se encuentran efectivamente bajo el cuidado de un adulto responsable» [8].

De acuerdo con Bravo y Santos [8], la llegada de un menor migrante no acompañado a cualquier territorio del Estado español supone la asunción de su tutela por parte de las autoridades locales, responsables de la protección a la infancia en cada territorio, según lo estipulado en esta definición, así como en los principios de la Convención sobre Derechos del Niño [9] y en las leyes nacionales de protección de la infancia.

No se sabe con exactitud la cifra exacta de menores extranjeros no acompañados en nuestro país. Bravo y Santos [8] apuntan a la falta de coordinación entre las comunidades autónomas y a la ausencia de rigor en el cálculo de estadísticas como causas fundamentales de esta imprecisión en la cifra de menores. No obstante, los datos se recogen anualmente en la Memoria de la Fiscalía, existiendo un Registro de Menores Extranjeros no Acompañados, donde se les inscribe cuando su edad no deja lugar a dudas [10]. Por arrojar una cifra, la Memoria de la Fiscalía del año 2016, correspondiente al ejercicio de 2015, indicaba la existencia de 3.660 menores, mientras que en octubre de 2017 la cifra subía hasta 5.380 inscritos en el registro [8].

De acuerdo con el Ministerio del Interior [11], cuando las Fuerzas y Cuerpos de Seguridad del Estado localizan a un menor extranjero cuya minoría de edad se puede establecer con seguridad por su documentación o su apariencia física, este será puesto a disposición de la comunidad autónoma pertinente, que asumirá su tutela. Si, por el contrario, su minoría de edad no pudiese ser establecida con certeza, será entregado a los servicios de protección de menores competentes, para que le presten la atención inmediata que precise, poniéndose tal hecho en conocimiento del Ministerio Fiscal, que dispondrá, en el plazo más breve posible, la estimación de su edad, para lo que deberán colaborar las instituciones sanitarias oportunas que, con carácter prioritario y urgente, realizarán las pruebas necesarias. Determinada la edad, si se tratase de un menor, el Ministerio Fiscal decidirá su puesta a disposición de los servicios competentes de protección de menores, dándose conocimiento de ello al delegado o subdelegado del Gobierno correspondiente.

Lógicamente, la estimación de la edad del menor extranjero es algo fundamental, en tanto que podrá ser penalmente responsable o no dependiendo de su edad, tal y como dispone el art. 19 del Código Penal. Las técnicas disponibles para la estimación de la edad en torno a los 18 años son variadas, centrándose fundamentalmente en métodos radiográficos, precisando del auxilio de médicos y antropólogos físicos.

ESTIMACIÓN DE LA EDAD EN MENORES DE EDAD

Como se ha señalado anteriormente, la estimación de la edad resulta esencial para el tratamiento jurídico de los menores migrantes y su efectiva tutela y protección por parte de las instituciones. Asimismo, es fundamental de cara a su tratamiento jurídico en caso de la comisión de delitos, siguiendo lo estipulado en el art. 19 del Código Penal,

que establece que los menores de 18 años no son penalmente responsables salvo lo que dispongan las leyes penales de menores.

En este sentido, se han desarrollado diferentes metodologías para la estimación de la edad en torno a los 18 años. El problema fundamental al que se enfrentan estas técnicas es la variabilidad interpersonal a la hora del desarrollo y maduración esquelética. De acuerdo con Prieto, *et al*. [12], como los individuos se desarrollan según patrones diferentes, en función de la variabilidad interindividual dependiente de multitud de factores genéticos y ambientales (herencia, nutrición, estado de salud, raza, nivel socioeconómico, factores climáticos, ejercicio, etc.), todos los individuos de una determinada edad cronológica no se corresponden necesariamente con el mismo estadio de maduración.

En Europa, con el propósito de unificar las metodologías de estimación etaria, el Arbeitsgemeinschaft für Forensische Altersdiagnostik der Deutschen Gesellschaft für Rechtsmedizin (AGFAD) publicó en el año 2000 [13] sus guías para las estimaciones forenses de la edad cronológica sobre individuos vivos. Estas guías recomendaban las siguientes técnicas para la determinación de la mayoría o minoría de edad [13]:

1. Examen físico: obtención de medidas antropométricas e identificación de patologías que puedan alterar el desarrollo madurativo.
2. Examen radiográfico de la mano izquierda.
3. Examen externo de la dentición y radiografía dental.
4. Examen radiográfico de la región cervical.

Las variables antropométricas han resultado ser poco útiles como factores de estimación de la edad, si bien pueden ser útiles como factores sugestivos de la existencia de condiciones patológicas que pueden provocar una madurez precoz o retardada y, con ello, alterar significativamente la interpretación de los resultados [14].

Por su parte, la estimación de la edad utilizando análisis de desarrollo dental resulta ser más sencillo durante la etapa de crecimiento, recomendándose el realizar una ortopantomografía, que permita observar el grado de desarrollo y osificación de los diferentes gérmenes dentales. Esto se complica durante la adolescencia, puesto que la única pieza que continúa en desarrollo es el tercer molar o muela del juicio. En este caso, el examen externo, centrado en la germinación de esta pieza dental, no es recomendable dada su alta imprecisión, por su frecuente ausencia congénita, malformación o extracción. Resulta, pues, más recomendable valorar la evolución de su maduración y osificación mediante radiografía, al ser un fenómeno más estable dentro de su alta variabilidad. Para ello, los métodos más recomendados son el método gráfico de Demirjian [15], o algunos numéricos como el de Kullman. Con todo, se apunta que el análisis dental no permite asegurar por sí solo con un grado de fiabilidad suficiente la mayoría o minoría de edad del sujeto.

Con respecto al análisis radiográfico de los huesos, los estudios más difundidos son aquellos centrados en el análisis de la muñeca y la mano. Los atlas más difundidos y utilizados con este propósito son: Greulich-Pyle, TW2 (Tanner-Whitehouse modificado) y Hernández. En este sentido, la recomendación unánime se centra en el análisis del carpo de la mano izquierda. No obstante, la interpretación de los resultados ha de ser adap-

tada a las características de la población objeto de estudio, en tanto que pueden darse factores, no del todo definidos, que alteren la estimación [12].

Finalmente, en aquellos casos dudosos con los estudios anteriormente recomendados y en los casos en los que se solicitan estimaciones de edad entre los 18 y 21 años de edad, las «Recomendaciones sobre Métodos de Estimación Forense de la edad de los Menores Extranjeros No Acompañados en el Entorno Judicial», elaboradas por un comité de expertos designados por la Defensora del Pueblo en 2010 [16], recomiendan la aplicación de los siguientes medios diagnósticos: estudio radiográfico de la extremidad proximal de la clavícula y estudio de tomografía computerizada de la extremidad proximal de la clavícula mediante método multicorte fino.

En resumen, el método más recomendado por su mayor fiabilidad es el análisis radiográfico del carpo de la mano izquierda, seguido del análisis dental del tercer molar [14], mientras que el análisis de variables antropométricas carece de eficacia como método de estimación de la edad, si bien es necesario para realizar una adecuada descripción del aspecto externo del sujeto y para constatar la posible presencia de factores patológicos causantes de una maduración precoz o retardada en caso de discrepancias. Se recomienda la aplicación de las guías del Arbeitsgemeinschaft für Forensische Altersdiagnostik der Deutschen Gesellschaft für Rechtsmedizin (AGFAD) [13].

IDENTIFICACIÓN DE FALLECIDOS

La identificación de migrantes se torna más difícil cuando se trata de migrantes fallecidos. Ya se ha señalado con anterioridad que los migrantes en manos de redes de tráfico de migrantes se exponen a riesgos tales como las agresiones o asesinatos, o muertes por deshidratación o ahogamiento, entre otras causas [6]. En muchas ocasiones, los cadáveres de estos migrantes son abandonados, lo cual causa que el cuerpo se descomponga y que resulte mucho más difícil identificarlo para repatriarlo a su país de origen y entregar los restos mortales a su familia. Sumado a ello, el hecho de que en muchas ocasiones no porten documentación lo hace aún más complicado, por no decir casi imposible.

Si bien el fallecimiento a gran escala de migrantes no se amolda a la definición de gran catástrofe proporcionada por la Oficina de las Naciones Unidas para la Reducción del Riesgo de Desastres (UNISDR) [17], sí podemos considerarla una catástrofe a nivel humanitario, dada la gran pérdida de vidas que se producen anualmente y la dificultad de la sociedad en la gestión de los fallecidos. En este caso, podríamos considerarla como una catástrofe abierta según el criterio de Interpol [18]: una catástrofe en la que no se posee ningún tipo de listado de control previo de las víctimas, como por ejemplo el 11S o el 11M, y por lo tanto no hay medios para contactar con los familiares para efectuar la identificación de los cuerpos, dificultando con ello las labores de identificación y repatriación.

En los casos en los que el cadáver se encuentra bien conservado, se recurrirá fundamentalmente a los métodos más comunes, como la identificación por huellas dactilares, métodos odontológicos o reconocimiento facial. Es en los casos en los que el cadáver

se encuentre descompuesto o incluso esqueletizado cuando se ha de recurrir en primer lugar al análisis antropológico de los restos (determinación del sexo, estimación de la edad, de la talla, del perfil poblacional, análisis de patologías…) para acotar la horquilla de potenciales víctimas y posteriormente recurrir a técnicas confirmatorias como el análisis genético [18].

En España, se recomienda el seguimiento de las Recomendaciones en Antropología Forense [19], dictadas por la Asociación Española de Antropología y Odontología Forense (AEAOF). En estas recomendaciones, cuyos autores conciben más como un texto abierto a futuras aportaciones y modificaciones, siguiendo el avance de la disciplina, se recogen las pautas básicas para el levantamiento de los restos óseos, el estudio en laboratorio, así como la estimación del sexo, de la edad, de la talla y de la ascendencia; también se recogen recomendaciones para los diferentes criterios de identificación, así como la toma de datos antropométricos y la elaboración del informe antropológico final. Con todo, la antropología forense tampoco hace milagros, encontrándose con el gran escollo de la ausencia de documentación o registros previos con los que comparar los datos *post-mortem* y poder efectuar una identificación de los restos. Sin parientes con quien comparar, o sin documentación previa, métodos tan útiles como el ADN presentan utilidad cero, ya que únicamente son métodos confirmatorios.

- Interpol diferencia los posibles resultados de la identificación de la siguiente manera [18]:
- Identificación inequívoca. Certeza absoluta de que los datos ante y post *mortem* pertenecen a la misma persona.
- Identificación probable. Correspondencias entre algunos datos concretos ante y post *mortem*, pero unos u otros, o ambos, son insuficientes.
- Identificación posible. Nada permite negar la identificación, pero los datos ante *mortem*, post *mortem*, o ambos, son insuficientes.
- Identidad descartada. Los datos ante y post *mortem* pertenecen a personas distintas.
- Comparación imposible.

Tristemente, son bastantes los casos en que no se logra la identificación por la imposibilidad de comparación de datos, pero los esfuerzos por trabajar en nuevas técnicas de identificación son numerosos, precisando obviamente un alto grado de colaboración internacional para ello.

CONCLUSIONES

Una de las más graves lacras a nivel global es el tráfico de migrantes, que cada año conlleva numerosas muertes de migrantes, ya sea por causas accidentales o a manos de traficantes de personas.

Para tratar de combatir el tráfico ilícito de migrantes, se desarrolló el Protocolo contra el Tráfico Ilícito de Migrantes por tierra, mar y aire, hecho en Nueva York el 15 de noviembre de 2000, y ratificado por España el 25 de noviembre de 2003. Sin embargo,

el protocolo no hace referencia en ningún momento a la identificación de migrantes, ni vivos ni mucho menos fallecidos.

Un problema aún mayor supone el de los menores extranjeros no acompañados, primero por su indocumentación, y segundo por su mayor vulnerabilidad como menores de edad.

En este sentido, la Administración de Justicia habrá de requerir el auxilio de los institutos de medicina legal para la determinación de la mayoría de edad de los posibles menores. La estimación de la edad se realizará fundamentalmente mediante radiografías del carpo izquierdo y el estado de maduración y osificación dental, y precisará de médicos forenses y antropólogos físicos, en tanto que las técnicas no son 100 % infalibles.

Más complicado es el caso de la identificación de migrantes fallecidos, especialmente cuando el cuerpo se encuentra descompuesto. En estos casos, las técnicas convencionales presentan una utilidad mucho más reducida, precisándose el auxilio de antropólogos forenses. Estos profesionales utilizarán, preferentemente, las Recomendaciones en Antropología Forense, dictadas en 2013 por la Asociación Española de Antropología y Odontología Forense. Con todo, ante la ausencia de datos *antemortem* para comparar, la identificación puede dificultarse enormemente, llegando incluso a no poder realizarse, si bien la antropología forense resultará, sin duda, de gran ayuda para la acotación del perfil biológico de la víctima y la reducción de potenciales candidatos para la identificación.

Pese a estas vicisitudes, los esfuerzos para mejorar las técnicas de identificación son constantes, precisando de la colaboración internacional para ello.

6. BIBLIOGRAFÍA

– INTERPOL. «Tráfico Ilícito de migrantes - problemática». Interpol. [En línea]. Disponible en https://www.interpol.int/es/Delitos/Trafico-ilicito-de- migrantes/Trafico-ilicito-de-migrantes-problematica. [Último acceso: 22/ 07/2019].

– ONU, Asamblea General. «Protocolo contra el tráfico ilícito de migrantes por tierra, mar y aire, que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional». 15/11/2000. [En línea]. Dispinible en https://www.boe.es/buscar/doc.php?id=BOE-A-2003- 22593. [Último acceso: 22/07/2019].

– MINISTERIO DE ASUNTOS EXTERIORES. «Flujos migratorios». Gobierno de España. [En línea]. Disponible en http://www.exteriores.gob.es/Portal/es/PoliticaExteriorCooperacion/Globali zacionOportunidadesRiesgos/Paginas/FlujosMigratorios.aspx. [Último acceso: 22/07/2019].

– DEPARTAMENTO DE SEGURIDAD NACIONAL. «Informe global de tráfico de migrantes 2018». Gabinete de la Presidencia del Gobierno, Gobierno de España. [En línea]. Disponible en https://www.dsn.gob.es/es/actualidad/sala- prensa/informe-global-trafico-migrantes-2018. [Último acceso: 22/07/2019].

– DEPARTAMENTO DE SEGURIDAD NACIONAL. «Ordenación de flujos migratorios». Gabinete de la Presidencia del Gobierno, Gobierno de España. [En línea]. Disponible en https://www.dsn.gob.es/es/sistema-seguridad- nacional/qu%C3%A9-es-seguridad-nacional/%C3%A1mbitos-seguridad- nacional/ordenaci%C3%B3n-flujos. [Último acceso: 22/07/2019].

– UNITED NATIONS OFFICE ON DRUGS AND CRIME. «Tráfico ilícito de migrantes: la dura búsqueda de una vida mejor». Naciones Unidas. [En línea]. Disponible en https://www.unodc.org/toc/es/crimes/migrant-smuggling.html. [Último acceso: 22/07/2019].

– PARTIDO NAVADIJO, M. «La identificación de restos humanos en conflictos armados: el efectivo cumplimiento de los arts. 15 a 17 del I Convenio de Ginebra». *Los retos de Europa. Respuesta integral ante riesgos compartidos*. Madrid: Secretaría General Técnica, Ministerio de Defensa, 2019.

– BRAVO, A. y SANTOS-GONZÁLEZ, I. «Menores extranjeros no acompañados en España: necesidades y modelos de intervención». *Psychosocial Intervention*, n.º 26. 2016, pp. 55-62.

– UNICEF. «Convención sobre los derechos del niño». 2006.

– LÁZARO GONZÁLEZ, I. «Menores extranjeros no acompañados. La situación en España». *Prolegómenos. Derechos y Valores,* vol. X, n.º 19. 2007, pp. 149-162.

– MINISTERIO DEL INTERIOR. «Menores extranjeros». Ministerio del Interior. 2013. [En línea]. Disponible en http://www.interior.gob.es/web/servicios-al- ciudadano/extranjeria/regimen-general/menores- extranjeros #Menores%20extranjeros%20no%20acompa%C3%B1ados. [Último acceso: 22/07/2019].

– PRIETO, y ABENZA, J. «Métodos para valorar la edad en el adolescente». *Revista Española de Medicina Legal* , vol. XXII, n.º 84. 1998, pp. 45-50.

– AGFAD. «Arbeitsgemeinschaft für Forensische Altersdiagnostik». [En línea]. Disponible en https://www.medizin.uni- muenster.de/en/rechtsmedizin/schmeling/agfad/recommendation/. [Último acceso: 22/07/2019].

– GARAMENDI P., y LANDA, M. «Estimación forense de la edad en torno a los 18 años. Revisión bibliográfica». *Cuadernos de Medicina Forense* , n.º 31. 2003, pp. 13-24.

– [DEMIRJIAN, A., GODSTEIN, L., y TANNER, J. «A new system of dental age assessment». *Human Biology*, n.º 42. 1973, pp. 211-227.

– [O. d. D. d. PUEBLO. «Recomendaciones sobre métodos de estimación forense de la edad de los menores extranjeros no acompañados en el entorno judicial». Madrid: Gobierno de España, 2010.

– ONU. «United Nations Office for Disaster Risk Reduction». ONU. [En línea]. Disponible en https://www.unisdr.org/. [Último acceso: 22/07/2019].

– INTERPOL. «Disaster Victim Identification Guide». Interpol Publications, 2009.

– SERRULLA, F. *Recomendaciones en antropología forense*. Ourense: Asociación Española de Antropología y Odontología Forense, 2013.

EL ESPACIO EUROPEO ANTE EL DESAFÍO DE LA DESINFORMACIÓN

FERNANDO MARTÍN CUBEL
Licenciado en Historia Moderna y Contemporánea Universidad de Zaragoza. Miembro investigador del SIP Zaragoza. Miembro expert del Observatorio de Paz, Seguridad y Defensa de la Universidad de Zaragoza. Analista del IEEE, de ESGLOBAL, de ARTICULO30.ORG. Profesor en la Fundación CAI de Zaragoza

«Ante todo estaba la certeza de que vivíamos en un mundo hermoso y justo, Y de que el hombre estaba por encima de todo, pues representaba la medida de todas las cosas»
Svetlana Alexiévich

INTRODUCCIÓN

La desinformación, al igual que la información de calidad y contrastada han estado —hasta muy reciente— en manos de unos pocos, la emisión procedía de unas pocas fuentes y se vehiculaba hacia muchos receptores —lectores de prensa, oyentes de radio,…— con escasa interactividad (tal vez las cartas al director o las llamadas a la radio). En el presente, todo ha cambiado, como bien indica Alfonso Marlos[1] «La sociedad de la información se ha transformado paulatinamente en una jungla en la que personas sin cualificación, sin formación o sin instrucción pueden erigirse en *influenciers* durante horas o días con efectos devastadores, colocándose en la privilegiada posición de actores con capacidad para producir materiales caseros y colgarlos en la Red, para obtener un impacto político que puede superar al de los medios convencionales, aprovechándose de un escenario de desintermediación, en el que los ciudadanos son a la vez productores y consumidores, objetos y sujetos, proveedores y usuarios…».

El imperante realismo político de décadas anteriores ha quedado desbordado por la proliferación y diversificación de actores, amenazas, circunstancias y desafíos. En estas nuevas amenazas como el cambio climático, la corrupción, la acción del narco global, entre otros, no cabe olvidar a los procedentes del ciberespacio, y con especial relevancia aquellos que causan un gran impacto en las opiniones públicas a través de la desinformación y de las noticias falsas. Las opiniones públicas se han convertido ya no en un sujeto activo o pasivo como sucedía hasta ahora, en realidad es el nuevo «campo de

---

[1] MARLOS, Alfonso. *Política de seguridad y defensa en la era de la posverdad. La Posverdad, Seguridad y defensa*. Cuadernos de Estrategia 197. IEEE. http://www.ieee.es/Galerias/fichero/cuadernos/CE_197.pdf.

batalla» en el que los actores estatales y no estatales pretenden enfrentarse y provocar una modificación en la percepción que las opiniones públicas tienen ante determinadas políticas públicas, caso de las relativas a la seguridad, política exterior, inmigración…, etc.

La comunicación, la información y el conocimiento se han convertido en los pilares básicos de nuestra sociedad, y son referentes en la reflexión de las nuevas narrativas estratégicas nacionales y globales de «sociedades de la información». Unido a ello, aparece la cuestión de la «reputación» en relación directa sobre qué información se maneja respecto a personas y organizaciones, un riesgo que ya es permanente. Es verdad, que hoy día siguen existiendo canales de difusión de gran fiabilidad así como fuentes muy reputadas que gracias al apoyo privado mantienen un alto nivel en la calidad de su información; sin embargo, junto a ellos se han desarrollado canales que son capaces de llegar a los ciudadanos y que son fuente de desinformación, de opacidad en sus fuentes, puntos de apoyo y modificación en las opiniones públicas (el denominado fenómeno *doxing*), y soporte de campañas como han sido: en el caso de la ultraderecha alemana, o a favor de la elección del actual presidente de Estados Unidos y sin olvidar el referéndum del Brexit.

La seguridad nacional comprometida en su lucha contra la desinformación

Quisiera iniciar esta parte del trabajo con el siguiente texto extraído de la Ciberestrategia de Seguridad Nacional de España de 2013: «El desarrollo de la tecnología de la información y comunicación ha generado un nuevo espacio de relación en el que la rapidez y facilidad de los intercambios de información y comunicaciones ha eliminado las barreras de distancia y tiempo. El ciberespacio, nombre por el que se designa el dominio global y dinámico impuesto por las infraestructuras de la información y de telecomunicaciones —incluida Internet—, las redes y los sistemas de información y de telecomunicaciones, han venido a difuminar fronteras, haciendo partícipe a usuarios de una globalización sin precedentes que propicia nuevas oportunidades, a la vez que comporta nuevos retos, riesgos y amenazas».

Evidentemente, entre las nuevas amenazas, riesgos y desafíos a los que las sociedades se enfrentan está la cuestión de la desinformación, realidad que no es nueva pero que alcanza a ser, una preocupación de primer orden. En el informe para España del Eurobarómetro[2] de otoño de 2018, se planteaba a los ciudadanos europeos todo un conjunto de cuestiones sobre la desinformación dentro del apartado QE 10[3]:

1 **Amenudo encuentra noticias o información que cree que distorsionan la realidad e incluso que son falsas**: cerca del 70 % de encuestados afirmaban que sí, siendo mayor en los encuestados españoles con un 79 %

[2] Eurobarómetro otoño 2018 para España. https://ec.europa.eu/spain/sites/spain/files/st90_-_report_repes_-_vf110219_limpia_.pdf.

[3] Ibíd.

2 **Le es fácil identificar las noticias o información que cree que distorsionan la realidad o que incluso son falsas**: en este caso, los encuestados europeos afirmaban que sí en un 58 %, mientras que los encuestados españoles solo alcanzaban al 52 %.
3 **La existencia de noticias o información que distorsionan la realidad o que incluso son falsas es un problema para la democracia en general**: los encuestados europeos afirmaban que sí en un 76 % siendo en el ejemplo español cercano al 83 %.

A través de estos datos, nuestros ciudadanos europeos reflejan una preocupación que es real y verosímil y al que bien es verdad que los Estados europeos y no europeos sino también la propia UE están empezando a tomar cartas en el asunto.

Algunos ejemplos de las implicaciones de la desinformación en las estrategias de seguridad nacional

Hasta el final del periodo de la Guerra Fría, dos parecían ser los espacios en los que se centraban las preocupaciones de la confrontación, por un lado la carrera espacial y por otro lado el desarrollo de la carrera armamentística nuclear. Junto a algún otro aspecto, estas realidades centraban la preocupación del relato estratégico de numerosas naciones así como de las dos grandes hiperpotencias caso de USA y URSS, «realismo político». Sin embargo, con la finalización del conflicto y sobre todo en el inicio de este nuevo milenio, la progresiva implantación de la denominada «sociedad digital» supone la aparición de nuevas amenazas, desafíos y riesgos, así como de oportunidades.

En los últimos relatos estratégicos de nacionales, la cuestión del impacto de la sociedad digital y del espacio ciber está ahora mismo muy presente, ya que gran parte de la actividad, movimientos de personas, ideas, productos, la propia actividad social de un país, las capacidades de crecimiento económico, entre otras cuestiones tienen una mayor presencia en la sociedad digital y , a su vez emergen desde la misma. Quisiera por ello, acercarme —aunque sea muy por encima— a algunas estrategias de seguridad nacional donde ya no solo se incluyen en el corazón mismo del análisis la ciberseguridad sino que va ganando espacio la cuestión de la desinformación y las falsas noticias.

Un primer ejemplo es Holanda[4], quien ha puesto en marcha su nueva estrategia de seguridad nacional denominada «Working Worldwide for the Security of the Netherlands. An Integrated International Security Strategy 2018-2022». En dicha estrategia se ha incorporado en su relato la preocupación de la disrupción digital, dedicando el capítulo 2 de la estrategia a dicha cuestión, destaca el punto *2.3 Aceleration of technological developments and hybrid conflicts,* en el que, por primera vez, la cuestión de la desinformación y el uso de recursos para influir en las opiniones públicas tiene un destacado papel. También, en la parte de la estrategia nacional holandesa dedicada

[4] Estrategia de Seguridad Nacional de Holanda. https://www.government.nl/documents/reports/2018/05/14/integrated-international-security-strategy-2018-2022.

a las cuestiones más urgentes, en su punto *3.3 Undesirable foreign interference and disruption,* la cuestión de la desinformación es una amenaza que se considera real, y dejando abierta la puerta a los diferentes tipos de actores que pueden provocar dicha desinformación en la opinión pública y en la sociedad holandesa pero también en terceros países, cuestión extraordinariamente interesante: «Some actors are trying to destabilise European and Dutch society in order to expand their own economic and political sphere of influence. These threats include disinformation disseminated by state actors, activities of international hackers' collectives, digital espionage and sabotage, as well as efforts to influence migrant communities in the Netherlands in pursuit of nationalist aims and undesirable foreign financing of religious institutions and places of worship. Undesirable foreign intervention in third countries also has an impact on Dutch society, by destabilising and eroding the rule of law in countries on the periphery of Europe». Otro ejemplo, es el caso sueco[5], cuya estrategia de seguridad nacional, *National Security Strategy* también incorpora dicha cuestión en su relato, entre los objetivos que dicha estrategia establece para seguir manteniendo la estabilidad y seguridad del país se sitúan la vigilancia y defensa de los mensajes e información que actores externos al país lanzan para generar desestabilización —y cómo no desinformación— en la opinión pública del país, en el capítulo denominado *Sweden aims to be an open and secure society for all* se señala esta idea cuando se afirma en el texto: «However, digitalisation also provides hostile actors with the opportunity to spread their message that challenges our fundamental values and the security of society. Managing these issues, while also safeguarding shared values and norms that form the basis of our society, is vital to promoting safety and security in the long term. Confidence in authorities and the media must be safeguarded, along with trust among citizens». La estrategia de seguridad nacional sueca apuesta en el capítulo *Our national interests*, por reforzar las infraestructuras de los sistemas de tecnología e información, en la existencia de un escenario de ciberseguridad y buena información en la sociedad, instituciones y empresas, que al igual que en el ejemplo holandés necesita de la cooperación dentro del espacio europeo. En el ejemplo español, dicha cuestión también tiene una gran importancia. En julio de 2018, el Consejo de Seguridad Nacional acuerda el procedimiento para la elaboración de un nuevo escenario que sustituyera la vigente Estrategia de Ciberseguridad Nacional de 2013, ya que no incluía el tratamiento de las noticias falsas, ya que en aquel momento las campañas de desinformación no constituían un riesgo consolidado. El secretario de Estado, director del Centro Nacional de Inteligencia, Félix Sanz, durante su comparecencia en la Comisión Mixta de Seguridad Nacional de febrero de 2019, diferenció la capacidad gubernamental para garantizar la seguridad informática de las elecciones de 2019 y las dificultades para hacer lo mismo con las *fake news* o acciones de influencia. En marzo de 2019, el Departamento de Seguridad Nacional hizo público el Informe Anual de Seguridad Nacional en el que se señalaba a las campañas de desinformación como uno de los peligros y amenazas más significativos para la seguridad de España. Este mismo mes se anunciaba la creación de un centro de operaciones que protegería de los ciberataques a la Administración General del Estado y de la desinformación al conjunto de la sociedad, así como de una unidad especializada.

---

[5] Estrategia de Seguridad Nacional de Suecia. National Strategy Security. https://www.government.se/information-material/2017/10/national-security-strategy/.

Actuación de la UE respecto al desafío de la desinformación

El 22 de febrero de 2018 tuvo lugar una reunión en el Centro de Estrategia Política Europea[6] entre expertos en el ámbito de la información, y como una iniciativa de la Comisión Europa, a quienes se les pidió su opinión respecto a cuestiones sobre el impacto de la desinformación para las democracias, dentro del espacio UE. En el mismo, se reconocía los serios problemas que podían generarse en las sociedades democráticas europeas un uso incontrolado de la desinformación, la responsabilidad que las plataformas de las redes sociales tienen en la exposición de dicha información, el efecto sobre las instituciones y las opiniones públicas, la generación de una mayor polarización en los discursos políticos y sociales que tiene una mayor tendencia a aceptar teorías conspiratorias y que sirven para retroalimentar sus discursos, y la labor para llevar a cabo una mejora en los acuerdos de las instituciones europeas con las compañías más reseñables en el ámbito de la «sociedad digital». Keir Giles[7] expresaba: «The first and most effective response to hostile subversive and destabilising activity is and always has been raising public awareness – and here the role of key leaders is absolutely crucial. Statements by senior figures like prime ministers and defence ministers recognising a state of conflict and the challenge have been shown in the front-line states to be an extremely powerful tool in empowering not only government but also society and media to take steps to protect themselves».

La UE inicia su actividad en este ámbito, en 2015, cuando y tras la reunión del Consejo Europeo de marzo crea el Grupo de Trabajo East StratCom[8] —aunque en 2018 es cuando cuenta con asignación presupuestaria a propuesta por el Parlamento Europeo, 1,1 millones de euros que le permite ser una realidad—, que estará dentro de la estructura del Servicio Europeo de Acción Exterior quien se encargará desde este momento en monitorizar toda la actividad respecto a la gestión y lucha de la nueva amenaza que ya supone en 2015 no solo las noticias falsas sino también, algo mucho más grave para la estabilidad de las sociedades europeas, como es la desinformación. ¿En qué dirección va a actuar UE? Por una parte, la detección, análisis de la desinformación; un incremento en la cooperación y acuerdos para una mejor respuesta a los desafíos de la desinformación; la implicación del sector privado; y, finalmente una mejora en las capacidades y resilencia de las sociedades[9].

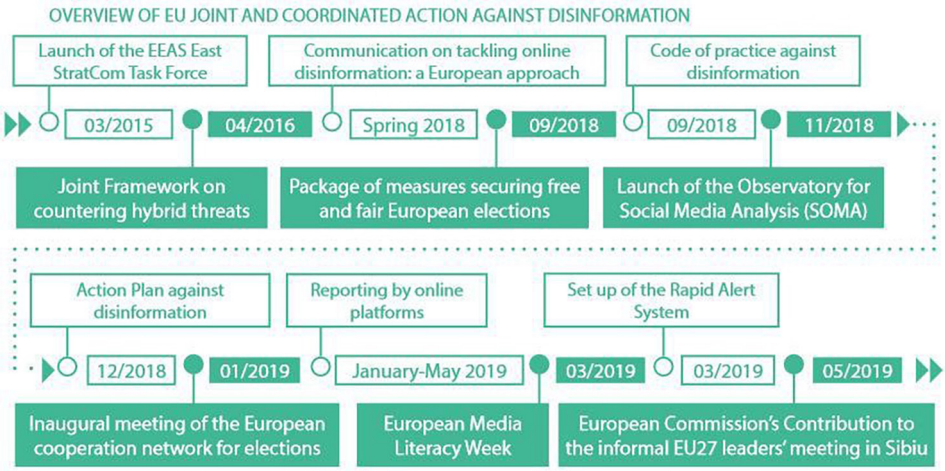
6 European Political Strategy Centre. High-Level Hearing, «Preserving Democracy in the Digital Age». https://reutersinstitute.politics.ox.ac.uk/risj-review/preserving-democracy-digital-age.

7 Ibíd.

8 East StratCom. https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-.

9 EEAS. «EU reports on progress in fighting disinformation». https://eeas.europa.eu/topics/countering-disinformation/64486/eu-reports-progress-fighting-disinformation_en.

En 2016, se adopta un marco común relativo a la lucha contra las amenazas híbridas, y al que sigue en 2018 la comunicación conjunta[10] sobre el aumento de la resilencia e impulso de las capacidades para hacer frente a las amenazas híbridas, entre ellas la desinformación. En abril de 2018, la Comisión Europea esboza un enfoque europeo y algunas herramientas para combatir la desinformación en la red como son el Código de Buenas Prácticas sobre Desinformación[11], reforzamiento de la alfabetización mediática, apoyo a los Estados miembros para asegurar la resilencia de las elecciones, generar una plataforma europea en línea segura sobre desinformación, apoyar una información plural y de calidad, entre otros. En octubre del mismo año, firman el código de buenas prácticas Facebook, Google, Twitter y Mozilla, así como las asociaciones comerciales que representan a las plataformas en línea, a la industria publicitaria y a los anunciantes. Además, Facebook, Google y Twitter se comprometieron a informar mensualmente sobre las medidas adoptadas antes de las elecciones al Parlamento Europeo de 2019. La Comisión, con apoyo del Grupo de Entidades Reguladoras Europeas para los Servicios de Comunicación Audiovisual (ERGA), supervisó de cerca los avances y publicó análisis mensuales junto con los informes presentados. El 22 de mayo, Microsoft se adhirió también al código de buenas prácticas y a todos los compromisos que contempla. Para que podamos ver los pasos que hasta ahora se han estado dando dentro de la UE la siguiente infografía[12]:



Entre enero y mayo de 2019, la Comisión Europea realiza una supervisión mensual de las medidas de las plataformas firmantes de los compromisos del Código, no hay que olvidar que las elecciones europeas se celebran este año, y la seguridad informativa se convierte en un pilar de acción de la UE. En marzo de 2019 se crea la plataforma tecnológica Rapid Alert System para reaccionar ante campañas de desinformación me-

[10] Comision Europea. Joint communication to the european. https://ec.europa.eu/commission/index_en.

[11] Destacan los primeros informes sobre el Código de Buenas Prácticas en enero de 2019. https://ec.europa.eu/digital-single-market/en/news/first-results-eu-code-practice-against-disinformation.

[12] EEAS. «EU reports on progress in fighting disinformation». https://eeas.europa.eu/topics/countering-disinformation/64486/eu-reports-progress-fighting-disinformation_en.

diante una vigilancia permanente de los contenidos publicados a través de los medios de comunicación y las redes sociales.

Finalmente, en las conclusiones del Consejo Europeo de 20 de junio de 2019[13], la cuestión de la desinformación tiene una especial atención, en las conclusiones se indica la preocupación de este desafío no solo en los procesos electorales, sino en la influencia que para la estabilidad de las sociedades democráticas tiene. Es situado dentro de las amenazas híbridas que puede sufrir cada Estado miembro y la UE, y aporta la siguiente recomendación de gran importancia que es la adopción de medidas conjuntas UE con los Estados miembros, así como la mejora de la cultura de seguridad en este ámbito **«**It invites the EU institutions, together with the Member States, to work on measures to enhance the resilience and improve the security culture or the EU against cyber and hybrid threats from outside the EU, and to better protect the EU's information and communication networks, and is decision-making processes, from malicious activities of all kinds**»**.

CONCLUSIONES

Carme Colomina, investigadora de CIDOB señala recientemente[14] **«**Los intentos de manipulación no tienen límites geográficos ni un único origen geográfico, ni un único origen. … La postverdad actual no responde únicamente a un desafío ideológico**»**. El riesgo para las sociedades y sus Estados es novedoso, los actuales relatos estratégicos corren el riesgo de estar desactualizados en días, en un ámbito como el digital donde la aceleración es un fenómeno esencial del mismo. Ya no solo la resilencia, sino las capacidades de adaptación a este nuevo desafío deben ser desarrollados por los propios Estados miembros de la UE sino que la actuación conjunta con las instituciones europeas se hace esencial, junto a la colaboración del sector privado, para adoptar las acciones y contar con los recursos necesarios, cada vez más, este ámbito de inseguridad tendrá una mayor presencia en las diferentes agendas de seguridad nacionales y de la propia UE, y se hace necesaria una especial reflexión y empeño en valorar el papel que tienen las opiniones públicas europeas en estos nuevos riesgos y amenazas.

---

[13] European Council. Council of the EU. «European Council conclusions on the MFF, climate change, disinformation and hybrid threats, external relations, enlargement and the European Semester, 20 June 2019». https://www.consilium.europa.eu/en/press/press-releases/2019/06/20/european-council-conclusions-20-june-2019/.

[14] COLOMINA, Carme. «La desinformación de nueva generación». https://www.cidob.org/es/articulos/anuario_internacional_cidob/2019/la_desinformacion_de_nueva_generacion.

LA SUSTRACCIÓN DE DATOS *CONTACTLESS* Y SU UTILIZACIÓN EN LAS *DEEP WEB* Y *DARK WEB*

SARA CASANS GABASA
Alumna 5.º curso de la Academia de la Guardia Civil. Graduada en Ingeniería de la Seguridad del Centro Universitario de la Guardia Civil

Resumen: el avance de las nuevas tecnologías en el sector financiero, y, concretamente, en las tarjetas bancarias, ha provocado importantes cambios en la forma de cometer actividades delictivas. Por ello, la Guardia Civil y otros cuerpos policiales, en el ejercicio de proteger los derechos y deberes de los ciudadanos, se encargan de trabajar de forma cooperada para evitar que tales comportamientos delictivos transgredan el marco legal que los regula.

Con el presente trabajo, se estudian una serie de conductas criminales concretas —en las que se utiliza la tecnología *contactless*, la cual permite una comunicación inalámbrica entre dispositivos— y su tipificación según el marco normativo vigente en cada momento. Además, a partir de estos supuestos, se pretende comprobar si la legislación actual cuenta con las herramientas jurídico-penales necesarias para sancionar las diferentes modalidades de crímenes que surgen, o, si, por el contrario, debe tomarse alguna medida correctiva en este ámbito.

Palabras clave: conductas delictivas, tecnología *contactless*, *Dark Web*, cibercriminal, ciberderecho.

INTRODUCCIÓN

La psiquiatría forense entiende una conducta delictiva como aquella que transgrede las normas dictadas en la sociedad en la que un individuo se desarrolla, es decir, que viola las reglas sociales o va contra los demás. El resultado de estas conductas se conoce como delito y queda definido como un comporta-

miento penalmente punible y antijurídico, que tiene señalada en el Código Penal una pena[1].

El término anglosajón *contactless* hace referencia a la tecnología de comunicación que se produce sin contacto físico entre dispositivos. En este trabajo se hará referencia al pago con tarjetas bancarias *contactless,* las cuales permiten una comunicación inalámbrica entre terminales, mediante el sistema Near Field Communication –NFC. Además, se estudiarán diferentes comportamientos ilícitos que pueden producirse por un mal uso de estas.

La Guardia Civil y otros cuerpos policiales serán quienes se encarguen de «proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana […]»[2]. Para ello, estos cuerpos deberán trabajar en constante armonía. Además, para poder sancionar las conductas antijurídicas surgidas, deberá producirse una adaptación legislativa a la sociedad de cada momento, la cual avanza en base al desarrollo de las tecnologías de la información y comunicación –TIC.

De este modo, el objetivo de la presente investigación es, partiendo del conocimiento de las conductas delictivas que pueden surgir de la utilización de la tecnología *contactless*, evaluar si nuestra legislación jurídico-penal cuenta con las herramientas suficientes en lo relativo a la tipificación y sanción de estos ilícitos.

EVOLUCIÓN DE LAS TARJETAS BANCARIAS

Para llevar a cabo procesos de compra existe una gran variedad de métodos de pago que han ido evolucionando a lo largo de la historia. Entre estas formas de pago, se encuentran las tarjetas bancarias. Estas surgieron en el siglo XX y se han desarrollado paralelamente a las TIC. Las primeras tarjetas eran documentos de papel o plástico que incorporaban escasas medidas de seguridad. Con el fin de convertir estas tarjetas en medios de pago más seguros, los datos del titular que contenían fueron almacenados y protegidos en una banda magnética. No obstante, estas medidas tampoco fueron totalmente efectivas y, dadas sus vulnerabilidades, fueron sustituidas por las conocidas *smartcards*[3]. Estas protegen los datos del titular almacenándolos en un elemento de seguridad, un chip electrónico. De esta manera, para poder realizar operaciones de pago, se debe introducir un número secreto –PIN (Personal Identification Number). Así, se impiden algunas actuaciones ilícitas como falsificar la firma del titular. A pesar de ello, estas tarjetas inteligentes tampoco están exentas de riesgos, de modo que, para disminuir la probabilidad de clonado —entre otros ilícitos—, surgieron las tarjetas *contactless*. Estas también incluyen el chip electrónico como elemento seguro, pero sustituyen el interfaz de comunicación físico por una comunicación inalámbrica, a través de NFC.

---

[1] MORE DAVIS, Ana Lucía. «Conducta delictiva y factores». https://es.slideshare.net/AnaluciaMoreDavis/conducta-delictiva-y-factores, 19 de mayo 2014, diapositiva 3.

[2] Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad. (*BOE* n.º 63, de 14 de marzo de 1986).

[3] *Smartcard*: término que significa «tarjeta inteligente».

SUSTRACCIÓN DE LOS DATOS EMITIDOS POR UNA TARJETA *CONTACTLESS* Y SU COMERCIALIZACIÓN EN LA *DEEP WEB* Y *DARK WEB*

Al mismo tiempo que evolucionan las tarjetas bancarias, el modo de delinquir en el sector económico y financiero también lo hace. El incremento del uso de Internet y las carteras virtuales como medio de pago ha supuesto un aumento de delitos tradicionales, aunque cometidos siguiendo otro *modus operandi*[4]. Son los llamados ciberdelitos[5]. Para llevar a cabo la práctica de estos, los delincuentes hacen uso de las TIC, equipos informáticos y diferentes partes de Internet.

La captación de datos de las tarjetas *contactless*

Podemos diferenciar algunos métodos fraudulentos a los que los usuarios del *contactless* quedan expuestos. Entre ellos, encontramos técnicas de *eavesdropping*[6], modificación del contenido de los paquetes transmitidos de forma inalámbrica o ataques de retransmisión. En las técnicas de *eavesdropping*, el cibercriminal intercepta los datos intercambiados entre un datáfono y la tarjeta, para usarlos, posteriormente, en beneficio propio. Esta monitorización queda limitada por la distancia —aproximadamente 10 centímetros—. Un tipo de «escucha» es el *hawking* o intrusión informática, que consiste en «comportamientos de acceso o interferencia no autorizados, de forma subrepticia, a un sistema informático o red de comunicaciones y al uso de los mismos sin autorización»[7]. El llevar a cabo este tipo de conducta podría castigarse, pues se atenta contra el derecho a la «intimidad informática»[8], evadiendo para ello las medidas de seguridad del protocolo NFC.

En cuanto a la modificación del contenido de los paquetes intercambiados, podemos diferenciar prácticas de inserción de nueva información, modificación de la ya existente o denegación del servicio. En estos casos, además de producirse una escucha pasiva, también se causan daños informáticos, lo que se conoce como *cracking*. De esta forma, se puede afirmar que el delincuente atentaría tanto contra la disponibilidad como la integridad de los sistemas. Por ello, lo correcto sería hacer referencia a la obstrucción, interrupción de un sistema informático o prácticas que facilitan la comisión de un ilícito —actividades también incardinadas en el CP.

Finalmente, los ataques de retransmisión o *relay* son fraudes en tiempo real en los que se rompe el principio de proximidad de la comunicación NFC. En ellos, se vincula la tarjeta «víctima», el terminal y el ciberdelincuente a una distancia superior a los 10 centímetros permitidos por esta tecnología. Para ello, el atacante utiliza, por un lado, un dispositivo que emula ser la tarjeta e interactúa así con el datáfono; y, por otro, un elemento

---

4 *Modus operandi*: expresión que significa «modo de operar».

5 NATIONALE NEDERLANDEN. «El dinero del siglo XXI: así han cambiado nuestras formas de pago». https://www.segurosdetuatu.es/posts/el-dinero-del-siglo-xxi-asi-han-cambiado-nuestras-formas-de-pago. 3 de septiembre 2015.

6 Técnicas de *eavesdropping*: métodos de «escucha» usados por el delincuente, sin que la víctima sea consciente de ello.

7 MORÓN LERMA, Esther.

8 Intimidad informática: derecho positivo, con una proyección social, dado que afirma la propia libertad y limita el poder informático.

que emula ser el datáfono e interactúa con la tarjeta. Así, entre ellos, se envían los datos que reciben el lector y la tarjeta.

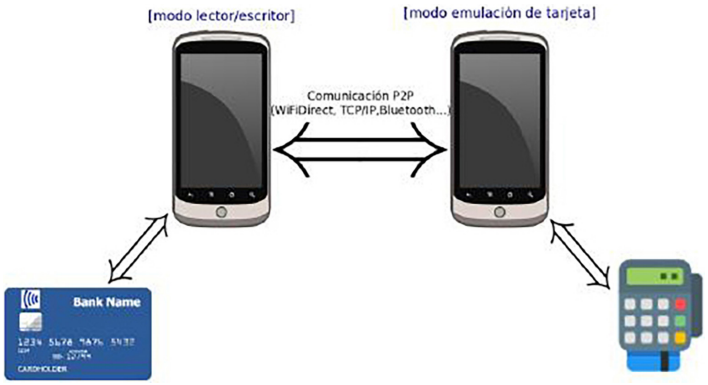


Ilustración 4: esquema de un ataque relay. Fuente: informe de amenazas CCN-CERT IA-05/16. NFC – vulnerabilidades.

Venta de datos en la *Deep Web* y la *Dark Web*

Internet es una plataforma mundial donde empresas, comunidades y personas interactúan compartiendo información y accediendo a servicios en línea tanto a nivel laboral como social. Este queda dividido en diferentes piezas:

a. Web de superficie o clara: parte indexada por motores de búsqueda estándar, tales como Google.
b. *Deep Web*: contenidos no indexados en motores de búsqueda tradicionales. Por ello, puede ser usado para evadir las leyes que rigen el derecho. Se accede a su contenido mediante búsquedas dentro de un sitio web particular, como intranets.
c. *Dark Web o Darknet*: se trata de una red cerrada de computadoras para compartir archivos. Para acceder a ella, se necesitan configuraciones de autorización o un *software* especial. Entre los principales motores de búsqueda de estas *darknets*, podemos destacar TOR.

La *Dark Web* es un entorno virtual que evita el filtrado del contenido publicado, proporciona a sus usuarios el anonimato y no conoce fronteras nacionales. Por todo ello, se favorece la comisión de actividades delictivas y alberga muchos de los mercados más críticos para varias organizaciones criminales —conocidos como *Dark Marketplaces*. Algunas de las actividades desarrolladas son el mercado negro de bienes como armas de fuego, droga, venta de datos bancarios[9] —robados previamente mediante diferentes técnicas—, o, también, el comercio de servicios de *hackeo*, como *malwares*.

[9] Entre los datos de las tarjetas bancarias que pueden ser robados, diferenciamos:

– CVV: registros que pueden obtener información del titular de la tarjeta, como su nombre, el número de la tarjeta, la fecha de vencimiento de la misma o los dígitos que se encuentran en el reverso de esta. Con esta información, los criminales pueden realizar compras *online*.
– DUMPS: datos sin procesar almacenados en las bandas magnéticas de las tarjetas bancarias. Son obtenidos para posteriormente clonar dichas tarjetas.

Entre los *Dark Marketplaces* más conocidos, aunque hoy en día cerrados, encontramos Alphabay y Halsa, donde el medio de pago más usado eran las criptomonedas como el *Bitcoin*. En ellos, los ciberdelincuentes podían comprar *Bitcoins* con los datos de las tarjetas bancarias sustraídas y continuar navegando en la *Dark Web*, dificultando así su posible persecución.

Mercados como estos son creados para facilitar la expansión de la economía criminal clandestina y, dado que enmascaran la identidad de sus usuarios y ubicaciones de sus servidores, dificultaban la capacidad de las Fuerzas y Cuerpos de Seguridad de llevar a los delincuentes ante la Justicia.

Las criptomonedas son usadas porque son independientes de supervisión gubernamental. Pueden ser tanto centralizadas, donde una entidad central controla el sistema de intercambio, como descentralizadas, las cuales funcionan gracias a una red punto-punto y un algoritmo de código abierto. Además, también pueden clasificarse según sean convertibles y tengan un valor equivalente en otra moneda fiel o no. En cualquier caso, cuando se efectúan pagos, existen complejos protocolos y algoritmos que hacen que los usuarios confíen en estas transacciones.

Estos mercados tienen un carácter dinámico y tamaños de muestra no representativos, de manera que los análisis estadísticos no son prácticos. Todo ello dificulta las investigaciones y prácticas de monitoreo, por lo que constituye un entorno fértil para los delincuentes[10].

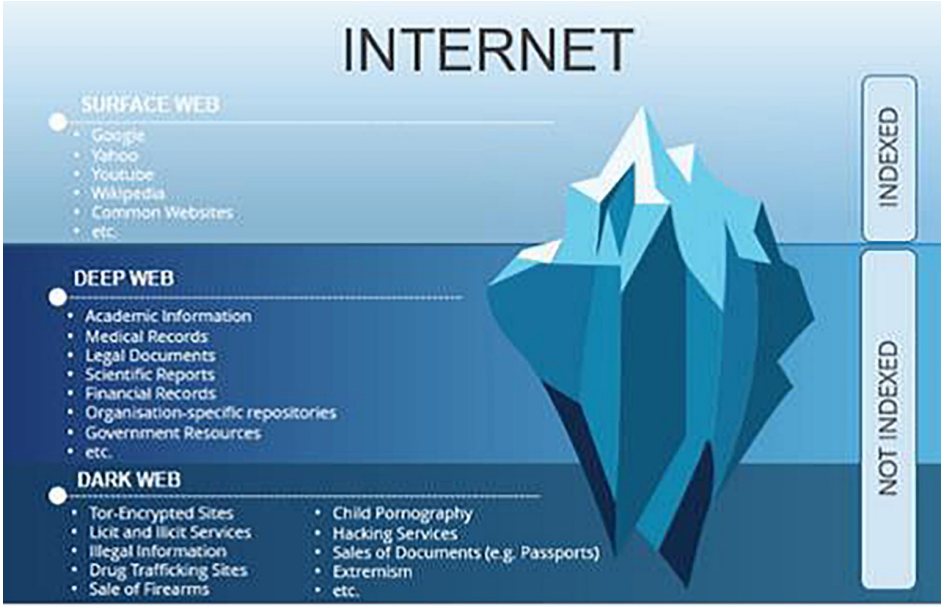


Ilustración 1: analogía de las partes de Internet con un iceberg. Fuente: SANTOS, Paulo. «Darknet: concepts». Curso online CEPOL. Octubre 2018.

– FULLZ: información financiera completa de la víctima, es decir, el nombre, la dirección, la información de la tarjeta de crédito, el número de seguro social o la fecha de nacimiento, entre otros. Esta información permite a los piratas informáticos robar la identidad de los titulares de la tarjeta.

10 EUROPOL. «Drugs and the darknet. Perspectives for enforcement, research and policy».

MODUS OPERANDI: LA RECOLECCIÓN Y ENVÍO DE DATOS

Conductas relacionadas con el sistema NFC y el *contactless*.

Para llevar a cabo pagos con el teléfono movil, es necesario que los *smartphones* y dispositivos que comuniquen con ellos dispongan de la tecnología NFC. Así mismo, también se requiere que el móvil disponga de una aplicación de «monedero electrónico». De esta manera, podríamos pagar con nuestros teléfonos si olvidásemos nuestra cartera —incrementando así la seguridad de las tarjetas bancarias físicas, pues además de las propias medidas de estas, se incluyen las del teléfono móvil y la aplicación del monedero.

No obstante, estos pagos también quedan expuestos a riesgos, de tal forma que es conveniente usar una tarjeta inteligente que almacene los datos tanto de las tarjetas asociadas a este monedero electrónico como de las aplicaciones que acceden a ellas. Así, al realizar un pago, el monedero se comunica vía *contactless* con el datáfono y esta tarjeta inteligente captura los datos de todos los intervinientes. En estos supuestos, si el cibercarterista leyera dicha comunicación sería capaz de obtener la información necesaria para, posteriormente, realizar compras con la tarjeta de la víctima, incurriendo así en un delito de estafa informática y usurpación de estado civil —suplantación de identidad de su víctima. Una alternativa a estas compras sería la venta de dicha información en la *Deep Web* o *Dark Web*.

Otras conductas delictivas.

Es posible que los cibercarteristas usen diferentes técnicas para hacerse con los datos del titular y, posteriormente, usarlos en beneficio propio o publicar dicha información en la *Deep Web* o en la *Dark Web*.

Entre estas técnicas podemos distinguir el *phishing*, que consiste en enviar mensajes de correo electrónico a la víctima, de manera que el ciberdelincuente se hace pasar por un servicio de seguridad —por ejemplo, del Banco— para apremiar a los usuarios a conectarse a una página web fraudulenta y, en ella, ceder los códigos de acceso y contraseñas de seguridad. Además, puede intervenir la figura del «mulero». Los muleros son terceras personas que participan de este entramado delictivo en su última fase, dado que estos abren cuentas bancarias donde se producirán los ingresos ilícitos de dinero, para, ulteriormente, enviarlos al delincuente —que puede encontrarse incluso en otra nación. Toda esta actividad queda penada como un concurso de delitos de robos de identidad, falsedad de documento mercantil, descubrimiento de datos informáticos secretos e incluso delitos de receptación.

Si estas mismas prácticas se llevan a cabo a través del teléfono, reciben el nombre de *smishing*. Otra de las actuaciones a destacar en la manipulación informática es el *pharming*, que consiste en modificar la relación entre las direcciones IP y las direcciones reales de las páginas del servidor informático. Así, cuando el usuario trata de acceder a una página web, lo hace a una imitada por el ciberdelincuente, donde la víctima cede sus claves bancarias secretas sin ser consciente de ello.

En la mayoría de las ocasiones, los ciberdelincuentes optan por la venta de los datos robados en la *Deep Web*. Ello se debe a los límites geográficos con los que chocan los poderes legislativo y ejecutivo; fronteras fácilmente superables a través de Internet, dado que no son aplicables ciertos principios del derecho y la legislación, lo que facilita la actuación de los criminales[11].

CONCLUSIONES

La vertiginosa revolución que se produce del uso masivo de las TIC y el surgimiento de Internet ha creado un nuevo entorno conocido como ciberespacio. Este ofrece algunos problemas desde el punto de vista legislativo, como la dificultad de persecución de los delitos cometidos en él, dada su capacidad de expansión transfronteriza, o la gran variedad de ciberamenazas que pueden surgir, lo cual obstaculiza su categorización en un hecho penal u otro.

Para resolver toda esta problemática, es de suma importancia dar un enfoque coordinado en la aplicación de la ley y la participación conjunta de todos los agentes involucrados. Así pues, existen varias alternativas a la cuestión de cómo categorizar un hecho penal en un tipo u otro:

a. Elaborar normas internacionales que delimiten un marco normativo en el que deberán operar los poderes legislativos de las naciones involucradas en una problemática concreta.
b. Creación *ex novo*[12] de leyes penales especiales que tipifiquen las nuevas conductas surgidas del uso de las TIC.
c. Intentar reconducir estas nuevas conductas a actividades ya penadas con la legislación vigente, es decir, tratar de sancionar estos supuestos de hecho en base al ordenamiento jurídico vigente en cada momento.

Sin embargo, a pesar de existir diferentes soluciones, personalmente, considero que los mecanismos y herramientas del derecho tradicional español han quedado obsoletos frente a este nuevo mundo virtual. Por ello, a título de *lege ferenda*[13], se debe trabajar con el objetivo de crear una nueva disciplina del derecho que persiga la cibercriminalidad. Esta nueva rama jurídica será la del ciberderecho.

BIBLIOGRAFÍA

– CEPOL. VESSZOS, Gergely. «Cryptocurrencies». 2 de octubre 2018.

– CCN-CERT. «Informe de amenazas CCN-CERT IA-05/16. NFC – vulnerabilidades».

[11] VELASCO NÚÑEZ, Eloy. «Estafa informática y banda organizada. *Phishing*, *pharming*, *smishing* y "muleros"». *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía*, 2008.

[12] *Ex novo*: expresión que significa «de nuevo».

[13] *Lege ferenda*: locución latina a la que se hace referencia cuando se necesita crear una nueva legislación acerca de una materia determinada

– ÉCIJA BERNAL, Álvaro. *El ciberespacio, un mundo sin ley. Internet: la revolución que cambió las normas del juego*. Febrero 2017. Ed. Especiales Wolters Kluwer.

– EUROPOL. «Drugs and the darknet. Perspectives for enforcement, research and policy».

– EUROPOL. «Massive blow to criminal Dark Web activities after globally coordinated operation». https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation. 20 de julio 2017.

– GUDÍN RODRÍGUEZ-MAGARIÑOS, Faustino. «Nuevos delitos informáticos: *phishing*, *pharming*, *hacking* y *cracking*».

– INFOSEC. «Card fraud in the Deep Web». 16 de junio 2015.

– MINISTERIO DE INTERIOR. «Documento de Análisis de Riesgos y Difusión Operativa: fraude con medios de pago en cajeros y datáfonos», 2014.

– MORE DAVIS, Ana Lucía. «Conducta delictiva y factores». https://es.slideshare.net/AnaluciaMoreDavis/conducta-delictiva-y-factores. 19 de mayo 2014.

– NATIONALE NEDERLANDEN. «El dinero del siglo XXI: así han cambiado nuestras formas de pago». https://www.segurosdetuatu.es/posts/el-dinero-del-siglo-xxi-asi-han-cambiado-nuestras-formas-de-pago. 3 de septiembre 2015.

– RODRIGUEZ CARO, María Victoria. «Estafa informática. El denominado *phishing* y la conducta del "mulero bancario": categorización y doctrina de la Sala Segunda del Tribunal Supremo». *http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10617-estafa-informatica-el-denominado-phishing-y-la-conducta-del-ldquo%3Bmulero/*. 30 de octubre 2015.

– SANTOS, Paulo. *Darknet: concepts*. Curso online CEPOL. Octubre 2018.

– VELASCO NÚÑEZ, Eloy. «Estafa informática y banda organizada. *Phishing*, *pharming*, *smishing* y "muleros"». *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía*, 2008.

EL AGENTE ENCUBIERTO EN LA LUCHA ANTITERRORISTA

MONTSERRAT LÓPEZ MELERO
Graduada en Criminología en la Universidad Europea Miguel de Cervantes (UEMC). Licenciada en Derecho en la Universidad Complutense de Madrid

DANIEL LÓPEZ MELERO
Doctorando en Ciencias de la Salud. Universidad Alcalá (UAH)

Resumen

El agente encubierto, como medida y/o técnica de investigación en el crimen organizado, tiene como base un contexto internacional, suponiendo una adecuada iniciativa para la política preventiva en diferentes ámbitos, siendo uno de ellos el terrorismo, es decir, política preventiva de lucha antiterrorista. El elemento clave del agente encubierto es la prevención y represión del crimen organizado en una diversidad de vertientes.

INTRODUCCIÓN

El crimen organizado se viene desarrollando en la sociedad de una forma paralela a la vida «normal», si bien, llevan a cabo una serie de acciones que suponen un rechazo de la sociedad de forma íntegra. El crimen organizado en el siglo XXI supone un problema de seguridad tanto nacional como internacional. Convirtiéndose, por tanto, en uno de los mayores enemigos de la sociedad, en general, y del Estado, en particular; dado que, en este último caso, se va introduciendo en el tejido de la sociedad democrática, para el caso de España. Sin olvidar el carácter dinámico y versátil del fenómeno, prueba de ello es en ámbito del terrorismo internacional de carácter yihadista.

Los diferentes Estados, no solo España, de una forma individual, pero también de cooperación por medio de las organizaciones internacionales, han creado instrumentos para neutralizar las actividades delictivas. Instrumentos de carácter legislativo, en algunas ocasiones, pero también penales o de técnicas especiales de investigación, en otros, como es el caso del agente encubierto como estrategia de seguridad, con la

intención de frenar, limitar e, incluso, anular el fenómeno del crimen organizado. En el caso que aquí investigamos, en el ámbito de la lucha antiterrorista.

Es necesario, como punto de partida, establecer la delimitación conceptual de algunos términos para adentrarnos, posteriormente, en la figura del agente encubierto en el terrorismo como medida de investigación preventiva. Respecto a *crimen organizado*, debemos advertir que, al abordar este tema, se vislumbra un problema fundamental, consistente en la multiplicidad de denominaciones, dificultando, en consecuencia, el concepto exacto de *crimen organizado*[1]. Se habla de *crimen organizado*, *delincuencia organizada* o de *criminalidad organizada*. Si bien, puede ser definido el *crimen organizado* como «grupo de delincuentes organizados, que se encuentran en condiciones de actuar tanto en la vertiente legal como en la ilegal de la actividad política y económica, cuya influencia en estos ámbitos se extiende hasta el poder, incluso condicionar negativamente sectores amplios de la vida productiva, social e institucional»[2]. Afinando más la cuestión, Zúñiga[3] manifiesta que cuando utilizamos el término *delincuencia organizada* estamos frente a una definición de carácter penal, si el término que se utiliza es *criminalidad organizada*, viene a ser empleado desde la perspectiva criminológica, incidiendo que *crimen organizado* viene de la traducción en inglés de *organised crimen*.

CONCEPTO DE AGENTE ENCUBIERTO

Partimos de Montero (*et al.*)[4] que manifiesta que «es un agente de las Fuerzas y Cuerpos de Seguridad que, ocultando su identidad y sus propósitos verdaderos, se hace pasar por otra persona, se infiltra en las organizaciones criminales, con el objetivo de prevenir y reprimir, así como conocer los miembros que integran la organización, como el tipo de estructura, su funcionamiento en información de sus actividades delictivas por medio de una falsa confianza». Benítez[5] señala que «funcionarios de la Policía Judicial, mediante resolución fundada y teniendo en cuenta su necesidad a los fines de la investigación, van a actuar bajo identidad supuesta y a adquirir y transportar los objetos, efectos e instrumentos del delito y definir la incautación del mismo». Zafra[6] dice «se entiende por agente encubierto el miembro de la policía judicial que se infiltra en una organización criminal participando del entramado organizativo bajo identidad supuesta, para detectar la comisión de delitos e informar sobre sus actividades con el fin de obtener pruebas inculpatorias y proceder a la detención de sus autores». Solo resta por concluir que se trata de una técnica de investigación especial, en la que algunos autores[7] consideran que genera subcategorías, tales como agentes encubiertos públicos, infiltración semiprivada y las infiltraciones privadas. Si bien, pese a que puede generar casos de incompatibilidades con los derechos y principios fundamentales de todo Estado democrático, se

---

1 Vid., (McLaughlin & Muncie, 2012, págs. 145-147) (Hobbs, 1998)

2 (Arlacci, 1985, pág. 83)

3 (Zúñiga, 2006)

4 (Montero, Gómez, Montón, & Barona, 2013, pág. 221)

5 (Benítez, 2007, pág. 17)

6 (Zafra, 2006, pág. 228)

7 (Gómez de Llaño, 2004, pág. 130)

ha de afirmar que es una de las técnicas más eficaz en la lucha contra la delincuencia organizada[8].

EL AGENTE ENCUBIERTO EN LA LUCHA ANTITERRORISTA

Es el artículo 282 bis de la LECrim el que regula el agente encubierto, destacando los puntos 6 y 7 del precepto que indican: «6. El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta[9] en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos […]. El agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos. 7. En el curso de una investigación llevada a cabo mediante agente encubierto, el juez competente podrá autorizar la obtención de imágenes y la grabación de las conversaciones que puedan mantenerse en los encuentros previstos entre el agente y el investigado, aun cuando se desarrollen en el interior de un domicilio». El citado artículo regula la diligencia de infiltración, o de introducción de un agente encubierto en una red delincuencial, teniendo por objetivo la averiguación de hechos delictivos, incluyéndose el delito de terrorismo.

La doctrina jurisprudencial, (STS de 6 de febrero de 2009), manifiesta que «el agente encubierto virtual deberá ser un miembro de la Policía Judicial español o extranjero y deberá asumir, de forma voluntaria, la misión de infiltrarse en la organización criminal, estando las actuaciones necesarias para desarrollar su investigación, exentas de responsabilidad criminal[10], siempre que sean proporcionales a su finalidad y no constituyan provocación al delito. Las pruebas obtenidas bajo esa circunstancia constituirían una incitación al delito, y deberán ser excluidas, como pruebas obtenidas con mala fe» (SAN 12/2018, de 26 de abril). La referida sentencia de la Audiencia Nacional, estima que un agente encubierto se puede convertir en agente provocador[11].

El agente encubierto actuará bajo la identidad supuesta otorgada por el Ministerio de Interior, por un plazo de 6 meses prorrogables por periodos de igual duración, si bien, el agente encubierto podrá participar en el tráfico jurídico y social bajo la identidad simulada, además, de adquirir y transportar objetos, efectos e instrumentos del delito, y diferir la incautación de los mismos. El párrafo seis del art. 282 bis de la LECrim establece que el agente encubierto solo puede ser autorizado por el juez de instrucción, nunca por el fiscal, por entender que su actuación en el ámbito virtual afecta siempre a la privacidad, al secreto de las comunicaciones o a la protección de los datos personales, todos ellos

---

8 (Montero, Gómez, Montón, & Barona, 2013, pág. 221)

9 (Oseth, 1985, pág. 26)

10 El artículo 282 bis 5) así lo indica.

11 Vid., las SSTS 28 de junio de 2014, 1344/1994, de 21 de junio, 1140/2010, de 29 de diciembre, entre otras. Vid. la STS 1992/1993, de 15 de septiembre sobre el delito de provocación y el agente encubierto. El Tribunal Europeo de Derechos Humanos admitió la figura del agente encubierto en su sentencia 1992/51, de 15 de junio (*Caso Lüdi contra Suiza*) considerando que la figura del agente provocador es ilegítima. Vid. la Sentencia del Tribunal Europeo de Derechos Humanos (Caso Teixeira de Castro contra Portugal) (Vid., SÁNCHEZ. 2005, p. 235).

derechos fundamentales recogidos en la Constitución española, por lo que son materias que exclusivamente el juez podrá valorar. Ambos párrafos establecen una serie de peculiaridades propias para el agente encubierto virtual:

– Solo es necesaria tal autorización cuando el agente policial vaya a actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación.
– Solo con autorización específica para ello, podrá intercambiar o enviar archivos ilícitos, por razón de su contenido (delito simulado) pretendiendo con ellos el reclutamiento, radicalización, adoctrinamiento o adiestramiento de terroristas. Ahora bien, la autorización judicial inicial para usar una identidad virtual falsa en redes sociales o *chats* y comunicaciones restringidas no será suficiente, en este caso, el juez deberá otorgar una segunda autorización especial, tal es el caso de la obtención de imágenes o grabación de conversaciones mantenidas en los encuentros previstos entre el agente y el investigado, aun cuando se desarrollen dentro de un domicilio.

Como se puede observar, durante toda y cualquier actuación del agente encubierto virtual, va a existir un completo y exhaustivo control judicial de la investigación, puesto que la información obtenida se pondrá en conocimiento del juez aportándose al procedimiento con objeto de ser considerada como prueba por lo que deberá ser valorada por el órgano de instrucción. En suma, el principal quehacer del agente encubierto es la obtención de prueba.

Ahora bien, cabe la posibilidad de que el agente encubierto deba dejar de ser virtual para iniciar encuentros en el exterior con la intención de continuar con la investigación, para el caso el juez podrá ampliar la autorización inicial señalando la identidad «no cibernética» que ha de usar. En suma, el juez deberá, además, facultarle para transportar objetos, efectos y herramientas «delictivas» diversas a las utilizadas en el ámbito cibernético.

EL AGENTE ENCUBIERTO Y LAS POLÍTICAS PREVENTIVAS

Nos encontramos ante una técnica de investigación que tiene como base un contexto internacional —Consejo de Europa, Unión Europea, al desarrollarse acuerdos, recomendaciones, tratados internacionales, etc.— considerada como una política preventiva, considerándose que, con políticas preventivas adecuadas y oportunas, los costes en seguridad se verán reducidos[12]. En esta línea, en 1997, el 18 de diciembre destaca el convenio celebrado sobre la base del artículo K.3 del Tratado de la Unión Europea, relativo a la asistencia mutua y la cooperación entre las Administraciones aduaneras[13]. El Convenio de la Unión Europea[14] regula las operaciones encubiertas internacionales, alegando que los Estados deberán realizar en sus legislaciones las adaptaciones nece-

[12] (Ballbé, 2007, págs. 215-276)

[13] Vid., art. 23 del Convenio. (BOE, 1997)

[14] Acto del Consejo 2000/C 197/01 de 29 de mayo de 2000.

sarias para que los funcionarios de policía puedan ser autorizados a actuar en territorio de otro Estado miembro como si fueran agentes policiales nacionales[15].

En este sentido, el Convenio de Palermo de 2000 propone algunas técnicas especiales de investigación —entregas vigiladas, vigilancia electrónica y las operaciones encubiertas—, concretamente en su artículo 20.1. El precepto objeto de análisis, invita a los Estados a que, en sus legislaciones, se incluyan y puedan realizar técnicas especiales de investigación, por lo que en el ámbito nacional español tiene respaldo internacional, admitiéndose y regulándose técnicas como agentes encubiertos, operaciones encubiertas, tecnovigilancia, etc., con la intención de combatir el crimen organizado y el terrorismo como crimen organizado[16]. De otro lado, el Convenio entre los Estados miembros de la Unión Europea de Asistencia Judicial Penal de 2000 regula las operaciones encubiertas internacionales en su artículo 14. En el mismo sentido, la Recomendación Rec (2001) 11 del Comité de Ministros del Consejo de Europa, sobre principios directrices en la lucha contra el crimen organizado, indica que deben desarrollarse nuevos métodos de trabajo policial que muden su foco de atención de una policía reactiva (*reactive policing*), a una policía proactiva (*proactive policing*), incluyendo el uso de inteligencia estratégica y análisis del crimen.

Si bien, algunos autores[17] manifiestan la falta de consenso o armonización de algunas legislaciones de los Estados miembros en relación con la cooperación policial y judicial, en este sentido, hablan de que los componentes del crimen organizado han encontrado verdaderos paraísos jurídico-penales. Tal situación hizo que se modificara la Carta de Derechos Fundamentales de la Unión Europea —17 de diciembre de 2007, con el Tratado de Lisboa—[18].

A pesar de toda la normativa que se ha señalado, en España es escasa, ajustándonos a la Ley de Enjuiciamiento Criminal, si bien, hay figuras que hoy en día se adaptan eficazmente como agente encubierto en organizaciones terroristas como son los miembros del Centro Nacional de Inteligencia. Si bien, su normativa legal[19] en ningún momento recoge la figura de agente encubierto, pese a que hable de «tareas de neutralización». En este sentido, se afirma que los servicios de inteligencia son una herramienta útil para la lucha contra el crimen organizado dada su versatilidad que les permite que se adapten con mayor rapidez a objetivos heterogéneos que pueden presentar las organizaciones de crimen organizado de carácter político o de bienes y servicios ilegales[20].

---

15 (Guzmán Flujá, 2016, pág. 11)

16 (Von Lampe, 2006, págs. 77-95)

17 (De Hoyos Sancho, 2008, pág. 68)

18 Con posterioridad se desarrolla el Programa de Estocolmo. Vid. Directiva 2012/13/UE del Parlamento Europeo y del Consejo, de 22 de mayo de 2012, relativa al derecho a la información en los procesos penales; la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea; la Directiva 2013/48/UE, de 22 de octubre, sobre el Derecho a la asistencia de letrado en los procesos penales en los procedimientos relativos a la orden de detección europea, y sobre el derecho a que se informe a un tercero en el momento de la privación de libertad y a comunicarse con terceros y con autoridades consulares durante la privación de libertad; entre otras normas.

19 Vid. Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia. Vid., (Jordán Enamorado, 2005)

20 (Herrero de Castro & Barras, 2009, pág. 10 y 16)

Si bien hay una serie de inconvenientes de la utilización del agente encubierto como sistema de investigación: a) el riesgo por parte del funcionario policial es elevado al infiltrarse en una organización criminal como es la terrorista; b) las operaciones realizadas no tienen límite de tiempo, por lo que pueden verse alargadas, con el consiguiente de que primero ha de ser aceptado como miembro por la organización criminal, es decir, hay un proceso de confraternización. En ese tiempo, el agente puede verse en situaciones en las que se vulnere garantías constitucionales de los sujetos investigados, por lo que la información obtenida no podrá ser utilizada como prueba en un procedimiento judicial penal; y c) que el tiempo del que hablamos en el punto anterior suponga una contaminación intelectual de hábitos y comportamientos para el agente encubierto[21].

CONCLUSIONES

A. Los servicios de inteligencia pueden ser una de las herramientas más útiles para luchar contra el crimen organizado y, en este caso, contra una organización terrorista, a través de los agentes encubiertos. Son útiles en el nuevo contexto global dada su capacidad de adaptación en tiempo y forma.
B. El ámbito de investigación de un agente encubierto no debería estar circunscrita a una lista cerrada de delitos. Incluso se podría dar la posibilidad a una víctima —como acusación particular— que solicite la práctica de la diligencia de investigación a la autoridad judicial. Preguntando, en este caso, el juez a la Policía Judicial la posibilidad de practicar esa diligencia[22].

BIBLIOGRAFÍA

– ARLACCI, P. «Tendencias de la criminalidad organizada y de los mercados ilegales en el mundo actual». *Poder Judicial*. 1985.

– BALLBÉ, M. «El futuro del derecho administrativo en la globalización: entre la americanización y la europeización». *Revista de Administración Pública, n.º* 174, septiembre-diciembre de 2007, pp. 215-276.

– BENÍTEZ, I. *El colaborador con la justicia. Aspectos sustantivos procesales y penitenciarios derivados de la conducta del «arrepentido»*. Madrid: Dykinson, 2007.

– *BOE*. Convenio celebrado sobre la base del artículo K.3 del Tratado de la Unión Europea, relativo a la asistencia mutua y la cooperación entre las Administraciones aduaneras. Bruselas: 18 de diciembre de 1997. Recuperado el 3 de septiembre de 2019, de https://www.boe.es/boe/dias/2002/08/20/pdfs/A30814-30824.pdf.

[21] Teoría de la neutralización (García-Pablo de Molina, 2009, pág. 777)

[22] (Suita, 2006, pág. 241)

– DE HOYOS SANCHO, M. «La armonización de los procesos penales, reconocimiento mutuo y garantías esenciales». En DE HOYOS SANCHO, M. *El proceso penal en al Unión Europea: garantías esenciales*. Valladolid: Lex Nova, 2008, pp. 42-79.

– GARCÍA-PABLO DE MOLINA, A. *Tratado de Criminología*. Valencia: Tirant lo Blanch, 2009.

– GÓMEZ DE LIAÑO, M. *Criminalidad organizada y medios extraordinarios de investigación*. Madrid: Constitución y Leyes, S.A., 2004.

– GUZMÁN FLUJÁ, V. «El agente encubierto y las garantías del proceso penal». Publicaciones del Portal Iberoamericano de las Ciencias Penales. Instituto de Derecho Penal Europeo e Internacional. Universidad de Castilla La Mancha, 2016. Recuperado el 3 de septiembre de 2019, de http://www.cienciaspenales.net/files/2016/10/6vicente-guzman-es.pdf.

– HERRERO DE CASTRO, R., & BARRAS, R. «Globalización y crimen organizado. Mecanismos de lucha contra el crimen trasnacional: la inteligencia». *Inteligencia y Seguridad* (6). 2009, pp. 99-121.

– Hobbs, D. «Going down the glocal». *The Howard Journal of Criminal Justice* (37). 1998, pp. 1-19.

– JORDÁN ENAMORADO, J. «Servicios de inteligencia y lucha antiterrorista. Al servicio del Estado: inteligencia y contrainteligencia en España». *Arbor, CLXXX* (709). Enero de 2005.

– MCLAUGHLIN, E., & MUNCIE, J. *Diccionario de criminología*. Barcelona: Gedisa, 2012.

– MONTERO, J., GÓMEZ, J., MONTÓN, A., & BARONA, S. *Derecho Jurisdiccional III* (21 ed.). Valencia: Tirant lo Blanch, 2013.

– OSETH, J. *Regulating U.S. Intelligence Operations. A Study in Definition of the National Interest*. Lexington: The University Press of Kentucky, 1985.

– Sánchez, I. *La criminalidad organizada. Aspectos penales, procesales administrativos y policiales*. Madrid: Dykinson, 2005.

– SUITA, N. «La diligencia de investigación por medio del agente encubierto». En MARTÍN, P. *La actuación de la Policía Judicial en el proceso penal*. Barcelona: Marcial Pons, 2006, pp. 238-267.

– VON LAMPE, K. «The Interdisciplinary Dimensions of the Study of Organized Crime». *Trends in Organized Crime, 9*(3). 2006, pp. 77-95. Recuperado el 3 de septiembre de 2019, de http://www.organized-crime.de/kvllnterdiscDimStudyOC-TOC-9-3-2006.pdf.

– ZAFRA, R. «El agente encubierto en el ordenamiento jurídico español. En *La prueba en el espacio europeo de libertad, seguridad y justicia penal.* Navarra: Aranzadi, 2006, pp. 227-270.

– ZÚÑIGA, L. (2006). «Criminalidad organizada, derecho penal y sociedad. Apuntes para el análisis». En SANZ MULAS, N. *El desafío de la criminalidad prganizada.* Granada: Comares, pp. 40-68.

TERRORISMO Y DEPORTE. PERSPECTIVA DESDE EL PSICOANÁLISIS

MONTSERRAT LÓPEZ MELERO
Graduada en Criminología en la Universidad Europea Miguel de Cervantes (UEMC). Licenciada en Derecho en la Universidad Complutense de Madrid

DANIEL LÓPEZ MELERO
Doctorando en Ciencias de la Salud. Universidad Alcalá (UAH)

Resumen

Desde el psicoanálisis, se puede afirmar que la decisión de un joven de convertirse en terrorista puede venir motivada por el *deseo de ser aceptado* en el entorno social —amigos, barrio, escuela, en la sociedad en general—, el joven precisa de una identidad dentro de una colectividad, en este sentido, esta identidad se trata de un incentivo no material basada en criterios de racionalidad. A través de la actividad física y el deporte se pueden crear esos ámbitos carenciales de los que precisa todo jóven.

MALESTAR SOCIAL

Hay que partir de la teoría de Freud que determina que la conducta y comportamiento del ser humano no se caracteriza por regirse, exclusivamente, por el placer o por la realidad, sino que hay que tener en cuenta la vida psíquica del ser humano que da lugar a conflictos en los requerimientos. Estos conflictos generan un malestar. Dice que el malestar puede venir determinado por[1]: la hostilidad que existe; la posible insatisfacción que se tiene respecto de las relaciones con los demás; la posible insatisfacción que se tiene respecto de las relaciones con instituciones. Todo ello genera infelicidad y frustración. Porque gira en torno a la demanda de cariño, apego y goce, por lo que estos son aspectos que se deben construir de forma correcta desde niños. Pero, parece ser que, ese malestar, está en la propia civilización, siendo un componente estructural de la misma, lo que supone que viene estableciendo la hipótesis de anular el bienestar y del discurso que

[1] Vid., CERDEIRA GUTIÉRREZ. 1988.

es utilizado para teorizar el bienestar. Dahrendorf[2] afirmaría que el Estado del bienestar se caracteriza porque viene apoyándose en la defensa de los intereses de las personas desposeídas frente a la resistencia de los privilegiados. Esta posición se ve reflejada en las teorías utilitaristas de Bentham que determinan la necesitad y posibilidad de que el mayor número de bienes debe ser para el mayor número de personas. También viene amparada en la política social en la que debe tenerse en cuenta el principio de igualdad de oportunidades para todas las personas, si bien, debemos entender esa igualdad en derechos y no de resultados.

Dado que existen conceptos vacíos de valor, es ahí donde surge la tiranía, en la que muchos no se pueden permitir el pensar, surgiendo el aislamiento, teórico y práctico, la marginación y la automarginación. Así, en el terrorismo, hay una interpretación vacía de contenido a lo que en valores se refiere, a lo que se entiende por estructuras democráticas y a lo que el espacio político entiende por bienestar. Se caracteriza por la persistencia de comportamientos inadaptados a la sociedad actual —por cuestiones políticas, ideológicas o falta de identificación en valores—. Puede entenderse, que el malestar que se genera viene determinado por el simple hecho de pensar y sentir. Freud habló de las fuentes del ser humano: el cuerpo mortal, la naturaleza y la propia cultura. La cultura es especialmente significativa porque puede obligar a reprimir instintos naturales, y tener conciencia sobre la fragilidad moral y mental de los sujetos. Los jóvenes que se unen a las filas de las diferentes organizaciones terroristas internacionales pueden deberse al decaimiento de la subjetividad junto con el decaimiento de la figura paterna. Tal situación puede generar cierta exhortación al goce, es decir, la organización terrorista promete continuamente cómo conseguir la felicidad y las soluciones al consumo.

Hoy en día, en muchos casos, se afirma que la estructura de la familia es importante, la desorganización y la existencia de problemas internos puede predecir acciones violentas, actos de delincuencia y actitudes negativas. Se ha demostrado que una escasa o nula supervisión o control parental, una disciplina errónea o severa, relaciones maritales problemáticas, el rechazo de los padres hacia los hijos, etc., son importantes y claros predictores de conductas violentas. Da lugar a que se tenga una tendencia hacia uno mismo, de manera que prima el yo como centro del mundo, no permitiendo la entrada de valoraciones externas —y mucho menos de los padres— en su entorno. Desde una perspectiva sociológica, supone la existencia de falta de adaptación social, o incluso, una impotencia por integrarse a unos grupos, eso supone un aislamiento en el que el adolescente solo va a aceptar valores e intereses propios[3]. Todo ello, es un proceso que se puede adquirir en el núcleo familiar. La teoría de la anomia produce efectos egocéntricos importantes (incluso narcisismo), dando lugar a aspectos temperamentales en los sujetos[4]. Estos comportamientos temperamentales pueden ser iniciados en el ámbito familiar y ser agravados en el contexto social. Esto puede ocurrir en el ámbito del terrorismo.

---

[2] DAHRENDORF. 1983.

[3] LÓPEZ MELERO. 2018.

[4] Vid., HERNÁNDEZ ESPINOSA. 2014, pp. 1-16.

Se puede decir que el egocéntrico y el narcisismo dan lugar a conductas y comportamientos muy peligrosos, en el que las técnicas y métodos empleados son más planificados y refinados. Incluso, este tipo de sujetos justifican sus conductas mediante mecanismos defensivos de racionalización y compensación; lo que supone que desvaloriza los argumentos de los demás —de su familia y los argumentos sociales— porque siempre adopta una postura crítica y acusadora, culpabiliza a la sociedad y a la política de su no integración y no tener identidad con lo que le rodea[5].

En el ámbito del terrorismo se puede afirmar que la decisión de un joven de convertirse en terrorista puede venir motivada por el *deseo de ser aceptado* en el entorno social —amigos, barrio, escuela, en la sociedad en general—, es decir, el joven precisa de una identidad dentro de una colectividad, en este sentido, esta identidad se trata de un incentivo no material basada en criterios de racionalidad. Lo característico no es el propio proceso de radicalización, sino la desconexión social que sufren, el resentimiento a que no le dejen formar parte de algo. Es aquí donde se incluye a la mayoría de los jóvenes descendientes de inmigrantes musulmanes, sufren crisis de identidad y necesitan a alguien que les valore, ese alguien puede ser una organización terrorista que pretenda darle el lugar que la sociedad no les da.

¿PODEMOS HABLAR EN EL TERRORISMO DE NARCISISMO PRIMARIO Y SECUNDARIO?

Respecto del *narcisismo primario* aquel estado precoz, en el cual el niño catectiza toda su libido sobre sí mismo[6]; mientras que el *narcisismo secundario* es una vuelta de la libido sobre el yo, retirada de sus catexis objetales[7]; para Freud representa estados extremos de regresión y una estructura permanente del sujeto. Freud considera que el sujeto está construido sobre la base de un narcisismo primario. Lo define como «un estado posterior donde el yo retira su libido de las *figuras objetales* y la vuelve a dirigir hacia sí mismo, como en el periodo inicial del narcisismo primario». No obstante, se aplica la conceptualización de *narcisismo primario* a un primer estadio de la vida, es decir, anterior a la construcción del yo; su arquetipo es la vida intrauterina. Es decir, no hay separación entre sujeto y mundo externo. Se pregunta si aquellos sujetos que tienen narcisismo primario se relacionan con el otro, a lo que responde que no se tiene en cuenta al otro. Y no hay relación con el ambiente[8]. El narcisismo primario designa el «primer» narcisismo, es decir, el del niño que se considera a sí mismo objeto de amor antes de elegir objetos exteriores[9]. Corresponde a su creencia en la omnipotencia de sus pensamientos. El secundario designa ciertos estados extremos de regresión.

Podemos hablar en el terrorismo de narcisismo, pero no podemos decir que todos los terroristas son narcisistas: porque el narcisismo es la variante más extrema del rasgo

5 Ver la Teoría de Hirschi sobre el apego.

6 *Diccionario de Psicología*. 2016-2019.

7 GRIPPO. 2012,

8 INUPSI. 2019, pp. 10-15.

9 *Diccionario de Psicología*. 2016-2019.

de la personalidad del egocentrismo y no de los otros rasgos de la personalidad —labilidad afectiva, agresividad e indiferencia afectiva—; y porque el que un sujeto terrorista sea narcisista es algo complicado, por no afirmar que es imposible, que sea lábil afectivamente. Ya que el sujeto lábil es aquel que cambia de opinión constantemente, dejándose llevar por las opiniones y palabras de otro sujeto. Por lo que es más propio afirmar que un líder de una organización terrorista internacional tiene más acentuado el rasgo de la personalidad del egocentrismo (y narcisismo) y no es lábil, mientras que los seguidores tendrán más acentuado el rasgo de la labilidad afectiva. Sería conveniente hacer un estudio individualizado de cada terrorista y no aplicar rasgos de la personalidad de forma generalizada para no incurrir en errores. Además, hay que acuñar que se debe adjudicar a los sujetos terroristas un narcisismo primario y no secundario, en el que se evaden de la sociedad y crean un contexto social personal en el que prima, teniendo en cuenta el proceso psicológico utilizado por Moghaddam[10] que son: —personas infelices en la sociedad; —buscando justicia; —frustrados; —miembro de un grupo radical; para llegar y pasar por las diferentes etapas de la radicalización y cometer actos de terrorismo. En cada uno de los bloques hay un número de personas implicadas psicológicamente, si va subiendo de peldaños cuanto más arriba esté, más difícil será la vuelta atrás.

Teniendo en cuenta los *factores biológicos o físicos*, podemos señalar, en la estructura psicológica del terrorista, el siguiente modelo o teoría: las relaciones entre apego, genética y trastornos de personalidad son complejas y no han sido bien establecidas. Podemos considerar que el apego inseguro causa disregulación emocional. Pero tanto el apego inseguro como la disregulación emocional podrían estar mediadas por las mismas diferencias heredables en el temperamento o los rasgos de personalidad[11]. En lo que respecta a los *factores psicológicos*, es explicada a través de Silke con cuestiones psicopatológicas. Si bien, es interesante la conclusión a la que llega: «la normalidad es una norma en los terroristas y no la excepción». Especialmente, porque tienen un modo de pensar, de discernir que son normales y coherentes, no son enfermos mentales. Y, respecto de los *modelos o teorías sociológicas* que prevalecen en la estructura psicológica del terrorista, señalamos la *teoría del aprendizaje*. Citando a García-Pablos en cuanto a la adquisición de pautas y modelos criminales, «se lleva a cabo a través de un proceso de aprendizaje evolutivo que descansa en la observación y en la imitación del comportamiento criminal, aprendizaje vicario, observacional o proceso de modelado»[12]. Si bien, para explicar la teoría del aprendizaje y poderla asociar a los sujetos terroristas, se recurre a la *Teoría de la Asociación Diferencial* de Sutherland, quien la desarrolla en proposiciones. Esta teoría supone un marco contextual adecuado y oportuno, ya que el sujeto es capaz y tiene disposición y aptitud para interiorizar acciones. En un determinado momento esas acciones podrán convertirse en conductas delictivas terroristas —*proceso de socialización*[13]—. En este proceso juega un papel fundamental el entorno más cercano, (familia y amigos), aseverando esa crisis de identidad, una frustración, de manera que la única salida que ven los jóvenes de padres emigrantes es hallar su sitio, que alguien les dé su lugar y, en la mayoría de los casos, ese lugar se lo ofrece

[10] MOGHADDAM. 2005, pp. 161-169.

[11] GOLDSMITH & HARMAN. 1994, pp. 53 y ss.

[12] GARCÍA-PABLOS DE MOLINA. 2009, pp. 600-601.

[13] VALERO MATAS. 2009, p. 82.

la organización terrorista internacional, abasteciéndole de valores y técnicas propias de la organización terrorista y del terrorismo. Técnicas que serán aprendidas por la falta de identidad. Pero, es *la teoría de la imitación de Tarde* la más acertada[14]: Primera ley. El hombre imita a otro en proporción directa al grado de proximidad o intimidad de la relación entre ellos existente de su naturaleza. Segunda ley. El superior es imitado por el inferior. Tercera ley. *Ley de la inserción*, el incremento de la moda criminal más reciente es correlativo al descenso del anterior (puede haber excepciones).

EL DEPORTE COMO PROCESO DE SOCIALIZACIÓN

Teniendo en cuenta todo lo anteriormente reseñado, se ha de indicar que los jóvenes terroristas tienen una tendencia a la agresividad. Como posibilidad o como una de las alternativas a esa agresividad, a esa frustración, falta de identidad, a ese egocentrismo y narcisismo, los jóvenes pueden y deben recurrir a la actividad física y al deporte. La consideración del deporte como motivación para suplir las posibles carencias y algunas estructuras psicológicas. El deporte como proceso de socialización. Podemos definir la *socialización* como la adquisición, por parte de las personas, de un conjunto de hábitos prosociales, esa adquisición se produce mediante asociación. Afinando más la cuestión, se produce a través del sistema de reflejos condicionados debiendo de cumplir el requisito que debe consolidarse en la memoria, ya que un hábito es una tendencia internalizada que predispone a la acción[15]. Para muchos sujetos, el delinquir puede suponer una actividad intrínsecamente placentera, aportando beneficios más rápidos que consiguiéndolo a través de otras vías legales. Sin embargo, esta tendencia de búsqueda de placer choca directamente con el desarrollo de la conciencia, que se adquiere mediante la respuesta de temor condicionada. Por tanto, la probabilidad de que una persona cometa un crimen depende de la fuerza de su conciencia.

El deporte puede proporcionar un sentimiento de continuidad a los sujetos que lo practican, además de una identificación colectiva con el grupo con el que se practica, genera una identidad junto con una responsabilidad compartida lo que puede difuminar la línea del egocentrismo-narcisismo (cada sujeto tiene un rol concreto y dependiente de los demás componentes). Si tenemos una violencia escondida es hora de sacarla a través del deporte ya que puede convertirse en una forma de vida, por controlar estados emocionales. Es un medio adecuado para conseguir y adquirir valores personales y sociales[16], sirviendo como modelo de comportamiento según en la estructura deportiva que se practique.

Así, podemos destacar unos valores por la práctica deportiva (tabla 1), valores que, en la dimensión general y dimensión psicosocial, son recomendables de adquirir por los jóvenes que deciden unirse a las filas de cualquier organización terrorista internacional para evitar la situación.

---

14 GARCÍA-PABLOS DE MOLINA. 2009, pp. 415-418.

15 GARDNER, 2001.

16 Vid., GUTIÉRREZ. 1995.

Tabla 1. Valores de la práctica deportiva[17].

DIMENSIÓN GENERAL	
Justicia y honestidad	Comportamiento ético
Autosacrificio	Autocontrol
Lealtad	Justicia
Respeto a los demás	Humildad
Respeto por las diferencias culturales	Perfección en la ejecución
Juego limpio	Verdad
Eliminación de prejuicios	Intercambio cultural
Amistad internacional	Autorrealización máxima
DIMENSIÓN PSICOSOCIAL	
Disfrute, diversión, alegría	Lealtad, integridad
Autoestima, autorrespeto	Honestidad, deportividad
Respeto a los puntos de vista diferentes	Valor
Respeto a los adversarios	Respeto a las decisiones de los árbitros
Control emocional, autodisciplina	Determinación
Juego con los límites propios	Autorrealización
Tolerancia, paciencia, humildad	Salud y bienestar físico
Liderazgo y responsabilidad	Amistad, empatía, cooperación
DEPORTE RECREATIVO Y AIRE LIBRE	
Uso creativo del tiempo libre	Iniciativa, originalidad
Estética	Reconocimiento personal
Disfrute y satisfacción personal	Independencia
Participación familiar	Intereses vocacionales
Evasión emocional	Nuevos y continuos desafíos
Participación no competitiva	Logro personal, autorrealización
Autodisciplina y autorrespeto	Aprecio y respeto por la naturaleza
Bienestar físico y psicológico	Control emocional y responsabilidad
Comunicación	Comprensión de sí mismo y de los demás
Liderazgo	Lealtad hacia el grupo
Promoción del logro y la experiencia	Relajación

CONCLUSIONES

Lo fundamental en los actos terroristas cometidos por una variabilidad de sujetos no es el propio proceso de radicalización, sino la desconexión social que sufre. Por lo que

[17] FROST & SIMS. 1974, *cit.* GUTIÉRREZ. 2003.

se afirma que, con la actividad física y el deporte, se pueden crear esos ámbitos carenciales de los que precisa todo joven.

El deporte y la actividad física debe ser vista como posibilidad o alternativa a la agresividad, frustración, falta de identidad, al egocentrismo y narcisismo. Partir de la base o de la consideración del deporte como motivación para suplir las posibles carencias y algunas estructuras psicológicas, siendo un elemento más para el proceso de socialización. Necesidad de imitación en el deporte.

BIBLIOGRAFÍA

– CERDEIRA GUTIÉRREZ, I. «El malestar social». *Escuela Universitaria de Trabajo social* (1). 1988, pp. 129-142. Recuperado el 25 de junio de 2019, de file:///C:/Users/MINERVA/Downloads/9505-Texto%20del%20art%C3%ADculo-9586-1-10-20110531.PDF.

– DAHRENDORF, R. *Oportunidades vitales*. Madrid: Espasa Calpe, 1983.

– *Diccionario de Psicología*. 2016-2019. Recuperado el 23 de julio de 2019, de http://psicopsi.com/Diccionario-de-psicologia-letra-N-Narcisismo-primario-narcisismo-secundario.

– FROST, R., & SIMS, E. *Manual sobre educación física y el deporte*. Barcelona: Paidós, 2003.

– GARCÍA-PABLOS DE MOLINA, A. *Tratado de Criminología* (4.ª ed.). Valencia: Tirant Lo Blanch, 2009.

– GARDNER, H. *Estructuras de la mente, la teoría de las inteligencias múltiples*. Colombia, Santafé de Bogotá; Fondo de Cultura Económica, 2001.

– GOLDSMITH, H., & HARMAN, C. «Temperament and Attachment: individuals and relationships». *Current Directions in Psychological Science* (1). Abril de 1994, pp. 53 y ss.

– GRIPPO, J. *Psiconotas.com*. 28 de abril de 2012. Recuperado el 23 de julio de 2019, de https://www.psiconotas.com/narcisismo-primario-y-secundario-273.html.

– GUTIÉRREZ, M. *Valores sociales y deporte*. Madrid: Gymnos, 1995.

– HERNÁNDEZ ESPINOSA, V. «El narcisismo relacional de Freud». *Temas de psicoanálisis, 8*. 2014, pp. 1-16. Recuperado el 23 de julio de 2019, de http://www.temasdepsicoanalisis.org/wp-content/uploads/2014/07/El-Narsicismo-relacional-de-Freud-PDF.pdf.

– INUPSI. «Dinámica intrapsíquica». *Tema 2. Módulo I. Introducción. Psicología y concepto de terrorismo. Experto en Psicología del Terrorismo*. Madrid: Inupsi, Instituto Universitario de Psicología Dinámica, 2019.

– LACAN, J. *El estado del espejo.* Buenos Aires: Siglo Veintiuno editores, 1946.

– LÓPEZ MELERO, M. «La indiferencia afectiva como rasgo nocivo de la personalidad». *Anuario de Derecho penal y Ciencias penales, LXXI* (MMXVIII). Ministerio de Justicia, Ed., 2018, pp. 265-305.

– MARTÍNEZ DE SALAZAR, A. «Agresividad y violencia en el desarrollo». En GÁZQUEZ, J., PÉREZ, M., CANGAS, A. & YUSTE, N. *Situación actual y características de la violencia escolar* (pp. 3-21). Granada: Grupo Editorial Universitario, 2007.

– MOGHADDAM, F. «Straicase to Terrorism. A psychological exploration». *Dans The American Psychologist*. February-March de 2005, pp. 161-169.

– PARIS, J. *Borderline personality disorder: A multidimensional approach.* Washington, D.C: American Psychiatric Publishing, 1994.

– PELEGRÍN, A. *El comportamiento agresivo y violento: factores de riesgo y protección como mediadores de inadaptaciones y adaptaciones en la socialización del niño y el adolescente*. Tesis doctoral no publicada. Murcia: Universidad de Murcia, 2004.

– REINARES, F. *Terrorismo y antiterrorismo.* Barcelona: Paidós, 2001.

– SILKE, A. *Research on Terrorism: Trends, Achievements and Failures.* Portland: Fank Cass, 2004.

– TARDE, G. *Estudio penales y sociales.* Madrid: La España Moderna, 1890.

– TRIANES, M. *La violencia en contextos escolares.* Málaga, Archidona: 2000.

– TUCKER, P. «Why Do People Join ISIS? Here's What They Say When You Ask Them». *Defense One (8 diciembre de 2015).* 2015.

– VALERO MATAS, J. *Una mirada a la sociología desde las ciencias sociales.* Madrid: Tecnos, 2009.

TERRORISMO *LOW COST* [1]

MONTSERRAT LÓPEZ MELERO
Grado en Criminología. Máster de Terrorismo Global.
Doctora en Derecho por la Universidad de Alcalá.
Doctoranda en Ciencias Forenses en Escena del Crimen

MODUS OPERANDI

Para poder hablar del *modus operandi* debemos afirmar, en primer lugar, la versatilidad del fenómeno del terrorismo internacional del corte yihadista y, en segundo lugar, el poseer una alta capacidad de adaptabilidad y cambio en su evolución criminal. Respecto de la versatilidad, acertadamente indica Klandermans que hay dos elementos necesarios para la supervivencia de toda organización terrorista: 1. Una base social de apoyo y, 2. Captación de nuevos adeptos. Y, en cuanto a la evolución criminal, se observa tras un análisis exhaustivo de la conducta, que poseen una alta capacidad de adaptación, e incluso, de salir reforzados de determinadas situaciones que pueden tener una connotación dificultosa.

Basta con que hagamos un breve recorrido por los diferentes atentados terroristas de corte yihadista para que se observe la diversidad en la tipología de las acciones, desde un atentado complejo hasta los actores o lobos solitarios, pasando por atentados terroristas *low cost* (de bajo coste) por utilizar una única arma blanca o de fuego o un vehículo; todos estos instrumentos o herramientas forman parte de la clara evolución del *modus operandi*, aseverando que el terrorismo no tiene una metodología concreta ni un patrón claro de actuación, es decir, se trata de actuaciones *radonm events*.

Pero ¿qué es el *modus operandi*? Según Gross es la manera en la que un crimen se ha materializado, es decir, se refiere a:

– Acciones que se dan antes/durante/después de la génesis del hecho delictivo (*iter criminis*).

[1] Comunicación presentada en el XXVI Curso Internacional de Defensa. 2018.

– Actos de preparación.
– Actos de precaución.
– Cómo accede a una escena del crimen, cómo se marcha de la misma.
– Etc.

Como afirma Turvey respecto de los objetivos:

– Proteger la identidad del agresor, es decir, todos aquellos aspectos que puedan dificultar la identificación y que imposibiliten o dificulten establecer relación alguna con el hecho delictivo.
– Conseguir su objetivo de cometer la conducta criminal, en su totalidad.
– Facilitar la entrada y huida del agresor de la escena del crimen, es decir, los comportamientos que se efectúan para alejarse de la escena y no ser relacionado.

¿Por qué es importante conocer el *modus operandi*? Porque nos aporta datos de cómo se materializan los atentados terroristas, porque podemos establecer programas de prevención y de seguridad, entre otros aspectos. Los actos ejecutados que conforman el MO son necesarios para que el autor efectúe con éxito la acción criminal. Buscamos conductas como método de aproximación a la víctima (por engaño o sorpresa). Momento del día elegido para actuar, de esta manera se observa si trabaja o no zonas de la escena seleccionada para abordar o aproximarse o/y atacar a la víctima; arma utilizada y fuerza necesaria para controlar a la víctima; cómo accede el sujeto a la escena del crimen y cómo la abandona; las conductas o actos de precaución (actos que realiza para evitar que la víctima se oponga a sus deseos y para que no sea reconocido o capturado); planificación antes del crimen; vigilancia previa de la víctima y/o de la escena del crimen; solicitar a la víctima que colabore; método de matar a la víctima; lugar y posición del cuerpo de la víctima; nos tenemos que preguntar si los materiales que el agresor lleva a la escena del crimen y sus conductas son las apropiadas para realizar el acto de la conducta criminal.

DATOS SOBRE LA EXPERIENCIA DELICTIVA TERRORISTA

Tras analizar las diferentes fuentes que nos muestran y dan a conocer los diferentes atentados terroristas de corte yihadista, se han obtenido las siguientes conclusiones:

– El terrorista que comete el acto no tiene una previa experiencia criminal en terrorismo.
– El terrorista suele cometer otros hechos delictivos menores.
– Hay una clara demostración de la vinculación de la delincuencia de baja intensidad con el terrorismo internacional.
– Supone una verdadera amenaza lo que se conoce como *terrorista autodidacta.* Ya no se necesita esa formación que ofrecían las organizaciones terroristas tradicionales. La escuela es Internet y las redes sociales.

¿CÓMO ES EL *MODUS OPERANDI* DE LOS TERRORISTAS?

Pregunta sin respuesta concreta, dado que existen diversidad de factores —políticos, ideológicos, etc.,— por los que una organización comete los atentados. Ahora

bien, debemos tener en cuenta que el terrorismo es uno de los máximos exponentes de delitos contra las personas y, por ello, conviene tener en cuenta para su análisis cuatro criterios que son fijados por el Tribunal Supremo sentando doctrina jurisprudencial —STS 2807/2017, Sala de lo Penal, Sección 1.ª de 21 de julio—, de análisis para la alevosía, eliminando cualquier tipo de defensa por parte de la víctima: normativo, objetivo, subjetivo y teleológico.

- Elemento normativo. La alevosía solo puede proyectarse a los delitos contra las personas, aspecto que concuerda plenamente con el terrorismo.
- Elemento objetivo. Radica en el *modus operandi,* supone que el autor utilice en la ejecución medios, modos o formas que han de ser objetivamente adecuados para asegurarla mediante la eliminación de las posibilidades de defensa, sin que sea suficiente el convencimiento del sujeto acerca de su idoneidad.
- Elemento subjetivo. Significando la doctrina jurisprudencia del Tribunal Supremo que el dolo llevado a cabo por el autor debe proyectarse no solo sobre la utilización de los medios, modos o formas empleados, sino también sobre su tendencia a asegurar la ejecución y su orientación a impedir la defensa del ofendido, eliminando así conscientemente el posible riesgo que pudiera suponer para su persona una eventual reacción defensiva de aquel.
- Elemento teleológico. Impone la comprobación de si en realidad, en el caso concreto, se produjo una situación de total indefensión, siendo necesario que se aprecie una mayor antijuricidad en la conducta derivada precisamente del MO, conscientemente orientado a aquellas finalidades —STS 1866/2002, Sala de lo Penal, Sección 1.ª de 07 de noviembre—.

Para entender, por tanto, la versatilidad del terrorismo internacional de corte yihadista, acertadamente el profesor Petter Nesser manifiesta que **«**Los yihadistas han adaptado siempre su *modus operandi* a las condiciones de seguridad de los países en los que actúan. El que haya aumentado el número de terroristas que actúan en solitario es un ejemplo de esta adaptación**»**. Es decir, muchas de las acciones terroristas se encuentran amparadas por el efecto *copycat* en un claro exponente de la vigencia de las *leyes de la imitación* de Gabriel Tarde. Según el autor, hay tres leyes que explican el comportamiento criminal, a saber: Primera ley. El hombre imita a otro en proporción directa al grado de proximidad o intimidad de la relación entre ellos existente de su naturaleza. Segunda ley. El superior es imitado por el inferior. Tercera ley. Conocida también como *ley de la inserción*, destaca el carácter subsidiario o alternativo con que actúan ciertas modas criminales recíprocamente excluyentes cuando concurren en el tiempo, es decir, que el incremento de la moda criminal más reciente es correlativo al descenso del anterior (puede haber excepciones).

Pasado al ámbito del terrorismo internacional de corte yihadista salafista, se puede afirmar que: - muchos de los sujetos que forman parte de las filas de las organizaciones terroristas internacionales de corte yihadista salafista imitan los actos, imitan las conductas y los comportamientos, y lo hacen en proporción a la cercanía o relación que tienen con otros miembros de la organización terrorista; - de otro lado, imitan a sus líderes, además cumplen «órdenes» de ellos; - el modo de actuar en los atentados va progresando, como veremos en los cuadros, al principio la «moda criminal» era con inmolaciones,

pasó a armas, para luego terminar con vehículos, unas excluyen a otras cuando concurren en el tiempo, aunque hay excepciones.

Como acertadamente indican Nesser y Stenersen, «La dimensión salafí tiene implicaciones para el *modus operandi*, en el sentido de que cualquier acto de violencia por parte de los yihadistas debe encontrar justificación y precedente en las tradiciones del Profeta (hadiz). Por ejemplo, un veredicto de un erudito salafí reconocido sobre el deber individual de los musulmanes de matar personas que insultan al profeta Mahoma, ha tenido efectos directos sobre la situación de amenaza en Europa. También se debe subrayar que la dependencia de los yihadistas de la justificación religiosa de ninguna manera contradice el pensamiento estratégico. Por el contrario, el movimiento tiene una fuerte tradición de producir textos estratégicos y evaluar la fecundidad de sus métodos de lucha. En el pensamiento yihadista, los principios y la estrategia religiosa van de la mano, ya que los militantes consideran que es un deber religioso imitar las estrategias y tácticas bélicas de los primeros musulmanes».

Afinando más la cuestión, hay que tener en cuenta la identidad como motivación, existen una serie de tendencias a circunscribir las indagaciones sobre *formas de acción política*, en el sentido de que los terroristas se desvían de aquellas normas que son ampliamente aceptadas por el resto de la sociedad y, esos estudios, hacen que busquemos posibles *aspectos de psicopatías, sociopatía, psicopatologías* o cualquier otra variable.

Por regla general, los estudios demuestran que los terroristas no se convierten en tal por *anormalidades psicopatológicas* ni por trayectorias psicóticas o de trastornos de la personalidad previas a la ejecución de sus crímenes. Pero, esto no excluye que se puedan tener en cuenta factores que son susceptibles de un metódico y estricto análisis psicológico, criminológico o incluso estratégico. Fernando Reinares señala que «las motivaciones de las organizaciones terroristas constituyen un tema difícil de aprehender. Establece, además, que los *objetivos políticos* son de particular relevancia para inducir a la participación individual, precisamente en organizaciones que, como las terroristas, tratan de afectar a la distribución del poder en una sociedad». No obstante, lo anteriormente indicado aparece combinado con otras motivaciones tales como criterios afectivos, de conformidad o no normativa, frustraciones, etc., algunas de las motivaciones que se pueden asociar a las conductas y comportamientos de los terroristas de corte yihadista salafista pueden ser:

– La *motivación racional*, o el *terrorista racional,* es partidario de pensar en la ley de costes y beneficios que pueden tener todas las opciones que le llevan a cometer el hecho delictivo o conseguir las metas planteadas. Es por ello, que a la hora de ejecutar los hechos delictivos pretende obtener el máximo beneficio al menor coste posible y, pese a ello, pese a que la balanza esté o no equilibrada, normalmente, la motivación racional hace que el terrorista alcance su objetivo. Por ejemplo, el del mercadillo navideño de Berlín en diciembre de 2016; o el de Londres en marzo de 2017, entre otros, se trata de atentados en el que el coste de llevar a cabo los mismos han sido mínimos frente al beneficio consistente en obtener un elevado número de víctimas (el cometer un atentado terrorista con un vehículo significa que utilizan una herramienta barata). Si bien es cierto, va a evaluar todos

los riesgos que pueda tener a la hora de cometer este hecho delictivo, riesgos no solo en cuanto a la magnitud del terrorismo sino, también, en cuanto al número de víctimas, llevando a cabo capacidades defensivas en cuanto a los *blancos de oportunidad* que son las víctimas.

– Respecto de la motivación psicológica, para un terrorista, supone ese descontento personal en cuanto a su vida y proyectos, esa frustración que se traduce en odio y en venganza. Tiene motivaciones antisociales que polarizan teniendo una única perspectiva o fin; lo que significa que proyectan su motivación psicológica hacia todas aquellas personas que no forman parte del grupo, de su ideología, de sus principios, de sus valores, y esto es lo que les permite a los miembros de las organizaciones terroristas a *deshumanizar a las víctimas*.
– Respecto a la motivación cultural viene a decir que el *tratamiento de la vida individual* tiene un impacto entre los militantes del terrorismo. Es, en este aspecto, donde se puede hablar con mayor extensión sobre el terrorismo de corte yihadista que, principalmente, participan jóvenes de la segunda generación de inmigrantes aquí en España, en el que no se sienten identificados con la sociedad española, pero tampoco con la sociedad respectiva de su nacionalidad, puesto que cuando acuden a esos países tampoco se sienten identificados con la gente de su pueblo.

  • Motivación ideológica y política. Respecto a las motivaciones del terrorismo de corte yihadista, y especialmente con el terrorismo de Dáesh, hay un éxito extraordinario a la hora de atraer jóvenes para que actúen como combatientes extranjeros. Las motivaciones más importantes y significativas son:
  • Las imágenes del conflicto en Siria.
  • Las noticas sobre el comportamiento de las fuerzas gubernamentales.
  • La idea y percepción de pasividad, así como de falta de apoyo por parte de Occidente respecto a los dos puntos anteriores.

Esto hace que una parte de los jóvenes que deciden formar parte del Dáesh genere un sentimiento de pertenencia a la comunidad musulmana o *umma* por lo que adoptan una ideología y motivación ideológica y religiosa radical.

El Informe de 2015 del *International Centre for Counter-Terrorism* (ICCT) asegura que las motivaciones específicas para desplazarse a Siria e Irak varían, oscilan desde el altruismo y la solidaridad hasta razones prosaicas y egoístas. Desde mejorar su situación social y económica hasta motivaciones identitarias. Un informe del *Soufan Group* sugiere que la motivación de los jóvenes que se unen es de carácter más personal que político. La explicación que se da es que la mayoría de la propaganda del Dáesh va dirigida a atraer a aquellos que buscan un nuevo futuro y no a los que tratan de encontrar venganza por actos pasados (este sería el caso del terrorismo de ETA). La búsqueda por una causa a la que dedicar la vida, la pertenencia a un grupo, la aventura, parecen ser las motivaciones más significativas (8 de diciembre de 2015).

Ahora bien, las motivaciones de los combatientes que proceden de países occidentales tienen, «como primera motivación, la identitaria y, como segunda, la búsqueda de aventuras» (Tucker). Lo característico no es el propio proceso de radicalización, sino la

desconexión social, la desafección y el resentimiento. Es aquí donde se incluye todo el colectivo de descendientes de inmigrantes musulmanes que sufren crisis de identidad.

LOBO SOLITARIO

Partimos del art. 577 del Código Penal, que dictamina: «Será castigado con las penas de prisión de cinco a diez años y multa de dieciocho a veinticuatro meses el que lleve a cabo, recabe o facilite cualquier acto de colaboración con las actividades o las finalidades de una organización, grupo o elemento terrorista, o para cometer cualquiera de los delitos comprendidos en este capítulo». Dudosa figura que se incorpora a nuestra Ley penal en su modificación, como indica acertadamente mi maestro García Valdés. Aseverando, además, «Extravagante donde los haya, este tipo encaja mal con el carácter organizado y plural de la delincuencia terrorista».

Los actos terroristas son parte de una estrategia global. Esta estrategia exige una jerarquía y la jerarquía demanda comunicación. Históricamente se han realizado una serie de estudios y tratados en los que se ha llegado a la conclusión de que «la suprema excelencia no es combatir y conquistar a tus enemigos en todas tus batallas. La suprema excelencia consiste en romper la resistencia de tu enemigo sin combatir» (Sun Tzu. Manual *El arte de la guerra*).

Las acciones y conductas llevadas por los actores solitarios son las más difíciles de prever por las fuerzas de seguridad, debido a que los actores son personas integradas en la sociedad occidental, lo que conlleva una dificultad añadida a la hora de monitorizar la amenaza que suponen, por la incapacidad de previsión de la comisión de dichos ataques. Muchos de estos sujetos tienen como características el que están aislados, se sienten insatisfechos o frustrados con su vida, tienen baja autoestima, son hijos de emigrantes, forman grupos marginales, con bajo estatus económico y educativo, en muchos casos. Sin embargo, su vida cotidiana transcurre con normalidad siendo sus hábitos sociales, religiosos o laborales normales, su comportamiento diario transcurre sin incidentes, lo que hace aún más complicada su detección. Otra característica que acompaña al actor solitario es su expansión a través de redes sociales (Internet), ya que facilita el posible contacto con otros individuos de carácter yihadista, pertenecientes principalmente a la organización terrorista Dáesh, proporcionándoles una identidad que les hacen sentirse parte de una comunidad virtual.

Como indica Spaaij, «Los límites del terrorismo de lobo solitario son inevitablemente confusos y arbitrarios. La táctica del terrorismo tiene una orientación política más que meramente personal o criminal. El objetivo inmediato y directo del ataque suele ser de importancia secundaria para su objetivo secundario o su mensaje o efecto más amplio». Afirma, que «El terrorismo de lobo solitario no es un fenómeno nuevo. Equivalentes de este tipo de terrorismo se pueden encontrar en el anarquismo del siglo XIX (no quiere ello decir que los anarquistas son terroristas».

Estos sujetos tienen, además, como características en el *modus operandi* las siguientes:

- Método de aproximación: aborda a sus víctimas valiéndose del factor sorpresa, aspecto que impide o dificulta cualquier acto de defensa.
- Método de ataque: existe una amplitud de medios —armas blancas, explosivos como terrorista suicida o bien vehículos—.
- Grado de planificación: generalmente se trata de acciones poco planificadas donde prima la improvisación.
- Actos de precaución: no existe una excesiva preocupación por este aspecto, pues el terrorista tiene claro que morirá en la acción o bien será detenido por las autoridades.
- Frecuencia y duración de los ataques: los ataques se caracterizan por su rapidez y en ocasiones por su alta letalidad, dependiendo del medio agresor que se utiliza (arma blanca, fuego o vehículo).

TERRORISMO *LOW COST*

Actualmente, Dáesh se está caracterizando por llevar a cabo ataques terroristas con una menor sofisticación, supone una apuesta por el denominado terrorismo *low cost*, aspecto de gran actualidad y que ha puesto en jaque a las diferentes agencias de inteligencia y cuerpos policiales de los diferentes países europeos por la dificultad que supone evitar atentados en los que escasamente se llevan a cabo actos preparatorios del *modus operandi*. Dentro de este terrorismo *low cost* se encuentra el fenómeno de los actores o lobos solitarios.

Los lobos solitarios pueden definirse como individuos que operan de forma individual, no pertenecen a ningún grupo o red terrorista y su *modus operandi* está concebido y dirigido por el propio individuo sin ningún tipo de órdenes ni jerarquía externa.

Teniendo en cuenta lo anterior, en un terrorismo de bajo coste podemos observar atentados con diferente arma o herramienta, a saber: con arma blanca, arma de fuego y con vehículos.

Atentados con armas blancas

Se llevan a cabo con un cuchillo de grandes dimensiones o de cocina.

AL QAEDA	**DÁESH**
Acciones terroristas muy elaboradas. Cierta sofisticación	Ha tenido la capacidad de materializar sus atentados con una inversión mucho menor o en ocasiones mínima, en un claro paradigma de lo que se ha venido a denominar «terrorismo *low cost*»
Fáciles de detectar	Difíciles de detectar
	Se está caracterizando por un aumento en el uso de cuchillos y otro tipo de armas blancas.

Una explicación criminológica al fenómeno puede ser: que la utilización de armas blancas es más fácil de adquirir que otros tipos de armas más letales, como pueden ser los explosivos.

El primer ataque del que existen registros en Occidente fue el asesinato del imán por el GIA en Francia en 1995, si bien, el caso más mediático y paradigmático fue el asesinado del cineasta Theo van Gogh en la ciudad de Amsterdam, en noviembre de 2004. El agresor utilizó una pistola, con la que efectuó dos disparos, para acto seguido decapitar al director.

No fue hasta el año 2010, cuando un terrorista de origen somalí trató de asesinar al caricaturista Kurt Westergaard con un hacha. De acuerdo con los datos oficiales, entre los años 2008 a 2013 hubo un destacado aumento del uso de cuchillos en las agresiones de los terroristas yihadistas, siendo el 33 % de estas agresiones en combinación con armas o de fuego o en ocasiones con explosivos.

En el siguiente cuadro, se sintetizan las principales acciones que han sucedido en el periodo de 2017 en el que este medio es efectivo.

19 de agosto de 2017 (SURGUT)	Siete personas resultaron heridas como consecuencia del ataque perpetrado en Surgut por un individuo con un cuchillo que se abalanzó sobre ellas apuñalándolas antes de resultar abatido por agentes de seguridad rusos. El atentado fue reivindicado por DÁESH a través de su agencia afín Amaq.
19 de agosto de 2017 (TURKUT)	Un individuo marroquí de 18 años identificado como *Abdulrahman Mechkan,* solicitante de asilo, fue detenido tras protagonizar un apuñalamiento masivo en la ciudad finesa de Turkut, falleciendo dos personas y provocando heridas a otras ocho.
1 de octubre de 2017 (MARSELLA)	Un individuo de origen tunecino identificado como *Ahmed Hanachi* fue abatido en la estación de tren de Saint-Charles, en Marsella, tras apuñalar a dos mujeres al grito de *allahu akbar*. La acción fue reivindicada por DÁESH a través de su agencia de noticias afín Amaq. El agresor fue abatido por los disparos efectuados por varios agentes de policía que repelieron el ataque. El DÁESH, a través de la agencia Amaq, reivindicó la acción terrorista.

Atentados con arma de fuego

Se puede valorar que el armamento ligero —pistola, fusil, escopeta— siempre ha estado ligado a todo tipo de delincuencia, bien para facilitar la comisión del hecho delictivo, bien (o incluso) como medio de protección en su huida. Ahora bien, podemos señalar un arma que ha estado presente en las acciones armadas llevadas a cabo en Occidente por el terrorismo internacional, el fusil de asalto AK-47. Tras preguntar a fuentes policiales sobre la posible explicación del uso, se indica que:

– Se trata del fusil más extendido, aspecto que abarata su coste en el mercado negro.

– Su letalidad, hay que tener presente que la munición de dicho fusil tiene un calibre (7,62 mm) lo suficientemente importante para causar muertos y heridos graves, aspecto que siempre está presente en el cálculo terrorista.

En este sentido, diversos informes de las agencias de seguridad, entre ellas EUROPOL, ponen el foco de atención acerca de la facilidad para cometer acciones terroristas con armas de fuego.

A continuación, se relacionan varias acciones con arma de fuego acontecidas en Europa en el año 2017.

1 de enero de 2017 (ESTAMBUL)	Un terrorista abrió fuego en el club de ocio Reina, situado en una exclusiva zona de Estambul, causando la muerte a 39 personas y heridas a otras 69. El atentado fue reivindicado por el D***Á***ESH a través de la agencia Amaq.
20 de abril de 2017 (PARÍS)	Un policía falleció y otros dos resultaron heridos, además de una viandante, como consecuencia de un tiroteo registrado en los Campos Elíseos de París.

Atentados con vehículos

Esta metodología de ataque que viene utilizando últimamente el terrorismo internacional en sus acciones en distintos puntos de Occidente, revela que en el binomio coste/oportunidad que efectúa todo terrorista antes de materializar su acción, la cual se puede relacionar criminológicamente con la *teoría criminológica de la elección racional* de Cornish y Clarke.

De la misma manera, es importante enfatizar que los atentados con vehículos han causado un gran número de víctimas, siendo en términos terroristas de un gran éxito, aspecto que lógicamente representa un **«**efecto imitación**»** para este tipo de terrorismo.

Parece evidente, que el cálculo que la organización terrorista D***Á***ESH, está apostando por un método que se caracteriza por ser seguro y barato. Son un medio de transporte de uso habitual y que, por tanto, dificultan un control preventivo sobre los mismos.

De la misma manera, se expone en un cuadro las principales acciones con este medio en el 2017.

7 de abril de 2017 (ESTOCOLMO)	Cuatro personas fallecieron y unas 15 resultaron heridas, como consecuencia del atentado perpetrado por un individuo el cual, conduciendo un camión de reparto que previamente había sustraído, arrolló a las numerosas personas presentes en una concurrida calle comercial. Posteriormente fue detenido un individuo de nacionalidad uzbeka, que se encontraba en el país con una orden de expulsión, tras habérsele denegado una petición de asilo.

19 de junio de 2017 (PARÍS)	En la Place Verdum de Levallois-Perret (Hauts de Seine-92), un individuo al volante de un vehículo BMW atropelló a seis militares integrantes de una patrulla cuando se disponían a ocupar sus vehículos e iniciar su turno de vigilancia en el marco de la Operación Sentinelle, resultando dos de ellos heridos graves y el resto heridos leves. Posteriormente fue detenido el autor de los hechos cuando circulaba por una autovía en la región de Paso de Calais, cerca del Canal de la Mancha. El detenido resultó herido por disparos efectuados por la policía, que creyó apreciar que portaba un arma. Fue identificado como *Hamou Benlatreche,* súbito argelino de 36 años de edad, carente de antecedentes y sin relaciones aparentes con radicalismos religiosos islámicos.

Atentados mixtos

Como último punto, no debe de obviarse la relación de atentados donde los terroristas han hecho una combinación de medios de ataque. Debido de significarse particularmente, que ese método de ataque se ha mostrado tremendamente efectivo, en términos de muertos y heridos, aspecto que pone de relieve que a futuro pudiera volver a reproducirse.

A continuación, se refleja una tabla que recoge las agresiones para el periodo expresado.

22 de marzo de 2017 (LONDRES): ATROPELLO+ACUCHILLAMIENTO	Un individuo de nacionalidad británica identificado como Adrian Russell-Ajao o Russell-Elms, que tras convertirse al islam cambió su nombre por el de *Khalid Masood,* atropelló con un vehículo todoterreno a numerosos transeúntes en las inmediaciones del Parlamento británico, para posteriormente estrellarse contra la valla perimetral del mismo. Tras apearse del vehículo, el terrorista atacó con un cuchillo a los agentes que vigilaban el acceso a la entrada del citado edificio, dando muerte a un policía. El balance total fue de cuatro muertos (incluido el propio terrorista) y al menos 50 heridos. La acción fue reivindicada por el DÁESH a través de la agencia Amaq.
3 de junio de 2017 (LONDRES): ATROPELLO+ACUCHILLAMIENTO	Ocho personas fallecieron y otras 48 resultaron heridas como consecuencia de un atentado terrorista perpetrado en Londres por tres individuos que atropellaron con una furgoneta a un numeroso grupo de personas que se encontraban en la zona de London Bridge. Posteriormente, y tras apearse del vehículo, se dirigieron a la zona de Borough Market, donde apuñalaron a varias personas antes de ser abatidos por agentes de la policía metropolitana. El ataque fue reivindicado por el DÁESH a través de la agencia Amaq.

Las investigaciones de Nesser y Stenersen demuestran los siguientes resultados:

– Los artefactos explosivos improvisados son el tipo de arma preferida entre los yihadistas en Europa.
– Los explosivos hechos en casa se han vuelto más comunes, dejando atrás los explosivos militares y comerciales. El terrorista yihadista ha empleado desde mezcla de clorato en contenedores, cerrado como ollas a presión, mezclas de peróxido, cilindros de gas, o fertilizantes.
– Se da paso a las armas como cuchillos y armas de fuego, disminuyendo los materiales químicos, biológicos, radiológicos o nucleares.
– Se ha dejado de usar la piratería de sistemas informáticos.

CONCLUSIONES

1. Las revistas de las organizaciones terroristas son una propaganda mediática y efectiva donde queda plasmado el *modus operandi* de las conductas y comportamientos de los actos delictivos. Dada la diversidad de métodos en la forma de ejecutar el *modus operandi*, hace que se configure como una amenaza difícil de combatir. Dado que no existen aspectos particulares que denoten la comisión del hecho y, a partir del mismo, se pueda planificar estrategias de protección.
2. Existe un vacío legal, jurisprudencial y, especialmente, doctrinal para una definición de terrorismo, lo que conlleva que no haya una concreta definición de actor o lobo solitario y, por ende, una concreta apreciación de cómo será el *modus operandi* de este tipo de sujetos. Todas las investigaciones que se han llevado a cabo han demostrado que dentro del terrorismo internacional de corte yihadista existen tipologías criminales, lo que hace que sea aún más difuso el modus operandi, variando sustancialmente. La diversidad de tipologías criminales pondera en una diversidad en la elección de la forma del ataque, desde armas al azar en la escena, hasta la combinación de armas o instrumentos de uso cotidiano (cuchillo o vehículo).
3. El aprendizaje vicario y las leyes de la imitación de Gabriel Tarde constituyen una vía eficaz de captación para la comisión de las conductas terroristas. Lo anteriormente indicado, ha dado lugar a un perfil criminal muy diferente del que estábamos «acostumbrados», en el que una única persona es capaz de tener en el punto de mira a un número de víctimas elevado.

BIBLIOGRAFÍA

– BRYNJAR, L., y HEGGHAMMER, T. «Estudios estratégicos yihadistas: el presunto estudio de política de Al Qaeda previo a los atentados de Madrid». *Estudios sobre conflictos y terrorismo*, 27, n.º 5. 1 de septiembre de 2004, pp. 355-375.

– DAY, J. **«**Terrorist Practices: Sketching a New Research Agenda**»**. *Perspectives on terrorism Volumen 9,* (6). 2015.

– DE LA CORTE IBÁÑEZ, L. y JORDÁN ENAMORADO, J. *La yihad terrorista*. Ed. Síntesis, 2007.

– EUROPOL. *Changes in Modus Operandi of Islamic State (IS) Revisited.* 2016.

– GARCÍA VALDÉS, C. «La legislación antiterrorista Española». *La Ley Penal*, n.º 74, Sección legislación aplicada a la práctica. 2010.

– GROSS, H. *Criminal Psychology. A Manual for judges, practitioners, and students*. Boston: Little, Brown, and company, 1911.

– KLANDERMANS, B. *Social Movements and Culture (Social Movements, Protest, and Contention).* Pencil Margin Notes; University of Minnesota Press, 1995.

– LÓPEZ MELERO, M. «Motivaciones de los terroristas». Tema 1 de la asignatura *Perfiles, radicalización y motivaciones de los terroristas.* Máster Universitario en Estudios Internacionales en Terrorismo Global de la Universidad Internacional de la Rioja (UNIR), 2018.

– MURGA, A. «Coches y cuchillos: la estrategia 'low cost' del Estado Islámico para extender el miedo». *El español*. 2017. https://www.elespanol.com/mundo/europa/20170323/202980378_0.html.

– NESSER, P. *Islamist Terrorism in Europe: A History.* Published to Oxford Scholarship, 2016.

– NESSER, P. y STENERSEN, A. «The Modus Operandi of Jihadi Terrorists in Europe». *Perspectives on terrorism Volumen 8* (6). 2014.

– REINARES, F. *Terrorismo y antiterrorismo*, Barcelona: Paidós, 2001.

– SPAAIJ, R. «The enigma of lone wolf terrorism: an assessment». *Studies in conflict & terrorism*, vol. 33, n.º 9. 2010, pp. 854-870.

– TARDE, G. *Estudios penales y sociales*. Madrid: La España Moderna.

– TUCKER, P. «Why Do People Join ISIS? Here's What They Say When You Ask Them». *Defense One*. 8 de diciembre de 2015.

– TURVEY, B. E. *Criminal Profiling: an introduction to behavioral evidence analysis.* Elsevier Science, 2008.

WEBGRAFÍA

– LA GACETA. «Terrorismo de baja intensidad». 2017. https://gaceta.es/noticias/terrorismo-baja-intensidad-14062017-2157/.

– EL ESPAÑOL. «Los terroristas aprenden con cada atentado frustrado». 2017. https://www.elespanol.com/mundo/europa/20170421/210229415_0.html.

– MARTÍ. «La policía francesa sigue las pistas serbia e islámica en el atentado del metro». *El País*. 1995. https://elpais.com/diario/1995/07/27/internacional/806796019_850215.html.

– EL PAÍS. «Asesinado en Amsterdam el polémico cineasta y escritor holandés Theo van Gogh». 2004. https://elpais.com/cultura/2004/11/02/actualidad/1099350001_850215.html.

– LA PROVINCIA. «Detenido un joven al asaltar la casa del caricaturista de Mahoma». 2010. http://www.laprovincia.es/mundo/2010/01/02/detenido-joven-asaltar-casa-caricaturista-mahoma/277928.html.

IMPACTO GEOECONÓMICO Y GEOESTRATÉGICO EN EUROPA DE LA PREVISIBLE FINALIZACIÓN DE LOS GASEODUCTOS NORD STREAM Y TURKISH STREAM POR PARTE DE LA REPÚBLICA FEDERATIVA RUSA

ARES CAPDEVILA BRUALLA
Grado en Derecho y Diploma Global Skills. Máster universitario en el Ejercicio de la Abogacía y de analista de Inteligencia

INTRODUCCIÓN

La Unión Europea ha dependido de la energía rusa desde la Guerra Fría. Instrumentalizando Moscú sus recursos energéticos con fines geopolíticos y geoeconómicos, abordando a los países europeos de manera bilateral.

El uso estratégico de los recursos energéticos permiten a Rusia contar con una gran influencia en la geopolítica mundial ejerciendo una importante posición de liderazgo cosechando éxitos en política exterior y contribuyendo a la estabilidad política doméstica.

Los gasoductos North Stream y Turkish Stream persiguen objetivos de la política exterior rusa, siendo las empresas alemanes las mayores beneficiarias económicamente de la construcción del North Stream. Ucrania, el país más afectado, no solo estratégica, sino también económica y políticamente, pudiendo así Rusia conseguir la soberanía de Ucrania y la solidaridad entre los países miembros de la UE.

La respuesta de Europa ante la estrategia del Kremlin fue desde el Parlamento Europeo en diciembre de 2018 donde se aprobó una moción que definía la construcción del North Stream 2 como un «proyecto político que representa una amenaza para la seguridad energética europea».

ANÁLISIS

Rusia y Occidente se han visto relacionados energéticamente desde la década de los 60 con la construcción de grandes conductos tubulares para conectar Argelia, Noruega y Rusia con los principales mercados europeos. Debido al incremento de los precios de hidrocarburos y la demanda europea al inicio del siglo XXI, Rusia llegó a controlar una cuarta parte del mercado del gas natural en Europa.

Contando con una gran cantidad de recursos energéticos, Rusia, respecto al gas es el primer país en términos de reservas con 47,8 billones m3 y el segundo en producción mundial, 635,5 millones m3, después de EE. UU., usando así estos recursos para ganar influencia sobre la comunidad internacional.

La geoeconomía definida como «el uso de instrumentos económicos para promover y defender los intereses nacionales, y para producir beneficios geopolíticos» (Blackwill y Harris, *War by other means*. 2017), incluye «los efectos de las actividades económicas

de otras naciones en los objetivos geopolíticos del país». Conforme lo establecido por ambos autores, el mejor país en la actualidad que utiliza la energía en la geopolítica es Rusia, al poner por encima el alcance de objetivos geoestratégicos a la maximización de los beneficios económicos de las empresas energéticas, cuya estrategia se debe al nivel de estatalización de las principales compañías energéticas, como en el caso de Gazprom, siendo la principal compañía energética Rusa con una participación estatal del 50,23 %.

Continuando con su estrategia energética hasta 2020, Rusia iba adquiriendo un mayor protagonismo en el sector energético con un conjunto de objetivos; entre ellos prohibir la reexportación de gas, cultivar vínculos estratégicos con Estados grandes e influyentes y mantener la competencia bajo control, convirtiéndose en mediador de la venta del gas de otras compañías.

Por otro lado, los países de la UE no consideraban que la dependencia del gas ruso fuera una amenaza geopolítica.

Sin embargo, cuando hubo una interrupción de los suministros rusos a Europa a través de Ucrania en 2009, a causa de las disputas por los precios del gas, se demostró que la seguridad energética europea está vinculada a los objetivos de la política exterior rusa y a los intereses de las compañías, dirigidas de manera poco transparente y controladas por los Estados.

Dicha crisis, ocasionó la construcción del North Stream para evitar que el suministro del gas a Europa dependiera de las disputas entre Rusia y Ucrania. Por ello, se anexionó Crimea en 2014 creando la UE la Unión Energética garantizando un suministro seguro, diversificando los países proveedores y evitando el monopolio de un proveedor; y en segundo lugar, con la promoción de una nueva estrategia energética de Rusia, la construcción de los North Stream 2 y Turkish Stream.

La construcción del gasoducto North Stream 2, ha ocasionado debate desde el 2015 siendo el centro de las discusiones sobre las relaciones entre la UE y Rusia.

A diferencia del proyecto del gasoducto Turkish Stream en 2014, que acaparó mucha menos atención, siendo una alternativa al South Stream (proyecto que fue cancelado por «la inflexibilidad de la UE» según la argumentación de Putin).

¿Pero que regulan las normas antimonopolio de la UE? Las tuberías de ambos gasoductos no pueden ser de propiedad directa de los proveedores. Por lo tanto, Gazprom tendrá que reajustar la propiedad de los North Stream 2 y Turkish Stream. En el caso de North Stream 2, tiene cinco socios europeos en la construcción, Uniper y Wintershall (Alemania) y Angie de Francia, Anglo-Dutch Shell y OMV (Austria). En Turkish Stream, siguen explorando posibles acuerdos con operadores europeos.

Con la construcción del nuevo proyecto, el gasoducto North Stream 2, se generaron una serie de implicaciones económicas y geopolíticas para el resto de la UE y los países vecinos.

La Comisión Europea manifestó el peligro que supone la construcción del nuevo gasoducto para las rutas ya existentes. Como también aportó un plan actual que consiste

en la creación de una Unión de la Energía que se basa en la política energética de la UE existente, como la Estrategia de Seguridad Energética y el Marco de Energía y Clima 2030. La estrategia consistiría en crear un «mercado único para la energía», promoviendo la energía renovable.

CONCLUSIONES

Después del análisis de las estrategias, podemos establecer que Europa se encuentra ante una situación de cierta gravedad que se verá aún más alterada con el proyecto del nuevo gasoducto que conecta a Rusia con la UE puede ser conflictiva.

La construcción de estos dos gaseoductos, no solo aumentan la dependencia europea a Rusia, sino también se reflejan los intereses nacionales alemanes frente a los comunes con la UE, lo que a su vez perjudica la cohesión y debilitando las relaciones interestatales.

No hay que olvidar que el mayor beneficiario económico de la construcción del North Stream 2 es el conjunto de empresas alemanas, dejando a Ucrania a un segundo plano, afectada no solo a nivel económico al perder los beneficios de tránsito, político al estar más aislada de Europa y estratégico al ser más vulnerable a las agresiones de Rusia.

Manifestándose el Parlamento Europeo en diciembre de 2018, aprobando una moción estableciendo que la construcción del North Stream 2, representa una amenaza para la seguridad energética europea.

Por otro lado, cabe destacar que ambos gasoductos no dirigen únicamente una finalidad meramente económica, sino también geoestratégica. Mientras la Unión Europea no consiga un consenso firme en materia energética, Rusia seguirá aumentando su poder y ganando influencia en el panorama político internacional a través de las exportaciones de gas natural. La unificación del mercado de gas europeo sería la forma más eficaz de disminuir el riesgo geopolítico de la dependencia de Rusia.

BIBLIOGRAFÍA

– CIA. «The World Factbook. Guide to country comparisons». https://www.cia.gov/library/publications/the- world-factbook/rankorder/rankorderguide.html.

– DIRECTORATE GENERAL FOR EXTERNAL POLICIES OF THE UNION. «Energy as a tool of foreign policy of authoritarian states, in particular Russia». Policy Department for External Relations, European Parliament, 2018.

– Fuente REPSOL. 2019.

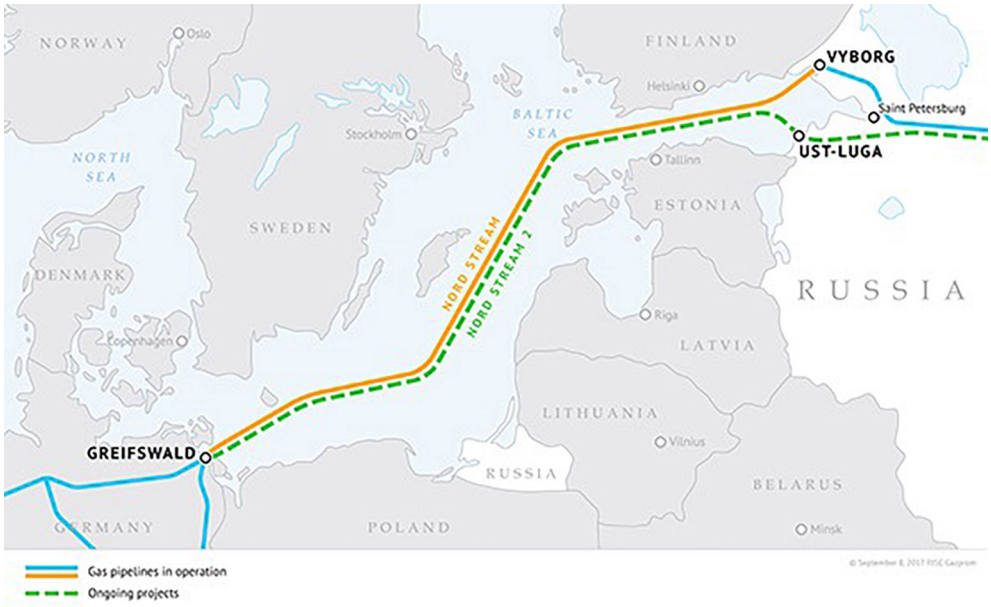
– GACHO CARMONA, Isabel. «Las implicaciones de la construcción de Nord Stream 2 para la Unión de la Energía de la Unión Europea». IEEE, 2019.

– LOPÉZ MARÍA, Paz. «El gasoducto de la discordia avanza». *La Vanguardia*. 2019.

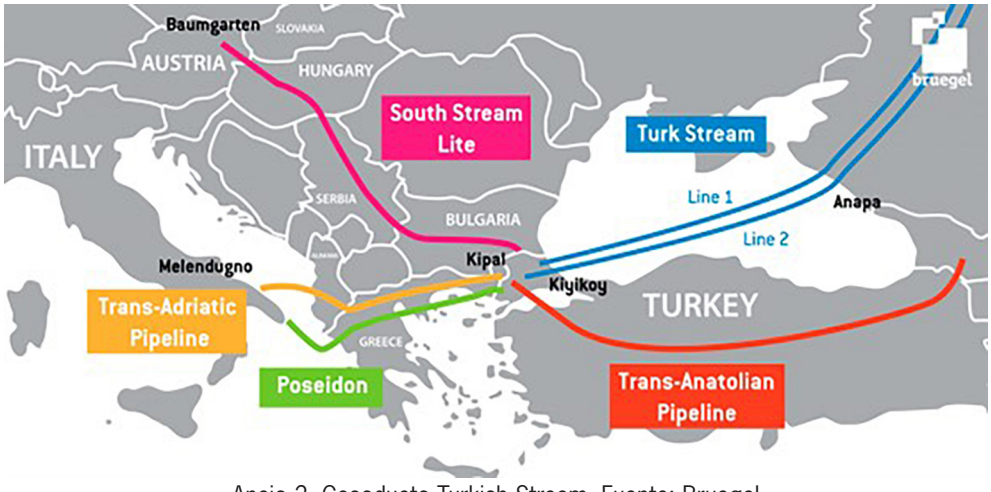
– MILOSEVICH, Juaristi. «Los aliados de Rusia: su ejército, su armada y su gas». Real Instituto el Cano, 2019.

– PIEDRAS MARTÍNEZ, Beatriz. «Geostrategia energética de Rusia en Europa». IEEE, 2017.

ANEJOS



Anejo 1. Gasoducto Nord Stream y Nord Stream II. Fuente: Gazprom



Anejo 2. Gasoducto Turkish Stream. Fuente: Bruegel

LO SOCIAL Y LA CIBERSEGURIDAD

MARÍA ENCARNACIÓN VÍLCHEZ VIVANCO
Licenciada en Sociología y en Ciencia Política y de la Administración por la Universidad de Granada. Master en Derecho Internacional y Relaciones Internacionales. Investigadora del Centro Mixto UGR-MADOC

PALOMA SALCEDO TAMAYO
Licenciada en Administración y Dirección de Empresas por la Universidad de Granada. Opositora al Cuerpo de Intendencia del Ejército

CRISTINA GUTIÉRREZ CORDERO
Capitán del Cuerpo de Artillería del Ejército de Tierra. Instructora del Tactical combat casualty care. Estudiante del master en Relaciones Internacionales de la Universidad Carlos III

Una mentira repetida muchas veces
se convierte en una gran verdad.
Lenin

Resumen

El ámbito cibernético se ve afectado por diferentes dinámicas sociales. Muchas de ellas son las mismas en un contacto cara a cara o en un entorno virtual. No podemos olvidar que el receptor de la interacción siempre es el individuo, y este se encuentra en el mundo físico y en el virtual.

La seguridad —también, la ciberseguridad— no es un concepto de fronteras perfectamente definidas. Muy al contrario, en su configuración intervienen, se superponen, se integran y, en ocasiones, se erosionan mutuamente, conceptos, métodos, procedimientos, herramientas y regulaciones que construyen una realidad multiforme y multidisciplinar (Galán y Galán, 2016 -305) donde la relación social es el motor.

Existen muchas teorías sobre las relaciones sociales que pueden explicar cómo funciona la información en entornos virtuales, pero en esta exposición solo se van a tratar tres de ellas. Estas tres son: la Teoría de Thomas, la Teoría de las Ventanas Rotas y el

Efecto Mateo. En realidad la comunicación que se establece en lo virtual no es muy diferente de lo que encontramos en otros entornos.

Estas tres teorías forman parte de la base explicativa del recorrido de la información y de cómo esta llega a sus destinatarios y es interpretada. Este devenir es fundamental, ya que ayuda a comprender de una manera más clara y eficaz el funcionamiento del ámbito cibernético. Esto permite poder desarrollar estrategias de seguridad en este ámbito, ya que el conocimiento lleva a establecer medidas más acertadas de la realidad en la que se actúa.

Palabras clave:

- Ciberseguridad.
- Efecto Mateo.
- Teoría de Thomas.
- Teoría de las Ventanas Rotas.
- Sociedad.

INTRODUCCIÓN

Desde el momento en que se emite un estímulo y llega a un receptor, desde ese momento ya se está produciendo comunicación[1]. El espacio en el que se produce esa comunicación condiciona al emisor y al receptor, de modo que exactamente aquello que se quiere transmitir no es aquello que se recibe. El mensaje queda condicionado. Además, el proceso de la comunicación se encuentra afectado por la interpretación, que lo condiciona.

Este condicionamiento es propio del ambiente. No podemos controlar todos los aspectos que se producen en la comunicación, resulta imposible, teniendo presente que ese ambiente por lo general no es estable, es cambiante, hace más difícil ese control de la comunicación. A pesar de todo, sí se puede hablar de una estabilidad, de unas líneas principales, unas ideas, que se mantienen en todo acto comunicativo.

En la comunicación interviene el individuo. Este puede ser emisor, receptor, o para el caso que nos interesa, ambas partes. La comunicación social[2] es esta, la que se produce entre individuos. Esta es la comunicación que más análisis y más interés despierta.

Podemos identificar, como señala Fojón y Sanz (2010), relaciones proveedor-consumidor no solo entre empresas y usuarios domésticos, sino también entre empresas, administraciones públicas y ciudadanos y, por supuesto, entre individuos.

---

[1] Tiene incidencia en el ámbito de los *mass media* y en la gestión política han analizado ampliamente cuáles son las características tanto del emisor como del receptor y del medio de transmisión en la gestión y divulgación masiva de información.

[2] La disciplina que estudia los diversos fenómenos sociales que intervienen en la comunicación.

Estas relaciones han existido desde mucho antes de la aparición de las TIC[3], a mediados del siglo XIX, con la invención del telégrafo y, por supuesto, antes de su revolución a partir del descubrimiento y aplicación de las propiedades de los materiales semiconductores que permitieron el nacimiento de la «era digital». Pero es a partir de ese momento, precisamente, cuando las TIC se convierten en el catalizador de los servicios tradicionales que prestaban las empresas a sus clientes, tanto de su extensión o capilaridad como de su eficiencia económica, al mismo tiempo que permitían la aparición de nuevos servicios.

Volviendo a los condicionantes de la comunicación, son estos de los más tratados. Estos condicionantes, como se ha dicho antes, son productos, pueden ser fruto de la propia comunicación, pero se producen concionantes creados por los propios intervinientes para controlar la comunicación. El control de la comunicación es el control de la información y ya alguien dijo «*la información es poder*»[4].

La comunicación cara a cara[5] se puede ver afectada por interferencias, intereses, pero la que se produce en un entorno virtual se ve afectada por estos mismo procesos pero de manera multiplicada. Aquí perdemos las certezas que nos dan el ver la persona de manera física. Los fenómenos que afectan a la transmisión de información en lo virtual son muy parecidos a los que se producen en el mundo físico. En el ambiente virtual tenemos que sumar que los efectos se generan a un mayor número de individuos y en mucho menor tiempo.

La opinión pública siempre ha sido objeto en cuestiones de seguridad. Esta se ha buscado ganar desde todos los ámbitos posibles, actuando de manera que se obtuviera el resultado esperado, alentar en un conflicto, demonizar al enemigo, estimular la compra, etc. Los medios utilizados siempre han sido, cualquieras que estuvieran al alcance.

Todo esto siempre se ha permitido en un entorno de seguridad. Seguridad que en lo virtual ha venido a llamarse ciberseguridad. Esta, al igual que la seguridad que podemos sentir en un entorno real, se ve condicionada por diferentes teorías sociales que llevan al individuo a ser participe, creer y reprobar esa información que le llega.

Dice el coronel Baños (2017, 245-246) que siempre ha sido primordial ganar la opinión pública, pero cada vez se está haciendo más importante, conquistar «mentes y corazones», vencer en la guerra de las ideas. Una manera de convencer a la sociedad de algo en concreto es repetir esa idea hasta la saciedad.

Así lo entendía Josep Goebles[6] a quien se le atribuye la frase «*miente, miente que algo quedará; cuanto más grande sea la mentira, más gente se la creerá*» a la que

---

[3] Tecnología de la información y la comunicación.

[4] Se atribuye habitualmente a Francis Bacon, pero no aparece en ninguna de sus obras y sí puede ser encontrada en escritos de Thomas Hobbes.

[5] Es la comunicación que se establece entre dos personas que se encuentran de manera física frente a frente.

[6] Fue ministro para la Ilustración Pública y Propaganda de la Alemania nazi en el periodo 1933-1945.

suma: «*Afirma una mentira cien veces, y al cabo todo el mundo la creerá como un hecho fidedigno*».

¿Qué lleva a que una mentira sea entendida como una verdad, y que esta pueda llevar a perder los ahorros, a acceder para sustentar un ataque terrorista o a demonizar a un Estado?, esta es una cuestión primordial en el mundo actual. Se encuentra estrechamente relacionado el tema con la seguridad. Comunicación y seguridad están hoy obligados a entenderse.

Muchos afirman que los controles sociales informales pueden ser una estrategia efectiva para reducir el comportamiento rebelde, como el que se produce en el ámbito cibernético. Garland (2001) expresa que «las medidas de vigilancia comunitaria en la comprensión de que el control social informal ejercido a través de las relaciones e instituciones cotidianas es más efectivo que las sanciones legales». Esas acciones que no se entienden como forma de intromisión, es uno de los medios más efectivos en controlar una opinión.

TEORÍAS SOCIALES APLICABLES

En este apartado analizaremos las tres teorías explicativas del funcionamiento de la información en el ámbito cibernético. Estas tres teorías son: la Teoría de Thomas, la Teoría de las Ventanas Rotas y el Efecto Mateo.

Estas no son las únicas que actúan en el entorno de la comunicación, son solo tres seleccionadas a tal efecto, que unen su acción a las de otras muchas más.

Teoría de Thomas

La Teoría de Thomas es una teoría sociológica que fue formulada en 1928 por William Isaac Thomas y Dorothy Swaine Thomas (1899–1977). Esta teoría se basa en el siguiente axioma: «si los hombres definen situaciones como reales, estas son reales en sus consecuencias». (Thomas and Thomas, 1928: 571–572).

En otras palabras, la interpretación de una situación provoca la acción. Esta interpretación no es objetiva. Las acciones se ven afectadas por las percepciones subjetivas de las situaciones. Si hay una interpretación objetivamente correcta, no es importante para ayudar a guiar el comportamiento de los individuos.

En 1923, W. I. Thomas declaró más precisamente que cualquier definición de una situación influiría en el presente. Además, después de una serie de definiciones en las que un individuo está involucrado, dicha definición también «gradualmente influirá en una política de vida completa y en la personalidad del individuo mismo» (Thomas, 1967: 42).

En consecuencia, Thomas enfatizó que los problemas sociales como la intimidad, la familia o la educación son fundamentales para el papel de la situación al detectar un

mundo social «en el que las impresiones subjetivas pueden proyectarse en la vida y, por lo tanto, volverse reales para los proyectores» (Volkart, 1951: 14).

Teoría de las Ventanas Rotas

La Teoría de las Ventanas Rotas es una teoría criminológica y social que establece que los signos visibles de delincuencia, comportamiento antisocial y desorden civil, crean un entorno urbano que fomenta la delincuencia y el desorden, incluidos los delitos graves.

La teoría sugiere que los métodos de vigilancia que atacan delitos menores como el vandalismo, el consumo público y la evasión de impuestos ayudan a crear una atmósfera de orden y legalidad, evitando así delitos más graves.

En resumidas cuentas, viene a señalar que el individuo actúa conforme al entorno en el que se encuentra. Si el entorno es conflictivo y violento, el individuo no se ve limitado y actúa conforme a esos patrones.

La teoría apareció en 1982 de mano de los científicos sociales James Q. Wilson y George L. Kelling[7]. Se popularizó aún más en la década de 1990 por el comisionado de policía de la ciudad de Nueva York William Bratton y el alcalde Rudy Giuliani (Fagan and Davies, 2019), cuyas políticas policiales fueron influenciadas por la teoría. Es de destacar que el crimen disminuyó de manera significativa.

La teoría supone que el paisaje «informa» a las personas. Una ventana rota transmite a los delincuentes el mensaje de que una comunidad muestra una falta de control social informal y, por lo tanto, no puede o no quiere defenderse de una invasión criminal (Kelling and Cole, 1997). Lo importante no es tanto la ventana rota real, sino el mensaje que la ventana rota envía a las personas. Simboliza la indefensión y la vulnerabilidad de la comunidad y representa la falta de cohesión social.

Con respecto a la geografía social, la teoría de las ventanas rotas es una forma de explicar a las personas y sus interacciones con el espacio. La cultura de una comunidad puede deteriorarse y cambiar con el tiempo con la influencia de personas y comportamientos no deseados que cambian el paisaje (Childress, 2016).

Todos los espacios tienen sus propios códigos de conducta, y lo que se considera correcto y normal variará de un lugar a otro. Este es un método de control social informal.

Efecto Mateo

El Efecto Mateo se puede observar en muchos aspectos de la vida y campos de actividad. A veces se resume con «los ricos se hacen más ricos y los pobres se hacen cada

[7] WILSON, James Q.; KELLING, George L. «Broken windows». *Atlantic monthly*, vol. 249, n.º 3. 1982, pp. 29-38.

vez más pobres»[8]. El concepto es aplicable a asuntos de fama o estatus, pero también puede aplicarse literalmente a la ventaja acumulativa del capital económico.

El término fue acuñado por el sociólogo Robert K. Merton[9] en 1968 y toma su nombre de la parábola de los talentos del Evangelio de San Mateo.

«Y él les respondió: A ustedes se les ha dado conocer los secretos del reino de los cielos, pero a ellos no se les ha dado. Porque al que tiene más se le dará, y él tendrá abundancia; pero de él quien no tiene, incluso lo que tiene será quitado». Mateo 13: 11–12.

Merton, para describir cómo funciona el ámbito científico, señala cómo los científicos eminentes a menudo obtendrán más crédito que un investigador relativamente desconocido, incluso si su trabajo es similar. Señala también que generalmente se otorgará crédito a los investigadores que ya son famosos.

Además, Merton argumentó que en la comunidad científica el Efecto Mateo (1998) va más allá de la simple reputación para influir en el sistema de comunicación más amplio, desempeñando un papel en los procesos de selección social y dando como resultado una concentración de recursos y talento (Mertón, 1988).

Da como ejemplo la visibilidad desproporcionada dada a los artículos de autores reconocidos, a expensas de artículos igualmente válidos o superiores escritos por autores desconocidos (Gadamuz, 2011).

Las investigaciones que siguen los conteos de descargas o las listas de libros más vendidos para libros y música han demostrado que la actividad del consumidor sigue la aparente popularidad (Sorenson, 2007).

En su libro de 2011 *The better angels of our nature: The decline of violence in history and its causes* de nuestra naturaleza: por qué ha disminuido la violencia, el psicólogo cognitivo Steven Pinker se refiere al Efecto Mateo en las sociedades, en el que todo parece ir bien y mal en otros lugares.

Expone que esto podría ser el resultado de un ciclo de retroalimentación positiva en el que el comportamiento imprudente de algunos individuos crea un ambiente caótico que fomenta el comportamiento imprudente de otros. Cita la investigación de Martin Daly y Margo Wilson[10] que muestra que cuanto más inestable es el entorno, más abruptas son las personas con el futuro y, por lo tanto, menos prospectivo es su comportamiento.

---

[8] Para conocer más sobre la acumulación y crecimiento de capital ver Altszyler, E.; Berbeglia, F.; Berbeglia, G.; Van Hentenryck, P. «Transient dynamics in trial-offer markets with social influence: Trade-offs between appeal and quality». 2017.

[9] Merton acredita a su colaboradora y esposa, la socióloga Harriet Zuckerman, como coautora del concepto del efecto Mateo.

[10] DALY, Martin; WILSON, Margo. *Homicide: Foundations of human behavior*. Routledge, 2017.

CONCLUSIONES

Una vez conocidas de manera sucinta lo que es la esencia de estas tres teorías sociales, es el momento de relacionarlas con la ciberseguridad.

La Teoría de Thomas viene a referirse a que si ves algo como real, actuarás de manera que sientes eso como real. Aquí el que algo sea real no tiene que ver con que sea real, lo único necesario es que se sienta como tal.

La Teoría de las Ventanas Rotas expone cómo un entorno ordenado y legal lleva a un comportamiento por parte de los individuos de esa misma manera, en cambio si ese entorno es violento, desordenado, descuidado, actuaremos de esa misma manera. El entorno condiciona nuestro comportamiento. Nos dejamos llevar por el entorno.

El Efecto Mateo, de las tres teorías posiblemente la más conocida, nos dice que más lleva a más y menos a menos. Si alguien tiene un prestigio reconocido en cualquier área, se le prestará más atención y no se dudará de su palabra. En cambio quien no tiene esa condición, aunque lo que expone sea producto de un trabajo concienzudo, su opinión será puesta en duda.

En la ciencia de redes, el efecto Mateo se usa para describir el apego preferencial de nodos anteriores en una red, lo que explica que estos nodos tienden a atraer más enlaces desde el principio. Debido al apego preferencial, un nodo que adquiere más conexiones que otro aumentará su nivel de conexión a una tasa más alta, y por lo tanto, una diferencia inicial en la conectividad entre dos nodos aumentará aún más a medida que la red crece, mientras que el grado de nodos individuales crecerá proporcionalmente a la raíz cuadrada del tiempo. Explica el crecimiento de algunos nodos en grandes redes como Internet.

Por ejemplo, podemos tener por tanto a un individuo, con muchos seguidores en las redes sociales, que cada vez tendrá más seguidores que en un ambiente agitado y violento lleve a expresar una opinión sobre un Estado denostándolo con argumentos que no se basan en la realidad. En este entorno, quien reciba esta información no dudará de que esa opinión es verdad, cree en quien la expresa ya que son muchos los que lo siguen (Efecto Mateo). Considera que esa opinión es verdad y que debe de actuar con respecto a esa verdad, ese Estado está encarcelando a personas por su condición sexual, por ejemplo, y busca actuar para defender esa situación (Teoría de Thomas). El individuo se encuentra dentro de una red que es agresiva, que insulta a los contrarios y los humilla, en el momento que actúa lo hace en esas condiciones, se ve amparado por ese entorno, no es diferente, es como el resto del grupo (Teoría de las Ventanas Rotas).

En esta situación, ya tenemos a un individuo que puede creer aquello que quiere creer y que siente que la verdad es solo eso que recibe de esas fuentes que considera reales. En la red, es un ejemplo de quiebra de la seguridad. La ciberseguridad rota por los ciudadanos de a pie.

BIBLIOGRAFÍA

– BAÑOS, Pedro. *Así se domina el mundo. Desvelando las claves del poder mundial*. Barcelona: Ariel, 2017.

– CHILDRESS, Sarah. «The Problem with Broken Windows Policing». *Public Broadcasting Service (PBS)*. PBS Frontline, 2016.

– CORMAN, Hope. *Carrots, Sticks and Broken Windows*. Washington: 2002.

– FAGAN, Jeffrey; DAVIES, Garth. «Street Stops and Broken Windows: Terry, Race, and Disorder in New York City». *Fordham Urban Law Journal*, 28 (2). 2019.

– FOJÓN, J. E., & SANZ VILLALBA, Á. F. «Ciberseguridad en España: una propuesta para su gestión». *Boletín Elcano*, (126), 8. 2010.

– GALÁN, C. M., & GALÁN, C. G. «La ciberseguridad pública como garantía del ejercicio de derechos». *Derecho & Sociedad*, (47). 2016, pp. 293-306.

– GARLAND, David (ed.). *Mass imprisonment: Social causes and consequences*. Sage, 2001.

– GUADAMUZ, Andres. *Networks, Complexity And Internet Regulation – Scale-Free Law*. EEUU: Edward Elgar, 2011.

– JENS, Ludwig. *Broken windows*. U Chicago: 2006.

– KELLING, George; COLES, Catherine. *Fixing Broken Windows: Restoring Order and Reducing Crime in Our Communities*. 1997.

– MERTON, Robert K. «The Matthew Effect in Science». *Science*. 1968.

– MERTON, R. K. «The Thomas Theorem and the Matthew Effect». *Social Forces*. 74 (2). 1995.

– MERTON, Robert K. «The Matthew Effect in Science, II: Cumulative advantage and the symbolism of intellectual property». 1998.

– PINKER, Steven. *The better angels of our nature: The decline of violence in history and its causes*. Penguin uk: 2011.

– SORENSON, Alan T. «Bestseller Lists and Product Variety». *Journal of Industrial Economics*, 55. 2017.

– SULLIVAN, Christopher M.; O'KEEFFE, Zachary P. «Evidence that curtailing proactive policing can reduce major crime». *Nature Human Behaviour*, 1 (10). 2017, pp. 730–737.

– THOMAS, W. I. & THOMAS, D. S. *The child in America: Behavior problems and programs*. New York: Knopf, 1928.

– THOMAS, W. I. «The Unadjusted Girl. With Cases and Standpoint for Behavioral Analysis». THOMAS, W. I. *Evanston*. London: Harper & Row, 1967.

– VOLKART, Edmond H. *Social Behavior and Personality. Contribution of Thomas to Theory and Social Research*. N.Y.: Social Research Council, 1951.

RUSIA COMO AMENAZA HÍBRIDA: DE LA GEOESTRATEGIA A LA CREACIÓN DE OPINIÓN

PABLO REY GARCÍA
Doctor en Comunicación. Profesor encargado de Cátedra en la Facultad de Comunicación de la Universidad Pontificia de Salamanca. Máster en Paz, Seguridad y Defensa por el Instituto Universitario «Gutiérrez Mellado»-UNED. Diplomado en Estudios Avanzados en Historia Contemporánea por la Universidad de Salamanca

JORGE MIRANDA GALBE
Doctor en Comunicación. Profesor en diversas áreas en la Facultad de Comunicación de la Universidad Pontificia de Salamanca

NURIA QUINTANA PAZ
Doctora en Comunicación. Profesora en diversas áreas en la Facultad de Comunicación de la Universidad Pontificia de Salamanca

RAQUEL MARTÍN MARTÍN
Alumna en la Facultad de Comunicación de la Universidad Pontificia de Salamanca

SILVIA LÓPEZ CORRAL
Alumna en la Facultad de Comunicación de la Universidad Pontificia de Salamanca

INTRODUCCIÓN

En esta comunicación pretendemos esbozar la respuesta a la hipótesis de que Rusia pretende volver a la influencia imperial a través de caminos indirectos, entre los que se cuentan los tradicionales de la amenaza híbrida: la potencia de las nuevas tecnologías y la propaganda travestida de información.

En las diferentes partes que componen la comunicación se planteará que, en primer lugar, Rusia no ha abandonado los usos habituales, la fuerza convencional, y que no solo tiene capacidad disuasoria, sino que la emplea, de forma abierta o encubierta, para lograr sus fines geoestratégicos.

En un segundo término se probará que las herramientas tecnológicas actuales le permiten a la Federación Rusa generar una presencia internacional, bien sea en forma de corrientes de opinión, bien sea a través de la actividad directa, favorable a sus intereses.

En una tercera instancia, mediante el análisis de caso sobre un medio de comunicación internacional como *Russia Today*, se demostrará la existencia de una sutil forma de narrativa, no específicamente pro-rusa, sino en general antioccidental.

LA TRADICIÓN DE LA FUERZA CONVENCIONAL

Hace ya veinte años que se cataloga a Rusia como uno de los «países emergentes», cuando en realidad nunca ha estado sumergido. A lo sumo, durante la caída del muro de Berlín y los años inmediatamente posteriores, Rusia estuvo dormida. Pero si la primera cabezada la daba en aquel noviembre de 1989, el despertar sería tan temprano como diciembre de 1994, cuando la artillería de la Federación Rusa abrió fuego contra Grozni, en Chechenia, apenas tres años después de que la Unión Soviética implosionase.

Bien es cierto que Rusia ha dado señales de saber leer perfectamente el contexto internacional. Acabado el mundo bipolar, no pretendió volver a armar un imperio, y contuvo las aspiraciones expansionistas e intervencionistas que habían caracterizado la exportación de la Revolución o el periodo de la Guerra Fría. La experiencia en Bosnia (el apoyo a los bombardeos de la OTAN sobre el cerco de Sarajevo en 1995) fue el exponente de la implicación de Rusia en el concierto internacional: un país colaborador, responsable, con una posición relevante, pareja a la de otras grandes potencias… pero no era más que un oso somnoliento.

La tremenda crisis financiera que convulsionó a Rusia en 1998 (el descenso de los precios del gas o el petróleo ocasionó una inflación del 75 %) supuso un parón en el desarrollo de todos los sistemas de armas, lo que el país sobrellevó priorizando la calidad sobre la cantidad.

Los cambios geopolíticos de los 90 —la independencia de Ucrania principalmente— obligaron a la reestructuración de flotas y arsenales, que en ocasiones afectaron a armamento nuclear. Kazakhstan y Bielorrusia también transfirieron sus arsenales, con menos problemas. Las medidas implantadas por Putin, a partir de 1999, permitieron un crecimiento económico cercano al 7 % anual durante casi una década, lo que se tradujo en un impulso a sus fuerzas armadas: en 2018 disponen de un presupuesto de 55.000 millones de dólares, el quinto del mundo, con un 3,93 % del PIB y el 11 % del gasto público (*Expansión*, 2019).

Ese mismo año de 1999, Rusia se oponía a los bombardeos de la OTAN sobre Belgrado, volviendo a cerrar filas con su aliado histórico, aunque no serían más que palabras. La misma posición volvería a mantener en el caso de la independencia de Kosovo, cuando en 2008 se produce la declaración unilateral de independencia.

Durante esos años de fricción, la OTAN ganó terreno y amplió sus fronteras, primero en Polonia y Chequia, en 1998, y con los países bálticos en 2004, lo que supone una

afrenta para Rusia, que se siente cercada. El escudo antimisiles impulsado por Estados Unidos es quizá la gota que colma el vaso, con destructores norteamericanos patrullando por el mar Negro y baterías instaladas en países de su antigua esfera de influencia.

Rusia estuvo ocupada en conflictos menores, aunque no de baja intensidad, en Georgia (Osetia y Abjasia) o Chechenia (la segunda guerra chechena), así como en el apoyo encubierto a las facciones en lucha en Crimea, Inghusetia, Daguestán o Transnistria; a través de la empresa Wagner se cree que ha estado presente en conflictos como la segunda guerra civil centroafricana, el conflicto de Sudán, apoyando al general Haftar en Libia o al presidente Maduro en Venezuela; pero no fue hasta la actual guerra de Siria cuando la Federación Rusa se implicó abierta y completamente en un conflicto exterior, con una dimensión internacional del más complejo nivel. El inicio de la implicación fue coherente con la línea de colaboración del concierto internacional que marcaba el temor universal al Daesh, pues la sociedad mundial se encontraba horrorizada, y así se entendieron los bombardeos de las posiciones del Dáesh desde el mar Caspio, pero el alineamiento posterior demostró claramente que el apoyo era para con el régimen de Assad. Lo ha hecho de manera constante, no solo con material, sino con fuerzas sobre el terreno, llegando a desplazar un grupo de combate (el del vetusto almirante Kunetzsov, con remolcador incorporado) circunnavegando Europa, casi como una demostración de fuerza. Aunque la participación de su ala embarcada fue importante, más lo fue su declaración de intenciones frente a Turquía e Israel, frente a otros presentes y futuros aliados, e incluso en última instancia, frente a la OTAN: Rusia no abandona a sus aliados.

Los roces, por otra parte con la OTAN, son constantes. A cada maniobra programada por esta última en el Báltico o el mar Negro, en Polonia o en los países bálticos, responde la Federación Rusa con otras maniobras simétricas. Los submarinos pulsan mares interiores y exteriores, los cazas hacen vuelos de reconocimiento con el objeto de conocer los tiempos de respuesta de cada país de la alianza; los espías renegados son ajusticiados allá donde hayan encontrado refugio; la integridad de la soberanía se reafirma en cada vuelo con el transpondedor apagado entre Kaliningrado y el resto del país… Es posible que la OTAN haya reformulado su estrategia, pero para la Federación Rusa la mera existencia de esta organización parece suponer una amenaza.

FUERZA NO CONVENCIONAL. LA CADENA DE DESINFORMACIÓN RUSA

Las nuevas tecnologías de la información y la comunicación, tales como las redes sociales e Internet, hacen que gobiernos, instituciones o personas individuales cuenten con mayor capacidad de influencia a nivel global. Esto se debe, entre otras cosas, a la gran cantidad de canales y mensajes que ofrecen medias verdades a los receptores de los mensajes (Paul y Mathews, 2016). A esto se suma la gran rapidez de respuesta de las redes sociales e Internet, donde la cultura de la inmediatez y la apariencia prima por encima de cualquier otro aspecto.

La credibilidad es un rasgo del que carecen, en gran medida, estas nuevas plataformas de comunicación, a no ser que los mensajes sean transmitidos por medios de contrastada reputación. Esta falta de credibilidad se debe a que son un producto de la Web

2.0, un medio que se basa en la cultura participativa y colaborativa. Esto quiere decir que son los usuarios quienes generan el contenido, dando lugar en muchas ocasiones a informaciones que no son adecuadas o verdaderas. Por lo tanto, es necesario contrastar la información en medios tradicionalmente bien considerados, así como la fuente de la información, algo clave para detectar noticias falsas o bulos.

Es por ello que algunos gobiernos, como el ruso, cuentan con una cadena de desinformación perfectamente orquestada en la que varios medios de diversas índoles presentan una misma información manipulada desde diferentes puntos de vista que, a su vez, dirigen el comportamiento de los receptores del mensaje en una dirección concreta.

Tal y como exponen Bodine-Baron, Helmus, Radin, y Treyger (2018), la cadena de desinformación rusa se compone de cuatro puntos fundamentales, y se conforma de la siguiente manera:

- *Liderazgo*: ejercido por el Estado ruso. En él se ven involucrados el Kremlin, el Ejército y altos cargos políticos y policiales. No queda claro cómo se organizan y coordinan con el resto de actores implicados en el desarrollo de la información pero, de lo que no queda ninguna duda, es de que las decisiones importantes y los objetivos que pretenden cumplirse mediante las informaciones que publican vienen dadas por los altos mandos del Gobierno.
- Órganos y representantes: en este segundo escalón aparecen los medios de comunicación atribuidos, tales como *Russia Today* –RT– o *Sputnik*. También aparecen medios no atribuidos como la Agencia de Investigación de Internet –IRA, *Internet Research Agency*–, conocida como la «factoría de troles de San Patersburgo». Estos órganos, a menudo, funcionan de forma individual creando contenidos favorables a los deseos del Kremlin. Por esta razón, aunque algunos de estos medios de comunicación no estén directamente asociados con el Gobierno ruso, es importante que mantengan una sincronía con sus políticas y creen contenidos afines a ellas.
- *Canales de amplificación*: en este tercer punto encontramos las redes sociales, principalmente *Facebook* o *Twitter*, aunque también juegan un papel importante otras como *Instagram.* Estas desempeñan un rol clave en la amplificación de sus políticas y publicidad, sirviendo al propósito de la desinformación expandiendo las noticias falsas. Para llevar a cabo esta tarea cuentan con *troles*, *bots* y con empresas que se encargan de incrementar los seguidores de sus cuentas, publicando o comentando información generada en las mismas. De esta forma, gracias a los algoritmos que manejan estas redes sociales, aumentan su visibilidad. Todo esto, además, «tiene su eco y se ve reforzado por las constelaciones de organizaciones de la sociedad civil, partidos políticos, iglesias y otros actores»[1] (Helmus *et al.*, 2018, p. 8) que ayudan a propagar la información y a otorgarle una veracidad ficticia.
- *Consumidores*: el último eslabón en la cadena de desinformación rusa está representado por los consumidores, una audiencia muy variada que va desde ciudadanos

[1] Traducción propia del original: «[…] it is echoed and reinforced through constellations of "civil society" organizations, political par- ties, churches, and other actors».

> hasta políticos. Interactúan con la información y se convierten en prescriptores de los contenidos. Recogen la información y pueden llegar a cambiar su forma de pensar o actuar debido a la gran cantidad de mensajes que reciben en la misma dirección.

Por lo tanto, la información proporcionada a la audiencia surge de los medios o agencias atribuidos que se encuentran ligados al Gobierno ruso, siendo replicadas o corroboradas por otros medios de dudosa atribución. El siguiente paso supone la creación de contenido generado por los usuarios, el cual es colgado en diferentes plataformas como pueden ser *YouTube*, *Instagram*, *Facebook* o *Twitter*, niveles donde encontramos la figura de los *troles* y los *bots*.

Esta cadena de desinformación supone un bombardeo mediático que genera gran cantidad de contenido haciendo que, a ojos de la mayoría de los receptores de los mensajes, estas noticias parezcan verdaderas. De esta forma, debido a la repetición continua de una idea en concreto, las medias verdades se convierten en verdades completas. La narrativa empleada no es lineal, por lo que los contenidos pueden ser consumidos por los usuarios en cualquier orden sin que afecte al resultado final.

Troles y *bots*

Rusia cuenta en Internet con una serie de agentes denominados *troles*, que se dedican a atacar toda información que vaya en contra de sus intereses (Paul y Mathews, 2016). Se trata de cuentas operadas por personas reales que intentan dirigir las conversaciones *online* hacia determinadas formas de pensar o comportamientos que son adecuados para favorecer la propaganda rusa. Esto se lleva a cabo en foros, redes sociales o cualquier tipo de plataformas de la Web 2.0.

Existen gran cantidad de cuentas de *Facebook* o *Twitter* mantenidas por el sistema de desinformación ruso que publican y comparten informaciones que no son totalmente ciertas. Para ello, «los *troles* son parte del sistema de propaganda del Kremlin y de las técnicas de la guerra de la información: estos comentaristas reclutados distribuyen los mensajes de los líderes políticos de Rusia en línea» (Aro, 2016, p. 122), así como de los medios afines.

Estos usuarios que actúan a favor de la propaganda rusa se encuentran en lo que se denomina «factorías de *troles*», donde producen información de forma continua en turnos de doce horas. Estas factorías disponen de un departamento de creación de imágenes, un departamento de vídeo, un diario *online* y un departamento donde los *troles* desarrollan su labor (Volchek y Sindelar, 2015). De esta forma, se crea una narrativa multimedia cuya función es generar desinformación a través de diferentes medios.

Por otro lado, aparecen los *bots*. En este caso se trata de cuentas guiadas por personas pero que funcionan de forma automática, publicando o compartiendo contenidos en función de una serie de algoritmos. Detectan *hashtags* – # –, menciones a determinadas cuentas o palabras clave marcadas de antemano. Son empleadas, también, para crear tendencias en las redes sociales, haciendo que se hable más sobre determinados temas.

Tanto las cuentas que emplean los *troles* como las que están operadas por *bots* son denominadas cuentas falsas. No expresan la opinión personal de nadie en concreto, sino que sus mensajes van dirigidos a generar información falsa o medias verdades a favor de determinados actores políticos y sociales. No obstante, el principal problema es que gran cantidad de usuarios reales que aceptan esta propaganda de forma orgánica, comentándola o compartiéndola. Estos usuarios, de forma no intencionada, sirven a los propósitos rusos.

La cadena de desinformación rusa ha actuado en tres escenarios cercanos de una manera relevante, el Brexit, las elecciones presidenciales norteamericanas de 2016 y la crisis de Venezuela. En el primer caso, uno de los nombres más sonados durante todo el proceso ha sido el de Arron Banks, multimillonario (casado con la rusa Ekaterina Paderina) que financió, durante muchos años, al UKIP, el partido de la Independencia del Reino Unido y la campaña de Leave.eu. Se estima que las donaciones hechas a la campaña del Brexit ascienden a más de trece millones de euros. Además, Banks mantuvo varios encuentros con altos funcionarios y empresarios rusos antes, durante y después del referéndum (Fresneda, 2018). La noche del referéndum se celebró una fiesta en Notting Hill en cuya lista de invitados figuraban el embajador ruso en Londres, y el diplomático Alexander Udod; expulsado de Reino Unido ante la sospecha de trabajar para la inteligencia rusa.

Otro punto caliente de actuación de Rusia en el Brexit fue a través de las redes sociales, principalmente por Facebook y Twitter, donde se utilizaron cuentas falsas para difundir mensajes apoyando este proceso de ruptura con la Unión Europea. Además, estas cuentas incitaban al odio contra el islam, tras los ataques de Manchester y Londres, haciendo referencia a un endurecimiento en las leyes de inmigración.

Por otra parte, en el contexto electoral norteamericano el Gobierno de Putin se encargó de *hackear* el correo del Partido Demócrata. Esta acción le dio acceso a toda la información que guardaba el partido de Hilary Clinton, y al facilitarla a intermediarios permitió que se filtrara hasta proporcionar ventaja su contrincante. Los motivos que llevaron al Gobierno de Putin a llevar a cabo esta intervención fueron tres: perjudicar a Hilary Clinton, fortalecer a Donald Trump, pero sobre todo, debilitar la democracia liberal, (RTVE, 2018).

Esta ayuda duró dos años y tuvo un alto coste millonario. Los funcionarios rusos tenían muy claro cuál era su misión dentro de este entramando. Lo primero que tenían que hacer era hacerse pasar por americanos y abrirse cuentas financieras propias. En ellas disponían de un presupuesto mensual en algunos casos de 1,25 millones de dólares. Con este dinero, ocultaban su identidad rusa comprando espacios en servidores de Estados Unidos, creaban perfiles falsos en las redes, difundían información sobre Hilary Clinton y promovían mítines políticos, (BBC, 2018).

Por otro lado, los rusos fueron implantando *fake news* en las redes sociales acerca del partido de Hilary Clinton. Esta iniciativa contaba con alrededor de ochenta funcionarios que se encargaban de estar permanentemente las 24 horas del día generando contenido en Internet a través de cuentas falsas y robadas. Los perfiles de Instagram, Facebook y Twitter que manejaban los rusos tenían como fin crear

discordia política y dar apoyo a Donald Trump a través de temas polémicos como la religión, la inmigración y el nacionalismo entre otros. «Donald quiere acabar con el terrorismo… Hillary quiere patrocinarlo», «Hillary es Satán, y sus crímenes y mentiras prueban su maldad», (Martínez Ahrens, 2018). Asuntos con los cuales ponían a Hilary Clinton en entredicho, criticando a la candidata. Esta desinformación estuvo sobre todo presente en los estados de Virginia, Colorado y Florida, las zonas más indecisas del país. Con esta iniciativa pretendían poner a la sociedad en contra del Partido Demócrata y beneficiar a Donald Trump, haciéndoles creer que era el menos malo de los dos representantes.

Por último, durante los años de mandato de Maduro en Venezuela, el Gobierno ruso ha proporcionado diversos préstamos al país latinoamericano, muestra de lo cual es el protocolo intergubernamental para prevenir la reestructuración de la deuda venezolana firmado por ambos países en noviembre del año 2017 (Ivànnikova, 2018). Además de estos préstamos económicos, Rusia también tiene diferentes proyectos petroleros y de venta de armas que, desde la presidencia de Hugo Chávez, el país caribeño se ha convertido en el principal comprador de armamento y de material militar ruso en todo el hemisferio occidental (Marginedas, 2019).

Otro signo de intervención de Rusia en la crisis venezolana es la presencia de aviones militares rusos con personal armado. Es evidente la cooperación militar entre Rusia y Venezuela, una presencia militar indisimulada y excusada por parte del Gobierno ruso como una manera de mantenimiento de los equipamientos militares de Venezuela, pero que *blogs* como Bellingcat se encargan de hacer un seguimiento a partir de fuentes abiertas (Higgins, 2019).

EL CASO EMBLEMÁTICO: *RUSSIA TODAY*

Existe cierta convención académica y mediática en el mundo occidental sobre el papel del medio gubernamental *Russia Today* (en adelante, RT) en el ecosistema de medios internacional. Desde Estados Unidos y desde diversos países europeos se ha puesto especial énfasis en señalar a RT como una valiosa herramienta de desinformación del Kremlin para desestabilizar las democracias occidentales. Sin embargo, el Gobierno ruso insiste en definir a este canal de televisión como una fuente de información alternativa de ámbito global que da cobertura a cuestiones pretendidamente olvidadas por los medios occidentales (Erlager, 2017). La propia página web de la cadena destaca cómo su posicionamiento mundial ha sido gracias a saber dar respuesta al deseo de su audiencia de encontrar «una perspectiva diferente sobre los acontecimientos mundiales», lejos del *mainstream*.

Lo cierto es que RT se ha convertido en un interesante caso de análisis para comprender la propaganda posmoderna, donde resulta muy difícil para el espectador poder distinguir los hechos y la información de las percepciones utilitarias prorrusas o antioccidentales y de la propaganda. Si el Gobierno ruso desplegó diferentes estrategias a través de este canal televisivo para inferir en las últimas presidenciales de Estados Unidos, nos hemos preguntado si existieron informaciones pretendidamente interesadas

en la cobertura realizado por RT de las elecciones generales de España del pasado 28 de abril de 2019.

La sede central de RT está en Moscú y tiene canales y plataformas *online* en seis idiomas. Desde 2009 emite en castellano: está disponible en más de mil redes vía satélite y de cable en América Latina, España y Estados Unidos. Es uno de los principales proveedores de noticias en YouTube y su fuerza es patente en redes sociales y en visualizaciones de contenido en web. La prioridad de RT en español no es tanto el espectador de nuestro país como el público de América Latina (Villarino, Á., 2019). El corresponsal de la cadena en España es el periodista Francisco Guaita. Bajo este prisma, las noticias aparecidas en RT sobre los comicios generales en España llegan a un público potencial de cientos de millones de personas.

Para nuestro estudio, hemos analizado aquellas piezas noticiosas sobre las elecciones generales en España que fueron emitidas a través del cable y satélite y además subidas al canal propio de RT en YouTube entre el 22 de abril al 29 de abril de 2019. Las palabras clave insertadas para su búsqueda en la plataforma *online* han sido *elecciones, generales* y *España*. Sobre estas noticias, once en total, hemos realizado un análisis de contenido cualitativo. Este método nos permitirá conocer cuál fue el tratamiento informativo de este hecho noticioso y si hubo algún relato donde se pueda vislumbrar una distorsión deliberada de la realidad.

Todas las piezas analizadas proceden de informativos, con una estructura común: una entradilla o *intro* de un presentador desde Moscú que da paso a una conexión con el corresponsal en España. La mayoría de las veces esta conexión es en directo. A partir de ahí, la retransmisión desde España incluye noticias reportajeadas, presenciales, colas e incluso pequeñas tertulias que se celebran en la sede de RT en Madrid. En prácticamente todas las piezas, en plató y en vtrs, se incluyen declaraciones de expertos en la materia. La duración de las informaciones es amplia, situándose como media por encima de los cinco minutos.

Veamos a continuación qué cinco claves fueron las más destacadas a la hora de informar sobre las elecciones generales en España.

1. Alta participación: la posible movilización de votantes por parte de la izquierda fue uno de los temas más tratados en las piezas analizadas antes del día de los comicios. Ese mismo día el tema también fue tratado debido a la confirmación de la segunda mayor participación de la historia de la democracia en España.
2. Fragmentación política: tras el fin del bipartidismo en España, una de las características de las elecciones en España fue la fragmentación política y así lo reflejaron las piezas de RT. En las informaciones se indicaba cómo lo más probable era que el Gobierno resultante de la contienda electoral no sería monocolor. Los pactos adquirían mucha importancia ante el incierto panorama político. RT indicaba los posibles escenarios de Gobierno: si la unión del bloque de la derecha tendría suficiente fuerza para crear Gobierno, qué alianzas se establecerían si el PSOE ganaba o la repetición de elecciones generales ante la imposibilidad de formar Gobierno.

3. La España vacía y el voto de los indecisos y de las mujeres: otra de las claves de estas informaciones se centraba en la importancia del voto de los ciudadanos en las zonas rurales, de los indecisos y de las mujeres.
4. La irrupción de la extrema derecha en el Congreso de los Diputados: la consecución de 12 escaños por parte de VOX en el Parlamento andaluz en las elecciones autonómicas de diciembre de 2018, hacía presagiar una llegada con mucha fuerza a las Cortes españolas. Los partidos del bloque de la izquierda integraban en sus relatos este miedo a un eventual Gobierno integrado por la extrema derecha. El día de las elecciones y el día posterior se analizó el resultado de este partido, que finalmente consiguió 24 diputados.
5. Crisis territorial: en todas las piezas encontramos cómo se integra esta temática. El nacionalismo catalán y su consiguiente proceso separatista configuraban esa crisis territorial que, de forma muy persistente en el relato de RT, amenazaba la integridad de España.

De estos cinco ejes, los cuatro primeros formaron parte de la temática protagonista de la campaña electoral en los principales medios del país[2], por lo que existe una coincidencia en el *framing* informativo. Sin embargo, a pesar de ser una clave recurrente en RT, el nacionalismo catalán y la crisis territorial ya había perdido fuelle informativo en la agenda mediática española. Para el canal televisivo RT el procés y sus derivas sí mantuvieron la hegemonía informativa, como evidencia su presencia en prácticamente todas las piezas analizadas. Esta alusión de la incertidumbre separatista aparecía bien indicando «la crisis territorial más gigante que ha habido en España» o cómo había que resaltar «a nivel nacional y a nivel internacional la fuerza que el nacionalismo tiene en este país».

Si existió una interferencia del Gobierno ruso en Cataluña durante el proceso separatista de 2014 a 2017, según miembros del Comité de Inteligencia del Senado de Estados Unidos (Martínez Ahrens, 2017), no es descartable que la propia RT continúe con ese marco de conexiones desestabilizadores. Innegablemente, ese relato incide de manera sustancial sobre las instituciones democráticas, puesto que la salud institucional de un país no solo se sustenta en su propio funcionamiento, sino en la proyección que se realice de esa calidad del Estado de Derecho.

La propaganda más eficaz es aquella que resulta inadvertida. Inadvertida por su sutileza. Inadvertida por haber abandonado todo rastro de soflama burda y evidente. La propaganda más eficaz camina con desenvoltura sobre un discurso de escrupuloso *ropaje* informativo.

CONCLUSIONES

Queda demostrado, en la medida de las posibilidades de este sencillo trabajo, que Rusia vuelve con fuerza al escenario internacional, y lo hace con herramientas poderosas y a la

[2] Véase, como ejemplo, estos artículos resumen de la campaña electoral de RTVE y de El País: MENÉNDEZ, M. «Las diez claves de un 28A imprevisible marcado por los vetos, los pactos y los indecisos». (2019. Disponible en http://www.rtve.es/noticias/20190411/elecciones-generales-2019-diez-claves-28a-imprevisible-pactos-vetos-indecisos/1919920.shtml y LLANERAS, K. «Las claves de unas elecciones impredecibles». 2009. Disponible en https://elpais.com/politica/2019/04/05/actualidad/1554480869_922170.html.

vez sutiles, con capacidad tecnológica y con una narrativa que sirve a sus intereses, reformulando el concepto de propaganda, incidiendo en aquellos puntos débiles de las democracias occidentales, y sin necesitar vender la propia imagen, sino debilitar la del contrario.

BIBLIOGRAFÍA

– ARO, J. «The cyberspace war: propaganda and trolling as warfare tools». *European View,* 15. 2016, pp. 121-132.

– BBC MUNDO. «El departamento de Justicia de Estados Unidos acusa a 13 ciudadanos rusos de interferir en las presidenciales de 2016». 16 de febrero de 2018. Disponible en https://www.bbc.com/mundo/noticias-internacional-43092239.

– BODINE-BARON, E.; HELMUS, T.; RADIN, A. y TREYGER, E. *Countering Russian Social Media Influence*. Santa Mónica, CA: RAND corporation, 2018.

– ERLAGER, S. «¿Periodismo o propaganda. En el caso de RT, la distinción no es clara». 12 de marzo 2017. Disponible en https://www.nytimes.com/es/2017/03/12/periodismo-o-propaganda-en-el-caso-de-rt-no-es-clara-la-distincion/.

– EXPANSIÓN. «Datos macro». 2019. Disponible en https://datosmacro.expansion.com/estado/gasto/defensa/rusia.

– FRESNEDA, Carlos. «El 'oro ruso' del Brexit: El empresario Arron Banks se reunió con funcionarios rusos». *El Mundo* de 10 de junio 2018. Disponible en https://www.elmundo.es/internacional/2018/06/10/5b1d7075468aebe04c8b45aa.html.

– HELMUS, T.; BONDINE-BARONE, E.; RADIN, A.; MAGNUSON, M.; MENDELSOHN, J.; MARCELINO, W.; BEGA, A. & WINKELMAN, Z. *Russian Social Media Influence. Undersanding Russian Propaganda in Eastern Europe*. Santa Mónica, CA: RAND coporation, 2018.

– HIGGINS, Elliot. «Blog de verificación de inteligencia mediante Fuentes abiertas». 2019. Disponible en www.bellingcat.com.

– IVÀNNIKOVA, María. «¿Por qué Rusia perdona las deudas y piensa en nuevos préstamos para los países latinoamericanos?». *Sputnik*, 26 de noviembre 2018. Disponible en https://mundo.sputniknews.com/economia/201811261083700786-por-que-rusia-perdona-deudas-cuba-venezuela-concede-nuevos-prestamos/.

– MARTÍNEZ AHRENS, J. «El Senado de EE. UU. aborda la interferencia rusa en Cataluña con los titanes de la Red». 3 de noviembre 2017. Disponible en https://elpais.com/internacional/2017/11/02/estados_unidos/1509635338_098727.html.

– MARTÍNEZ AHRENS, J. «EEUU destapa la 'fabrica de las *fake news*' y acusa a 13 rusos por la injerencia electoral». *El País*. 2018. Disponible en https://elpais.com/internacional/2018/02/16/estados_unidos/1518805614_412828.html.

– MARGINEDAS, Marc. «Rusia apuntala a Maduro con préstamos, proyectos petroleros y venta de armas». *El Periódico*. 1 de febrero 2019. Disponible en https://www.elperiodico.com/es/internacional/20190201/rusia-apuntala-maduro-prestamos-proyectos-petroleros-compra-armas-7276596).

– PAUL, C. & MATTHEWS, M. *The Russian «Firehose of Falsehood» Propaganda Model: Why It Might Work and Options to Counter It.* Santa Monica, CA: RAND Corporation, 2016. Disponible en https://www.rand.org/pubs/perspectives/PE198.html.

– RTVE. «El senado de EE. UU. afirma que Rusia interfirió en las elecciones para favorecer a Trump». 2018. Disponible en http://www.rtve.es/noticias/20180517/senado-eeuu-afirma-rusia-interfirio-elecciones-para-favorecer-trump/1734742.shtml.

– VILLARINO, Á. «RT en español. La fábrica de noticias de Putin para que odies Occidente», 15 de enero 2017. Disponible en https://www.elconfidencial.com/mundo/2017-01-15/la-maquina-del-fango-de-putin-en-espanol_1316352/.

– VOLCHEK, D. & SINDELAR, D. «One Professional Russian Trol Tells All». *Radio Free Europe / Radio Libery.* 25 de marzo 2015. Disponible en https://www.rferl.org/a/how-to-guide-russian-trolling-trolls/26919999.html.

ESTUDIO DIFERENCIAL DE ACTITUDES RADICALES HACIA LA INMIGRACIÓN EN ESPAÑA (2009-2017). DEL MITO AL DATO

JOSÉ MANUEL RODRÍGUEZ GONZÁLEZ
Doctor en Psicología. Profesor titular de las Facultades de Psicología y Derechos, Universidad de Sevilla. Profesor de la Escuela de Seguridad Pública de Andalucía en Consejería de Justicia e Interior. Máster Universitario en Estudios Estratégicos y Seguridad Internacional de la Universidad de Granada

MARÍA DEL PILAR CEBALLOS BECERRIL
Licenciada en Psicología por la Universidad de Sevilla. Máster Universitario en Psicología General Sanitaria. Máster en Psicología Jurídica por la Universidad de Valencia. Colaboradora en Escuela de Seguridad Pública de Andalucía en Consejería de Justicia e Interior

PABLO REY GARCÍA
Doctor en Comunicación. Profesor encargado de Cátedra en la Facultad de Comunicación de la Universidad Pontificia de Salamanca. Máster en Paz, Seguridad y Defensa por el Instituto Universitario «Gutiérrez Mellado»-UNED. Diplomado en Estudios Avanzados en Historia Contemporánea por la Universidad de Salamanca

PEDRO ÁLVAREZ NIETO
Teniente coronel de Artillería de la Escala de Oficiales del Ejército de Tierra. Director del Departamento de Ciencias Jurídicas y Sociales de la Academia de Artillería de Segovia. Profesor de número de Relaciones Internacionales, Mundo Actual e Historia de la Artillería en la Academia de Artillería. Experto en Relaciones Internacionales (URJ)

INTRODUCCIÓN

La radicalización, unida a conductas agresivas y violentas, constituye en el presente la base del terrorismo y las acciones terroristas que se convierten en la pesadilla de

nuestra sociedad. Hablamos de posicionamientos ideológicos, morales o religiosos llevados a un extremo tal que permiten la justificación (según un estilo de razonamiento particular) de dichos actos por parte de quienes los llevan a cabo y de seguidores y de colaboradores ocasionales o frecuentes. De ahí que en fechas recientes Mellón y Parra (2014) distingan entre una radicalización cognitiva (que solo implica la identificación o el apoyo ideológico) y otra de tipo comportamental (en la que ya se contemplan las acciones operativas).

Ese tipo de radicales constituyen un problema, una realidad que ocasionalmente golpea a nuestra sociedad y aunque no son tantos como a veces tememos, son capaces de provocar daños importantes con efectos emocionales devastadores entre la población. No obstante, existe otro problema (aparentemente menos significativo, extendido y lesivo) que solemos obviar; pero que con la ayuda de catalizadores dispares (problemas económicos, laborales, sanitarios, relacionales…) alcanza una significación preocupante. Hablamos de las «actitudes radicales» en el hombre y la mujer del siglo XXI. Se trata de una realidad mucho más insidiosa y corrosiva de lo que determinados sectores de la comunidad científica alcanzan a comprender.

Todo ser humano debe afrontar pulsiones y miedos atávicos que, si bien suele controlar a través de la razón, en ocasiones emergen de forma virulenta. Uno de esos miedos es «al otro», al foráneo, al extranjero, a quien se identifica como riesgo potencial y fuente de problemas y a quien, por tanto, se rechaza.

Cualquiera de nosotros, a la hora de abrir alguna de nuestras redes sociales habituales (Twitter, Facebook, Instagram…) nos vamos a encontrar con un número significativo de *fake news* (en concreto hacia los inmigrantes), que constituyen el universo de la desinformación que estas redes facilitan en su faceta negativa. Dadas las posibilidades de difusión e inmediatez que dichas redes permiten, junto al manejo de emociones y sentimientos básicos mediante mensajes simples, cortos, directos y en los que siempre subyace una pretendida realidad de riesgo, la respuesta (consistente en la emisión de nuevos *likes* o en compartir dicha *fake*) de quien recibe dicho mensaje no se suele dejar esperar. Usualmente la información no se verifica, se asume como auténtica y se responde con comentarios que en ocasiones muestran actitudes extremas, polarizadas cargadas de emociones inadecuadas.

Las consecuencias no se dejan esperar y de forma más frecuente de lo que cabe esperar nos encontramos cómo cualquiera de las personas a las que conocemos o nos rodean, hace comentarios y afirmaciones de sustrato xenófobo y racista; pero que ellas no consideran como tales y que refrendan a menudo en la desinformación a la que hemos hecho referencia más arriba.

Esta es, por tanto, la realidad que nos envuelve, que contamina a ciertos sectores de nuestra sociedad y que beneficia a grupos y organizaciones a modo de *feed-back* y potencia sus proyecciones. Hablamos, por tanto, de una situación que sirve de caldo de cultivo de conductas de rechazo hacia el extranjero (especialmente si tiene otro color de piel u otra religión) y que, llegado el caso, puede potenciar la aparición de un radicalismo

cognitivo o comportamental que cristalice en un rechazo sutil (xenofobia) o manifiesto (racismo).

OBJETIVOS

- Analizar la evolución de las actitudes radicales hacia extranjeros e inmigrantes en la población española.
- Confrontar dichas actitudes con los datos oficiales facilitados por las instituciones y organismos al uso.

METODOLOGÍA

Con el fin de recabar el posicionamiento de la población española con respecto a los temas que nos ocupan, hemos recurrido a las encuestas que realiza el Centro de Investigaciones Sociológicas (CIS) sobre actitudes hacia la inmigración desde hace 12 años.

El análisis evolutivo lo hemos trazado a partir de delimitar 2 secuencias temporales diferentes: 2009 y 2017 (CIS 2009, 2017).

El año 2009 es identificado a niveles económicos y sociopolíticos como un momento en el que la crisis económica mundial (y más concretamente española) alcanza su máxima significación. Es bien sabido que es precisamente en dichas ocasiones cuando los posicionamientos tienden a polarizarse hacia diversos temas, en particular hacia quienes se identifican como una posible fuente que va a mermar los consabidos apoyos estatales a los nacionales que se consideran necesitados.

Por su parte, 2017 (aparte de ser el año en el que se ha publicado la última encuesta llevada a cabo por el citado organismo) representa, siguiendo los mismos parámetros ya indicados, el momento de un nuevo despegue económico y el progresivo abandono de la mencionada situación de crisis.

De las diversas cuestiones contempladas, 61 en el caso de 2017 y 62 en 2009 (aunque, en ambas, en algunos casos algunas cuestiones se hallan secuenciadas en otras preguntas de segundo orden) hemos procedido a realizar una selección siguiendo los siguientes filtros:

Debían repetirse las mismas cuestiones planteadas de igual forma y con las mismas opciones de respuestas en ambos años.

Evidenciar, en su planteamiento o en sus alternativas de respuesta, manifestaciones de posicionamientos extremos de rechazo bien hacia población extranjera, bien inmigrante.

En cuestiones clave, que dichas preguntas abordasen temas susceptibles de ser contrastados con fuentes oficiales, evitando así recurrir a datos oficiosos.

RESULTADOS

El cuadro 1 aborda un tema esencial, ¿a qué se asocia el término inmigrante un español?, aunque no se han incluido por razones de espacio, respuestas manifiestamente negativas (irregularidad, delincuencia e inseguridad, privilegios frente a los españoles, …) alcanzan un peso de 29,2 % en 2009 y de 19,5 % en 2017. Aunque se denota una reducción destacada, se mantiene casi un 20 % en un posicionamiento negativo, a ello debemos aunar el vínculo con búsqueda de trabajo, la pobreza y la desigualdad, facilitando así una imagen no muy favorable del inmigrante.

AÑO	NECESIDAD TRABAJO	EMPATÍA/SOLIDADRIDAD	POBREZA DESIGUAL	SENT NEGATIVOS
2017	22,2 %	13,1 %	11 %	1,1 %
2009	17,7 %	11,6 %	8,4 %	3,2 %

Cuadro 1.- ¿A qué vinculan los españoles el término inmigrante?

En cuanto a la percepción acerca del origen, lo habitual es identificar al inmigrante con otra raza, otra cultura u otra religión (estos 2 últimos criterios avalados por posibles diferencias de indumentaria), es decir, detectar signos que le identifiquen. El cuadro 2 recoge de manera manifiesta esta tendencia.

Los últimos datos facilitados por el Ministerio de Trabajo, Migraciones y Seguridad Social (MTMSS) en 2018 (ver cuadro 3) desmienten la percepción de la población y corroboran el hecho de la búsqueda de diferencias del que acabamos de hablar. Los extranjeros suponen el 9,8 % de la población actual, según el Instituto Nacional de Estadística (INE, 2017) y de estos, casi el 50 % son ciudadanos de la UE, que para la mayoría de la población no son ni visibles ni identificados como tales. Por ejemplo, unificando los residentes de Reino Unido, Alemania e Italia, su número supera al de los procedentes de Marruecos y norteafricanos, que se considera han aumentado significativamente de 2009 a 2017 (ver cuadro 2).

AÑO	MARROQUIES/NORTEAFRICANOS	LATINOAMER	RUMANOS
2017	41,08 %	28,6 %	24,9 %
2009	25,6 %	24,1 %	20,6 %

Cuadro 2.- ¿A qué nacionalidad se vincula la inmigración?

El mismo cuadro 3 nos sirve para dar respuesta a los resultados incluidos en el cuadro 4. Acabamos de afirmar que el número de inmigrantes registrados ronda el 9,8 % de la población, lo cual no impide que los encuestados (tanto en 2009 como en 2017) considere que su número es excesivo y elevado. Nótese, no obstante, la reducción del porcentaje de excesivo con el paso de los años (61,11 % en 2017 frente a 78,5 % en 2009). El hecho de ubicarse 2009 en plena crisis económica polariza más la percepción y la sensación de que su número es muy alto (con el posible riesgo que ello pudiese representar para la propia subsistencia).

Extranjeros con certificado de registro o tarjeta de residencia en vigor a 31-12-2018. Principales nacionalidades

	31-12-2018	% Mujeres	Edad media	Variación semestral respecto a 30-06-2018	Variación interanual respecto a 31-12-2017
Total	5.424.781	47,7%	38,5	1,7%	3,6%
Rumanía	1.054.458	46,9%	36,6	1,1%	2,4%
Marruecos	786.058	43,7%	31,8	0,5%	1,6%
Reino Unido	330.911	49,6%	53,1	3,3%	5,4%
Italia	302.102	43,1%	39,6	4,8%	9,6%
China	218.219	48,5%	32,6	1,5%	3,3%
Bulgaria	195.950	47,0%	39,7	0,8%	1,7%
Alemania	169.661	52,0%	47,9	1,9%	3,3%
Portugal	165.543	36,4%	42,0	2,2%	4,5%
Francia	159.210	50,4%	42,0	3,2%	6,3%
Ecuador	157.271	44,6%	37,5	-0,9%	-2,0%
Colombia	126.494	54,1%	39,5	1,6%	2,8%
Polonia	100.401	52,0%	38,4	1,4%	2,7%
Bolivia	91.147	55,8%	35,7	-2,1%	-3,8%
Ucrania	90.362	56,7%	40,1	1,7%	3,2%
Pakistán	82.805	31,7%	32,1	2,4%	5,7%

Cuadro 3.- Extranjeros registrados en España. (Fuente: MTMSS, 2019)

AÑO	EXCESIVO	ELEVADO	ACEPTABLE
2017	29,3 %	31,8 %	27,5 %
2009	45,6 %	32,9 %	16,8 %

Cuadro 4.- Percepción del número de inmigrantes.

¿Qué condiciona la aceptación del inmigrante? En este caso no vamos a recurrir a datos oficiales, ya que las respuestas de la población son significativas de por sí. Aunque en el cuadro 5 no se han incluido todas las respuestas, reseñamos que el hecho de que sean blancos es poco relevante para el 58 %, en 2009, y el 63 % en 2017. Es algo similar a lo que ocurre con el nivel económico (de poco valor para el 47,5 % en 2009 y el 50,9 % en 2017) lo que no deja de ser curioso en función de lo que hemos analizado hasta ahora.

De otro lado se moderan las posturas en el resto de los argumentos planteados, aunque destaca cómo el 48,4 % (en 2009) y el 36,1 % (en 2017) de la muestra opta por considerar que es muy importante la adopción del *spanish way life*, es decir, la asimilación, en detrimento de la propia cultura original del migrante. Evidentemente esto indica que la integración (considerada por parte de la población española) va a venir condicionada por la capacidad y la rapidez de esos foráneos para adoptar principios, valores y costumbres ibéricas. Los planteamientos multiculturalistas no tienen aún un peso significativo. No obstante, es bien conocido el hecho de que la asimilación y la posterior integración

pueden servir de germen para conflictos posteriores por parte de los propios asimilados, sirva de muestra para ello el reciente estudio de Reinares, García-Calvo y Vicente (2019).

AÑO	ADOPTAR MODO VIDA	CUALIFICA-CIÓN LABORAL	DOMINIO CASTELLANO	NIVEL EDUCATIVO
2017	36,1 %	14,7 %	13 %	12,7 %
2009	48,4 %	33 %	20,9 %	22 %

Cuadro 5.- ¿A la hora de permitir que un inmigrante viva en España qué predomina?

Por su parte, en el cuadro 6 hallamos aquellas acciones y derechos que la muestra entiende que no deben ser accesibles a la población inmigrante regular. Es evidente que, a pesar de la pretendida necesidad de asimilación, se restringe el acceso al voto o a la reunificación familiar.

AÑO	TRAER FAMILIA	SUBSIDIO DESEMPLEO	VOTO MUNICIPALES	VOTO GENERALES	OBTENER NACIONALIDAD
	NO	NO	NO	NO	NO
2017	12,6	8,2	22,2	28,8	13,2
2009	14,1	8,4	29,5	36,9	20,3

Cuadro 6.- ¿Los inmigrantes instalados en España, de manera estable y regular, deberían tener el derecho de...?

De nuevo los resultados resultan llamativos. El cuadro 7 nos aporta datos acerca de la opinión de la muestra acerca de lo importante (valorado de 0, muy negativo, a 10, muy positivo) que es que la sociedad española esté compuesta por personas diferentes. Los datos que se incluyen son valores promedio y dejan clara la asunción de este hecho tanto con lo que respecta a cultura, religión, color de piel o país de origen. Seamos conscientes de que se trata, en última esencia, de una aceptación; pero con limitaciones.

AÑO	PAÍSES	CULTURAS	RELIGIONES	COLOR DE PIEL
2017	6,87	6,9	5,82	6,96
2009	6,19	6,38	5,28	6,04

Cuadro 7.- Valorar el hecho de que la sociedad española esté compuesta por personas de diferentes.

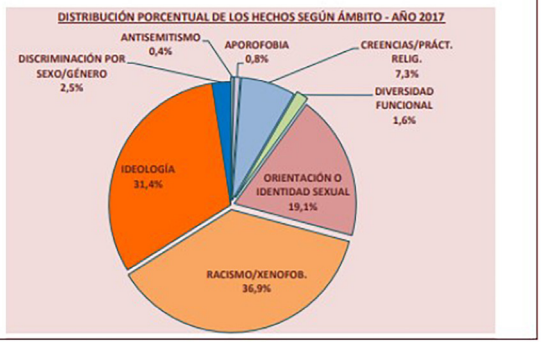
¿El español se considera racista y/o xenófobo? ¿Qué posicionamiento adopta ante estos comportamientos?

AÑO	SIEMPRE	EN LA MAYORÍA	OCASIONALMENTE
2017	32 %	25 %	26 %
2009	52,4 %	16 %	22,4 %

Cuadro 8.- ¿Sancionar a quienes emitan en público insultos racistas y xenófobos?

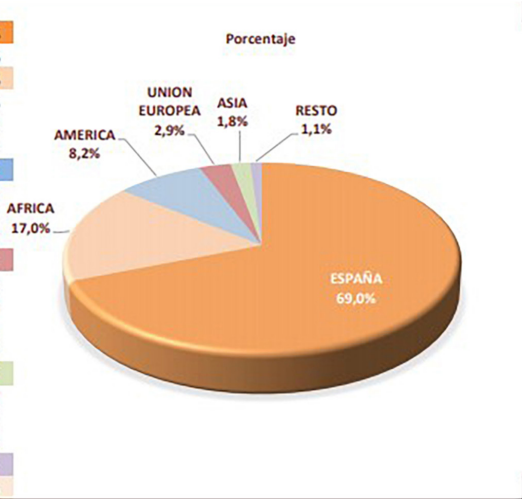
Los valores expuestos en el cuadro 8 informan de que casi el 60 % (en 2017) frente a casi un 70 % (en 2009), se muestra partidario de sancionar los comentarios racistas y xenófobos; aunque es destacable cómo la categoría «sancionar siempre» sufre un descenso significativo con el paso de los años, es decir, el posicionamiento ya no es tan próximo a una aplicación ajustada de la norma jurídica. Aun así, los datos facilitados por el Ministerio del Interior en 2017, y recogidos en los cuadros 9 y 10, nos dejan bien claro que los delitos de odio se incrementaron significativamente en 2017 y que, dentro de aquellas acciones dirigidas contra inmigrantes, las víctimas más frecuentes eran africanos, con lo que debemos estimar de nuevo la consideración de la raza.

INCIDENTES DE DELITOS DE ODIO	2016	2017	%Variación
ANTISEMITISMO	7	6	-14,3%
APOROFOBIA	10	11	10,0%
CREENCIAS O PRÁCTICAS RELIGIOSAS	47	103	119,1%
DIVERSIDAD FUNCIONAL	262	23	-91,2%
ORIENTACIÓN O IDENTIDAD SEXUAL	230	271	17,8%
RACISMO/XENOFOBIA	416	524	26,0%
IDEOLOGÍA	259	446	72,2%
DISCRIMINACIÓN POR SEXO/GÉNERO	41	35	-14,6%
TOTAL	1.272	1.419	11,6%



Cuadro 9. Modalidades y evolución de los delitos de odio. (Fuente: Ministerio del Interior, 2017)

NACIONALIDAD	Víctimas	%
1.- ESPAÑOLES	1.167	69,0%
2.- EXTRANJEROS	524	31,0%
2.1.- ÁFRICA	287	17,0%
Marruecos	211	12,5%
Argelia	19	1,1%
Resto	57	3,4%
2.2.-AMÉRICA	139	8,2%
Colombia	28	1,7%
Ecuador	23	1,4%
Resto	88	5,2%
2.3.-UNIÓN EUROPEA	49	2,9%
Italia	14	0,8%
Rumanía	12	0,7%
Reino Unido	5	0,3%
Resto	18	1,1%
2.4.- ÁSIA	31	1,8%
Pakistán	9	0,5%
China	7	0,4%
Resto	15	0,9%
2.5.- RESTO PAÍSES	18	1,1%
TOTAL	1.691	100%



Cuadro 10. Distribución de las víctimas por nacionalidad. (Fuente: Ministerio del Interior, 2017)

Finalmente, el cuadro 11 permite concluir que ha habido una evolución tal que el español de a pie es menos desconfiado con el extranjero, se incrementa la percepción del trato amable y el normalizado, a la vez que descienden las conductas de indiferencia y desprecio; aunque no de forma tan significativa como la mencionada desconfianza.

AÑO	INDIF	DESPR	AMABILIDAD	DESCONF	NORMALID	AGRES
2017	5,9 %	7,1 %	19,5 %	29,5 %	30,3 %	0,4 %
2009	8,7 %	8,8 %	14,2 %	41,4 %	21,6 %	0,5 %

Cuadro 11.- ¿Cómo tratan los españoles a los inmigrantes extranjeros?

El uso y abuso de la sanidad por parte de los inmigrantes siempre ha sido y es un foco conflictivo, una crítica usual de la población española hacia la población inmigrante y, en este caso, no siempre influida por la posible raza de los beneficiarios. Los medios de comunicación dejan en evidencia este hecho cuando acuñan el término «turismo sanitario».

Siempre se les atribuye a los foráneos un uso banal y que acaba perjudicando al español medio, tanto en la mediatez de la atención como en la calidad de la atención recibida por el enfermo. Los cuadros 12 y 13 son un fiel reflejo de estas creencias injustificadas, si bien el retroceso que tiene lugar a ellas en las fechas más recientes es digno de destacar.

Recurriendo a los datos facilitados por la organización Stop Rumores, que a su vez cita los correspondientes al Ministerio de Sanidad, encontramos que la población inmigrante hace un 7 % menos uso de los servicios de atención primaria que los propios españoles. En cuanto al coste farmacéutico, este es de 374 euros por cada español, mientras que en el caso de los inmigrantes es de 73,70 euros. Para concluir este punto, el 61 % (españoles), frente al 41 % (inmigrantes) precisan atención continuada a causa de padecer una enfermedad crónica. En este último caso la causa es evidente: la población inmigrante suele tener una media de edad más baja que la de la nacional, reduciéndose así la probabilidad de padecer este tipo de trastornos.

AÑO 2017	MAS BIEN DEACUERDO	MUY EN DESCUERDO
La presencia de inmigrantes hace que disminuya la calidad de la atención sanitaria	14,8 %	26,4 %
Los inmigrantes abusan de la atención sanitaria gratuita	21,6 %	29,5 %
Los españoles deberían tener preferencia a la hora de acceder a la atención sanitaria	17,1 %	23,3 %
Aunque tengan los mismos ingresos, se les da más ayudas sanitarias a los inmigrantes que a los españoles	21,8 %	26,3 %

Cuadro 12.- Sanidad e inmigración, 2017.

AÑO 2009	Más bien de acuerdo	Muy en de acuerdo
La presencia de inmigrantes hace que disminuya la calidad de la atención sanitaria	22,7 %	30,6 %
Los inmigrantes abusan de la atención sanitaria gratuita	25,7 %	28,6 %
Los españoles deberían tener preferencia a la hora de acceder a la atención sanitaria	19 %	24,6 %
Aunque tengan los mismos ingresos, se les da más ayudas sanitarias a los inmigrantes que a los españoles	23 %	24,2 %

Cuadro 13.- Sanidad e inmigración, 2009.

CONCLUSIONES

Tal y como hemos podido ir verificando a lo largo de estas páginas, la población española, el español promedio (que es a quien pretende representar las encuestas del CIS) posee una percepción incorrecta de determinados aspectos relacionados con el fenómeno de la inmigración: su número, procedencia, imagen asociada a su categoría de inmigrante o el efecto que su vida en España provoca a nivel sanitario.

Las diferencias en cuanto a credo, raza o costumbres, entendidas como algo que distorsiona el devenir de la propia cultura española, intentan conjurarse mediante la solicitud, hacia el inmigrante, del olvido de sus raíces y opte por una asimilación completa de la cultura española; aunque ello no implicaría la completa aceptación, dado que hay una tendencia a no reconocerle ciertos derechos (al voto, por ejemplo).

La consideración de la raza es importante, el racismo sutil o manifiesto están presentes, especialmente el primero de ellos. Se trata de un problema real que precisa un abordaje.

Finalmente, corroboramos cómo la situación de crisis económica provoca una polarización de las opiniones que, a medida que esta mejora, tienden a normalizarse. La sensación de ver peligrar la satisfacción de las necesidades básicas lleva a las personas, y a sus opiniones, a extremos más radicales, hace que dichas opiniones se dejen llevar más por las emociones o el sentir del momento que por la razón. Si en ese momento son influidos por fuentes externas interesadas a través de medios de comunicación o de redes sociales, polarización se maximiza y se posibilita la aparición de conflictos manifiestos.

BIBLIOGRAFIA

– CENTRO DE INVESTIGACIONES SOCIOLÓGICAS (CIS). «Actitudes hacia la inmigración III. Estudio 2817». Octubre 2009. Disponible en http://www.cis.es/cis/export/sites/default/-Archivos/Marginales/2800_2819/2817/es2817.pdf.

– CENTRO DE INVESTIGACIONES SOCIOLÓGICAS (CIS). «Actitudes hacia la inmigración X. Estudio 3190». Septiembre 2017. Disponible en http://www.cis.es/cis/export/sites/default/-Archivos/Marginales/3180_3199/3190/es3190mar.pdf.

– MELLÓN, Juan Antón y PARRA ARNAIZ, Ignacio. «El concepto de radicalización». *CÁLAMO, Revista de Estudios Jurídicos*, 1. 2014, pp. 75-90.

– MINISTERIO DE TRABAJO, MIGRACIONES Y SEGURIDAD SOCIAL. *Extranjeros residentes en España a 31 de diciembre de 2018. Principales resultados*. Madrid: 2019.

– MINISTERIO DEL INTERIOR. *Informe sobre la evolución de los incidentes relacionados con los delitos de odio en España*. Madrid: 2017.

– REINARES, Fernando; CARGÍA-CALVO, Carola & VICENTE, Álvaro. *Yihadismo y yihadistas en España. 15 años después del 11M*. Madrid: Instituto de Estudios Estratégicos. 2019.

GUERRA HÍBRIDA RUSIA-ESTONIA 2007

JAVIER BALAÑA HENAREJOS
Investigador externo del Instituto Universitario Gutiérrez Mellado. Experto universitario en Terrorismo, Contrainteligencia y Geoestrategia Internacional. Máster Internacional en Ciberdefensa y en Ciberseguridad y técnico en Análisis de Tecnologías Militares y de la Industria de Defensa

Resumen

Esta comunicación pretende describir el procedimiento de las operaciones híbridas rusas, detallando para ello cada una de sus seis fases de ejecución, como especifica el jefe de la Defensa Rusa general Valery Gerasimov, en el ensayo que publicó en el año 2012 con el título «El valor en la ciencia de la anticipación» en la Revista *Voyenno Promyshlennyy Kurier.*

También se muestra, la implantación de este concepto militar híbrido, en el caso del conflicto de Rusia-Estonia del año 2007, donde por primera vez mediante ciberataques contra el Gobierno de una Nación se logra incomunicarlo y anularlo, impidiéndoles liderar la crisis que paralizó Estonia.

Palabras clave

Guerra híbrida, Estonia, Gerasimov, ciberataques, Rusia.

INTRODUCCION

Según el profesor Vasily Kopytko, profesor de la Academia General Militar Rusa, el arte operacional ruso se divide en varios periodos, el primero va de 1920 a 1924 y se caracterizó por un *frente y operaciones a escala*, el segundo periodo de 1925 a 1953, por las *batallas en profundidad* con una abrumadora potencia de fuego, el tercer periodo de 1954 a 1985 por las *armas nucleares y misiles*, el cuarto periodo, de 1986 a 2000 por las *armas de alta precisión* (Valery, 2012) y el periodo actual o quinto, se caracteriza por las *medidas no militares* y los *dominios no tradicionales* en los conceptos operacionales. En el oeste estos conceptos son conocidos como «*doctrina Gerasimov*», (Kopytko, 2008, pp. 202, 214).

La guerra no lineal rusa, conocida en Occidente como doctrina Gerasimov o también guerra hibrida rusa, les permite integrar medidas militares y no militares, como los grupos ciudadanos de protesta, efectivos paramilitares, medios de comunicación, y las cibercapacidades, actuando todo de forma simultánea, tanto en los dominios físicos como en los virtuales de información y ciberespacio, mediante acciones indirectas y asimétricas cuyo objetivo es mitigar las capacidades del adversario. Para ello aíslan a sus líderes, ocupan zonas físicas vitales y crean desestabilización y caos.

La amenaza híbrida es un tipo de guerra imprevisible porque en ella no existen declaraciones de guerra ni tampoco de cese de hostilidades, sin embargo, en el caso ruso, una vez iniciada se visualizan distintas fases que puede hacerla predecible.

El ciberespacio constituye un medio, cada vez más relevante para las operaciones híbridas, y en este sentido, destacar el conflicto ruso-estonio, del año 2007, donde por primera vez a través de ciberataques, se logra inmovilizar y aislar al Gobierno de una nación, en ese caso de Estonia.

Desde la Federación Rusa para anexionar áreas, lo primero que hacen en vez de iniciar acciones militares, es lanzar campañas de información en medios de comunicación e Internet. Su objetivo es la opinión pública nativa, a través de la manipulación de las percepciones de sus ciudadanos, concretamente a través de su sistema de control reflexivo, aunque para lograr efectos psicológicos como la desorientación o la sugestión, deben superar la percepción de provocación. Estas operaciones psicológicas pueden llegar a producir cansancio, parálisis y desesperación entre sus líderes políticos y militares, que pueden orientarles hacia las fases finales de la doctrina Gerasimov, de resolución y de restauración de la paz, sobre bases de negociación en términos favorables para Moscú.

El general Valery Gerasimov, es el jefe del Estado Mayor de la Defensa rusa y ha sido el primero en describir estas operaciones híbridas[1], desde la visión de Moscú, en su famoso y polémico ensayo «El valor de la ciencia en la anticipación», que publicó en la revista *Voyenno Promyshlennyy Kurier,* en el año 2012. El artículo tuvo amplia difusión en la comunidad militar rusa, pero pasó desapercibido para la mayoría de analistas occidentales, hasta que se produjo la anexión rusa de la región de Crimea, en Ucrania, en el año 2014.

Gerasimov analiza las lecciones aprendidas de los principales conflictos, desde el fin del mundo bipolar, como la guerra del Golfo en 1991, los conflictos en Afganistán e Iraq, las primaveras árabes, la revolución naranja[2], o la intervención en Libia[3] (Piella, 2018, p. 4).

---

1 Aunque Gerasimov, en su ensayo, no usa el termino de guerra híbrida.

2 Promovida por el occidentalista Viktor Yushchenko.

3 Para Gerasimov, Libia ha sido el paradigma de guerra del siglo XXI, al integrar medidas no militares como las humanitarias, políticas, informativas, económicas, además de sumar el potencial de las movilizaciones populares. Todo ello con el apoyo de medios militares clandestinos canalizando operaciones de información y otras especiales. Además también participaron unidades militares regulares para el mantenimiento de la paz y la gestión de crisis, para lograr objetivos políticos, debidamente coordinados con el resto de actores.

En su artículo, Gerasimov describe pensamientos, medios, fases y acciones usadas en el nuevo concepto operacional híbrido, en donde resalta la importancia de las medidas no militares y la necesidad de una coordinación superior de todas las acciones en marcha, sin embargo no detalla la participación de las Fuerzas Armadas rusas, ni tampoco explica en qué consisten esas operaciones civiles, que permiten lograr objetivos. Tampoco revela cuál es el objetivo estratégico de las operaciones híbridas.

Rusia, ha experimentado acciones de guerra híbrida, con el uso de medidas no militares y la creación de condiciones sociales[4], como las movilizaciones civiles, para crear conflictos, en Estonia, Georgia y Ucrania, en algunos casos complementados con operaciones miliares, clandestinas y regulares. En cualquier caso les ha servido como «lecciones aprendidas».

Gerasimov, dentro de su concepto operacional híbrido, describe los métodos no militares, en algunas ocasiones, como más efectivos, que los medios militares, para la resolución de conflictos interestatales, y añade la importancia de la explotación de los nuevos dominios como el ciberespacio y la información, (Selhorst, 2016, p. 4).

La aplicación de la «doctrina Gerasimov, produce cambios en las percepciones sociales y supone un desafío, en la manera de hacer la guerra, a la que Occidente no está familiarizado. Según Gerasimov, cada conflicto es distinto, por lo que las soluciones operacionales también lo son.

SEIS FASES DE OPERACIONES HÍBRIDAS

Según Gerasimov el nuevo concepto operacional de la guerra híbrida rusa, se compone de seis fases, como él mismo plantea en el artículo el «Valor de la ciencia en anticipación», que publicó en la revista rusa Voyenno Promyshlennyy Kurier, en el año 2012, donde especifica que la primera fase es; origen oculto, la segunda fase; escalada, la tercera fase; arranque de actividad conflictiva, la cuarta fase; crisis, la quinta fase; resolución y la sexta fase; restaurar la paz.

En las dos primeras fases tienen su inicio las operaciones de información, que se incrementan en la fase de «crisis» con la formación de coaliciones civiles de oposición. La finalidad estratégica de todas estas operaciones es lograr objetivos políticos, cercanos y lejanos de Moscú.

CRISIS RUSIA - ESTONIA 2007

En esta crisis se pueden visualizar las distintas fases del concepto de guerra híbrida. La primera fase o de «origen oculto», pudo tener lugar en 1991 al independizarse Estonia de Rusia y su posterior acercamiento a OTAN[5].

[4] Para conceptos operacionales.

[5] En 2008 se crea en Tallin, el Centro de Excelencia OTAN en Ciberseguridad.

En la segunda fase denominada de «escalada», según el propio Gerasimov, los integrantes de la minoría rusa residentes en Estonia se manifestaron por todo el país, especialmente en la capital Tallin, para pedir la recolocación de la estatua de bronce del soldado ruso, que el nuevo Gobierno, quitó de su emplazamiento. Paralelamente también hubo manifestaciones frente a la embajada de Estonia en Moscú. Durante esta fase también se manifestaron un grupo de jóvenes activistas rusos denominado «Nashi»[6], al parecer apoyados por fuerzas de operaciones especiales (SOF), y por los medios de comunicación rusos, que ayudan a organizar manifestaciones a favor de la minoría rusa, mientras pedían derechos humanos para ellos y comparaban a las autoridades de Estonia con los nazis de la Segunda Guerra Mundial, (Manwaring, 2012, p. 91). A continuación la Federación Rusa dió pasaportes rusos a la minoría rusa en Estonia y presionó al Gobierno de Estonia para que el idioma ruso fuera el segundo idioma oficial y a través de Estonia también fuera idioma oficial en la U.E.

La tercera fase de la *Doctrina Gerasimov* o de «arranque de actividad conflictiva», tuvo lugar en forma de dos olas de potentes ciberataques, que paralizaron el país. El primer ciberataque tuvo lugar el 27 de abril del 2007, fué más espontáneo, estaba dirigido contra el Gobierno de Estonia, sus entidades bancarias y económicas, las agencias de noticias y la red de ordenadores militares. A través de Internet y de medios de comunicación rusos animaron a simpatizantes de Occidente de todo el mundo a participar en los ataques, para ello tenían algunas páginas web con el *software* necesario, que solo tenían que descargarlo. La intención era establecer una red de ataque mundial. El grupo de jóvenes rusos «Nashi» apoyó y participó abiertamente en estos ciberataques. El segundo ciberataque tuvo lugar el 8 de mayo de 2007, aniversario de la victoria soviética sobre los nazis en la Segunda Guerra Mundial. Este ciberataque fue más sofisticado y coordinado[7], lograron desconectar al Gobierno de Estonia e instituciones de sus; *websites,* correo electrónico y comunicaciones telefónicas. El resultado fué que durante varios días impidieron al Gobierno liderar la crisis en su país y tampoco podían comunicarse ni con sus fuerzas armadas, ni con sus aliados. La respuesta técnica del Gobierno de Estonia fué bloquear todo el tráfico procedente de Rusia, filtrando para ello todas las dirección con extensión «punto.ru», si bien no lograron evitar que les paralizaran el país.

Aunque Rusia negó la autoría, se les considera los autores de estos ataques cibernéticos y es que en el ciberespacio, Rusia tiene dos lideratos, el primero unos conocimientos técnicos muy elevados y el segundo su capacidad para permanecer invisibles, donde hacen grandes esfuerzos para que sus ciberataques no sean detectados, identificados o analizados (Balañá, 2015 p. 14).

A pesar de encontrarse Estonia en plena «fase de crisis» según *la Doctrina Gerasimov,* tras la batalla de la estatua, del idioma y del corto periodo de aislamiento

[6] Este grupo y otros parecidos habían sido fundados por el Kremlin a partir de la Revolución Naranja en Ucrania la cual había sido liderada por jóvenes. La intención era crear una red leal con organizaciones civiles controladas por el gobierno, que en caso de un levantamiento disidente, pudieran ocupar la plaza Roja antes que la oposición.

[7] El procedimiento de estos ataques fue el *DDoS* o denegación de servicio.

por ciberataques, parece que no fué suficiente, porque hubo un incremento de presión al Gobierno, al reducir Rusia el suministro de gas a Estonia, siendo su único proveedor.

Ya en la fase de «resolución», de la *Doctrina Gerasimov,* Estonia decide cambiar la Estatua a un emplazamiento mejor del previsto que era un depósito municipal, y acepta el idioma ruso como segundo idioma oficial.

Finalmente pasaron a la fase de «restauración de la paz», momento en que los ciberataques cesaron y debido a su poca duración, el impacto en la economía y en sus sistemas militares, fue mínimo.

Esta crisis verifica que las operaciones de la guerra híbrida, van dirigidos contra la población, sectores económico y financiero, la administración del estado y los sistemas militares. Además Rusia ha encontrado un tipo de ataques que no tienen respuesta legal.

CONCLUSIONES

Este tipo de guerra híbrida, tiene formas irregulares de combatir, que van desde procedimientos y medios no regulados por las actuales leyes y convenios internacionales, al empleo de medios convencionales y de sofisticadas tecnologías que cada día van adquiriendo nuevas complejidades.

Por otra parte, el *ciberespacio* es el principal teatro de operaciones de la guerra híbrida y a través de este medio, han podido llegar a paralizar un país entero, como fué el caso de Estonia en 2007. El origen de los ciberataques procedía de Rusia, pero debido al problema técnico de la atribución, no se pudo probar la autoría, con lo cual evitaron que OTAN activara el artículo 5 de la defensa colectiva, y también las condenas de tribunales internacionales. La lección aprendida para futuros conflictos con Rusia, es que estos no se basan exclusivamente en medidas físicas.

Estrategas rusos de primer nivel, como el asesor personal de presidencia desde 2013 Vladislav Surkov, tienen claro que Rusia no cuenta con el poderío militar necesario para desafiar a Estados Unidos o a la OTAN. Sin embargo han comprendido que Rusia es capaz de tener a la comunidad internacional desorientada tratando de adivinar qué es lo que están haciendo, o más complicado aún, qué es lo que van a hacer. Para ello, en sus intervenciones militares, concentran recursos limitados, pero emplean a sus mejores hombres, material y armamento, mientras logran que nadie sea capaz de descifrar sus planes. En este aspecto, el literato Surkov es un maestro de la confusión para guiar a Rusia en la «guerra híbrida».

En 1999 los coroneles chinos Qiao Liang y Wang Xiangsui, describían en su popular ensayo, *La guerra sin restricciones*, lo que serían las guerras del futuro. Esta denominación parece muy apropiada para definir los modos de *guerra híbrida* rusa, también conocida como Doctrina Gerasimov.

BIBLIOGRAFIA

– BALAÑÁ, Javier Henarejos. *Ciberguerra global - El fantasma ruso.* 2015, p. 14.

– GERASIMOV, Valery. *El valor en la ciencia en la anticipacion.* Moscú: s.n., 2012, p. 1.

– KOPYTKO, Vasily. *Evolution of Operational Art in Voyennaya.* Vol. 1. 2008, pp. 202-214.

– MANWARING, Max G. *The Complexity of Modern Asymmetric Warfare.* University of Oklahoma, [ed.] Norman Press. s.l., 2012, pp. 91-92.

– PIELLA, Guillem Colom.*¿Guerra híbrida a la rusa? Algunos apuntes sobre la «Doctrina Gerasimov».* Vol. 2. Madrid : Thiber, 2018, p. 4.

– SELHORST, A. J. C. *Russia´s Perception Warfare.* The Hague : Royal Netherlands Army, 2016, pp. 2-4, 36, 37, 48. Lieutenant colonel.

AMENAZAS SOBRE EL SECTOR DE DISTRIBUCIÓN DEL AGUA EN ESPAÑA

JAVIER DEL VALLE MELENDO
Profesor del Centro Universitario de Defensa

Resumen

Los Estados desarrollados cuentan con redes de captación, almacenaje, distribución, potabilización y depuración de aguas adecuadas para satisfacer las demandas de sus ciudadanos y de sus sectores económicos tanto en cantidad como en calidad. Estas infraestructuras pueden ser objetivo de terroristas tanto de manera directa como a través de ciberataques, debido a la creciente automatización de los sistemas. Dentro de las redes mencionadas hay algunos elementos que son más vulnerables a posibles ataques y entre las sustancias potencialmente empleadas también algunas cuentan con más posibilidades dadas sus características de precio, accesibilidad y consecuencias.

Palabras clave: agua, redes de distribución, seguridad de abastecimiento.

INTRODUCCIÓN

La dependencia de los Estados desarrollados de una correcta distribución de agua, tanto «en alta» como «en baja», es total, pues de ella dependen sectores tan imprescindibles para el funcionamiento normal de un país y su población como el abastecimiento a los ciudadanos e industrias, la generación de hidroelectricidad, la refrigeración de centrales nucleares y térmicas o la satisfacción de las demandas del regadío para la producción de alimentos.

La distribución adecuada de agua tanto en cantidad como en calidad se basa en una serie de instalaciones recogidas en el Catálogo Nacional de Infraestructuras Críticas.

En el caso de España la distribución de agua de calidad y con elevadas garantías alcanza al 100 % de la población durante todo el año, incluyendo a la población flotante en las numerosas zonas turísticas. Esta alta garantía, en buena medida, se basa en la existencia de numerosos embalses que regulan nuestros ríos, muchos de ellos en zonas de montaña alejados de los grandes núcleos de población, y canales y acequias de distribución de agua, complementados con el uso de agua subterránea o de desalación en algunas zonas del país. Es necesario reflexionar sobre las amenazas que existen sobre este sistema crucial para el país y los niveles de seguridad que dispone.

EL MODELO DE GESTIÓN DEL AGUA EN ESPAÑA

Según la Constitución de 1978, vigente en nuestros días, la gestión de las cuencas que abarcan territorio de varias comunidades autónomas corresponde a las confederaciones hidrográficas, organismos autónomos estatales en los que están representadas las comunidades autónomas con territorio en ellas, de forma proporcional a este, y los principales usuarios del agua.

La Ley de Aguas de 1985 crea los organismos de cuenca en las cuencas hidrográficas que excedan el ámbito territorial de una comunidad autónoma, que, siguiendo con la denominación de confederaciones hidrográficas, disponen de autonomía para regir y administrar los bienes confiados, pues tienen personalidad jurídica propia distinta de la del Estado, (Fanlo Loras 2002). Sus funciones son:

- La elaboración del Plan Hidrológico.
- La administración y control del Dominio Público Hidráulico.
- La administración y control de los aprovechamientos de interés general o que afecten a más de una comunidad autónoma.
- El proyecto, la construcción y explotación de las obras realizadas con cargo a los fondos propios del Organismo y las que sean encomendadas por el Estado y las que se deriven de los convenios con las comunidades autónomas, corporaciones locales y otras entidades públicas o privadas, o de los suscritos con los particulares.

Tras la trasposición de la Directiva Marco del Agua (2000/60/CEE) la demarcación hidrográfica es la base territorial para la consecución de los objetivos de calidad del agua, pues al espacio de las cuencas se añade el de las aguas de transición y costeras de acuerdo con el art. 16 bis del Texto Refundido de la Ley de Aguas.

LOS RECURSOS HÍDRICOS EN ESPAÑA

España cuenta con 112 km^3 de agua/año, lo que suponía en 2.710 m^3/habitante/año en 2005 (4), cifra que no ha sido actualizada pero podemos considerar que hoy ha de ser ligeramente inferior debido al aumento de la población. En cualquier caso, es una cantidad media si la comparamos con otros países y más que suficiente para satisfacer todas las necesidades de agua. Sin embargo, la climatología impone una fuerte irregularidad temporal y la orografía, relacionada con la anterior, también establece que haya importante irregularidad en la distribución espacial del agua, de forma que podemos decir que en líneas generales las cuencas del Cantábrico, Galicia, Ebro y Duero no tienen problemas salvo en periodos excepcionales, en las del Tajo, Guadiana y Guadalquivir tampoco, aunque son más sensibles a la escasez debido a que se acentúa la irregularidad, y estas características se intensifican en la zona mediterránea, especialmente en el SE, y en Canarias, donde hay que complementar la demanda con transvases y agua procedente de desalación.

España a lo largo de la historia ha realizado un enorme esfuerzo de construcción y mantenimiento de infraestructuras de almacenamiento y transporte de agua para poder

cubrir las demandas con altas garantías, lo que en los últimos años se ha continuado con la construcción de numerosas depuradoras para mejorar la calidad del agua circulante por los ríos y cumplir con los requerimientos de la Directiva Marco del Agua (2000/60/CEE). En conjunto, podemos considerar que estamos al nivel de cualquier país desarrollado, es decir: suficientes infraestructuras de almacenamiento (embalses principalmente), distribución (red de canales, acequias y tuberías), potabilización y depuración para satisfacer las demandas de agua de boca para la población y el turismo, industria, regadío, sector energético, etc, en algunos casos complementadas con desaladoras en las zonas de recursos hídricos más escasos (Mediterráneo y Canarias).

LA SEGURIDAD DE LAS INFRAESTRUCTURAS HÍDRICAS

En España, el Centro Nacional de Protección de Infraestructuras y ciberseguridad (CNPIC) es el órgano responsable del impulso, coordinación y supervisión de todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas españolas y con la ciberseguridad en el seno del Ministerio del Interior. El CNPIC depende del secretario de Estado de Seguridad, máximo responsable del Sistema Nacional de Protección de las Infraestructuras Críticas y de las políticas de ciberseguridad del Ministerio.

Fue creado en el año 2007, mediante Acuerdo de Consejo de Ministros de 2 de noviembre, siendo sus competencias reguladas por la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y por el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas. Entre sus competencias está la evaluación de amenazas y análisis de riesgos sobre instalaciones estratégicas, y una de las doce áreas estratégicas que incluye es la de suministro de agua.

El día 7 de mayo de 2007 el secretario de Estado de Seguridad aprobó el Plan Nacional de Protección de las Infraestructuras Críticas.

La normativa europea que ha permitido este plan reconoce que el riesgo de «ataques terroristas catastróficos» contra infraestructuras críticas «va en aumento» y por ello crea un catálogo de instalaciones sensibles a estos atentados.

Establece que las infraestructuras críticas son aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción pueden tener una repercusión importante en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados miembros y dentro del sector del agua incluye embalses, almacenamiento, tratamiento y redes. Están incluidas en el Catálogo Nacional de Infraestructuras Críticas, que comprende más de 3.500 instalaciones e infraestructuras sensibles con contenido secreto.

En noviembre de 2018 Concepción Cordón, jefa de gestión de riesgos de la Empresa Municipal de Aguas de Málaga, declaraba en una entrevista a *El Periódico de Aragón* (1) que un ciberataque al agua sería criminal. Esta afirmación se basa en el

alto nivel de digitalización que tienen los sistemas de gestión en España. El sector del agua comparte, por lo tanto, el riesgo de ciberataques con cualquier otro. Su materialización podría significar, por ejemplo, la alteración significativa de los parámetros de calidad del agua potable desde la distancia, haciéndola inservible para el consumo humano.

Los ataques a los suministros de agua pueden tener unas consecuencias graves, enorme repercusión en los medios, pueden ser relativamente baratos y según su ejecución pueden dar tiempo suficiente a los terroristas a huir antes de ser detectadas las consecuencias, por lo que a priori son apetecibles para grupos terroristas.

Hay numerosos antecedentes de ataques o intentos de ataque al agua destinada al consumo humano en la historia, a modo de ejemplo podemos señalar algunas (2):

– 2002. Dos agentes de Al Qaeda fueron arrestados en Denver con planes para envenenar los suministros de agua.
– 2004. El FBI y el Departamento de Seguridad Nacional emiten un boletín advirtiendo que los terroristas estaban tratando de reclutar trabajadores en plantas de agua como parte de un plan para envenenar el agua potable.
– 2010. En la región de Cachemira, India, los rebeldes maoístas envenenaron un estanque utilizado como fuente de agua potable por la Central Reserve Police Force, un grupo paramilitar.
– 2011. En La Línea de la Concepción (Cádiz) se detuvo a un yihadista por su intención de envenenar los suministros de agua en zonas turísticas en respuesta a la muerte de Osama Bin Laden (3).

Al largo historial de ataques o intentos de ataques terroristas a los suministros de agua de forma directa, se suma en nuestros días, la posibilidad de realizarlo a través del ciberespacio tal y como hemos señalado.

Dentro del sistema de distribución de agua en España parece lógico considerar como más vulnerable por la repercusión directa en la población el sector del agua potable, que incluye:

– Fuentes de agua potable. Son muchas y de muy variada naturaleza, como tramos de ríos, fuentes y manantiales, embalses, acuíferos, plantas desalinizadoras, etc. Su contaminación intencionada es posible, pero el tiempo que tarda en llegar el agua al consumidor y los controles de calidad que hay en este camino disminuyen los posibles efectos y por lo tanto la vulnerabilidad.
– Redes de distribución *en alta*. Compuesta por canales, tuberías y acequias para llevar el agua desde las fuentes mencionadas hasta las plantas de tratamiento. En ocasiones también cuentan con tanques de almacenamiento de menor capacidad que los embalses, con frecuencia situados en lugares no habitados y escasamente vigilados. Su vulnerabilidad es menor si están cubiertas y mayor si están al aire libre, pero también existen controles de calidad hasta el destino final y transcurre un tiempo notable, por lo que la vulnerabilidad es escasa.

En algunos casos se ha avanzado en la automatización del control de la cantidad de agua que se deriva de las fuentes a las redes de distribución y de los parámetros de calidad, lo que obliga a protegerse de potenciales ciberataques.

- Plantas de potabilización. Suelen ser recintos con protección física y controles de calidad del agua al salir. En ocasiones son los últimos controles antes de la llegada del agua al usuario, pero en grandes ciudades es normal que haya otros a lo largo de la red de distribución. Estas características no las hacen especialmente vulnerables a ataques directos, pero sí que son susceptibles de sufrir ciberataques.
- Redes de distribución. Son ampliamente reconocidas como el elemento más vulnerable del sistema (2) sobre todo por su relativamente fácil accesibilidad y porque el potencial de dilución de los posibles contaminantes o elementos tóxicos se reduce debido a la proximidad al usuario y a que en algunos casos no existen sistemas de detección. También su progresiva automatización, especialmente en grandes ciudades, les hace vulnerables a los ciberataques.

Productos tóxicos potencialmente utilizados

Son muchos los productos que se pueden utilizar, aunque es muy variable la facilidad para conseguirlos, su precio y su toxicidad, lo que determina su peligrosidad. Sin ánimo de ser exhaustivos, señalamos algunos:

- Los metales pesados son baratos y fáciles de obtener, de alta toxicidad, pero sus consecuencias no suelen ser inmediatas en el ser humano.
- Los herbicidas también son baratos y fáciles de obtener, pero en general su toxicidad no es muy alta, por lo que su efecto sería más bien psicológico.
- El caso de los insecticidas y nematocidas es diferente, pues también son baratos y sencillos de obtener pero su toxicidad es mayor. En este caso su peligrosidad depende en buena medida de la solubilidad, pues cuanto mayor sea, peores pueden ser sus efectos. También en este grupo podemos incluir a los rodenticidas, especialmente dañinos para los mamíferos como el ser humano.
- Productos químicos industriales. Son muchos y de diversa naturaleza, pero por sus características hemos de destacar el cianuro. Es muy tóxico por ingestión y su letalidad deriva de que impide la llegada de oxígeno a las células impidiendo su respiración. Es muy soluble en agua (600g/l a 20º) lo que le convierte en potencialmente muy peligroso.
- Elementos radiactivos. Son difíciles de obtener los de alta actividad, por lo que su uso no es probable. Sí que es posible la utilización de residuos radiactivos, de menor actividad.
- Toxinas y agentes biológicos. Son muy numerosos y algunos fáciles de obtener, por lo que se han de considerar potencialmente peligrosos.
- Hemos de considerar los productos químicos utilizados en los procesos de potabilización del agua como el cloro y el flúor, por lo tanto antes de su distribución. En cantidades adecuadas son útiles para ese fin y no tóxicos, pero por encima de ciertos niveles son tóxicos, además de fáciles de obtener pues están en las propias instalaciones. Su mal uso intencionado o como consecuencia de la alteración

de los sistemas automáticos de control mediante un ciberataque les convierte en potencialmente peligrosos.

Aunque los posibles ataques a redes de distribución destinadas a la población son los que tendrían mayor repercusión, también se ha de señalar la posibilidad de dirigir ciberataques a otras infraestructuras como los sistemas de refrigeración de centrales térmicas y nucleares, que podrían dejarlas temporalmente fuera de uso, con los consiguientes efectos para el sector energético.

El caso de los embalses merece algún comentario específico. Su construcción cumple estrictos controles de seguridad para disminuir el riesgo de roturas, pero la mayoría actualmente están automatizados, por lo que un ataque a estos sistemas podría producir un desembalse masivo incontrolado o una inutilización de las compuertas y sistemas de regulación, que podría ocasionar un llenado excesivo e incluso un desbordamiento.

Defensa ante posibles ataques a la red de distribución de agua

Sin duda la primera barrera es la prevención, que tiene varias variables, entre ellas la investigación de los Cuerpos y Fuerzas de Seguridad del Estado de posibles planes de ataque, pero también la protección física y vigilancia discreta pero efectiva de las infraestructuras, especialmente de las más sensibles recogidas en el Catálogo Nacional de Infraestructuras Críticas.

En redes de distribución es fundamental reforzar la detección de parámetros que puedan dispararse de forma repentina por encima de parámetros admisibles. Para ello actualmente existen sondas capaces de medir en continuo numerosos parámetros y detectar anomalías que permitirían una rápida interrupción del suministro si se da la circunstancia.

CONCLUSIONES

- España cuenta con recursos hídricos suficientes, aunque el reparto irregular tanto espacialmente como temporalmente genera fuertes desequilibrios.
- Nuestro país cuenta con altas garantías en el suministro de agua en cantidad y calidad suficiente para satisfacer las demandas de la población y de los principales sectores económicos, aunque en situaciones de intensas y prolongadas sequías se pueden sufrir restricciones o limitaciones.
- La red de infraestructuras hídricas es fundamental para el normal funcionamiento del país y su economía, por lo que algunas de ellas han sido incluidas en el Catálogo Nacional de Infraestructuras críticas.
- Existen bastantes antecedentes de ataques con elementos tóxicos vertidos a la red de agua en el mundo, por lo que es necesario considerarlo un riesgo.
- A este riesgo se suma la posibilidad de sufrir ciberataques que podrían ir dirigidos al manejo de las compuertas y desagües de presas, el funcionamiento de canales, potabilizadoras o incluso el vertido de productos químicos de estas

en cantidades no adecuadas, por lo que es necesario reforzar los sistemas de seguridad.
– La seguridad en las infraestructuras hídricas tradicionalmente se ha basado en dificultar el acceso a ellas, pero es necesario identificar los puntos más débiles y establecer, si es necesario, sistemas de refuerzo.

BIBLILGRAFÍA

– https://www.elperiodicodearagon.com/noticias/la-contra/concepcion- ordon-un-ciberataque-criminal-agua-seria-devastador_1325516.html. Consultado en septiembre de 2019.

– https://www.iagua.es/blogs/luis-martin-martinez/agua-objetivo-terrorista. Consultado en septiembre de 2019.

– https://www.elmundo.es/elmundo/2011/08/20/espana/1313850621.html. Consultado en septiembre de 2019.

– UNESCO 2008. «El Agua, una responsabilidad compartida. 2º informe de las Naciones Unidas sobre el Desarrollo de los Recursos Hídricos en el Mundo». Ed. ExpoZaragoza, 2008.

THE HYBRID THREATS AND THE NEW CONCEPT OF MAKING WAR

ANA CRISTINA DEL PASO GALLEGO
Periodista de Seguridad y Defensa. Doctora en Ciencias de la Información por la Universidad Complutense de Madrid y profesora de Periodismo y Comunicación Global en la UCM

When politics and diplomacy do not work, but you also do not want to opt to openly initiate armed conflict by not having ensured its outcome, the hybrid threat offers an insurmountable measure of coerration. Its tools are basic, effective and inexpensive. They just need to know how and when to be used. Hence his discreet advancement that no one wants to advertise for fear of showing his letters as an executor or executed because it is not easy to remain invulnerable to cyberattacks, disinformation campaigns, smear or manipulation or intelligence operations, for example give some examples. The use of unlimited ways of warfare such as unconventional and irregular combatants, cyberattacks, propaganda and manipulation of mass media, economic warfare and even energy resources pressure could be a good definition for hybrid threat tools. This new way of war requires managing of military intelligence and the use of especial forces in specific operations for achieving a destabilizing the *statu quo*. But, is Western ready for the so called hybrid attacks? We have hybrid war examples in Hezbollah confrontation in Lebanon in 2006, the Islamic State of Iraq and Al Sham (ISIS) and in the Russian actions in the Crimea Peninsula in 2014, Estonia in 2007 and Georgia in 2008. Analysts may anticipate that some current or potential state or non-state adversary will also learn from these hybrid-warfare low cost activities, potentially including states in East Asia or the Middle East[1]. The time has arrived to better defend ourselves form actors employing hybrid warfare.

Key words: hybrid warfare, NATO, deterrence, cybersecurity, defense, Russia, irregular tactics, asymmetric, manipulation, resilience

---

[1] The Military Balance, (2015), Chapter 1, Part III: Hybrid warfare: challenge and response. International Institute for Strategic Studies. http://www.iiss.org/en/publications/military%20balance/issues/the-military-balance-2015-5ea6/mb2015-01-essay-hybrid-warfare-9ec7

According to the analyst of National Defense University Frank G. Hoffman[2], «Hybrid war» is defined as a «blend of the lethality of state conflict with the fanatical and protracted fervor of irregular war». In fact, it has «the ability to employ irregular tactics and advances naval capabilities along with illegal or terrorist activity»[3]. But, behind asymmetric enemy, it happens to be there is always a State. The times of conventional war like *Dessert Storm Operation* in the Persian Gulf (1990-1991) are over. We have to dust off lessons learned from Balkans, Middle East or Africa to better prepare for the future.

After the NATO Wales Summit in September 2004[4], the North Atlantic organization expressed the need to fight the «hybrid warfare threats» and «hybrid threats» with new and necessary tools and procedures to deter and respond effectively to these threats, as well as the capacities to warrant the forces of each nation. However, among NATO members, there is not agreed definition of terms related to hybrid warfare and therefore is difficult to have a specific military strategy.

Michael Kofman, analyst of Center for New American Security and a fellow at the Wilson Center´s Kennan Institute thinks «the West has been terrorizing itself with specters of hybrid war to an extent that it should qualify as one of history's better disinformation operations, even if it was wholly unintentional. The problem is most pronounced for European allies who are undergoing a modern version of America's red scare from the 1940s and 50s. Someday, we may look back on this time in Europe and call it the hybrid war scare. Russian influence and subversion are real throughout much of Europe, but whipping up fears of this mystical hybrid warfare has led European officials to see the Kremlin's agents behind every corner[5]».

On the same line, Chris Tuck, analyst of Defense Studies Department at King´s College London, recalls that «intellectually, the concept of hybrid war says more about our fears than it does about any genuinely new model of war. This is not to say that the current security environment isn't difficult and dangerous. However, if we stopped connecting together all of our difficulties, multiplying them by the assumption of superior adversaries and then labelling them hybrid war, we might find these challenges easier to address[6]».

The issue is that hybrid war is not a spectrum but a real fact. Actually, we have recent evidences of intrusive role from hackers acting from Russia and Venezuela in France, Germany, Netherlands and United States elections, and United Kingdom´s Brexit and Catalonia referendum. There are evidences showing the overall cyberattacks to the mention countries have been made from trolls working in Russia —55 % of the cases— and

---

2 Hoffman, Frank G. (2007): *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington, VA, Potomac Institute for Policy Studies, p. 38.

3 Hoffman, Frank G.: «´Hybrid threats`: Neither Omnipotent Nor Unbeatable», *Orbis*, Volume 54, Issue 3, 2010, pp. 441-445.

4 NATO, Wales Summit Declaration, Press Release (2014): p. 13 and p. 104. http://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en

5 Kofman, Michael. (11 March 2016): «Russian Hybrid warfare and other dark arts», https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/

6 Tuck, Chris. (25 April 2017): «Hybrid War: The Perfect enemy». Defense-In-Depth Blog, Defense Studies Department, King´s College London. https://defenseindepth.co/2017/04/25/hybrid-war-the-perfect-enemy/

in Venezuela —30 %—, and only three profiles have been identified as from authentic internet accounts, according to different sources.

It looks like the Kremlin sought to manipulate public opinion with propaganda to separate Europe creating discrepancies in major issues such as refugee policy, economic stability, access and distribution of energy resources, human rights agreements and so.

Russia has violated the allied airspace and continues with its test of missiles and the intermediate range nuclear forces or neutralized networks as part of the hybrid attacks that Vladimir Putin, president of the Russian Federation, launches against the West, designed to achieve any number of Russian objectives through actions short of an Article 5 threshold-crossing event. In response, Western strategy remains mostly opaque, or at least not explicit. The reasons for this are too complex to address here, but they include both domestic and political as well as intra-alliance factors and dynamics», says John R. Deni, research professor of security studies at the Strategic Studies Institute of the U.S. Army War College and an adjunct professor at the American University's School of International Service[7].

Damien Van Puyvelde, professor of Security Studies and associate director for Research at the National Security Studies Institute, University of Texas, believes that rather than developing strategies based on 'hybrid' challenges, the warfare must be considered as it has always been: a complex set of interconnected threats and forceful means waged to further political motives.

Hybrid warfare has a large number of capabilities which confers into brutality, security disorder and terrorist attacks. This new face of war could be timeless with no limits since can use irregular and conventional tactics, cyberattacks that breaks the cybersecurity, criminal and terrorist procedures, organized crime, covert operations, sea disputes, satellites, control of the energy resources and so, in an unpredictable way.

This new way of making war can be done within a perfect structure with dispersed units equipped with IEDs, UAVs, missiles and munitions of last generation, high technology like cyberwarfare against key infrastructures, able to combine all kinds of capabilities —conventional or not—, to pursue the disruption and disorder of its opponent. This warfare is irregular and difficult to confront, not because of its capabilities but the philosophy of conventional response. Resilient response is the only way to win all kinds of hybrid threat such as irregular, unconventional, asymmetric, terrorist, special guerrilla or death squads attack operations.

But, how can we defeat an enemy who combines cyberattacks, criminality, irregular guerrillas and conventional structures? Maybe it would take a while to reach that target, but in the meanwhile, NATO and European Union members discuss from what we have learnt at a regional level and how and to cooperate in the Strategic Concept of collective defense, crisis management and cooperative security.

---

[7] Deni, John. R. :«More of the Same in Response to Russia?», Carnegie Europe, Judy Dempsey´s Strategic Europe, 23 november 2017. http://carnegieeurope.eu/strategiceurope/74811

NATO, UE AND PESCO PERSPECTIVES

Asymetric, hybrid and counter-insurgency operations will frame the future armed conflicts changing the actual paradigms of ways to do war. It´s time to review our capabilities, technology and to update again the allied command structure as we did once within NATO. The North Atlantic Alliance and the European Union have an opportunity for deterring hybrid warfare and the only way to succeed in this purpose is working together.

NATO and European Union must be prepared for the «new generation of war» with special weapons, appropriate hardware, enough resources and specific fighter outfit. On the contrary, NATO and EU may fail and lose a chance to detain Vladimir Putin, president of the Russian Federation, who employed urban swarming tactics against Chechens, Georgians or, moreover, Ukrainians. Somalia, Chechnya, Lebanon, Georgia and Ukraine are good examples on how to use hybrid weapons to confront all kinds of enemies, such us non-conventional threats, guerrillas, terrorist and criminal mercenaries. So, it is a good time for NATO and EU to cooperate as brothers in arms.

In words of NATO Secretary General Jens Stoltenberg: «Russia has used proxy soldiers, unmarked Special Forces, intimidation and propaganda, all to lay a thick fog of confusion; to obscure its true purpose in Ukraine; and to attempt deniability. So NATO must be ready to deal with every aspect of this new reality from wherever it comes. And that means we must look closely at how we prepare for; deter; and if necessary defend against hybrid warfare»[8].

One of the big steps already given is the EU Global Strategy for Foreign and Security Policy (EUGS) that started a process of «closer cooperation in security and defense. Member States agreed to step up the European Union's work in this area and acknowledged that enhanced coordination, increase investment in defense and cooperation in developing defense capabilities. These are part of the key requirements to achieve. This is the main aim of a Permanent Structured Cooperation on security and defense (PESCO), as outlined in the Treaty of the EU, Articles 42 (6) and 46, as well as Protocol 10. Through PESCO, Member States increase their effectiveness in addressing security challenges and advancing towards further integrating and strengthening defense cooperation within the EU framework[9]».

PESCO members are aware of the need to develop defense capabilities and make them available for European Union military operations and to maximize the effectiveness of defense spending, but, how is PESCO going to reach that target? European Union makes the force and the international organizations involved keep an eye on this.

As we know, in PESCO, the participation stays voluntary, decision-making remains in the hands of participating Member States and the commitments must be common. But

---

[8] NATO keynote speech by NATO Secretary General Jens Stoltengberg at the opening of the NATO Transformation Seminar, (25 March 2015), Washington, DC. https://www.nato.int/cps/en/natohq/opinions_118435.htm?selectedLocale=en

[9] Permanent Structured Cooperation (PESCO): «Deeping Defense Cooperation among UE Members States», European External Action Service. 2017 https://eeas.europa.eu/sites/eeas/files/pesco_factsheet_14-11-2017.pdf

again: How are they going to coordinate themselves to be successful? Are they going to be able to share deeper sensitive information like the one regarding with cyberspace?

Considering the nowadays instability, to be efficient against hybrid threats is a must and can be done revising coordination of military capacities, increasing the operational readiness, unifying weapon systems and improving the interoperability of rapid reaction force.

DECISION MAKING

The Baltic countries see Russia as a threat *per se*: at first, after the Ukraine operation and, now, moreover with joint strategic military exercise ZAPAD 2017 of the Russian Federation and Belarus (12,700 personnel –just under the figure of 13,000 that requires OSCE observers- and tested Russia´s defensive capabilities).

Eve Hunter and Piret Pernik, from International Centre for Defense and Security (ICDS) think: «Currently, we lack a legally or politically-recognized division to determine at what point network intrusion and sabotage becomes an act of war. These issues are of particular concern for the Baltic States, which are some of the most at risk for Russia's aggressive expansionist policies»[10] .

One of the steps taken already to face hybrid challenges is the creation of the NATO Centre of Excellence for Strategic Communication in Riga (Latvia), agreed during the Wales summit of 2014 and announced in its final declaration[11]: «We will ensure that NATO is able to effectively address the specific challenges posed by hybrid warfare threats, where a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design. It is essential that the Alliance possesses the necessary tools and procedures required to deter and respond effectively to hybrid warfare threats, and the capabilities to reinforce national forces. This will also include enhancing strategic communications, developing NATO and other organizations, in line with relevant decisions taken, with a view to improving information sharing, political consultations, and staff-to-staff coordination. We welcome the establishment of the NATO-accredited Strategic Communications Centre of Excellence in Latvia as a meaningful contribution to NATO's efforts in this area. We have tasked the work on hybrid warfare to be reviewed alongside the implementation of the Readiness Action Plan». This project is not enough and can´t be the only decision making to fight against hybrid warfare.

In the opening ceremony of the NATO summit, the Latvia Foreign Ministry State Secretary Andrejs Pildegovi's said: «Developments in Ukraine remind us that the security situation is changing, and we must be able to respond to emerging challenges. One of such challenges is the information space and communication, which acquire an ever increasing

---

[10] Hunter, Eve y Pernik, Piret (2015): The challenges of Hybrid Warfare, Tallinn, Estonia, International Centre for Defense and Security (ICDS), p. 3. https://www.icds.ee/fileadmin/media/icds.ee/failid/Eve_Hunter__Piret_Pernik_-_Challenges_of_Hybrid_Warfare.pdf

[11] NATO, Wales Summit Declaration, *op. cit.* 13th point. https://www.nato.int/cps/en/natohq/official_texts_112964.htm

significance in any crisis situation. Through pooling their efforts, NATO members have a great potential for developing the sector, and Latvia is full of resolve to contribute considerably toward achieving that goal[12]».

This was a crucial statement of warning to all NATO members to strengthen the bond between Europe and North America and to face the 21st century challenges.

After the meeting of the North Atlantic Council in Warsaw (july 2016), the heads of State and Government agreed to adapt defense and deterrence posture to respond to threats and challenges, increasing investment in capabilities and the development of highly-capable and deployable forces sustainable and interoperable. The Defense Investment Pledge agreed at the Wales Summit[13] (September 2014) was an important step in this direction and NATO Head of States and Government reaffirmed its significance.

In NATO Warsaw summit, the members recalled -according to the Package of Measures for the Implementation of the Minsk Agreements- the immediate and comprehensive ceasefire in certain areas of the Donetsk and Luhansk regions of Ukraine to be implemented as of 15 February 2015[14] and called on Russia to stop its political, military and financial support to the militants including the withdrawal of its forces and equipment from Ukraine and to allow that country to reinstate full control over its state border. In spite of these demands, Putin took his time for his next movement.

On the other hand, OSCE made its own efforts with the mission of special monitoring to reduce the intensity of the conflict using all kinds of soft power resources to avoid bigger and worse consequences. The reason was that the Russian developments in Ukraine had serious implications for the stability and security of the entire Euro-Atlantic area.

According to different sources, the adopted strategy and actionable implementation plans of NATO in countering hybrid warfare was not effective enough, although the North Atlantic NATO is prepared to assist an ally at any stage of a hybrid campaign and as part of collective defense included when the Council invokes Article 5[15] of the Washington Treaty. The Alliance is committed to effective cooperation and coordination with partners and relevant international organizations, in particular the EU, as agreed, in efforts to counter hybrid warfare. The wishes and intentions are clear as well as the message that the work must be done as a hole within the Alliance.

NATO has the challenge to deal with the new procedures to defense its members from unconventional attacks changing the pattern of State against State, unless countries like North Korea decides to attack South Korea, Japan or United States and starts a nuclear war. The results will be the total destruction of North Korea.

---

12 Latvia Ministry of Foreign Affairs (2014): NATO Center of Excellence for Strategic Communication in Latvia. http://www.latvia.lv/news/nato-centre-excellence-strategic-communication-latvia

13 NATO, *op. cit,* p.1 https://www.nato.int/cps/ic/natohq/official_texts_112964.htm

14 NATO, Joint statement of the NATO-Ukraine Commission at the level of Heads of State and Government (9 july 2016). https://www.nato.int/cps/en/natohq/ofçficial_texts_133173.htm?selectedLocale=en

15 NATO, (1949): The North Atlantic Treaty, Article V. https://www.nato.int/cps/en/natohq/official_texts_17120.htm

The Article 5 of the North Atlantic Treaty says:

> «The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.
> Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security».

The ambiguity of Article V of NATO concerned to operations in Afghanistan left behind the United States desire to give a blunt response to terrorism. However, things happened differently.

At that time, NATO Secretary General Lord George Robertson explained that, «it was premature to speculate on what military action would be taken by the Alliance, be it individually or collectively». He did not consider the information given by Frank Taylor, then NATO ambassador of United States, who provided to the organization Council all kinds of information about Al Qaeda attacks of September 11, 2001, headed by Osama bin Laden and protected by the Taliban regime in Afghanistan. When the Alliance invoked the principle of Article V of the Washington Treaty on 12 September, it stated that it needed to know whether such actions had been conducted from abroad before the Article could become fully operative. Some analysts think the NATO Article V needs to be reviewed.

The NATO decision made United States to give an unilateral response to the Taliban regime in Afghanistan sending expeditionary operations of special forces easy and fast to be deployed and no need of a traditional military structure. The president of Unites States George W. Bush and his CHOD (Chief of Defense) were ready to start an asymmetric warfare with hybrid tools against all possible threats.

The answer to a new generation on hybrid combat from the United States was a seven-week campaign to topple the Taliban in Afghanistan.

After the end of that campaign against Taliban, Donald Rumsfeld, Defense Secretary and the president George W. Bush, engaged in a transformational campaign that basically changed the rules of warfare focused on the use of small, light-footprint Special Operations Forces (SOF) on the ground and backed by precision air power. That was Rumsfeld´s description of what «the recipe was for success».[16]

---

[16] H. A. S. C. (2000): Counter-insurgency an irregular warfare: issues and lessons learned, Hearing Held May 7, 2009, Committee on Armed Services, House of Representatives No. 111-55, US Government Printing Office, Washington.

It was also crucial to defeat the Talibans, the roll played by general Tommy Franks, commander of US Central Command and responsible of the Force, Intelligence, Surveillance and Reconnaissance (ISR) coming from space-based and high altitude as well as unmanned systems critically important[17].

From now ahead, the war will combine covert and overt military operations with paramilitary, guerrilla or death squads as main task force with non-state actors, which includes the need to update our procedures of combat and to ensure the ability to effectively address the challenges posed by hybrid warfare where the rules of engagement differ from the ones of a conventional war. As US general Douglas MacArthur said: «we are not retreating, we are advancing in another direction».

The final statement made at the NATO Warsaw summit (July 2016) by the heads of State and Government of the member countries of the North Atlantic Alliance was clear when they recognized that «there is an arc of insecurity and instability along NATO's periphery and beyond» (Russia is surrounded by NATO member countries).

The Alliance faces a range of security challenges and threats that originate both from the east and from the south; from state and non-state actors; from military forces and from terrorist, cyber, or hybrid attacks. Russia's aggressive actions, including provocative military activities in the periphery of NATO territory and its demonstrated willingness to attain political goals by the threat and use of force, are a source of regional instability, fundamentally challenge the Alliance, have damaged Euro-Atlantic security, and threaten our long-standing goal of a Europe whole, free, and at peace. Our security is also deeply affected by the security situation in the Middle East and North Africa, which has deteriorated significantly across the whole region. Terrorism, particularly as perpetrated by the so-called Islamic State of Iraq and the Levant (ISIL)/Da'esh, has risen to an unprecedented level of intensity, reaches into all of Allied territory, and now represents an immediate and direct threat to our nations and the international community. Instability in the Middle East and North Africa also contributes to the refugee and migrant crisis[18]».

The next NATO summit, taking place July 2018 in Brussels, the members need to take a step forwarded to evolving threats and reinforce its collective defense. It is true that things have been done as the NATO secretary general said «our multinational battlegroups in the east of the Alliance are now fully operational and we are strengthening our presence in the Black Sea region. We are also stepping up our efforts against cyber-attacks and hybrid threats[19]».

Jens Stoltenberg said that NATO will build on our valuable work with partner nations and organizations to fight terrorism and keep our neighborhood stable. We are boosting our mission to train, advice and assist the Afghan forces to ensure their country never again becomes a safe haven for international terrorists. We are supporting the Global Coalition to Defeat ISIS, and working to strengthen partners like Iraq. We are further

---

17 *Ibid*, p. 4.

18 NATO Warsaw Summit Communiqué, *op. cit.* 13th Point. https://www.nato.int/cps/en/natohq/official_texts_133169.htm

19 NATO Secretary General statement. 20 October 2017.

deepening the relationship between NATO and the European Union, for the benefit of all our nations[20]».

As we see unconventional war is becoming a global threat. We have to face it and combat with our capabilities and if we do that in a number of areas such as Somalia, Yemen and so forth, we have to know the way you can really figure out what your force requirement is what your large strategy is going to be, because the solution set for each one of those problems is going to be different.[21]

David J. Kilcullen considers that «counterinsurgency is feasible, though definitely not preferred in the current strategic environment. But if we do need the engage in it, especially in traditional tribal societies, then an emphasis on local partnerships and local security forces that a protect communities and guard against extremist presence is likely to be an essential component of such a campaign. At a more strategic level, such local partnerships are also a key component in coping with the threat of transnational takfiri terrorism[22]».

Now that we have identified the problem, the way and the means with which it fights, the concern of international organizations, it is time to maneuver. As Qiao Liang and Wang Xiangsui say, «in warfare and non-military warfare, which is primarily national and supra-national, there is no territory which can´t be surpassed; there is no means which cannot be used in the war; and there is no territory and method which cannot be used in combination[23]».

CONCLUSIONS:

1. Is a fact that unconventional war is becoming a global threat and dealing with terrorists and hybrid enemies will require unconventional responses.
2. NATO is able to effectively address the specific challenges posed by hybrid warfare threats, where a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design. But, it is a must deepening the relationship between NATO and the European Union. The transnational organizations are stronger together but European Union cannot depend on NATO.
3. We must be mindful that we have to be able to respond to emerging challenges. One of such challenges is the information space and communication which acquire an ever increasing significance in any crisis situation and maybe might need to be reviewed.
4. We have to adjust to the changing rules of warfare, maybe improving our Special Operations Forces when are deployed on the ground and backed by precision air power.

---

20 Ibid, 20 October 2017.

21 H. A. S. C. *op. cit.* p. 10 .

22 Kilcullen, David J. (2009): *The accidental guerrilla*, Oxford University Press, extract from chapter 5.

23 Liang, Qiado and Xiangsui, Wang (1999): *University Warfare*, Beijing, PLA Literature and Arts Publishing House.

BIBLIOGRAPHY:

– DENI, John. R. (23 november 2017): «More of the Same in Response to Russia?», Carnegie Europe, Judy Dempsey´s Strategic Europe, p. 4. http://carnegieeurope.eu/strategiceurope/748114

– EUROPEAN EXTERNAL ACTION SERVICE (2017): Permanent Structured Cooperation (PESCO): «Deeping Defense Cooperation among UE Members States», https://eeas.europa.eu/sites/eeas/files/pesco_factsheet_14-11-2017.pdf

– H. A. S. C. (2000): Counter-insurgency an irregular warfare: issues and lessons learned, Hearing Held May 7, 2009, Committee on Armed Services, House of Representatives No. 111-55, US Government Printing Office, Washington.

– HOFFMAN, Frank G. (2007): *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington, VA, Potomac Institute for Policy Studies, p. 38.

– HOFFMAN, Frank G. (2010): «´Hybrid threats`: Neither Omnipotent Nor Unbeatable», *Orbis*, Volume 54, Issue 3, pp. 441-445.

– KOFMAN, Michael. (11 march 2016): «Russian Hybrid warfare and other dark arts», https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/

EL NORTE Y EL ESTE DE SIRIA: PROCESOS DE ESTABILIZACIÓN

JUSAIMA MOAID-AZM PEREGRINA
Alumna de la Universidad de Granada

Resumen

El conflicto en Siria ha evolucionado constantemente desde su estallido. Actualmente, las fuerzas del régimen sirio controlan prácticamente todo el territorio del país, excepto la zona comprendida al norte del río Éufrates donde se ha desarrollado un proceso paralelo de estabilización y gobernanza. Así, las preguntas que vertebran esta investigación se dirigen a determinar los factores que han propiciado esta estabilización y la actual gobernanza de esta zona en el marco del conflicto sirio; sobre las hipótesis de que, por un lado, las redes internacionales de oposición al ISIS han actuado como variable causal determinante del primer proceso; mientras que, para el segundo, lo han sido los precedentes auto-organizativos de gobernanza en la zona. De esta forma, en el proceso de verificación de la primera, se procede a contrastar la evolución de estas redes con el avance de las fuerzas combatientes del norte en tanto que brazo armado de esta gobernanza; mientras que, para la segunda, se analiza la influencia de los precedentes sobre la gobernanza actual de la zona, la administración autónoma democrática del norte y este de Siria.

Palabras clave: Siria, gobernanza, estabilización, norte y este de Siria, EE. UU., Fuerzas Democráticas Sirias, ISIS.

Abstract

The conflict in Syria has evolved constantly since its outbreak. Currently, the forces of the Syrian regime control most of the territory of the country, except from the northern area of the Euphrates River, where a parallel process of stabilization

and governance has been developed. Thus, the questions that guide this research are aimed at determining the factors that have led to this stabilization and the current governance of this area in the framework of the Syrian conflict, based on the hypothesis that, on the one hand, international networks opposing ISIS have acted as the causal variable determining the first process; while, for the second, it has been prompted by the self- organizing origins of governance in the area. In this way, in the verification process of the first one, we contrast the evolution of these networks with the progress of the northern combat forces as the armed arm of this governance; Meanwhile, for the second one, the influence of the origins of the current governance of the area, the Democratic Autonomous Administration of the North and East of Syria, is analyzed.

Keywords: Syria, governance, stabilization, North and East of Syria, USA, Democratic Syrian Forces, ISIS.

INTRODUCCIÓN: OBJETO E HIPÓTESIS DE INVESTIGACIÓN

«El conflicto sirio ha estado caracterizado por su absoluto desprecio de los más mínimos estándares». Así describía el alto comisionado de Naciones Unidas para los Derechos Humanos el escenario sirio al Consejo de Seguridad, en una reunión informal organizada el pasado mes de marzo de 2018, tras recibir el veto de Rusia para hacerlo en una sesión oficial. En efecto, el año 2011 marcó el comienzo de uno de los grandes centros de conflictividad abierta más cruentos en Oriente Próximo debido a las represivas respuestas gubernamentales del presidente Bashar al-Asad a las manifestaciones y protestas enmarcadas en el proceso que se dio a conocer como la Primavera Árabe. En consecuencia, según el *Global Peace Index*, Siria ocupa desde 2016, la última posición en la clasificación de un total de 163 países según su nivel de conflictividad.

A pesar de tener su origen en acontecimientos intra-fronterizos, desde su comienzo, la crisis política siria ha sido objeto de una progresiva regionalización e internacionalización, donde se han superpuesto la pugna por la hegemonía regional e internacional de un amplio abanico de potencias en un escenario de *war by proxy* que ha producido en consecuencia, altos niveles de sectarización y una progresiva balcanización del conflicto. A mediados de 2012, el conflicto sirio contaba ya con la presencia de tropas iraníes, saudíes, turcas, afganas, pakistaníes, cataríes, emiratíes, entre otras, a las que, progresivamente se unirían diferentes potencias occidentales y Rusia.

Este progresivo aumento de la conflictividad está en el origen más inmediato de los éxodos y desplazamientos masivos de personas en el país, la región y hacia Europa, produciéndose el desgarre de los tejidos social, político-institucional, cultural y económico sirios. En materia humanitaria, los números que reflejan la pérdida de vidas humanas alcanza cotas sobrecogedoras; en el ámbito jurídico, los crímenes, asedios, bombardeos ilegales, empleo de armas prohibidas, etc…, perpetrados indistintamente por las partes contendientes, supondrán en el mejor de los casos, un verdadero

desafío para la justicia nacional e internacional; en materia de seguridad y defensa, la crisis siria añade una capa más de tensión e inseguridad al conjunto de la sociedad internacional; en materia económica, la sensibilidad de la inversión, la merma de la fuerza de trabajo o la quiebra de la actividad industrial y primaria han supuesto fuertes cambios en los mercados, tanto nacionales como internacionales. Todo ello sin mencionar las grandes cuestiones identitarias y étnico-religiosas que afloran a raíz de la crisis siria y que son empleadas estratégicamente en el marco del juego político-partidista occidental y, concretamente europeo, cuyo impacto político está aún por determinar.

Sumergida en este complejo panorama, las dinámicas del conflicto en Siria han sido múltiples y han tenido como protagonistas numerosas alianzas con diferentes grados de liquidez y volatilidad de actores procedentes de los niveles local, regional e internacional. A esta razón, el influjo ruso en apoyo al régimen de Bashar al-Asad en el conflicto, sumado al iraní, entre otros actores locales, han sido determinantes en el logro de la actual situación de primacía del mismo en el campo de batalla. En consecuencia, el mes de marzo del presente 2019 arrojaba la siguiente partición del territorio sirio entre las principales facciones contendientes:

Tabla 1. Territorio bajo control de las principales facciones contendientes.

	Superficie bajo control (en Km2) Porcentaje sobre la superficie total siria	
Fuerzas de la oposición	18.694	10 %
Fuerzas leales al régimen de Bashar al- Asad	116.193	62,7 %
Fuerzas Democráticas de Siria (FDS)	52.460	28 %

Fuente: elaboración propia a partir de los datos provistos por Infogram (2019).

Esta situación difiere sobremanera con la aún más fragmentada distribución del territorio en los años previos, acompañados asimismo por el avance del autoproclamado Estado Islámico (ISIS en adelante), quien en marzo de 2017 llegó a controlar hasta el 43,40 % del territorio total sirio según el *Institute for the Study of War.*

No obstante, el panorama actual del territorio sirio se encuentra marcado por fuertes contrastes. Frente a las áreas bajo control del régimen y las fuerzas de la oposición, caracterizadas por la presencia de combates y bombardeos continuos, las Fuerzas Democráticas de Siria (FDS en adelante) que controlan el noreste del país, han conseguido garantizar la estabilidad en el área. En efecto, las autoridades político-militares, locales y regionales, del noreste sirio no solo han asegurado un espacio libre de las fuerzas del ISIS, sino que han establecido mecanismos de autoadministración y gobernanza, incluyendo diferentes formas políticas de organización local dependientes de la Federación Democrática del Norte de Siria (FDNS) proclamada en 2016, más adelante, anunciada como Administración Autónoma del Norte y Este de Siria (AAS).

La AAS, caracterizada por su multietnicidad, integra fuerzas kurdas, tanto en su rama política (el Partido de la Unión Democrática Siria, PYD), como militar (las Unidades de Protección Popular, YPG/YPJ), árabes, asirias, turcomanas, armenias, circasianas, chechenas, entre otras, y actúa como una estructura de gobierno de facto en el noreste sirio, que ha sido organizado a través de tres regiones o cantones, que cuentan asimismo con un gobierno propio a través de un sistema de consejos y comités locales. Así, el presente análisis mantiene como objeto de investigación la estabilidad y la gobernanza en la zona del norte y noreste sirio bajo la influencia de la Administración Autónoma para el Norte y Este de Siria.

La estabilidad y autogobierno de la zona no solo contrasta enormemente con la situación en el resto del país, sino que ha supuesto un destino seguro dentro del caos sirio para un total de 35.800 desplazados internos en el periodo comprendido entre noviembre y diciembre de 2018, según el informe *Syria Crisis: Northeast Syria Situation Report No. 30* de la Oficina de la ONU para la Coordinación de Asuntos Humanitarios (OCHA). Todo lo cual, nos lleva a la siguiente pregunta de investigación, a saber, ¿qué factores han determinado la estabilización del territorio bajo control de la AAS?

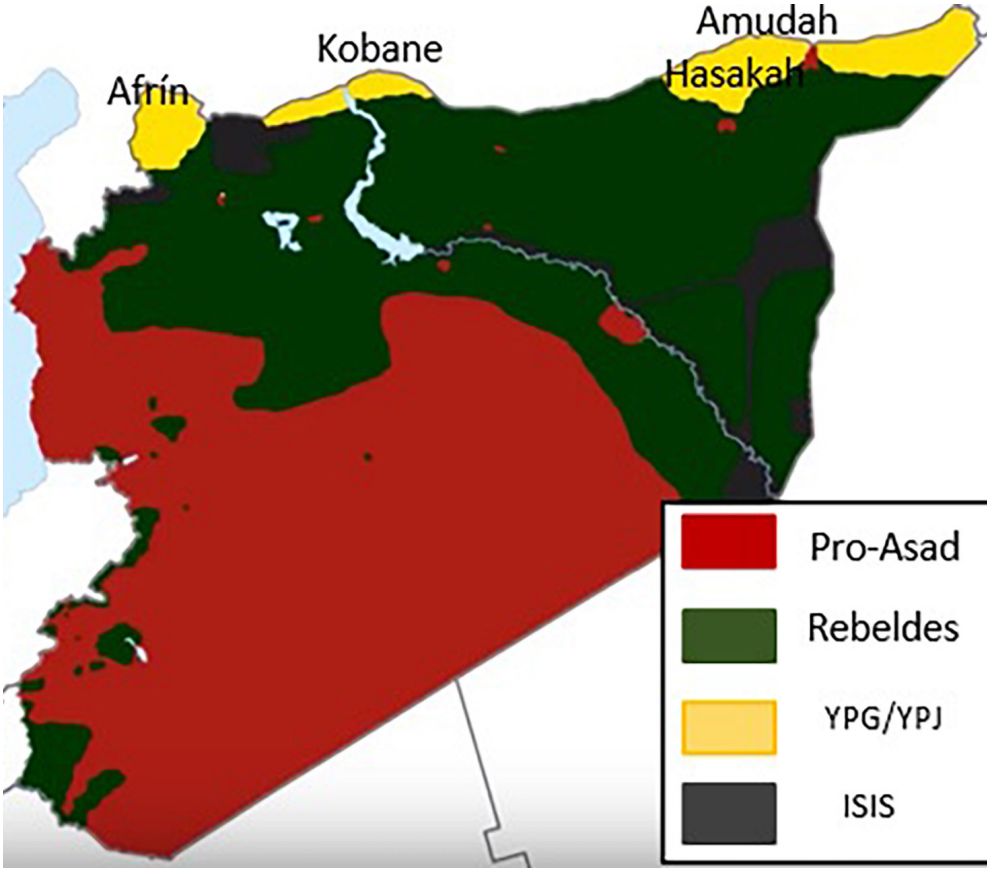
En este sentido, bajo las orientaciones estratégicas señaladas, el conjunto de esfuerzos teóricos y metodológicos que se adscriben a la presente investigación pretenden ofrecer un proceso de verificación de la hipótesis siguiente: las redes internacionales de oposición al ISIS fueron determinantes para la estabilización de la zona bajo control de la AAS.

La hipótesis queda orientada a verificar el impacto de las redes internacionales de oposición al ISIS urdidas en el contexto sirio sobre la progresiva estabilización del territorio de la AAS. Estas redes, en tanto que variable causal, comprenden no solo la creación y actuación de la Coalición Internacional contra el ISIS, sino también los esfuerzos estadounidenses dirigidos a la promoción de una fuerza terrestre que combatiese al ISIS, las FDS, así como sus precedentes más inmediatos, de origen eminentemente kurdo, que enfrentaron al autoproclamado ISIS en el norte sirio en el origen de su trayectoria.

LA ESTABILIZACIÓN DEL NORTE Y ESTE DE SIRIA

El control del territorio por las fuerzas kurdas: fase expansiva

Al inicio de la guerra en siria, el PYD y su brazo armado emergían como la principal fuerza activa en la región norte-noreste de Siria. Tras la retirada de las fuerzas de Asad de las áreas kurdas más pobladas, las YPG/YPJ capturaron Kobane (Ayn al-Arab) en julio de 2012, extendiéndose más adelante a Amudah, Afrín, el norte y este de Hasakah con relativa facilidad. Así, en el periodo 2011- 2014, las fuerzas kurdas consiguieron extenderse sobre tres grandes núcleos del norte del país, a saber:



Mapa 1. Control del territorio sirio en julio de 2013. Fuente: Syrian Civil War: Everyday (NY Mapper)

Los factores que explican esta eficaz conquista del territorio mantienen una naturaleza eminentemente interna que enraíza en las relaciones *de facto* del PYD con el régimen de Bashar al-Asad, así como en su organización logística y militar.

Por un lado, el hecho de que el régimen y el PYD adoptasen *de facto* en el periodo objeto de análisis en este apartado, un *modus vivendi* caracterizado por la tolerancia en un sentido estricto, y el apoyo en determinados puntos cronológicos, ha resultado beneficioso para ambas partes, en la medida en que, la retirada en julio de 2012 de tropas gubernamentales de la zona del norte de Siria habilitaba al PYD a extender el territorio bajo su control rápidamente. Para el régimen, esta estrategia se enmarca en una política étnica empleada con anterioridad, que tiene por objeto el aprovechamiento de la fuerza del factor identitario en árabes y kurdos en Siria. En efecto, el régimen confía tanto en la posición dominante del PYD como en su demostrada aversión a la oposición rebelde que busca el derrocamiento del régimen, alimentando así una estrategia sectaria que aprovecha las relaciones árabo-kurdas en el norte

del país en beneficio de Bashar al-Asad (Sary, 2016: 17, International Crisis Group, 2014: 9).

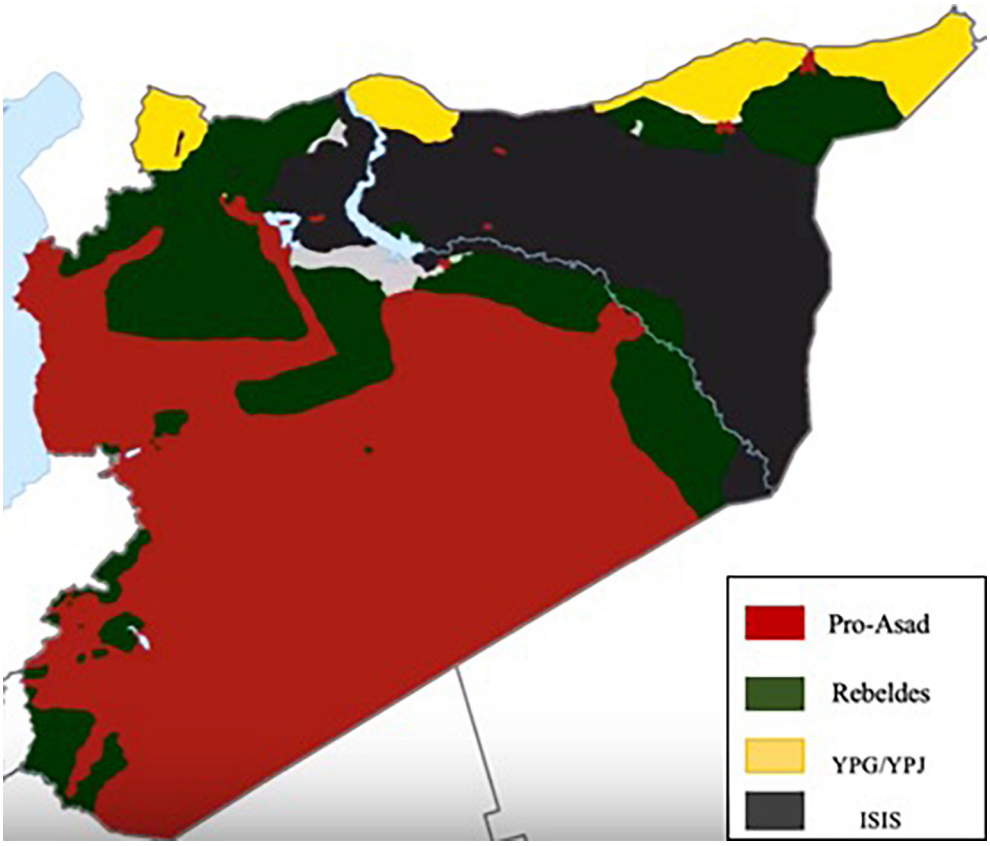
Por otro lado, el segundo factor clave que permitiría al PYD extender su territorio en el periodo 2011-2014 hasta alcanzar un punto álgido en julio de 2013 (véase mapa 1), radica en la propia organización político-militar de su fuerza. En efecto, aunque algunos sitúan la creación de las YPG kurdas después de las revueltas de Qamishli, en 2004 (Gold, 2012), fue al inicio de la revolución en 2011 cuando declararon oficialmente su existencia y, a partir de mediados de 2012, cuando actuaron en el conflicto de forma más activa, alcanzando unas cifras que oscilan entre 20.000 y 30.000 efectivos (Casagrande, 2016), según la fuente.

En términos organizacionales la herencia recibida por el PYD del PKK en Turquía es notable. No cabe duda de la colaboración entre ambas organizaciones al comienzo de la revolución; no solo las fuerzas de las YPG/YPJ recibieron entrenamiento militar y armamento por parte del HPG, Fuerza de Defensa del Pueblo, el brazo armado del PKK, sino que, incluso algunos militantes de este último, se unieron a las YPG/YPJ al inicio del conflicto (International Crisis Group, 2012). De hecho, en una entrevista concedida por Salih Muslim a Al-Quds Al-Arabi el 2 de enero de 2016, el líder del PYD reconocía que «(…) es solo natural que un kurdo que anteriormente era uno de los luchadores en las montañas [del PKK] quiera defender su hogar [en Siria]» (Al- Quds Al-Arabi, 2016).

La pérdida de control sobre el territorio del norte de Siria: fase regresiva

El año 2013 estuvo marcado igualmente por la intromisión de un nuevo actor en el escenario sirio. En efecto, aunque las redes del autoproclamado Estado Islámico ya habrían accedido al país en 2011, fue a principios de 2013 cuando la organización realizaba toda una declaración de intenciones de «expandir su influencia a la región del Levante, que englobaría no solo Siria sino también Líbano, Israel y Jordania» (Jordán, 2015: 121). A lo largo de 2013, el ISIS afianzaba su posición en Siria, de forma que, en enero de 2014, conseguiría arrebatar Raqqa a otras milicias y organizaciones de corte yihadista, siendo utilizada desde entonces como «capital» del supuesto califato proclamado en junio del mismo año (Jordán, 2015).

La progresiva conquista de territorio por el ISIS en el país resultó especialmente rápida, a la par que iba constituyéndose como una evidente amenaza a las áreas bajo control del PYD. En enero de 2014, el ISIS habría conseguido extenderse por gran parte del noreste sirio, territorio en el que habitaban una cifra estimada de seis millones de personas (véase mapa 2).



Mapa 2. Control del territorio sirio en enero de 2014. Fuente: Syrian Civil War: Everyday (NY Mapper)

El avance del ISIS, que había situado los tres enclaves kurdos del norte de Siria en el punto de mira para continuar su expansión territorial, motivó a las fuerzas kurdas del PYD a estrechar su colaboración con varios grupos cristianos (Allot, 2015). De hecho, cuando las unidades del ISIS alcanzaron Hasakah en agosto de 2014, nunca tomaron completamente la ciudad, pues esta había sido dividida en tres sectores controlados respectivamente por el régimen, el ISIS y las fuerzas kurdas y cristianas (Drott, 2013).

La minoría cristiana en Siria representa aproximadamente un diez por ciento de la población total del país y con anterioridad al inicio del conflicto, esta se encontraba distribuida por todo el país, destacando las ciudades de Damasco, Alepo, Latakia, Homs y, en el norte sirio, Jazire y Hasakah. Asimismo, el entrelazamiento étnico-religioso también está muy presente en estas comunidades, caracterizadas por una profunda pluralidad que queda manifiesta en la multiplicidad de combinaciones entre iglesias (católica, ortodoxa, maronita, caldea, asiria, etc…), y etnias (asiria, armenia, etc…) (Minority Rights Group International, 2018).

No obstante, aunque la guerra en el país ha impactado indudablemente sobre esta distribución inicial de minorías en el territorio del país, implicando cambios demográficos en la geografía siria cuyos efectos aún están por determinar, el noreste sirio vio nacer a lo largo del año 2013 un abanico de milicias cristianas dirigidas a coordinar una acción armada contra el ISIS.

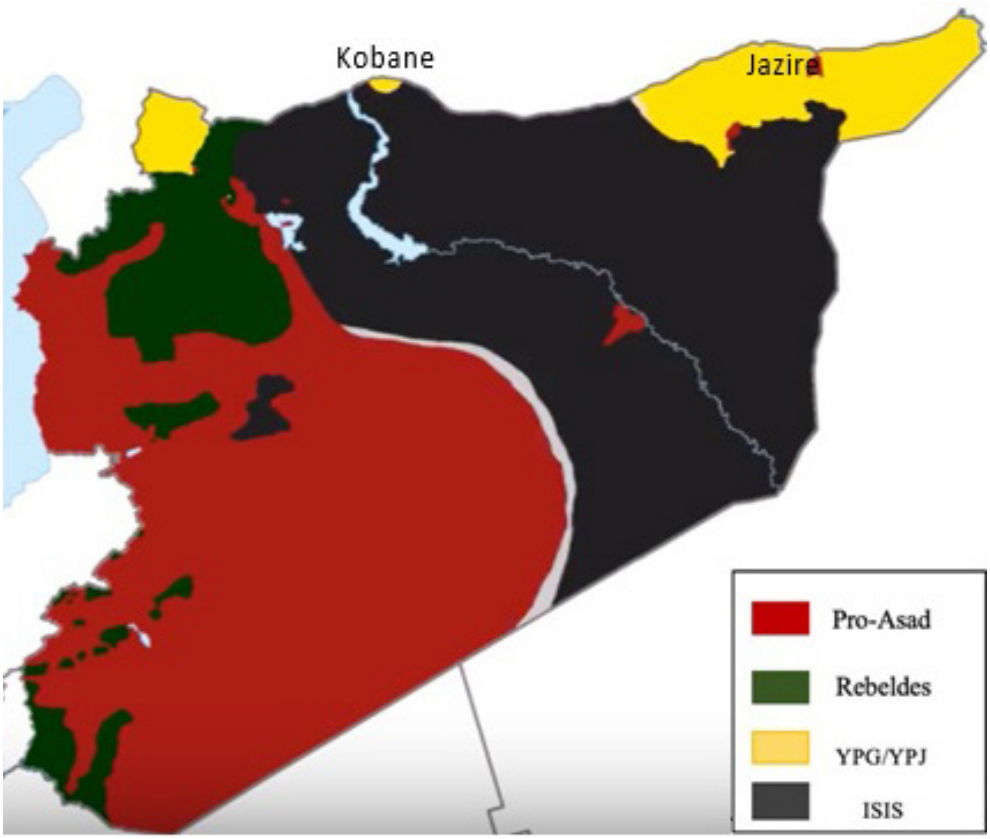
En este sentido, el Partido de la Unión Siríaca (SUP por sus siglas en inglés), que integra comunidades siríacas-asirias es el ejemplo más destacado. Considerada uno de los principales miembros de la organización del Consejo Nacional Bethnahrim (CNB) y del movimiento de Dawronoye, que actúan como paraguas de los partidos siríacos en Siria, Líbano, Irak y Turquía, esta organización no solo mantiene estrechos vínculos con la Unión Siríaca Europea y su Fundación Cultural, sino que además dispone de una larga trayectoria de reivindicaciones étnico-religiosas que se remonta a principios del siglo xx, tanto en Siria como en la región (Mulla, 2018).

Cuando las YPG/YPJ tomaron el control de los enclaves señalados del norte sirio, especialmente de Jazire, donde la comunidad siríaca-asiria mantenía una mayor presencia, el SUP que, de forma similar al PYD había mantenido una política de recelo hacia los rebeldes árabes, decidió a finales de 2013 establecer una alianza con el PYD para proteger el territorio y hacer frente a la entonces creciente amenaza yihadista.

A comienzos de 2013, bajo los auspicios del SUP, nace con el objetivo de defender la zona, el Consejo Militar Siríaco (CMS). En sus inicios, el CMS se mantuvo activo fundamentalmente en Hasakah y Jazire, mientras progresivamente extendía su presencia a otras zonas del noreste sirio y estrechaba su coordinación y vínculos con las YPG (Drott, 2013).

Dentro del paraguas cristiano, otras fuerzas combatientes de origen asirio progresivamente se alinearon con el YPG. Sirvan de ejemplo las Khabur Guard Forces que, con un número de efectivos que se aproxima a los 150 combatientes, habían alcanzado una estrecha coordinación con las fuerzas kurdas hacia finales de 2015 (Mulla, 2018). Paralelamente, a lo largo de 2014, se formó una alianza entre las YPG y las Fuerzas Sanadid, árabes pertenecientes a la tribu Shammar (Hubbard, 2015), que, en el norte, combatían igualmente al ISIS.

A pesar de estas alianzas, durante 2014 la pérdida de territorio en el norte sirio a favor del ISIS era cada vez más profunda hasta alcanzar un punto álgido en septiembre de este mismo año, cuando las fuerzas del autoproclamado ISIS arrebataron prácticamente en su totalidad el enclave de Kobane.



Mapa 3. Control del territorio sirio en septiembre de 2014. Fuente: Syrian Civil War: Everyday (NY Mapper)

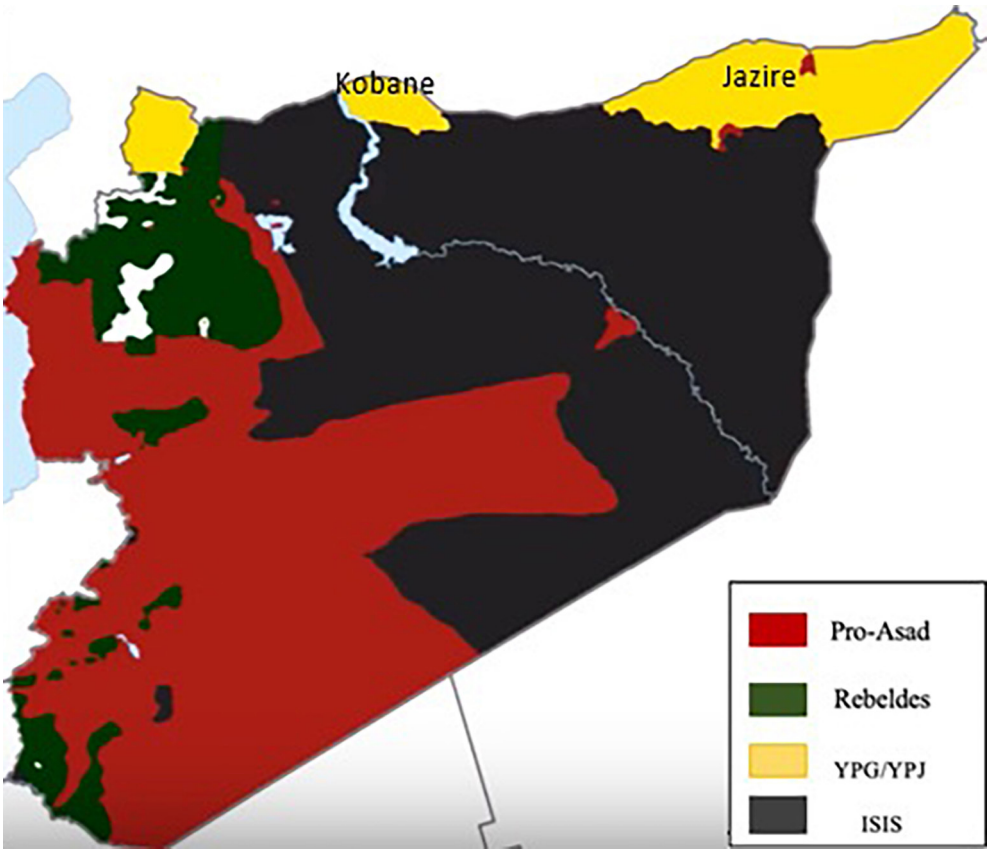
Esta pérdida progresiva de territorio que sumaba kilómetros a la geografía siria controlada por el ISIS activó en el corto plazo a los EE. UU. que iniciaron una campaña de ataques aéreos que coadyuvaba por vía indirecta a las fuerzas del PYD a desalojar al ISIS del norte de Siria y, concretamente, de la recién perdida Kobane. Este *modus operandi* se trasladaría igualmente a Hasakah y Raqqa, fraguando los inicios de lo que progresivamente sería una verdadera alianza entre la potencia y las fuerzas kurdas, sin olvidar en ningún momento el entramado de fuerzas cristiano-árabes referidas con anterioridad que se sumaban paulatinamente a esta cooperación (Barfi, 2016).

Expansión del territorio controlado por las fuerzas combatientes en el norte de Siria: fase de estabilización

El 23 de septiembre de 2014, EE. UU. ponía fin a los recurrentes titubeos de intervención en la guerra en Siria característicos de los años anteriores. En este momento, el entonces presidente Barack Obama anunciaba el inicio de una campaña de ataques aéreos contra objetivos del ISIS en Siria (Bassets, 2014). Esta campaña de ataques sería respaldada en octubre de este mismo año por la recién creada Operación Resolución Inhe-

rente (*Operation Inherent Resolve*), desarrollada por la Coalición Internacional contra el ISIS (*Combined Joint Task Force,* CJTF-OIR) que, liderada por los EE. UU., integraría apoyos de Reino Unido, Francia, España, Italia, Canadá, Alemania, Australia, Nueva Zelanda, Jordania, Irak, Catar y Arabia Saudí, entre otros (Departamento de Defensa de los EE. UU., 2014).

Los ataques aéreos de la Coalición comenzaron en enero de 2015, marcando un verdadero punto de inflexión en la campaña interna de las fuerzas kurdas, cristianas y árabes contra el ISIS, de forma que el mapa pronto había adquirido otra tonalidad. Así, entre los meses de enero y junio, las campañas aéreas desarrolladas por la Coalición permitieron la total recuperación del enclave de Kobane por las fuerzas del PYD en cooperación con las fuerzas árabo-cristianas referidas (mapa 4).



Mapa 4. Control del territorio sirio en abril de 2015. Fuente: Syrian Civil War: Everyday (NY Mapper)

En consecuencia, el ritmo en la recuperación y ampliación del territorio del norte sirio por las fuerzas combatientes kurdas y sus aliados cristianos y árabes, ha estado íntimamente ligado a la actuación de la Coalición contra el ISIS, en tanto que red principal de oposición al ISIS; cuya distribución mensual y anual de ataques explica en gran medida el avance terrestre de las fuerzas del PYD y sus aliados cristianos y árabes.

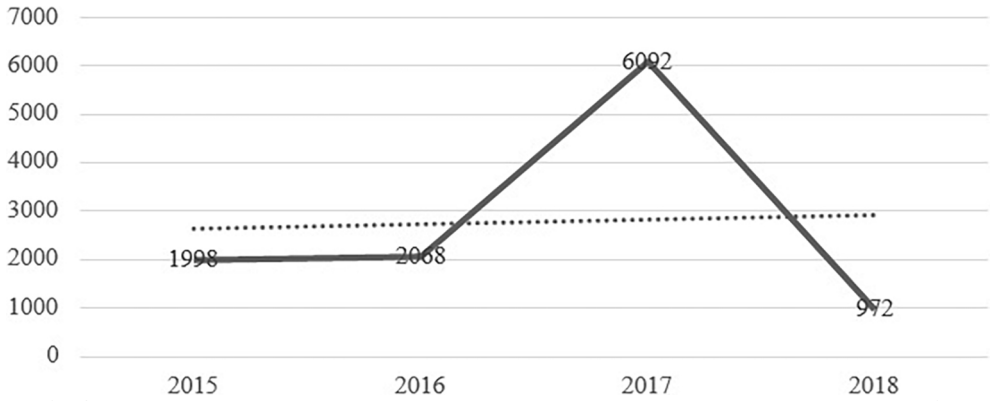
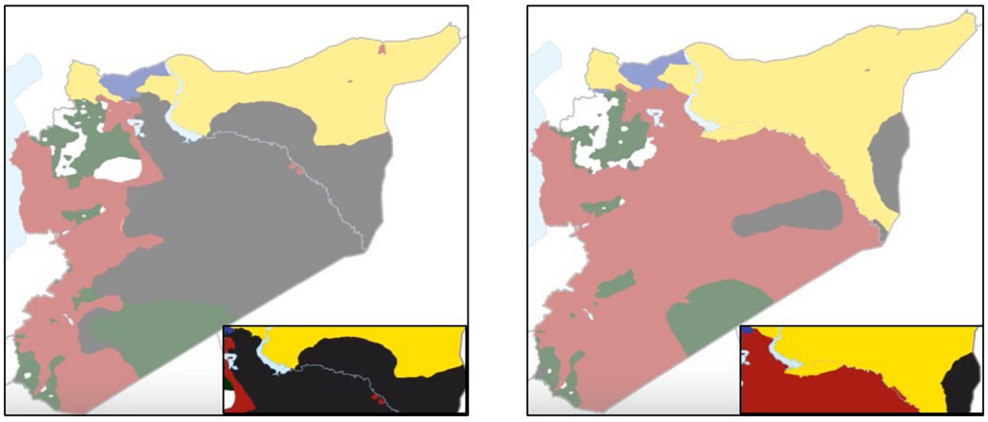


Gráfico 1. Evolución del número de ataques aéreos anuales sobre el territorio de la FDNS.
Fuente: elaboración propia a partir de Operation Inherent Resolve (2015); Operation Inherent

De hecho, si contrastamos el año 2017, punto de mayor número de ataques por la Coalición en la zona del norte y este sirios (FDNS), con la evolución del control terrestre de la zona por el PYD, alcanzaremos a vislumbrar el grado de imbricación de estas variables.



Resta por analizar la segunda red internacional de oposición al ISIS promovida en el norte y este sirios por los EE. UU.: las Fuerzas Democráticas Sirias (FDS). A mediados del mes de octubre de 2015, la creación de las Fuerzas Democráticas Sirias (FDS) fue anunciada en una rueda de prensa en Hasakah en la que esta nueva fuerza señalaba «(…) debido a la acelerada situación política y militar, y las sensibles fases por las que ha pasado nuestro país, debe establecerse una fuerza de unidad nacional (…) que integre a kurdos, árabes, asirios y todos aquellos que vivan en la geografía siria. Las Fuerzas Democráticas Sirias buscan lanzar un auto-gobierno sirio (…)» (IHS, 2015).

De acuerdo con este anuncio, las FDS, que formalmente comenzaban con un total de siete milicias (Barfi, 2016), progresivamente consiguieron multiplicar considerablemente

el número inicial de grupos integrantes, entre los que han mantenido, sin embargo, abierta preponderancia las fuerzas kurdas de las YPG/YPJ (Ignatius, 2016) (Ilustración 1).

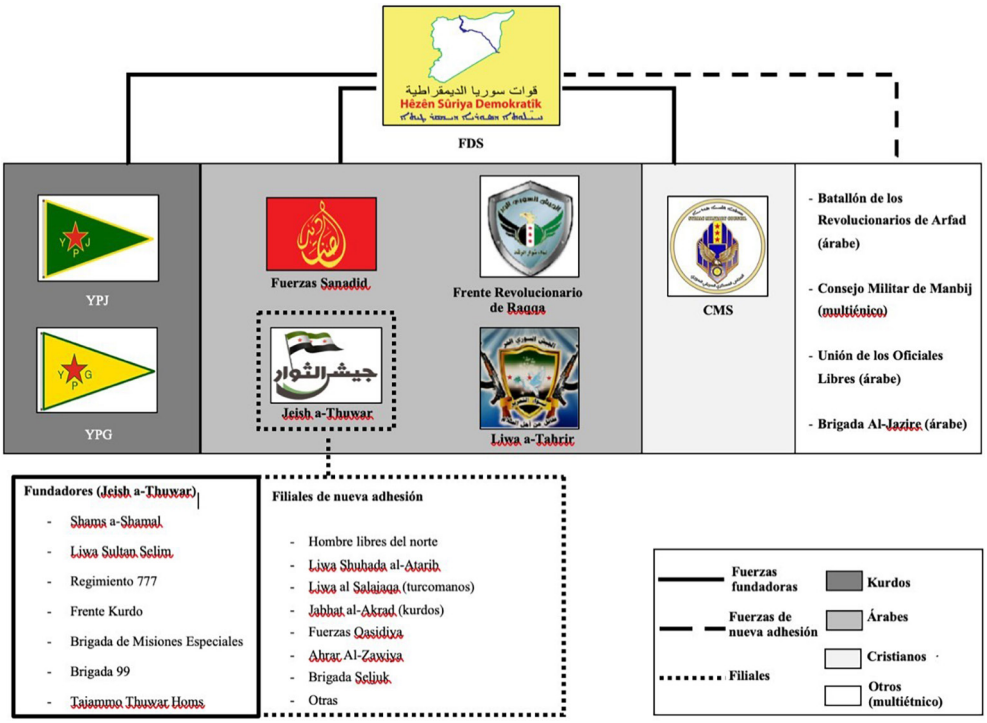


Ilustración 1. Grupos integrantes de las FDS. Fuente: elaboración propia a partir de Casagrande (2016); Masarat (2016); Agenfor

El apoyo estadounidense a la creación de esta fuerza debe ser calificado como determinante. Previamente, en septiembre de 2015, el general Lloyd Austin, ya anunció ante el Comité del Senado estadounidense empleado en la supervisión de las actuaciones de la Operación Resolución Inherente, que «en los últimos meses, los kurdos sirios se ha[bían] desempeñado excepcionalmente bien en el noreste de Siria. Ellos, junto con [sus aliados], ha[bían] recuperado unos 17.000 km2 del enemigo. Esto presenta una oportunidad significativa y un potencial punto de inflexión en la campaña contra el ISIL» (general Lloyd J. Austin, 2015). En efecto, ante los EE. UU. se planteaba una doble opción a la hora de adoptar una estrategia terrestre para enfrentar al ISIS, bien podían continuar construyendo un grupo armado a partir de las fraccionadas fuerzas rebeldes árabo-sunníes, o bien, instrumentalizar en la lucha contra el ISIS un grupo combatiente que había demostrado capacidad sobre el terreno para recuperar y controlar el norte sirio (Ignatius, 2016).

En consecuencia, a comienzos de octubre de 2015, la Administración Barack Obama decidía cancelar la ejecución de un programa diseñado para entrenar y armar a las fuerzas de la oposición árabes (Hubbard, 2015), adoptando una posición más proactiva

respecto a las fuerzas del norte sirio (tabla 2), dirigida, por un lado, al equipamiento y entrenamiento de estos grupos y, por otro, a presionar por la formación de unas fuerzas que uniesen bajo un mismo mando a los combatientes del norte, sin ligarse a una etnia exclusivamente.

Tabla 2. Apoyo de los EE. UU. a las FDS.

Dimensión del apoyo	Fecha de inicio	Variable de apoyo
Apoyo indirecto	Enero, 2015	
		Ataques aéreos de la Coalición Internacional contra el ISIS liderada por los EE.UU
		Apoyo político-diplomático
Apoyo directo	Octubre, 2015	
		Creación de las FDS
		Provisión de armamento y demás material logístico
		Envío de expertos y personal de apoyo
		Coordinación de los ataques aéreos con operaciones terrestres llevadas a cabo por las FDS

Fuente: elaboración propia a partir de Hubbard, 2015; Ignatius, 2016; Mulla, 2018.

CONCLUSIONES

El proceso de estabilización de la zona del norte y este sirios ha mantenido una dinámica propia desde el inicio del conflicto en el país. Habiendo adoptado toda una serie de formas de gobernanza más o menos complejas que resultaron en la Federación Democrática del Norte y Este de Siria y, más recientemente, en la Administración Autónoma Democrática del Norte y Este de Siria, el tercio del país que comprende la ribera norte del río Éufrates ha experimentado un proceso de estabilización ligado esencialmente a las redes internacionales urdidas en oposición al ISIS.

En la primera fase del conflicto, de carácter expansivo, dos factores se alzan claves para entender la evolución de este proceso de estabilización. Por un lado, la relación de

«tolerancia» del PYD y el régimen de Bashar al-Asad que, aunque tradicionalmente han mantenido una evidente rivalidad, han optado por evitar el enfrentamiento directo desde el inicio del conflicto, permitiendo a una parte el control efectivo de zonas demográficamente kurdas, y a otra, focalizar sus esfuerzos en la lucha contra la oposición árabe rebelde que se extendía por el resto del país.

Por otro lado, las YPG/YPJ anunciaron su activación al inicio del conflicto, permitiendo el desarrollo de una fuerza armada monolítica, con experiencia y fuertes lazos, al menos iniciales, con el PKK, bajo el control estratégico del PYD, aportando así una clara dimensión securitaria a los enclaves referidos. Esta fase se caracterizó así por el asentamiento de estas fuerzas en el norte sirio, extendiéndose exclusivamente por los enclaves característicamente kurdos.

La segunda fase, de carácter regresivo, estuvo dirigida por el enfrentamiento con el ISIS, que irrumpió con fuerza en el territorio del país, fagocitando tanto zonas bajo control rebelde o del régimen, como las zonas dirigidas por el PYD, cuya fuerza armada no pudo hacer frente al avance de este actor que terminó tomando por completo Kobane a finales de 2014. No obstante, otras fuerzas cristianas y árabes nacieron en el norte sirio a fin de enfrentar a este nuevo actor que, dado su fuerte potencial bélico y la incapacidad de hacerle frente por separado, favoreció la concertación de alianzas de facto entre fuerzas kurdas, árabes y cristianas, sentando un útil precedente para la futura creación de las FDS.

La entrada del ISIS en escena provocó la activación de toda una serie de redes internacionales de oposición al ISIS en una doble dirección: el inicio de los ataques aéreos de la Coalición y la creación de las Fuerzas Democráticas Sirias (FDS), cuya actuación conjunta, aérea y terrestre, determinaron el surgimiento de una última fase de ampliación y estabilización del territorio comprendido entre la frontera norte con Turquía, este con Irak y la ribera norte del río Éufrates, cristalizando así el proceso de estabilización característico de la zona.

FUENTES

Fuentes gráficas: mapas y datos relativos a los ataques aéreos de la Coalición contra el ISIS en el periodo 2015-2018

– OPERATION INHERENT RESOLVE. «Strikes Realeases 2015». 2015. Disponible en https://www.inherentresolve.mil/Media-Library/Strike-Releases/.

– OPERATION INHERENT RESOLVE. «Strikes Realeases 2016». 2016. Disponible en https://www.inherentresolve.mil/Media-Library/Strike-Releases/.

– OPERATION INHERENT RESOLVE. «Strikes Realeases 2017». 2017. Disponible en https://www.inherentresolve.mil/Media-Library/Strike-Releases/.

– OPERATION INHERENT RESOLVE. «Strikes Realeases 2018». 2018. Disponible en https://www.inherentresolve.mil/Media-Library/Strike-Releases/

– INFOGRAM. «Syrian civil war map. War Statistics». 2019. Disponible en: https://syriancivilwarmap.com/war-statistics/.

– «Syrian civil war: everyday». NYMAPPER. Disponible en: https://www.youtube.com/watch?v=BnM2bQJitjw.

Fuentes académicas y documentación oficial de Estados y organizaciones internacionales

– BARFI, B. «Ascent of the PYD and the SDF». *Research Notes*, 32. The Washington Institute for Near East Policy. 2016. Disponible en: https://bit.ly/2SjbldF Consulta de 20 de mayo de 2019.

– CASAGRANDE, G. «The road to Ar-Raqqah: background on the Syrian Democratic Forces». Washigton DC: Institute for the Study of War. 2016. Disponible en: https://bit.ly/2nBOvlQ. Consulta de 5 de mayo de 2019.

– DEPARTAMENTO DE DEFENSA DE LOS EE. UU. «Combined Joint Task Force. Operation Inherent Resolve. History. APO AE 09306». 2014. Disponible en https://bit.ly/2L9r0w6. Consulta de 16 de mayo de 2019.

– DROTT, K. «Christian Militia Politics in Qamishli». Beirut : Carnegie Middle East Center, 2013. Disponible en: https://carnegie-mec.org/diwan/53801?lang=en. Consulta de 17 de mayo de 2019.

– GENERAL LLOYD J. AUSTIN. «Statement of General Lloyd J. Austin III Commander U.S. Central Command before the Senate Armed Services Committee on Operation Inherent Resolve». 2015, 16 de septiembre. Disponible en https://bit.ly/2RwMQek. Consulta de 20 de abril de 2019.

– IHS. «SDF plays central role in Syrian civil war». *Jane's Intelligente Review*. Disponible en http://cort.as/-J1-v. Consulta de 5 de junio de 2019.

– INTERNATIONAL CRISIS GROUP (ICG). «Flight of Icarus? The PYD's

– Precarious Rise in Syria». *Middle East Report*, 151. Washington: 2014. Disponible en https://bit.ly/2fyWPyc. Consulta de 12 de abril de 2019.

– INTERNATIONAL CRISIS GROUP (ICG). «Turkey: The PKK and a Kurdish Settlement». *Middle East Report,* 219. Washington: 2012. Disponible en https://bit.ly/2X3pcvL. Consulta de 12 de abril de 2019.

– JORDÁN, J. «El Daesh». *Cuadernos de Estrategia, 173*. Instituto Español de Estudios Estratégicos. 2015, pp. 109-147. Disponible en http://www.ugr.es/~jjordan/Daesh-Estado-Islamico.pdf. Consulta de 15 de mayo de 2019.

– MASARAT. «Syrian Democratic Forces (SDF): From the Washington - Moscow agreement to Animosity with Turkey». *King Faisal Center for Research and Islamic Studie,* 25. 2016. Disponible en https://bit.ly/2LfXxkc. Consulta de 26 de mayo de 2019.

– MINORITY RIGHTS GROUP INTERNATIONAL. «Syria. Christians, Armenians and Assyrians». London: Minority Rights Group International, 2018. Disponible en https://bit.ly/2N8xDBr. Consulta de 17 de mayo de 2019.

– MULLA RASHID, B. «Military and Security Structures of the Autonomous Administration in Syria». Istambul: Omran for Strategic Studies, 2018. Disponible en https://bit.ly/2X0o5lH. Consulta de 5 de mayo de 2019.

– SARY, G. «Kurdish Self-governance in Syria: Survival and Ambition». Chatham House. The Royal Institute Of International Affairs, 2016. Disponible en https://bit.ly/2ICORTp. Consulta de 7 de mayo de 2019.

Fuentes periodísticas

– AGENFOR. «Tribal governance to win the peace». Agenfor, 15 de marzo de 2016. Disponible en https://www.agenformedia.com/publications/2016/03/tribal- governance-win-peace. Consulta de 20 de abril de 2019.

– AL-QUDS AL-ARABI. «لحل يركلا يطارقميدلا داحتلاا بزحلك رتشملا سيئرلا ملسم حل سدقلا قنيتوّ نيتيركسع نيتيدرك يف ايروس فوس يدؤيي لإ لاتتقإ يدرك - يدرك»: يبرعلا دوجو. *Al-Quds Al-Arabi*. 2 de enero de 2016. Disponible en https://bit.ly/2L3ozgp. Consulta de 2 de enero de 2019.

– ALLOT, J. «Kurds and Christians fight back against ISIS in Syria». *National Review*. 19 de noviembre de 2015. Disponible en https://bit.ly/31QRzMD. Consulta de 14 de mayo de 2019.

– BASSETS, M. «EE. UU. entra en la guerra civil de Siria». *El País*. 23 de septiembre de 2014. Disponible en https://bit.ly/2ldbyGR. Consulta de 15 de mayo de 2019.

– GOLD, D. «Meet the YPG, the Kurdish Militia that doesn't want help from anyone».

– HUBBARD, B. «New U.S.-Backed Alliance to Counter ISIS in Syria Falters». *The New York Times*. 2 de noviembre de 2015. Disponible en https://bit.ly/2FuC9UW. Consulta de 2 de noviembre de 2015.

– IGNATIUS, D. «The new coalition to destroy the Islamic State». The Washington Post. 22 de mayo de 2016. Disponible en https://wapo.st/2RByiu2. Consulta de 26 de mayo de 2019.

– VICE. 31 de octubre de 2012. Disponible en https://www.vice.com/en_us/article/yv5e75/meet-the-ypg. Consulta de 12 de abril de 2019.

LAS GUERRAS DE AYER, LOS CONFLICTOS DE HOY. CÓMO ATENDER A LA DIMENSIÓN HÍBRIDA DE LOS CONFLICTOS

JACOBO MORILLO LLOVO
Licenciado en Periodismo por la Universidad Pontificia de Salamanca. Máster en Comunicación de la Defensa y Conflictos Armados por la Universidad Complutense de Madrid

SUMMARY

La forma de hacer la guerra en la actualidad ha adoptado unas características adaptadas a la era de la información, donde el filtro de los datos y la labor de una inteligencia integral y poliédrica encuentra su justificación en el tipo de amenazas derivadas del mundo globalizado. El cerco que la tecnología ha puesto al mundo ha supuesto que la población sea partícipe en un contexto donde la explotación de la información tiene mayor resonancia que el modo clásico de hacer la guerra. La inteligencia es la máxima filtración de la información, hecho que exige tanto optimizar su uso como formar a quienes la utilizan a efectos decisorios para su empleo más adecuado.

Las guerras han forjado las vértebras de los Estados, es así que no se entiende el concepto de guerra sin una estructura sociopolítica previa capaz de formar una suerte de Ejército. Así, Clausewitz subrayaba que la guerra era una prolongación de la política[1].

La historia tiene muchas formas de reflejar su pasado; que se repita o que conserve una relativa linealidad depende de nuestra capacidad para leer los escenarios, actores y elementos que forman cada hecho. Las batallas han supuesto puntos de inflexión en la historia; analizar y entender los factores que han delineado esos momentos cruciales permite encontrar una explicación y dar una aplicación práctica a los acontecimientos que hoy copan nuestro día a día. El estudio de la evolución de la guerra permite identificar sus componentes, evaluar la importancia de avances tecnológicos empleados en cada momento, y concretar los patrones que han definido el resultado de las batallas. El pasado es el primer paso para entender el presente y determinar el futuro.

Las guerras han evolucionado a la par que las sociedades, han sido elementos clave en el devenir de culturas y civilizaciones, donde han dejado su huella a la hora de generar filias y fobias. En 1648 la aceptación del Estado-nación tras la Paz de Westfalia[2] supuso un momento decisivo en la formulación de la historia de la guerra. A raíz de esto surgió la *razón de Estado,* que definió los parámetros estatales y territoriales que exigirían en adelante la estandarización del ejército como ejemplo de legitimidad.

La era napoleónica conllevó la movilización hacia la guerra de masas. La nueva implicación de la población en la contienda encarnó una nueva lectura de las guerras. En esta época se unirían las consecuencias de la Revolución Industrial, el auge de los nacionalismo y la figura de Napoleón Bonaparte; las innovaciones en artillería y comunicaciones precipitarían que la táctica y la organización de los ejércitos diera un salto evolutivo.

Los ritmos en la evolución de la guerra estuvieron marcados por el avance tecnológico. Durante la segunda mitad del siglo XIX, Helmuth von Moltke potenció la capacidad de movilización de las tropas gracias a dos novedades de su tiempo, el ferrocarril y el telégrafo, que permitieron maximizar la proyección de fuerza germana en las guerras contra Francia y Austria, que posteriormente darían pie al nacimiento de Alemania**.**

Tanto las guerras napoleónicas como la Gran Guerra englobaban un mismo formato de guerra[3]. Mientras el emperador galo empleó la movilidad como clave táctica, la 1.ª Guerra Mundial estuvo marcada por las patentes tecnológicas, pronto enquistada en la guerra de posiciones. Mientras que el submarino representó una seria amenaza a la talasocracia británica, el avión mostró una nueva dimensión de guerra, a pesar de no llegar a contar con la resolución que sí tendría en batallas posteriores.

En esta contienda, la guerra se hace total. Si bien la dimensión naval ha tenido un componente capital en la cronología bélica, el espectro aéreo da sus primeros pasos

---

1 CLAUSEWITZ, Karl Von. *De la Guerra.*

2 Se firmó para acabar con la Guerra de los 30 años.

3 Según W. Lind, de 2.ª generación.

durante la 1.ª Guerra Mundial. Sin embargo, ambas dimensiones serían cruciales a partir de 1939 con una tecnología que esta vez sí mutaría la morfología de guerra.

En la 2.ª Guerra Mundial se percibió cómo la tecnología amplía los planos de la batalla y la capacidad de profundidad gracias a la maquinaria acorazada y mecanizada. Se quiebra la inmovilidad patente de la Gran Guerra, tanto por las fuerzas acorazadas como por la capacidad de la dimensión aérea, que llega a cargar con el flujo de la guerra. Todo ello retratado en la *Blitzkrieg*, *guerra relámpago*, empleada por la Alemania nazi en su invasión de Polonia, en la Batalla de Francia y en los albores de la Operación Barbarroja. Bajo el liderazgo de Heinz Guderian, la Wehrmacht se concentró en puntos concretos del frente, que rompen con facilidad y aprovechan la falta de tiempo de reacción del enemigo. Sin embargo, esta guerra de maniobra vio diluido su impacto con el tiempo, al mutar el frente en una guerra de posiciones, una suerte de contienda en la que la Alemania nazi no tenía posibilidad de victoria. Del mismo modo, el submarino encontró su némesis en el portaaviones, capaz de marcar el devenir de la guerra en 2 dimensiones tan patentes de la 2.ª Guerra Mundial como la aérea y la marina. Fue este tipo de transformación estratégica, a merced de la tecnología, el responsable de un cambio en la historia bélica.

Asimismo, pocos años más tarde, la aparición de la bomba atómica también marcaría un punto de inflexión a la hora de entender la psicología de la guerra: su capacidad destructiva, tan definitiva, dio conciencia de la necesidad de unos límites bélicos en el escenario de una contienda total.

Si se analiza la cronología bélica, las guerras mantienen ciertos elementos estructurales comunes en lo que concierne a la batalla. Desde las batallas napoleónicas hasta las de hoy en día existe un mando, una fuerza, una vanguardia, unos apoyos de fuego, unos apoyos de movimiento de obstáculos, todo ello para cubrir las funciones de combate propicias.

Durante el siglo pasado, las guerras estaban aparentemente monopolizada por los Estados[4]. Las alianzas y las enemistades estaban sometidos a los equilibrios de poder y la fuerza estaba en manos de naciones vertebradas capaces de neutralizar a órganos divergentes de calado no estatal. Tras el levantamiento del Muro de Acero y la consolidación del mundo bipolar, las guerras comenzarían a menguar de talla y a ganar en número. Las alianzas de naciones y actores no estatales con las dos grandes potencias supondría la

incubadora sobre la que se desarrollarían las guerras del siglo XXI. Las guerras coloniales, antes y después de las guerras mundiales, significaron lecciones históricas no bien atendidas. Sus formas y consecuencias las vemos hoy en un mundo globalizado que debe encarar el paradigma de guerra asimétrica, esta vez con las tecnologías de la información como un factor pivotante. La guerra, al igual que la historia, tiene sus dinamismos y latitudes, responsable de unos factores en perenne disposición al cambio. Son estos los que permiten el análisis evolutivo de las guerras, en todas sus formas y asociado a unos instrumentos concretos que dan pie a la elaboración de conclusiones.

[4] BALLESTEROS, Miguel Ángel. «Desplazamiento de los centros de poder». Aula de Liderazgo Público. ICADE, 2012.

LOS CONFLICTOS DE HOY. CÓMO ATENDER LA DIMENSIÓN HÍBRIDA DE LA GUERRA

Las guerras, como la historia las conoce, son un fenómeno de ayer; los conflictos armados son la patente bélica de nuestro tiempo. Estos han encontrado nuevos formatos y vías para proyectar su cosmovisión, donde el terrorismo yihadista se presenta como el primer exponente de esta amenaza[5].

Adherido a la evolución civil y tecnológica, los escenarios bélicos actuales presentan un orgánico componente social derivado de la globalización que hace de las masas actores directamente partícipes. Los grupos no estatales, en referencia a los grupo terroristas, han desarrollado una multifuncionalidad que abarca diversas esferas de influencia diseñadas para dañar y desestabilizar gobiernos a través de la sensibilidad de las sociedades. Estos grupos, representantes de la guerra asimétrica, aprovechan el poder de las redes de comunicación presentes en nuestra rutina para usar a las sociedades como intermediario de su mensaje. «Es precisamente por este tipo de manipulación social la necesidad de elaborar una cultura de conciencia cívica capaz de desglosar las variables de conflicto, saber encontrar sus vínculos de causa y efecto para con ello poder contrarrestar el objeto propagandístico y psicológico del terrorismo».

Hay que ser consciente de que su objetivo no es destruir, sino herir y atemorizar; ganar la batalla psicológica. El último ejemplo de ello ha sido el autoproclamado Estado Islámico (ISIS)[6]. Su despliegue propagandístico consiguió atraer a miles de combatientes de distintos países a la causa del Califato. Su acierto en dotar de un contexto global al conflicto demostró su capacidad de simbiosis con los elementos de la globalización, respaldado sobre el terreno por los resultados del metabolismo plástico de su táctica. ISIS alcanzó su influencia ecuménica gracias su arquitectura propagandística, impulsado por sus propias plataformas de información. Hasta junio de 2017 el grupo fundamentalista había emitido 2.880 videos, 32.140 piezas gráficas y 4.540 comunicados escritos; el ISIS ha llegado a crear hasta 46 agencias de información.

Los grupos no estatales son el mayor exponente de guerra asimétrica —aunque no los únicos—, un tipo de conflicto discontinuo de baja intensidad, que emplea el tiempo como baza estratégica**;** sus tácticas ya quedaron patentes durante las guerras coloniales, y que siguieron patentes en las victorias revolucionarias en Cuba y China.

Antaño, la distancia anulaba la fuerza y el espacio contrarrestaba al poder militar; hoy la preponderancia en la tecnología es capaz de sortear los elementos que antes eran elencos ineludibles en la táctica bélica. La globalización ha distorsionado los espacios y gracias a las capacidades de comunicación cada individuo acapara una influencia nunca antes tan determinante.

En épocas pretéritas las poblaciones eran objeto de la propaganda tanto interna como enemiga; hoy su papel se extiende a agentes informativos partícipes —no solo

---

[5] BARDAJÍ, Rafael L. «Las raíces del Estado Islámico». *Papeles Faes Internacional*, n.º 182. 27/11/2015.

[6] BALLESTEROS, Miguel Ángel. «La estrategia del Daesh a través de su revista Dabiq». IEEE. 13/9/2017.

receptores— de la propia red mediática. Los conflictos de este siglo, el terrorismo yihadista, se nutren de ello. Solo hay que atender al atentado de Barcelona del pasado agosto, cuando en las redes sociales circulaban vídeos, fotos e historias que más tarde, en muchos casos, se probaron falsas, pero que demostraron la implicación indirecta que puede llegar a tener la población en la meta terrorista. Y bajo este contexto ha surgido el concepto de *guerra hí*brida[7], dotada con peso teórico por el James N. Mattis al concepto *híbrido*[8].

Por su parte, los Estados han vertebrado sus arquitecturas de guerra a partir del potencial ilimitado de la máquinas. El binomio humano-máquina ha marcado el devenir y las edades de la guerra. En las últimas décadas, el peso de las inversiones se encuentra en la tecnología, una decisión que ha limitado en gran medida las bajas humanas —ejemplo de ello fue la invasión de Afganistán en 2001, que se saldó con 30 bajas estadounidenses por 10.000 de los talibán— pero que también ha supuesto un coste en defensa constante y elevado. Este tipo de despliegue deriva de la revolución de asuntos militares (RMA)[9], que pivota en torno a tres elementos tecnológicos: sensores, sistemas de comunicación y armamento.

Esta última versión de la guerra abarca un espacio integral. A tierra, mar y aire se han sumado las dimensiones de espacio y ciberespacio; esta última presume de ser el tablero infinito de guerra del presente siglo. Amén de la ventaja tecnológica, los Estados pretenden hacer resaltar su fuerza de forma contundente y rápida, por ello, los actores no estatales, hoy exponentes de la guerra asimétrica**,** maquinan con el tiempo como baza estratégica. Para ellos, mantenerse en la lucha supone una victoria; son conocedores de que la presión popular en esos Estados puede ser aliado en una guerra prolongada.

Un ejemplo de ello es Hezbollah, organismo paralelo al Estado libanés[10], cuyo brazo armado ha resistido la fuerza israelí durante décadas. Gracias a esa primera supervivencia, con el transcurso de los años, ha desarrollado un proyecto que hoy le permite gozar de un peso político y social clave, prueba latente de la evolución híbrida de los conflictos de hoy.

Los conflictos armados ya no ponderan únicamente sobre la bota castrense. A expensas de la globalización, el mundo civil comparte estratos con las guerras de hoy. Esto convierte a cada civilización en objeto de uso propagandístico y operativo; una constante de la que los actores no estatales —y algunos Estados también— ya han tomado

---

7 «la integración de medios convencionales y no-convencionales, medidas militares abiertas y encubiertas, paramilitares y civiles por parte de actores estatales y no-estatales para lograr sus objetivos». Definición de la OTAN de la *amenaza híbrida* expuesta en la Declaración final de la Cumbre de Varsovia (9 de julio de 2016), para. 72.

8 MATTIS, J. y HOFFMAN, F. «Future warfare: The rise of hybrid warfare». *U.S. Naval Institute Proceedings*, 132-11. 2005, pp. 30-32.

9 La idea ha combinado las nuevas tecnologías de la información con el mando y control de las unidades militares en operaciones, un hecho que ha permutado el despliegue operativo. http://home.sogang.ac.kr/sites/jaechun/courses/Lists/b7/Attachments/78/11.%20G.%20Chapman%20-%20An%20Introduction%20to%20the%20Revolution%20in%20Military%20Affairs.pdf.

10 MARTINEZ-VALERA, Gabriel. «Una mirada al Líbano tras la contienda de 2006». Grupo de Estudios de Seguridad Internacional. 5/3/2014.

conciencia, un hecho que les ha granjeado la ventaja geopolítica en la morfología actual de los conflictos. Conflictos que no son monopolio de los Estados; grupos insurgentes son capaces de hacer la guerra gracias al dinamismo y a la movilización global. «La naturaleza del conflicto híbrido impulsa una nomenclatura bélica más social, dado que es el vehículo que hace global esta morfología bélica**»**. Por tanto, dada la inexorable implicación de las sociedades en este formato híbrido, se debe potenciar la conciencia social como una de las respuestas al efecto popular que el terrorismo busca en cada uno de sus actos. «Por tanto, si las masas son conscientes para no entrar en el proceso mediático de los actores hibridos, su impacto y efecto se yugulará**»**.

Nos dirigimos a un mundo de conflictos intermitentes e inconclusos, capaces de desgastar al mundo y a sus sociedades por su disposición estratégica del tiempo. El perfil de estos conflictos supone una estrategia de baja intensidad pero de alta frecuencia. Amén de estas características el orbe militar debe reformularse, seguir mejorando su tecnología pero sin desatender el primer y último activo de la guerra que es el factor humano. El coste y la exigencia de este tipo de guerra va a exigir menos grupo humano pero más tecnificado, mutable y con capacidad mixta para responder a la versatilidad del *modus operandi*[11] bélico de los órganos estatales y no estatales.

Es así que las características de los conflictos del siglo XXI, en su objetivo de minimizar la actividad beligerante del impacto social, convierten la infraestructura de inteligencia estatal en factor vertebral en el escenario de nuevas formas de conseguir la posición de fuerza, que antaño se alcanzaba a través del despliegue y actividad militar. Hoy estos conflictos forman parte de un marco más opaco y multidimensional, y que se encuentra a merced de alternativas específicas en cada plano estratégico relevante para cualquier nación, como son el económico, político, social-cultural o financiero. Todo ello en paralelo al despliegue de una pedagogía social que dé a la población la capacidad de entender y contrarrestar por sí misma efectos de la maquinaria psicológica de este tipo de conflictos, dado el poder exponencial como emisores informativos que cada individuo posee hoy.

BIBLIOGRAFÍA

– AZNAR FERNÁNDEZ-MONTESINOS, Federico. «Las generaciones de guerras. Guerras de primera generación (I)». IEEE. 25/11/2015.

– AZNAR FERNÁNDEZ-MONTESINOS, Federico. «Las generaciones de guerras. Guerras de segunda y tercera generación (II)». IEEE. 30/12/2015.

– AZNAR FERNÁNDEZ-MONTESINOS, Federico. «Repensando la guerra asimétrica». IEEE. 14/3/2018.

[11] «The Global SOF Network: Posturing Special Operations Forces to Ensure Global Security in the 21st Century». Journal of Strategic Security, Vol. 7. 2014. https://scholarcommons.usf.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1380&context=jss.

– BARDAJÍ, Rafael L. «Las raíces del Estado Islámico». *Papeles Faes Internacional,* n.º 182. 27/11/2015.

– CLAUSEWITZ, Karl Von. *De la guerra*. Ediciones Ejército.

– COLOM PIELLA, Guillem. «Guerras híbridas. Cuando el contexto lo es todo». *Revista Ejército* n.º 927. Junio 2018.

– COLOM PIELLA, Guillem. «La amenaza híbrida: mitos, leyendas y realidades». IEEE. 22/3/2019.

– GARCÍA GUINDO, Miguel; GONZÁLEZ, Valera. «La guerra híbrida: nociones preliminares y su repercusión en el planteamiento de los países y organizaciones occidentales». IEEE. 2/2015.

– HOFFMAN.«Future Warfare: The rise of Hybrid Wars». *Revista Proceeding*. 2005.

– MARTÍNEZ-VALERA, Gabriel.«Una mirada al Líbano tras la contienda de 2006». Grupo de Estudios de Seguridad Internacional. 5/3/2014.

– Multinational Capabillity Development Campaign [MCDC]. *Understanding Hybrid Warfare*. Enero 2017.

– Multinational Capabillity Development Campaign [MCDC]. *Countering Hybrid Warfare*. Marzo 2019.

– SÁNCHEZ HERRÁEZ, Pedro. «Comprender la guerra híbrida…¿el retorno a los clásicos?». IEEE. 21/6/2016.

– Artículo publicado en CISDE:

– https://observatorio.cisde.es/actualidad/las-guerras-de-ayer-la-importancia-de-entender-los-ciclos-de-la-historia-belica/

– https://observatorio.cisde.es/actualidad/los-conflictos-belicos-de-hoy-como-atender-a-la-dimension-hibrida-de-la-guerra/

LIDERAZGO HÍBRIDO: RESPUESTAS ADAPTADAS A UNA CAMBIANTE REALIDAD SOCIAL

CARLOS GARCÍA-GUIU LÓPEZ
Teniente coronel de Ingenieros director del Departamento de Ciencias Jurídicas y Sociales y profesor de Liderazgo. Licenciado en Piscología por la UNED y doctor en Psicología por la Universidad de Granada

Resumen

En un mundo complejo y asimétrico, donde los riesgos y amenazas exigen a los Estados plantearse estrategias híbridas en los entornos de seguridad y defensa, se requieren líderes con capacidad de adaptación y agilidad que sean capaces de enfrentarse a una realidad cambiante y paradójica.

El objeto de la presente comunicación es efectuar una aproximación psicosocial al concepto de liderazgo híbrido. Es un tipo de liderazgo que requiere que los responsables de las organizaciones, amplíen su percepción y capacidad de respuesta frente a las tensiones que se desarrollan en los grupos sociales y requiere la comprensión del mundo actual.

El liderazgo híbrido tiene su principal fundamento en el liderazgo paradójico, el liderazgo tridimensional y situacional. También se puede considerar como complementario al liderazgo de tipo integrador y cultural. Entre las estrategias que se plantean para desarrollar un liderazgo híbrido destaca saber desarrollar una capacidad para reconocer y valorar las paradojas, adaptarse y reaccionar de manera ágil a las demandas de la situación. También se requiere establecer y comunicar una visión común entre los componentes de los equipos y favorecer el desarrollo de una identidad, cultura y clima en las organizaciones que permitan afrontar los cometidos para los que están creadas.

Palabras clave: liderazgo híbrido, liderazgo paradójico, adaptación, cambio, conflicto.

LIDERAZGO HÍBRIDO: RESPUESTAS ADAPTADAS A UNA CAMBIANTE REALIDAD SOCIAL

Introducción

Capacidad de adaptación y agilidad son dos de los requerimientos que la sociedad actual exige a los responsables de las Fuerzas Armadas donde el espectro de las operaciones y los conflictos se fundamenta actualmente en conceptos tan complejos como amenaza hibrida[1], zona gris[2] o entornos VUCA[3].

Ciertamente, el empleo del concepto «híbrido» genera cierta confusión, y en ocasiones se ha realizado un desmesurado uso en los calificativos para referirse a la naturaleza de los adversarios, amenazas, estrategias, retos, tipo de guerra o modos de combatir. En dicha línea de argumentación el concepto derivado «lo híbrido» (MADOC, 2018) plantea de una manera doctrinal sus implicaciones para las fuerzas terrestres y su relación con el espectro de los conflictos y sobre estrategias empleadas por el adversario estatal o no y los diferentes ámbitos del conflicto.

No es posible entender las relaciones humanas y los conflictos sin comprender la dimensión social y limitar su estudio únicamente a intereses geográficos, económicos, religiosos, militares o de poder. Sin embargo, la influencia del término híbrido aplicado al plano psicosocial es un término apenas explorado y escasamente definido en la literatura científica.

Al tratar los conflictos híbridos Baqués (2015) apuesta por potenciar el factor humano en las fuerzas armadas occidentales, no solo a través del equipo y la tecnología, sino que se requiere profundizar en su formación en humanidades y en ciencias sociales, así como mejorar la capacidad de tomar decisiones rápidas en condiciones de presión. Se vislumbra que las demandas y retos en el ámbito del liderazgo también requieren profesionales que se adapten al entorno, ágiles y capaces de dar respuestas ante la complejidad del mundo entretejido por organizaciones e instituciones civiles y militares, de marcado carácter internacional forjado con alianzas, donde se materializan complejas relaciones psicosociales frecuentemente volátiles y en ocasiones ambiguas.

El objetivo del presente documento es efectuar una aproximación teórica desde el punto de vista psicosocial al concepto de liderazgo en su faceta de *lo híbrido*. Es un tipo de liderazgo que surge como una respuesta y adaptación, en su faceta humanística, de los responsables de las organizaciones, ampliando su percepción, concepción, respuesta y conducta ante los requerimientos del mundo actual.

En el presente trabajo se expondrá una propuesta del concepto de *liderazgo híbrido* describiendo los fundamentos y proximidad con el liderazgo paradójico, liderazgo tridi-

---

1 COLOM, G. «La amenaza hibrida: mitos, leyendas y realidades». Documento de opinión IEEE. 2019, pp. 1-14.

2 VILLANUEVA, C. D. «¿Es la "zona gris" el término de moda?». Publicación del GESI. Grupo de Estudios en Seguridad Internacional.

3 El concepto VUCA (*Volatility, Uncertainty, Complexity, Ambiguity*) fue desarrollado en la Escuela de Guerra del Ejército de Estados Unidos en los años 90. Entre los conceptos relacionados con dicho contexto de las operaciones futuras, el Ejército de Tierra español plantea un contexto global, el entorno operativo terrestre futuro 2035 (Mando de Adiestramiento y Doctrina, 2018).

mensional, situacional, integrador y cultural. Finalmente, se plantearán posibles líneas de acción para favorecer el desarrollo de este modelo de liderazgo que requieren las operaciones y los conflictos actuales y futuros.

Un concepto de liderazgo híbrido

Se entiende por híbrido[4], aplicado a lo inorgánico, a un producto de elementos de diferente naturaleza. El concepto de liderazgo híbrido lo encontramos en el liderazgo paradójico[5] y podemos observar antecedentes relacionados con el liderazgo tridimensional y situacional. Nos puede ayudar a configurar su concepto el modelo de liderazgo integrador y cultural como una forma fundamentada en la búsqueda de la comprensión sociocultural y política de los acontecimientos.

Liderazgo paradójico

El origen del liderazgo paradójico surge en las organizaciones como una respuesta al creciente entorno dinámico, competitivo y complejo en que es necesario afrontar sus contradictorias tensiones y demandas. Fundamentadas en las teorías de la complejidad en las organizaciones (Denison, 1995) los autores Zhang *et al*. (2015) desarrollan el constructo «conducta paradójica del líder» para explicar la tensión y competencia entre las respuestas orientadas tanto hacia las relaciones y toma de decisiones y la búsqueda de equilibrio entre aspectos personales y estructurales. Las cinco dimensiones que se plantean para definir dichas paradojas son: (1) combinar el egocentrismo con una actitud centrada en los demás; (2) mantener tanto la distancia como la cercanía; (3) tratar a los subordinados de manera uniforme frente a la individualización; (4) hacer cumplir los requisitos de trabajo, mientras que permite la flexibilidad; y (5) mantener la centralización en la toma de decisiones, frente a la autonomía. En el contexto militar Kark *et al*. (2016) plantea el liderazgo paradójico militar o híbrido situado por los vectores del liderazgo jerárquico o compartido, la creatividad y flexibilidad versus la conformidad y disciplina, la complejidad y el caos frente a la simplicidad y linealidad, el hegemónico o prototípico liderazgo versus un liderazgo de múltiples identidades, el distante frente a un próximo liderazgo.

Por ello, dichos autores resaltan su importancia para la efectividad en contextos organizacionales complejos e híbridos para atender efectivamente las expectativas competitivas y tensiones paradójicas que se dan frecuentemente en la vida real.

Liderazgo trifactorial

Un primer antecedente de este modelo los podemos encontrar en los estilos de liderazgo tridimensional de Yukl (2006) donde los factores de conducta adaptable de los

---

[4] Diccionario de la Real Academia Española (RAE) de la Lengua: adjetivo. Dicho de una cosa: que es producto de elementos de distinta naturaleza.

[5] KARK, R., KARAZI-PRESLER, T., TUBI, S. «Paradox and challenges in military leadership». *Monographs in Leadership and Management*, 8. 2016, pp. 159-187.

líderes se determinan por su manera de orientarse a la tarea, hacia las personas y hacia la innovación o cambio. Ciertamente las organizaciones, al estar en entornos de cambio continuo, necesitan líderes capaces de establecer modelos de liderazgo y conductas que favorezcan la efectividad y la satisfacción de los subordinados (Barrasa, 2003). Los modelos basados en los enfoques bifactoriales de conductas basados en orientación hacia las personas o hacia las tareas se completan con un tercer factor orientado a la modificación de los otros dos factores hacia la innovación, el cambio y en consecuencia a la adaptación y propuesto pro Yukl (2003).

El modelo trifactorial de Yukl (2003) se basa en que el propio líder favorece el cambio y hace planteamientos de innovación con entusiasmo y convicción, asume riesgos, favorece un pensamiento creativo y está en contacto con los cambios del entorno, analizando información sobre eventos, tendencias, amenazas y oportunidades para ser aprovechadas.

Liderazgo situacional

También está ampliamente difundido y es de aplicación en las organizaciones de seguridad y defensa el modelo situacional de Hersey y Blanchard. Este popular planteamiento de dirección y liderazgo mantiene con los años su utilidad al ser un modelo simple y muy intuitivo que permite a los líderes actuar de una manera más directiva o participativa, con una orientación hacia las personas o la tarea adaptando su posición a la situación planteada por las características del subordinado. En función de la madurez técnica, relacionado con su habilidad y experiencia profesional, y la madurez psicológica, el grado de motivación e interés, se deben adoptar los diferentes estilos de liderazgo. Dichos estilos son *directivo*, basado en ordenar y establecer criterios, *persuadir,* basado en el convencimiento y clarificar planteamientos, *participar*, facilitar la colaboración y consideración en la organización y toma de decisiones, o *delegar*, basado en permitir que asuma mayores responsabilidades al subordinado y poder, controlando su evolución.

Es un modelo que exige al líder conocer y evaluar a sus subordinados y sus equipos para poder diagnosticar el estilo más adecuado que debe emplear. Dicho estilo puede variar con el paso del tiempo, es necesario que sea flexible y adaptable para permitir un mejor desarrollo de las personas y los equipos.

Liderazgo integrador y cultural

También al plantear el liderazgo híbrido de manera complementaria al liderazgo paradójico, situacional o adaptativo es conveniente considerar su faceta relacionada con el aspecto integrador y cultural. Una aproximación del líder de carácter sociocultural se considera que es necesario para ser desarrollada por todos aquellos que participan en la resolución de conflictos —incluso a nivel tropa— para actuar de acuerdo con las exigencias de unas guerras que cada vez más, requieren una gran comprensión del entorno socio-político en el que se desarrollan (Baqués, 2015).

El liderazgo integrador fundamenta su potencia tanto en aprovechar la fuerza que ofrece sumar la participación de todos los componentes de los equipos como en bene-

ficiarse de las ventajas que aportan las diferencias derivadas de la diversidad humana. La diversidad y la inclusión permiten reconocer e incorporar a los equipos determinadas ventajas que pueden reportar aspectos diferenciales de las personas, permitiendo un enriquecimiento cultural y la existencia de recursos en los equipos que favorecen la adaptación e innovación.

Tanto los aspectos relacionados con el sexo, raza, etnia, religión o personalidad[6] son considerados por el líder como una oportunidad para generar una diversidad complementaria e impulsora de equipos polivalentes y multidisciplinares con capacidad de adaptación al cambio y sin el lastre de mantener un pensamiento único y los sesgos del pensamiento grupal[7]. En los equipos, es necesario aprender y tener habilidades para adaptarse y liderar a personas de diferentes características y tener capacidad para fomentar la cohesión entre los participantes, vivir en el respeto mutuo y compañerismo y mantener una orientación común hacia las metas compartidas.

El ejercicio del liderazgo híbrido

Es necesario asumir que la complejidad y las situaciones paradójicas son inherentes a la dinámica de las relaciones sociales que forman parte de un mundo complejo y ambiguo. Dichas circunstancias exigen que los líderes tengan capacidad para discernir y entender las diferentes características de las personas, los equipos y las situaciones. Dicha percepción es el primer paso para conocer aspectos relacionados con la motivación de las personas, las dinámicas de las relaciones humanas y cómo se origina la propia identidad, cultura y clima de las organizaciones.

Los líderes, tras percibir y conocer la realidad, deben mantener una estrategia adecuada para hacer frente a las tensiones y paradojas a las que debe enfrentarse, planteando soluciones y poniendo en práctica las respuestas necesarias. La necesidad de saber trabajar entre las tensiones nos orienta hacia la necesidad de que pensar y actuar paradójicamente también puede ser aprendido y puesto en práctica (Lewis, 2014). Entre las estrategias que se plantean a desarrollar para afrontar el liderazgo híbrido podemos destacar la necesidad de:

- Reconocer y valorar la existencia de paradojas en el liderazgo basadas en la manera de afrontar la relación con los subordinados.
- Favorecer tanto la estructuración del trabajo y una modulación de la participación y la puesta en común de información y respuestas para favorecer la toma de decisiones.
- Mantener una visión común y compartida por todos los componentes, considerando las diferentes características de los diferentes integrantes de los equipos.

---

[6] https://www.insights.com/resources/a-case-for-leadership-diversity/.

[7] El pensamiento único fue descrito originalmente por el filósofo Shopenhauer (1819) y se fundamenta por ser un sistema cerrado, autosostenido y sin apertura a los otros pensamientos. El pensamiento grupal es un término acuñado por el psicólogo Janis (1972) y se refiere a la situación en que los componentes a pesar de mantener una opinión contraria no plantean sus dudas o consejos provocando errores y decisiones desacertadas.

- Asumir que para favorecer la adaptación hay que innovar, es necesario invertir con personas, tiempo y dinero así como asumir ciertos riesgos.
- Favorecer el conocimiento del entorno exterior y las tendencias, tanto tecnológicas como sociales, que puedan afectar a los procedimientos y funcionamiento de los grupos.
- Acostumbrarse a trabajar en situaciones de tensión y ambigüedad.
- Favorecer la adaptación y el cambio basado en la evolución, las personas y los grupos sociales, tanto debido a factores intrínsecos como externos.
- Favorecer la creación de la identidad, cultura y clima de los equipos alineada con la establecida en las propias organizaciones.

Conclusiones

Un mundo complejo, asimétrico, donde se desarrollan amenazas y estrategias híbridas requiere a líderes con capacidad de adaptación y agilidad y en ocasiones afrontar la existencia de las paradojas de la realidad reinante.

El liderazgo híbrido tiene un fundamento en el liderazgo paradójico pero hunde sus raíces en el liderazgo tridimensional y situacional y se complementa con un liderazgo de tipo integrador y cultural.

Los líderes, para ser efectivos, tienen que saber reconocer y valorar la existencia de paradojas, adaptarse y reaccionar de manera ágil a las demandas de la situación. Es necesario establecer una visión común entre los componentes de los equipos y comunicarlo a todos los componentes de los equipos. La adaptación y el cambio es un fenómeno natural y continuo, tanto en las personas como en los grupos sociales, debiéndose forjar continuamente una identidad, cultura y clima en las organizaciones que sea favorable y permita mantener unos objetivos comunes para afrontar coordinadamente los cometidos para los que están creadas.

Bibliografía

- BAQUÉS, J. «Las guerras hibridas: Un balance provisional». Documento de trabajo 01/2015. IEEE, 2015, pp. 1-20. http://www.ieee.es/Galerias/fichero/docs_trabajo/2015/DIEEET01-2015_GuerrasHibridas_JosepBaques.pdf.

- BARRASA, A. *Hierarchical taxonomy of leadership behavior: Antecedents, structure, and influence in work groups effectiveness. Research Paper*. Doctorado Interuniversitario en Psicología de las Organizaciones y del Trabajo. 2003.

- COLOM, G. «La amenaza hibrida: mitos, leyendas y realidades». Documento de opinión. IEEE, 2019, pp. 1-14.

- DENISON, D. R., HOOIJBERG, R., y QUINN, R. E. «Paradox and performance: toward a theory of behavioral complexity in managerial leadership». *Organization Science*, 6. 1995, pp. 524-540.

– KARK, R., KARAZI-PRESLER, T., TUBI, S. «Paradox and challenges in military leadership». *Monographs in Leadership and Management*, 8. 2016, pp. 159-187.

– VILLANUEVA, C. D. «¿Es la "zona gris" el término de moda?». Publicación del GESI. Grupo de Estudios en Seguridad Internacional.

– YUKL, G. *Leadership in organizations*. Englewoods Cliffs: Prentice Hall, 2006.

– YUKL, G. «Tridimensional leadership theory: A roadmap for flexible, adaptive leaders». En BURKE, R. J. & COOPER, C. (eds.). *Leading in turbulent times*. London: Blackwell, pp. 75-92, 2003. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.573.6214&rep=rep1&type=pdf.

– ZHANG, Y., WALDMAN, D. A., HAN, Y. H., y LI, X. «Paradoxical Leader Behaviors in peopel managenment: antecedents y consequences». *Academy Management, 58*. 2015, pp. 538-566.

EL *DEEPFAKE* COMO AMENAZA COMUNICATIVA. DIAGNÓSTICO, TÉCNICA Y PREVENCIÓN

PABLO REY GARCÍA
Doctor en Comunicación. Profesor encargado de Cátedra en la Facultad de Comunicación de la Universidad Pontificia de Salamanca. Máster en Paz, Seguridad y Defensa por el Instituto Universitario «Gutiérrez Mellado»-UNED. Diplomado en Estudios Avanzados en Historia Contemporánea por la Universidad de Salamanca

NADIA MCGOWAN JORGE
Doctora en Comunicación Audiovisual y graduada en Historia del Arte

Resumen

En esta comunicación se presenta la problemática del *deepfake*, partiendo de la descripción del fenómeno, de una historia de su uso, los riesgos para la comunicación que presentan, la tecnología que permite fabricarlos, y partiendo de esto último, los recursos para reconocer este tipo de falsedades.

Palabras clave

Deepfake, vídeos falsos, *deeplearning*, redes generativas.

INTRODUCCIÓN

En el año 2016 el mundo del cine asistió a un prodigio: la cara juvenil de una actriz ya fallecida, Carrie Fisher, aparecía sobre el cuerpo de otra actriz, Ingvild Deila. Todo ello con apariencia normal (Rogue One, 2016). Los espectadores, prevenidos, aceptaron el juego y entendieron la circunstancia. El milagro se consiguió mediante la técnica de redes generativas antagónicas (GAN, por su acrónimo en inglés), un sistema de aprendizaje no supervisado, en el que dos sistemas de inteligencia artificial, el generativo y el discriminatorio, compiten para engañar o discriminar imágenes.

Los trabajos pioneros en este campo fueron llevados a cabo por Li, Gauci y Gross (2013), aunque su aplicación final, así como el diseño del sistema de redes generativas antagónicas se debe al equipo dirigido por Ian Goodfellow (2014). En la actualidad se ha conseguido un modelo de perfección asombrosa, basado en la retroalimentación entre

los dos sistemas paralelos (el *deeplearning*), lo que ha llevado no solo a la aplicación a la fotografía estática, sino al uso en imagen dinámica, esto es, en vídeo.

El riesgo es evidente: la dificultad de realizar un engaño en video era, hasta este momento, mucho mayor que en fotografía. La sociedad había asumido el hecho de que la fotografía puede mentir. Hay teóricos que niegan incluso la veracidad documental de la fotografía: son interesantísimos los trabajos en este sentido de Fontcuberta, que ha acuñado el término de «postfotografía» (1997, 2010, solo por citar dos representativos). Pero esta cautela no se ha tenido hasta el momento con el vídeo. Una fotografía necesita ahora mismo una serie de requisitos para ser tomada en serio como prueba fáctica (fundamentalmente, poseer el negativo digital, el RAW). De otro modo, su veracidad solo se sostiene en la credibilidad de la fuente. Sin embargo, el vídeo, por la dificultad intrínseca de ser alterado, se consideraba generalmente veraz… hasta ahora.

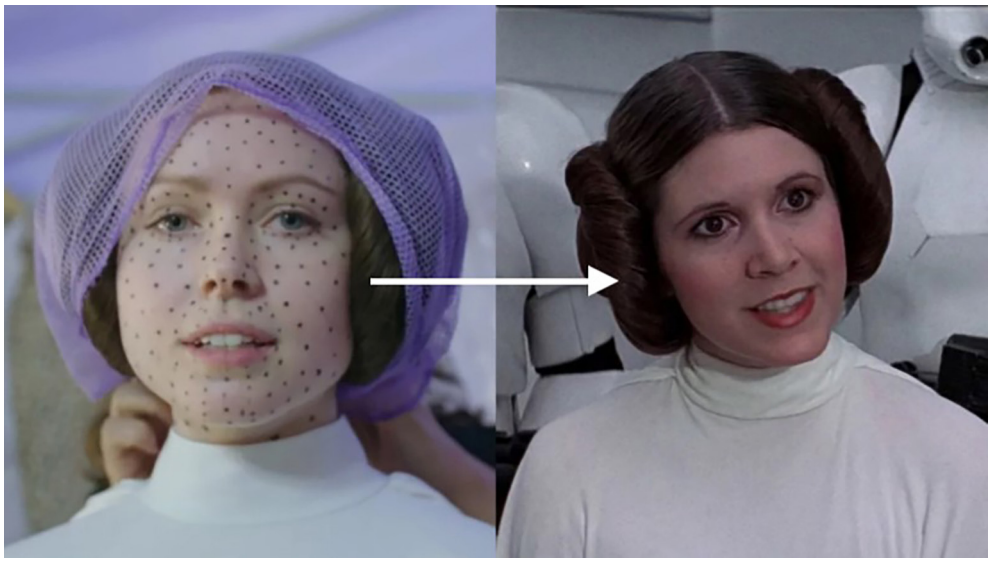


Figura 1: mapeado facial de Ingvild Deila (Oberoi, 2018)

Cuando Carrie Fisher aparece en la película de 2016, los espectadores saben de su muerte, no se sienten engañados, y tan solo se transportan por la verosimilitud magnífica conseguida por el CGI, las imágenes generadas por ordenador. Pero ¿y si este mismo procedimiento se aplicara a las informaciones, falseándolas? Ya ocurre. Se llaman *deepfakes*.

BREVE HISTORIA DEL *DEEPFAKE*

El nombre de *deepfake* pertenecía a un usuario de Reddit, un agregador de medios que por sus características se ha convertido en una red social a casi todos los efectos. Este usuario, el primero que utilizando la tecnología de las redes generativas antagónicas

creó un vídeo en el que sustituyó las caras de los protagonistas, con un resultado que se dio en llamar *faceswapping*. Con ello se generaba la duda de si el vídeo era realmente de ese famoso. Teniendo en cuenta que eran vídeos pornográficos, la repercusión no fue poca. La primera, expulsar a *deepfake* de Reddit. Desde diciembre de 2017 circulan por la red falsos vídeos pornográficos de Emma Watson, Scarlett Johansson, Taylor Swift y tantas otras actrices.

Tras la popularización del sistema, llegó una oleada de Nicolas Cage, actuando en diversas y muy variadas películas, ya no pornográficas, en las que su cara sustituía a los reales actores. El engaño era posible, pero no probable. Lo mismo ocurrió con los vídeos de carácter político, en los que la cara de Hitler aparecía sustituyendo a la del presidente Mauricio Macri (Zerocool22, 2018), o la del presidente Donald Trump sobre la de la presidenta Angela Merkel (Cage, 2018). Sin embargo, la maestría del vídeo del presidente Obama advirtiendo sobre los peligros de los *deepfakes* (BBC, 2017), creado por un equipo de la Universidad de Washington (Suwajanakorn, 2017), dan muestra de la capacidad tecnológica: se puede lograr que Obama diga de manera completamente verosímil, cualquier cosa. Cualquiera. Lo cual ha causado ya profunda preocupación entre los propios creadores de la tecnología (Pham, 2018). Señalamos estos ejemplos porque son líderes de opinión, prescriptores, lo que puede dar idea del engaño.

TECNOLOGÍA DE CREACIÓN

Existen múltiples métodos de creación de *deepfakes*. La primera instancia fue el programa Face2Face (Thies *et al.*, 2016) que analizaba las expresiones faciales de una imagen y las superponía sobre una segunda. Sin alterar el rostro, permitiría insertar palabras o gestos sobre una segunda persona. Un mayor avance es el desarrollo del programa FSGAN, *Subject Agnostic Face Swapping and Reenactmenet* (Nirkin *et al.*, 2019) donde no es necesario siquiera entrenar a la AI para intercambiar rostros. Como parte del mundo académico, su uso y acceso no están popularizados. Sin embargo, en el 2019 se lanzó una aplicación para teléfonos móviles llamada Zao en la que los usuarios pueden subir imágenes propias para superponerlas sobre rostros de gente famosa.

A su vez, ha habido un amplio desarrollo de programas de código abierto, disponibles en Internet, tales como FaceSwap[1] y DeepFaceLab[2], disponibles en GitHub. Este último es el utilizado por la popular cuenta de Youtube «Derpfakes[3]», con varios millones de seguidores, donde se incluyen tutoriales para su uso. La única limitación para ello, con unos conocimientos informáticos no excesivamente avanzados, es el *hardware* necesario. Además de amplia memoria en disco duro y RAM, es necesario una unidad GPU de gran capacidad, aunque su carencia podría suplirse invirtiendo un mayor tiempo en el procesamiento de imágenes.

---

1 Disponible en https://github.com/wuhuikai/FaceSwap.

2 Disponible en https://github.com/iperov/DeepFaceLab.

3 Disponible en https://www.youtube.com/channel/UCUix6Sk2MZkVOr5PWQrtH1g.

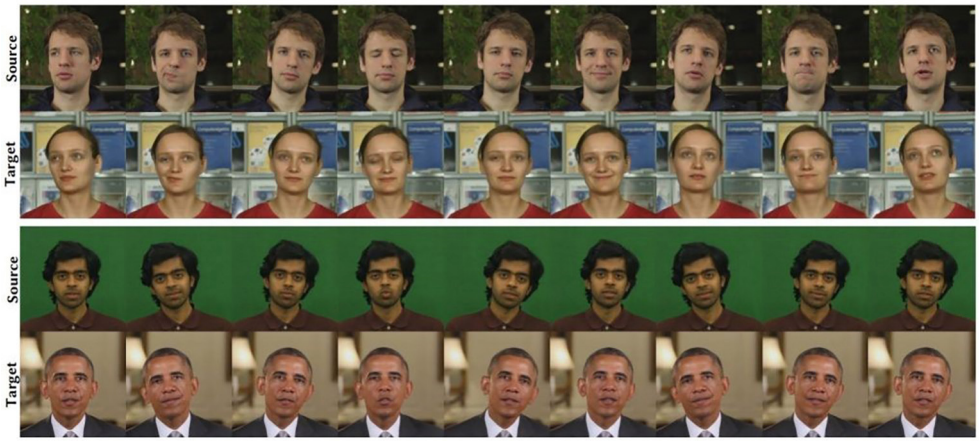


Figura 2: contraste de deep learning entre fuente y destino. Fuente: Galiana, 2019

Antes de procesar las imágenes, es necesario tener claro cuál es el objetivo que se desea. La selección de imágenes con buena iluminación y donde el objetivo y el destino compartan tonos de piel similares, facilitarán el proceso. Tiempo y calidad final son parámetros opuestos. Cuanto más tiempo se invierta en entrenar a la AI, mejor será el resultado. A su vez, cuanto mayor sea la longitud del vídeo que se desea manipular, la inversión de tiempo será mucho mayor para mantener la calidad.

El programa DeepFakeLab puede descargarse con facilidad, compatible con varios sistemas operativos. Su instalación no presenta dificultad, ya que es la mera extracción de líneas de comandos que se ejecutan de forma secuencial. Los archivos de fuente (*source* o src) y destino (*destination* o dst) se incluyen en una subcarpeta para su análisis. Estos vídeos se dividen en fotogramas individuales como archivos .png y son analizados para extraer los datos que se utilizarán para crear el *deepfake*. Se pueden añadir imágenes individuales a las creadas de esta manera, sumando así información de fuentes diversas para el análisis. Recogidas las imágenes, se analizan para buscar rostros en ellas. La extracción puede hacerse con varios *scripts* diferentes. El S3FD parece ser el que obtiene menos falsos positivos, pero el MTCNN obtiene un resultado más fluido. La extracción manual permite que el mismo usuario sea el que identifique los rostros y alinee los puntos de medición con ellos. Esto permite mejorar los resultados en caso de obstrucciones visuales. Este proceso se repite con ambos vídeos, el original y el de destino.

El siguiente paso importante es entrenar a la AI. Existen varios disponibles en esta aplicación. El primero de ellos es el H64, donde se utiliza una resolución de 64x64 píxeles para los rostros. Para el aprendizaje utiliza TensorFlow, una biblioteca abierta de aprendizaje automático desarrollada por Google. La segunda opción, H128, es similar a la previa, solo que los rostros cuentan con una resolución de 128x128 píxeles, lo cual consigue mejores resultados en planos cortos y vídeos de mayor resolución. El script D5 tiene la misma resolución de 128x128 pero parece conseguir una mayor cobertura del rostro. No funciona igual de bien con luces y tonos de piel diferentes, y necesita que los rostros tengan una forma similar, pero consigue mejores resultados si se consiguen

seguir estas directrices. El *script* SAE utiliza *morphing* para intercambiar los rostros, lo cual puede llevar a resultados irreconocibles.

En términos generales, parece que los rostros más estrechos son los más sencillos de superponer, puesto que no deforman la forma de la cara. Cada modelo puede tener ventajas según las características de imagen y de *hardware* disponible. La calidad de las imágenes que se analizan es fundamental para obtener un buen resultado, optimizándose con tonos de piel similares, buena iluminación, alta resolución y variedad gestual. Es necesario, después, revisar estas imágenes para eliminar falsos positivos, porciones borrosas o duplicados. En la medida de lo posible, es recomendable reducir las imágenes que se van a analizar para poder acelerar el aprendizaje, siempre y cuando haya suficientes para cubrir la escena. Un conjunto típico rondaría entre las mil y cinco mil imágenes. Idealmente una secuencia se debe dividir en planos individuales, cada uno para una dirección del rostro y entrenar a la AI para ella.

RIESGOS DE CONSUMO

Los *deepfakes* son perversos, pues aprovechan la credibilidad del portador para emitir mensajes que sirven a determinados intereses, una suerte de propaganda. En la figura 3 aparecen las noticias falsas que han causado mayor impacto (compartir, comentar o reaccionar) en la red social Facebook en las últimas elecciones de Estados Unidos, en 2016:

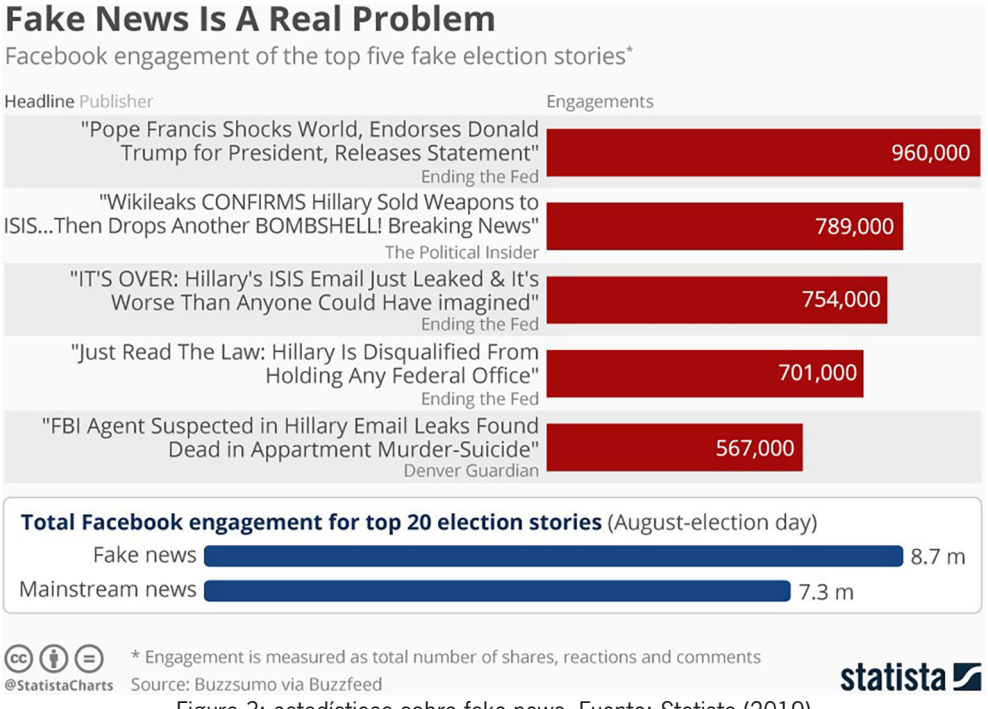


Figura 3: estadísticas sobre fake news. Fuente: Statista (2019)

Como se puede apreciar, 8,7 millones de reacciones se produjeron frente a noticias falsas, más que frente a las verdaderas. De esas cinco noticias, tomadas aleatoriamente como ejemplos llamativos, la primera se corresponde a unas supuestas declaraciones del papa Francisco. Una de las cualidades del busto parlante es la capacidad de aportar veracidad, credibilidad a una información. ¿Qué mayor prueba de veracidad que ver al propio declarante enunciando el discurso? En esa línea, ¿cuál sería el impacto de, por ejemplo, la primera noticia falsa, si es el propio papa el que aparece en persona hablando sobre Trump?

Todas aquellas informaciones basadas en declaraciones, comunicados o simplemente aquellas que utilicen como complemento de veracidad las palabras de un prescriptor, corren el riesgo de ser sujeto de *deepfake*. Y en una sociedad necesitada de certezas, inmersa en un superávit informativo, la vulnerabilidad parece clara. Frente a ello, parecen necesarios métodos de protección, de los que apuntamos algunos.

MÉTODOS DE IDENTIFICACIÓN

Es muy probable que los métodos de detección siempre estén por detrás de los mecanismos de creación pero, de momento, parece haber algunos indicativos para localizar *deepfakes*. El primero de ellos es una limitación relacionada con la captación fotográfica de personajes célebres. Rara vez se les muestra con los ojos cerrados, por lo que una imagen de este tipo resulta problemática para estos programas. Asimismo, esto se traduce en un menor número de parpadeos que en la vida real.

Otros indicativos son zonas borrosas en el rostro, pero no en el resto de la imagen, debido a la superposición. El emborronamiento también suele aparecer cuando un objeto cruza por delante del rostro. La superposición también puede llevar a cambios en el tono de piel en los extremos del rostro, que pueden permitir identificar la falsedad o a la aparición de dobles barbillas, cejas o marcas de cualquier tipo.

El *Deepfake Detection Challenge*, promovido por empresas tales como Facebook y Microsoft es una propuesta para la creación de métodos de detección en forma de competición, con la que esperan mejorar la identificación de este tipo de imágenes, que se auguran problemáticas. Hay también *startups* como Deeptrace que están trabajando en resolver el mismo problema.

CONCLUSIONES

Hasta este momento se consideraba que la imagen en vídeo podía considerarse razonablemente fiable, si teníamos en cuenta su contextualización, pese a la introducción de herramientas de creación de imagen por ordenador. Con la introducción de los *deepfakes*, esta veracidad queda tan en entredicho como la de la imagen fotográfica, pero con la dificultad de que es incluso más peligrosa por la percepción de verosimilitud que conlleva.

Las herramientas para crear *deepfakes* pueden ser una poderosa arma política en época electoral o como propaganda para cualquier tipo de movimiento, mostrando pruebas fehacientes de que alguien dijo o hizo algo de lo que no fue autor. Aunque después se desmienta, el daño puede estar hecho. El acceso a estos métodos de manipulación no es excesivamente complejo y puede conseguirse con medios de escasa sofisticación, al menos para las falsificaciones más sencillas, lo cual las deja en manos de un público relativamente amplio. Por este motivo, es necesario mejorar las herramientas de detección, ya que es de suponer que los métodos más fáciles de identificarlas (parpadeo, tonos de piel, emborronamiento), pronto quedarán superados gracias a los incesantes avances tecnológicos.

BIBLIOGRAFÍA

– BBC. «Fake Obama created using AI video tool». *BBC News*. 2019. Disponible en https://www.youtube.com/watch?v=AmUC4m6w1wo.

– CAGE, Nick. «Deepfakes». 2018. Disponible en https://www.youtube.com/watch?v=kqEZa6IkbG0.

– FONTCUBERTA, Joan. *El beso de Judas. Fotografía y Verdad*. Barcelona: Gustavo Gili, 1997.

– FONTCUBERTA, Joan. *La cámara de Pandora: La fotografí@ después de la fotografía*. Barcelona: Gustavo Gili, 2010.

– GALIANA, Patricia. «¿Qué son los *deepfakes* y cómo detectarlos?», en *Business and Tech*. 2019. Disponible en https://www.iebschool.com/blog/deepfakes-como-detectarlas-business-tech/.

– GOODFELLOW, Ian J.; POUGET-ABADIE, Jean; MIRZA, Mehdi; XU, Bing; WARDE-FARLEY, David; OZAIR, Sherjil; COURVILLE, Aaron; BENGIO, Yoshua. «Generative Adversarial Networks». arXiv:1406.2661. 2014. Disponible en https://arxiv.org/abs/1406.2661.

– LI, Wei; GAUCI, Melvin y GROSS, Roderich. «A coevolutionary approach to learn animal behavior through controlled interaction». En BLUM, Christian (ed.). *Proceedings of the 15th annual conference on Genetic and evolutionary computation* (GECCO '13). USA, New York, NY: ACM, 2013, pp. 223-230. DOI: https://doi.org/10.1145/2463372.2465801.

– NIRKIN, Y.; KELLER, Y., & HASSNER, T. FSGAN: «Subject Agnostic Face Swapping and Reenactment». arXiv preprint arXiv:1908.05932. 2019.

– OBEROI, Gaurav. «Exploring Deepfakes», en *KDNuggets*. 2018. Disponible en https://www.kdnuggets.com/2018/03/exploring-deepfakes.html.

– PHAM, Hai X.; WANG, Yuting y PAVLOVIC, Vladimir. «Generative Adversarial Talking Head: Bringing Portraits to Life with a Weakly Supervised Neural Network». *CoRR*. 28 de marzo de 2018. Disponible en https://arxiv.org/pdf/1803.07716.pdf.

– STATISTA. «Fake News is a real problem». 2019. Disponible en https://www.statista.com/chart/6795/fake-news-is-a-real-problem/.

– SUWAJANAKORN, S.; SEITZ, S. M.; KEMELMACHER-SCHLIZERMAN, I. «Synthesizing obama: learninglip sync from audio». *SIGGRAPH*. 2017.

– THIES, J.; ZOLLHÖFER, M., STAMMINGER, M.; THEOBALT, C., & NIEßNER, M. «Face-2face: Real-time face capture and reenactment of rgb videos». *Communications of the Acm, 62*(1). 2018, pp. 96-104. doi:10.1145/3292039.

– ZEROCOOL22. «Adolf Hitler «Downfall Movie» to Mauricio Macr». 2018. Disponible en https://www.youtube.com/watch?v=M8t6hGRtDac.

APROXIMACIÓN A LA SOCIALIZACIÓN FAMILIAR DE LA OFICIALIDAD Y SUBOFICIALIDAD DE LAS FUERZAS ARMADAS ESPAÑOLAS

CLAUDIA GONZÁLEZ RIEGA
Licenciada en Ciencias Políticas y Administración. Máster en Análisis político y asesoría institucional

La defensa no es uno de los ámbitos más debatidos y examinados en nuestro país. Así mismo, hasta la fecha, los estudios sobre las Fuerzas Armadas existentes se enfocan en la proyección internacional de estas. Sin embargo, escasean los estudios que abarquen una perspectiva interna que analice los miembros de los ejércitos que conforman el cuerpo de defensa español. Por todo esto, el presente estudio se centra en los militares integrantes de las Fuerzas Armadas españolas, desde un encuadre basado en la sociología militar que profundiza sobre el proceso de socialización familiar. De hecho, en el año 1997 se articuló un estudio titulado «El ejército español ante el siglo XXI: redefinición de las funciones de las Fuerzas Armadas y perfil profesional y político-institucional de la futura oficialidad y suboficialidad» que ya puso de relieve la importancia del proceso de socialización familiar entre los militares de las Fuerzas Armadas españolas. Es más, a partir de los datos de este estudio parte el presente análisis, el cual ha puesto de relieve la importancia de la ideología de los progenitores de los militares en la transmisión de las normas, valores y modelos de comportamiento que estos reproducen en su carrera profesional.

Palabras clave: defensa, militares, ideología, progenitores

INTRODUCCIÓN

La defensa no es, precisamente, uno de los ámbitos más debatidos y examinados en nuestro país. Así mismo, hasta la fecha los estudios sobre las Fuerzas Armadas existentes se enfocan en la proyección internacional de estas, es decir, en la acción exterior militar. Sin embargo, escasean los estudios que abarcan una perspectiva interna que analicen el órgano administrativo y los miembros de los tres ejércitos que conforman el cuerpo de defensa español: el Ejército de Tierra; la Armada y el Ejército del Aire. De ahí

que, en el presente estudio, el enfoque del análisis se centre en los militares integrantes de las Fuerzas Armadas, desde un encuadre basado en la sociología militar y a través de un análisis socio cultural íntimo que permita un nuevo acercamiento a las identidades y personalidades intrínsecas de estos.

Cuando se busca conocer íntegramente a cualquier individuo, algunos de los aspectos más importantes a analizar son, indudablemente, los agentes de socialización que le rodean, ya que estos son los responsables de «la transmisión de las normas, valores y modelos de comportamiento y, dentro de ellos, la familia es el más importante, no solo porque es el primero en actuar, sino porque se constituye en el nexo entre el individuo y la sociedad» (Pérez, 2007, p. 91). Es por esto que el proceso de socialización familiar se presenta como una pieza clave en la presente investigación. De hecho, en el año 1997 se articuló un estudio, desde la Universidad de Barcelona, titulado «El Ejército español ante el siglo XXI: redefinición de las funciones de las Fuerzas Armadas y perfil profesional y político-institucional de la futura oficialidad y suboficialidad» que ya puso de relieve la importancia del proceso de socialización familiar en los militares de las Fuerzas Armadas españolas. Ahora bien, cuando hablamos de este desarrollo experimentado por los miembros de la defensa nacional, se desconoce qué progenitor tiene más protagonismo en este. Es decir, la transmisión de las normas, valores y modelos de comportamiento: ¿proviene en mayor medida del padre o de la madre?

A nivel social, la importancia de responder satisfactoriamente a esta pregunta reside en profundizar el conocimiento *per se* del ámbito de defensa nacional, el cual, como se ha mencionado anteriormente, se queda en un segundo plano en cuanto a proyectos científicos. Acerca del presente terreno de investigación, es importante señalar que la Directiva de Defensa Nacional 1/2012 propone objetivos gubernamentales para la defensa y las directrices básicas para implementarlos, tomando como referencia el quinto objetivo: «la defensa de España debe ser asumida por todos los españoles», se ha articulado el examen de los procesos de socialización familiar en los militares españoles, puesto que permite un acercamiento por parte de la población civil a este colectivo.

A nivel científico, faltan estudios de sociología militar dentro del cuerpo de las Fuerzas Armadas españolas y no existe ninguno que se concentre en los progenitores de los militares. No obstante, sí que sabemos, en contra de todo pronóstico, que la socialización primaria familiar, tiene mucha más trascendencia en los milicianos que la socialización secundaria institucional, que se da durante la etapa de formación militar. Con todo, el primero no ha sido analizado en profundidad, de manera que no se ha tenido en cuenta en qué aspectos la figura materna tiene protagonismo por encima de la paterna y viceversa, lo cual brinda información social, cultural y política sobre los núcleos familiares de los militares que rodean el cuerpo de defensa nacional. Por todo esto, se considera un tema de relevancia y originalidad científica que, a su vez, ofrece la oportunidad de estudiar nuevas vías de análisis vírgenes.

Antonio M. Jaime Castillo (2000) evidenció cómo las correlaciones, analizadas en su estudio, entre la posición ideológica propia y la de la madre se mostraron ligeramente superiores a las existentes con el padre: «Tanto para hombres como para mujeres, la media de la distancia ideológica con el padre es ligeramente inferior a la media de la

distancia ideológica con la madre [...] la ideología de los españoles covaría más estrechamente con la ideología materna que con la paterna» (p. 16). De la misma manera, la *Revista Psicothema* señaló que las madres mantenían una influencia mayor en los hijos, con independencia del sexo. Esto es, los resultados extraídos de estudios heterogéneos expusieron cómo las madres obtuvieron puntuaciones más elevadas en cuanto a la implicación en la crianza y en la potenciación de la autonomía de la descendencia. «Los resultados muestran un efecto superior de la madre tanto en los hijos varones como en las hijas mujeres» (Tur-Porcar *et al.*, 2012, p. 287). Una situación semejante se generó al relacionar la crianza con la conducta internalizada y observar que el afecto de la madre, frente al del padre, presenta mayor poder predictor (Barón, *et al.*, 2008).

Dicho lo anterior, la hipótesis a corroborar en el vigente ensayo parte de la asunción expuesta sobre la mayor influencia de la figura materna en los hijos. Sin embargo, en esta ocasión se trasladarán las teorías ya corroboradas por anteriores estudios al ámbito de examen de la defensa española. Por consiguiente, la presunción que ocupará el desarrollo del análisis es:

H1: La madre desempeñará un mayor efecto e influencia sobre los militares en comparación al padre y, en consecuencia, estos proyectarán las normas, valores y modelos de comportamiento transmitidos por su figura materna en su perfil profesional y político como miembros de las Fuerzas Armadas.

METODOLOGIA

El presente análisis emplea la base de datos extraída del estudio «El ejército español ante el siglo XXI: redefinición de las funciones de las Fuerzas Armadas y perfil profesional y político-institucional de la futura oficialidad y suboficialidad». Dicha base, se trata de un cuestionario aplicado en la segunda quincena de enero de 2001, por un equipo de profesionales de la Universidad de Barcelona, a dos mil cuatrocientos setenta y tres alumnos de treinta y dos centros españoles de formación militar de un cuestionario cerrado. Esto es, en el presente estudio han sido empleadas una serie de variables, seleccionadas por su idoneidad, extraídas de dicho cuestionario con la finalidad de ser tratadas estadísticamente.

Como variables independientes explicativas, han sido empleadas tanto la ideología del padre como la de la madre, es decir, la ubicación ideológica de los progenitores según la respuesta, en base de la percepción del entrevistado, que se refleja en el cuestionario.

Como variables dependientes, se ha empleado la variable escala ideológica alumnos.

Hay que mencionar, además, que con el objetivo de facilitar el tratamiento de los datos y su posterior comprensión, se realizaron cinco grupos ideológicos en la escala numérica de las respuestas a través de la manipulación de las variables mediante el programa SPSS, aplicando puntos de corte en las variables del cuestionario, de manera que fueron generadas nuevas categorías: 1-2 extrema izquierda; 3-4 izquierda; 5-6 centro; 7-8 derecha y 9-10 extrema derecha.

RESULTADOS
Estadísticos descriptivos ideológicos

En el caso de la variable «escala ideológica alumnos» se observa que el mínimo apunta al grupo número 1, el cual agrupa las posiciones de extrema izquierda. Al contrario, el máximo señala al grupo número 5, exponiéndose así la existencia de un colectivo auto ubicado en la extrema derecha. La media de esta variable se encuentra en un 3,40, lo cual se encuentra en el grupo número 3 de la escala, identificado con el grupo de centro, con una ligera tendencia hacia la derecha.

Tabla 1. Estadísticos descriptivos escala ideológica alumnos.

	N	Mínimo	Máximo	Media	Desv. Desviación
escala ideológica alumnos	2.300	1	5	3,40	0,969

Fuente: elaboración propia a partir de datos extraídos de «Los mandos de las Fuerzas Armadas españolas del siglo XXI».

En cuanto a la variable «escala ideológica padre», se observa que, de nuevo, el mínimo apunta al grupo número 1, demostrando la existencia de un colectivo posicionado en la extrema izquierda. De la misma forma, el máximo señala al grupo número 5, exponiéndose la existencia de un colectivo masculino identificado con la extrema derecha. La media de esta variable se encuentra en un 3,28, lo cual se encuentra en el grupo número 3 de la escala, identificado con el grupo de centro.

Tabla 2. Estadísticos descriptivos escala ideológica padre.

	N	Mínimo	Máximo	Media	Desv. Desviación
escala ideológica padre	2.253	1	5	3,28	1,12

Fuente: elaboración propia a partir de datos extraídos de «Los mandos de las Fuerzas Armadas españolas del siglo XXI».

Por último, la variable «escala ideológica madre», revela la presencia de un colectivo posicionado en la extrema izquierda a su vez que un colectivo femenino situado en la extrema derecha. La media de esta variable se encuentra en un 3,20, lo cual se encuentra en el grupo número 3 de la escala, identificado con el grupo de centro, siendo esta media ligeramente inferior a la escala ideológica paterna.

Tabla 3. Estadísticos descriptivos escala ideológica madre.

	N	Mínimo	Máximo	Media	Desv. Desviación
escala ideológica padre	2.254	1	5	3,20	1,02

Fuente: elaboración propia a partir de datos extraídos de «Los mandos de las Fuerzas Armadas españolas del siglo XXI».

Correlación de Pearson

El valor de la «escala ideológica alumnos» con la «escala ideológica padre» tiene un índice de correlación R de Pearson de 0,498. A su vez, se observa una relación altamente significativa, ya que el p-valor calculado en este caso es de 0,000. De esta manera, puede concluirse que sí existe correlación y esta se encuentra en una categoría moderada[1].

Tabla 4. Correlaciones variables ideológicas.

Correlaciones			
		escala ideológica padre	escala ideológica madre
escala ideológica alumnos	Correlación de Pearson	,498**	,491**
	Sig. (bilateral)	0,000	0,000
	N	2205	2206
**. La correlación es significativa en el nivel 0,01 (bilateral).			

Fuente: elaboración propia a partir de datos extraídos de «Los mandos de las Fuerzas Armadas españolas del siglo XXI».

El valor de la «escala ideológica alumnos» con la «escala ideológica madre» también goza que un alto nivel de significación. De nuevo, el p-valor que nos proporciona el *software* es de 0,000. En esta ocasión el índice de R de Pearson es de 0,491, la cual, a pesar de ser una cifra ligeramente inferior a la obtenida por la variable «escala ideológica padre», también se sitúa en una medida de correlación moderada.

Estos resultados, por lo tanto, nos indican un alto grado de relación entre la ideología de los alumnos y sus progenitores, de manera que, un estudio exhaustivo de estas nos aportará información sobre «cómo» cada una de ellas impacta en la ideología de los entrevistados.

Regresión múltiple ideológica

A continuación se realiza una regresión múltiple con la finalidad de profundizar en el análisis de la relación entre las variables de «escala ideológica padre», «escala ideológica madre» y «escala ideológica alumnos». La especificación de la regresión múltiple realizada es:

- Escala ideológica alumnos = $\alpha + \beta 1$ escala ideológica padre + $\beta 2$ escala ideológica madre.
- Variable dependiente: escala ideológica alumnos.

[1] Las medidas de correlación R Pearson, son los Índices R y Rho: 0,00 - 0,20 (Ínfima); 0,20 - 0,40 (Escasa); 0,40 - 0,60 (Moderada); 0,60 - 0,80 (Buena) y 0,80 - 1,00 (Excelente). Disponible en: https://www.youtube.com/watch?v=sonEBK5-pnE.

– Variables independientes: escala ideológica padre y escala ideológica madre.

Lo primero que observamos en la tabla 5 es el valor del coeficiente de determinación en R cuadrado ajustado, el cual oscila entre 0 y 1, que nos ofrece la cifra de 0,296. Esto significa que el 29,6 % de la variación en el índice de la escala ideológica de los alumnos se puede predecir por las variables explicativas empleadas en el estudio, es decir, la escala ideológica padre y escala ideológica madre.

Tabla 5. Resumen del modelo ideológico.

Resumen del modelo									
					Estadísticos de cambio				
Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación	Cambio en R cuadrado	Cambio en F	gl1	gl2	Sig. Cambio en F
1	,544a	0,296	0,296	0,814	0,296	461,285	2	2190	0,000
a. Predictores: (constante), escala ideológica madre, escala ideológica padre.									
b. Variable dependiente: escala ideológica alumnos.									

Fuente: elaboración propia a partir de datos extraídos de «Los mandos de las Fuerzas Armadas españolas del siglo XXI».

A continuación, la tabla 6 expone que en el modelo se observa, a través de la constante, que cuando las variables independientes están a 0, el índice de la escala ideológica alumnos es de 1,658. Del mismo modo se puede extraer que por cada unidad adicional de la escala ideológica padre, es decir, cada vez que la ideología del padre se acerque más a la derecha, la escala ideológica alumnos aumentará en 0,269, acercándose a su vez, también a la derecha. De manera análoga, por cada unidad adicional en la escala ideológica madre, esto es, cada vez que la ideología de la madre se acerque más a la derecha, la escala ideológica alumnos acrecentará en 0,272, acercándose a su vez, también a la derecha.

Tabla 6. Coeficientes regresión múltiple ideológicos.

Coeficientes								
		Coeficientes no estandarizados		Coeficientes estandarizados			95,0% intervalo de confianza para B	
Modelo		B	Desv. Error	Beta	t	Sig.	Límite inferior	Límite superior
1	(Constante)	1,658	0,060		27,414	0,000	1,540	1,777
	escala ideológica padre	0,269	0,021	0,311	13,039	0,000	0,229	0,310
	escala ideológica madre	0,272	0,023	0,287	12,023	0,000	0,227	0,316

Fuente: elaboración propia a partir de datos extraídos de «Los mandos de las Fuerzas Armadas españolas del siglo XXI».

En cuanto a los coeficientes tipificados o estandarizados, ofrecen la posibilidad de poder evaluar y comparar el poder explicativo de cada predictor en la ecuación al ser directamente comparable. Es decir, nos señala qué variable es la más sólida. Los resultados apuntan a una preeminencia de las variables «escala ideológica padre», con un peso de 0,311, mientras que la «escala ideológica madre» se queda por debajo con un 0,287.

CONCLUSIONES

Una vez realizado el análisis se ha observado que, en efecto, las ideologías de los progenitores tienen un impacto muy significativo en las ideologías de los militares. Por lo tanto, puede concluirse que se ha demostrado el grado en que la ideología paterna y materna influyen en la ideología de los militares, siendo este muy notable a la vez que similar. Es decir, ambos progenitores ejercen el mismo importante grado de influencia.

BIBLIOGRAFÍA

– AGUILAR, P. «Justicia, política y memoria: los legados del franquismo en la transición española». Instituto Juan March de Estudios e Investigaciones. 2001. https://www.researchgate.net/profile/Paloma_Aguilar/publication/253382341_JUSTICIA_POLITICA_Y_MEMORIA_LOS_LEGADOS_DEL_FRANQUISMO_EN_LA_TRANSICION_ESPANOLA/links/5644f19508ae451880a8a282.pdf.

– ALONSO DEL REAL BARRERA, J. M. «Influencia de la familia en el desarrollo de las habilidades socioemocionales de los niños de Educación Primaria: la familia como recurso preventivo de la violencia de escolares y conflictos escolares». 2016. https://idus.us.es/xmlui/bitstream/handle/11441/45103/TFG%20Jose%20Mar%C3%ADa%20Alonso.pdf?sequence=1&isAllowed=y.

– BARÓN, M. J. O.; URQUIJO, P. A.; BILBAO, I. E.; REBOLLO, M. J. F., & SÁNCHEZ, F. L. «Predictores familiares de la internalización moral en la infancia». *Psicothema*, 20(4). 2008, pp. 712-717. http://www.psicothema.com/PDF/3545.pdf.

– CABALLERO, M. J. C.; AGUDEDO, A., & OCHOA, G. M. «Un análisis intercultural de la socialización familiar y los valores en adolescentes». *Escritos de psicología*, (5). 2001, pp. 70-80.

– CASTILLO, A. M. J. «Familia y socialización política. La transmisión de orientaciones ideológicas en el seno de la familia española». *Reis*. 2000, pp. 71-92.

– MARTÍNEZ, R. «Los mandos de las Fuerzas Armadas españolas del siglo XXI» (Vol. 243). CIS. 2007.

– PÉREZ, C. *Técnicas de análisis multivariante de datos. Aplicaciones con SPSS*. Madrid: Pearson, 2008.

– PÉREZ, A. R. «Principales modelos de socialización familiar». *Foro de educación*, 5(9). 2007, pp. 91-97.

– TORREGROSA, J. R., & VILLANUEVA, C. F. *La interiorización de la estructura social. Estudios básicos de Psicología Social*. Barcelona: Hora, S.A., 1984. https://eprints.ucm.es/41318/1/la%20interiorizaci%C3%B3n%20de%20la%20estructura%20social.pdf.

– TUR-PORCAR, A.; MESTRE, V.; SAMPER, P.; & MALONDA, E. «Crianza y agresividad de los menores: ¿es diferente la influencia del padre y de la madre?». *Psicothema*, 24(2). 2012, pp. 284-288.https://www.redalyc.org/pdf/727/72723578017.pdf.

– YUBERO, S. «Capítulo XXIV Socialización y Aprendizaje Social. Psicología Social, Cultura y Educación. s/f.[en línea]». (2005). Disponible en http://www. ehu. eus/documents/1463215/1504276/Capítulo XXIV. pdf. https://www.ehu.eus/documents/1463215/1504276/Capitulo+XXIV.pdf.

CONCLUSIONES DEL XXVII CURSO INTERNACIONAL DE DEFENSA

CONCLUSIONES DEL XXVII CURSO INTERNACIONAL DE DEFENSA

D. MIGUEL A. SANTAMARÍA VILLASCUERNA
Coronel director de la Cátedra Cervantes

Este curso se considera, después de sus 27 ediciones, una excelente herramienta al servicio de la difusión de la cultura de defensa. En el mismo se compaginan tanto conferencias a cargo de ponentes de prestigio, como exposiciones de comunicaciones a cargo de los asistentes, como el desarrollo de actividades culturales y de convivencia. Al final de 5 días de relación se consigue no solo aumentar los conocimientos de los asistentes en cuanto al tema tratado, sino favorecer el conocimiento mutuo entre los asientes de distintas procedencias (militares, civiles y componentes de fuerzas y cuerpos de seguridad del Estado, hecho que queda constatado por el gran número de grupos afines que se crean y que permanecen a lo largo del tiempo.

Por lo dicho, se consideran conseguidos los objetivos propuestos y para futuras ediciones, debe ser empeño fundamental de la organización, intensificar la participación del número de asistentes jóvenes y la inclusión de información en distintas redes sociales, pues esto repercutirá claramente de cara a enriquecer la visión, dimensión e internacionalización de este Curso Internacional de Defensa.

En el desarrollo de este curso se contó con un total de 223 participantes de procedencia civil y militar. De este total de 223 asistentes 154 (69 %), fueron de procedencia civil y 69 (31 %) pertenecientes a las Fuerzas Armadas y a los Cuerpos y Fuerzas de Seguridad del Estado. A este personal se debería de sumar el personal de la organización: un total de 19.

Asimismo, el porcentaje de asistencia ha sido algo superior en el género masculino: 61 % (136 hombres) y 39 % (87 mujeres).

Y con toda probabilidad el dato más importante es que de estos asistentes el 60 % disponía de menos de 34 años de edad. Este es el principal empeño de la organización del curso y que en cada edición se ve recompensado con un gradual aumento de asistentes con este perfil.

De la misma manera, se ha contado con personal de 9 nacionalidades: Chile, España, EE. UU., Brasil, Francia, El Salvador, Ecuador, Italia y Argentina, y de 33 provincias españolas, como son: Ávila, Burgos, Oviedo, Tarragona, Madrid, Cádiz, León, Navarra, Granada, Tenerife, Salamanca, Valencia, Álava, Huelva, Santander, Segovia, Guipúzcoa, Jaén, Málaga, Ceuta, Sevilla, Zamora, Lugo, Huesca, Guadalajara, Barcelona, Zaragoza, Teruel, Toledo, Girona, Pontevedra, Lérida y Logroño. Debiendo destacar, por más cuantiosas, las participaciones de: Zaragoza (42), Barcelona (33), Madrid (28), Huesca (16) o Sevilla (10).

También destacar que se ha contado con jóvenes de las universidades siguientes:

- Univ. La Rioja
- Univ. Zaragoza
- Univ. Granada
- Univ. Complutense Madrid
- Univ. Navarra
- Univ. San Jorge Zaragoza
- Univ. Pablo de Olavide Sevilla
- Univ. Deusto
- Univ. Carlos III Madrid
- Univ. Abat Oliba Barcelona
- Univ. Europea Madrid
- Univ. Nebrija Madrid
- Univ. Francisco De Vitoria
- Univ. Sevilla
- Univ. Barcelona
- Univ. Rey Juan Carlos
- Univ. Santiago De Compostela
- Univ. Alcala
- Univ. Pontificia Salamanca
- Univ. Europea Miguel de Cervantes.

Se han presentado 66 comunicaciones y pósteres científicos.

Además, las contribuciones y las interrelaciones de los participantes continúan en los momentos de descanso, tanto conclusiones del XXVII curso internacional de defensa en el propio Palacio de Congresos como en la residencia universitaria donde se alojan, o incluso por las calles de Jaca.

Esta edición del Curso Internacional de Defensa contó en el acto inaugural con la directora general de Política de Defensa del Ministerio de Defensa, Dª Elena Gómez de Castro, el general director de la Academia General Militar, general Car-

los Melero; el alcalde de Jaca, Juan Manuel Ramón Ipas; José Domingo Dueñas, vicerrector de la Universidad de Zaragoza para el Campus de Huesca y el delegado territorial del Gobierno de Aragón en la Jacetania y Alto Gállego, José Antonio Fau Avellanas.

Bajo el título «LA AMENAZA HÍBRIDA: LA GUERRA IMPREVISIBLE», se pretendió, a través de la opinión de especialistas en el género, poner el foco de interés en temas tales como las ciberamenazas y el ciberterrorismo, la posverdad y las *fake news*, los riesgos nucleares, la presión económica y los recursos energéticos y para ello, se definieron las áreas siguientes:

Conferencia inaugural: «Amenazas híbridas»
Área n.º 1: Mirando al futuro.
Área n.º 2: Amenaza híbrida y ciberdefensa.
Área n.º 3: Amenaza híbrida y posverdad.
Área n.º 4: Otras amenazas híbridas.
Área n.º 5: Europa, España y seguridad.

Conferencia de clausura: «Incertidumbres y certezas, en el futuro de las Fuerzas Armadas».

Conferencia inaugural: «Amenazas híbridas»

La directora general de Política de Defensa del Ministerio de Defensa, Dª Elena Gómez de Castro, impartió la conferencia inaugural del XXVII Curso Internacional de Defensa, e hizo una aproximación general al concepto «amenaza hibrida», destacando que «con la amenaza híbrida ya no hay campos de batalla definidos, en muchos casos ni siquiera hay Ejércitos, la guerra está entre la gente». En este sentido destacó que «ataca a nuestro modo de vida y a nuestra esencia por lo que es mucho más que una guerra como tal».

Área n.º 1: Mirando al futuro

El coronel D. Ángel Gómez de Ágreda, habló de ética y límites de la libertad de opinión y de prensa. En concreto, se refirió al papel de los medios de comunicación vinculado a las nuevas tecnologías y a la capacidad de manipulación de la información. «Ahora mismo —señaló— la guerra no se hace tanto por medios bélicos sino dentro de nosotros, manipulando incluso más que el conocimiento, los sentimientos, a través del impacto que pueda tener ese conocimiento en la percepción de la realidad».

El coronel D. Bonifacio Gutiérrez, subdirector de Investigación y Lecciones Aprendidas del MADOC, ofreció una visión general de las amenazas híbridas, sus antecedentes, cuándo apareció el concepto y cómo ha evolucionado hasta enmarcarlo en el sistema actual de riesgos y seguridad de carácter global. «Lo más importante que hay que entender —aseguró— es que estas amenazas tratan de influir y desestabilizar el modo de vida de las sociedades occidentales». Uno de los aspectos diferenciales de estas amenazas, del ataque y de la respuesta, según este ponente, «es que el elemen-

to militar pasa a tener un papel secundario. Por supuesto, lo sigue teniendo, pero las respuestas también hay que buscarlas en los ámbitos político, económico, diplomático, social...».

El doctor en Ciencias Políticas D. Josep Baqués, se refirió en su intervención a la denominada «zona gris», que según él mismo describió, «se caracteriza por ser la franja de esta amenaza en la que no se emplea la fuerza y, por lo tanto, el protagonismo de los efectos distorsionadores que pueda tener sobre el *status quo* recae en medidas pacíficas y legales: movilización de la gente, medidas económicas de presión o trabajar narrativas basadas en medias verdades». Para combatir esta «zona gris», concluyó, «debe hacerse con medidas similares a las que plantean estos actores».

Área n.º 2: Amenaza híbrida y ciberdefensa

El capitán de navío D. Enrique Cubeiro, jefe de Estado Mayor del Mando Conjunto de Ciberdefensa, se centró en cómo está actuando la amenaza híbrida en el ciberespacio y haciendo uso de este entorno. Destacó que el conflicto no solo afecta a lo militar, que se emplean estrategias no convencionales «políticas», informativas»… para debilitar al adversario o que ante la legislación difusa, existen zonas grises que favorecen a los que menos escrúpulos tienen.

El profesor de Ciencia Política en la Universidad Pablo de Olavide, Guillem Colom, profundizó en el empleo de las «zonas grises» y, especialmente, en el papel de Rusia y China ante este fenómeno. Dijo que hay que regular y controlar Internet, y generar ecosistemas propios y que en esta lucha occidente juega con la desventaja de las limitaciones políticas, legales y sociales.

D. Fernando Hernández, coronel jefe del Área Técnica de la Jefatura de Información de la Guardia Civil, habló del ciberterrorismo y el hackivismo en la red y señaló que «aunque suene un poco a informática ficción, las amenazas del ciberterrorismo y del hackivismo son muy reales y, además, pueden causar mucho daño a nuestra forma de vivir». «El problema —prosiguió el ponente— es que estamos en una sociedad muy tecnificada y tecno dependiente y ese es nuestro talón de Aquiles; cuanto más dependientes somos de la tecnología más débiles somos ante su pérdida». Otro punto débil, a su juicio, es «la obsolescencia tecnológica, porque mucha tecnología lleva años instalada y parece como que no interesa demasiado su mantenimiento».

Área n.º 3: Amenaza híbrida y posverdad

El periodista y doctor en Sociología, D. Manuel Campo Vidal, profundizó en su ponencia en cómo afrontan los medios de comunicación las *fake news*. «Debemos ser cuidadosos con las noticias falsas porque en una época tan convulsa en el mundo, los medios de comunicación nos jugamos mucho, no solo la repercusión que las informaciones puedan tener sobre la opinión pública, sino también la pérdida de la credibilidad», destacó que, paradójicamente, «las noticias falsas pueden convertirse en una oportunidad para que los medios recuperen credibilidad porque esta idea de que se haya democratizado la información está bien, pero a la hora de informarnos es fundamental asociar la difusión

de una noticia a un medio en concreto, que es el responsable de controlar y confirmar los datos que se difunden».

D. Emilio Andreu, presidente de la Asociación de Periodistas de la Defensa, centró su ponencia en la posverdad, en los antecedentes y la situación actual. Para enmarcar el tema, explicó que «del consenso social que generaba unos mínimos temas que la ciudadanía compartía, hemos pasado a un mundo de ignorancia, lo que se ha tratado de hacer es inundar a la sociedad del siglo XXI de ignorancia. Cuando tú eres ignorante ya no te interesan los hechos y a partir de ese momento se produce la deslegitimación de las instituciones que moldean el Estado como los Gobiernos, las Fuerzas Armadas, la educación o la sanidad».

El general D. Juan Antonio Moliner, subdirector del Instituto Universitario «General Gutiérrez Mellado», en su intervención destacó que «en una sociedad democrática, los militares son los que tienen delegado el uso de la fuerza, eso significa que nuestra función esencial es el combate, pero mientras estemos en paz también debemos desarrollar otras». Se refirió a la formación y la capacitación ética al lado de la logística, técnica, táctica y estratégica. Pero esa competencia ética a desarrollar en el uso de la fuerza, prosiguió, «se complica con las modernas tecnologías». En primer lugar, señaló «porque son novedosas y no estamos familiarizados con ellas y, segundo, porque ofrecen unas posibilidades desde la perspectiva teórica que van en contra de la naturaleza humana que tienen el combate y la guerra y que se manifiestan en la posibilidad de que la decisión de matar, en algún momento, en vez de ser tomada por el ser humano respondiendo a una serie de criterios éticos y morales, sea tomada por las máquinas, lo cual sería terrible».

Área n.º 4: Otras amenazas híbridas

El general D. Valentín Martínez, ex director del Centro de Inteligencia de las Fuerzas Armadas, analizó la vertiente económica. «Vivimos en un mundo complejo y volátil y esta es una de las amenazas más importantes; no hay más que ver todo lo que está ocurriendo entre Estados Unidos y China». «La tecnología que se ha desarrollado en los últimos 40 años lo ha cambiado todo —prosiguió—, nos encontramos, además, en un entorno incierto y ambiguo en el que pueden ocurrir caídas de los mercados, colapsos de las instituciones financieras, espionaje industrial, acciones de influencia hostiles, guerra de divisas o economía sumergida».

La secretaria general del Instituto de Fusión Nuclear Guillermo Velarde, D.ª Natividad Carpintero, habló sobre riesgos nucleares. En su intervención destacó que «en el siglo XX se vislumbraban guerras con armas químicas, biológicas y nucleares que afortunadamente no se dieron jamás». En el siglo XXI, sin embargo, «es como si hubiera desaparecido ese espectro de una guerra con ese nivel de armamento no convencional, pero sí tenemos la problemática del terrorismo y los países deben ser conscientes de que es una amenaza real».

El Sr. Iván Martén, se refirió a «la geopolítica de los recursos energéticos». En su intervención, habló, sobre todo, de «la fragilidad del ecosistema energético». En concreto,

destacó cómo «la energía es una necesidad de los países y gran parte de los conflictos en el mundo son por el acceso a ella y a los recursos naturales». En este sentido, pronosticó que «la demanda de energía va a seguir creciendo como consecuencia del incremento de la población y de su calidad de vida».

Área n.º 5: Europa, España y seguridad

El coronel Juan A. Mora, analista asociado del Instituto Español de Estudios Estratégicos, se refirió a la situación del Mediterráneo que, a su juicio, «ya no es el centro del mundo». «En la actualidad pasa a ser un escenario de la globalización, de entrada porque existe un pulso entre Estados Unidos, Rusia y próximamente China, además de la Unión Europea, por lo que en los próximos años veremos ese choque de potencias geopolíticas con enfrentamientos económicos importantes», aseguró. También habló del Mediterráneo como «un escenario de inestabilidad con los problemas en Libia y lo que suceda en el sur de Argelia».

Sonia Alda, investigadora principal del Real Instituto Elcano, habló sobre «tráficos ilícitos y redes criminales», planteando la complejidad de esta forma de criminalidad. La ponente comentó cuáles son los factores facilitadores que explican por qué en América Latina está muy implantado el crimen organizado. En este sentido, comparó la región con el resto del mundo analizando cuál es su situación. Su hipótesis de partida es que la implantación del crimen organizado se debe, fundamentalmente, a la debilidad del imperio de la ley. «La incapacidad del Estado de imponer la ley en todo el territorio y a todos los habitantes crea la posibilidad de negociar la ley y con esa negociación se crean espacios de corrupción y, en consecuencia, de impunidad, el caldo de cultivo idóneo para el crimen organizado».

Conferencia de clausura: «Incertidumbres y certezas, en el futuro de las Fuerzas Armadas»

El general de ejército, jefe de Estado Mayor de la Defensa (JEMAD), D. Fernando Alejandre Martínez, impartió la conferencia de clausura y en su intervención se refirió a «la necesidad de adaptación de las Fuerzas Armadas» y al cambio al que se van a enfrentar en los próximos años, «que probablemente sea lo único que sabemos que es seguro que va a ocurrir, ya que vamos a ser diferentes a como somos hoy». «Los cambios que se avecinan van a ser de tal magnitud que hacen muy difícil saber hoy en día, cómo deberán operar los Ejércitos en el futuro». En este sentido, aseguró que «las operaciones del futuro van a ser un conjunto de tierra, mar, aire y ciberdefensa en el espacio. Es decir, una amplia zona gris y una amenaza híbrida. Además, habrá una presencia inevitable de población en las zonas de operaciones que tendrá que acostumbrarse a interactuar con nuestras fuerzas y al revés».

El acto fue clausurado por el general de ejército D. Fernando Alejandre, jefe de Estado Mayor de la Defensa y acompañado en la mesa presidencial del teniente general, D. Jerónimo de Gregorio y Monmeneu, jefe de Mando de Adiestramiento y Doctrina, del general de Brigada, D. Carlos Melero Claudio, director de la Academia General Militar, D.ª María Victoria Mora Gómez, concejal de fiestas, pueblos y recursos humanos del

Excelentísimo Ayuntamiento de Jaca, D. Jaime Sanau Villarroya, profesor de la Universidad de Zaragoza, D.ª Isabel Blasco González, subdelegada del Gobierno en Huesca y el delegado territorial del Gobierno de Aragón en la Jacetania y Alto Gállego, D. José Antonio Fau Avellanas.

Además, por quinto año consecutivo y durante las tardes de los días 30 de septiembre y 3 de octubre se ha celebrado de manera paralela al Curso Internacional de Defensa un ciclo de conferencias en el patio de la Infanta de IBERCAJA en Zaragoza. En este ciclo, bajo el título: «La seguridad y defensa: una breve mirada al futuro», los ponentes han trasmitido su experta opinión sobre temas fundamentalmente relacionados con la ética en las operaciones. Esta actividad, después de cinco ediciones, se considera completamente consolidada, gracias a la predisposición de los ponentes que participan en Jaca a reiterar su conferencia ante los zaragozanos, a las facilidades proporcionadas en todo momento por el personal de las instalaciones del patio de la Infanta y por supuesto a la buena acogida por parte del público.

Y como colofón final de esta XXVII edición del Curso Internacional de Defensa, me gustaría expresar mi más sincero agradecimiento a todos los asistentes al curso por el interés y afán de colaboración demostrado en todo momento, a todas las entidades que constantemente nos han mostrado su apoyo, tales como: Palacio de Congresos de Jaca, Unidad de Música de la Academia General Militar, Policía Nacional, Guardia Civil, Policía Local, también al Gobierno de Aragón, Diputación Provincial de Huesca, Ayuntamiento de Jaca, Centro Universitario de la Defensa, Cátedra Paz, Seguridad y Defensa de la Universidad de Zaragoza, Fundación Fernando el Católico, Fundación Manuel Giménez Abad, Obra Social de Ibercaja y la empresa aragonesa ALTUS y no menos importante a los medios de comunicación, que han permitido que el desarrollo de este evento llegue a los ciudadanos, colaborando así al éxito del mismo y a la difusión de la cultura de defensa.

PROGRAMA DE ACTIVIDADES

PROGRAMA DE ACTIVIDADES
Lugar: Palacio de Congresos y Exposiciones de Jaca

Lunes, 30 de septiembre

09:30 h.: Inauguración

10:00 h.: **Amenazas híbridas**
D.ª Elena Gómez de Castro
Directora general de Política de la Defensa del Ministerio de Defensa

10:45 h.: Descanso

Área n.º 1: Mirando al futuro

11:30 h.: **Ética y límites de la libertad de opinión y de prensa**
D. Ángel Gómez de Ágreda
Coronel jefe del Área de Análisis Geopolítico de la División de Coordinación y Estudios de Seguridad y Defensa (DICOES)

12:20 h.: Mesa redonda: **El concepto de lo híbrido: de las amenazas híbridas a la zona gris**

Ponentes:
D. Bonifacio Gutiérrez de León
Coronel subdirector de Investigación y Lecciones Aprendidas del MADOC

D. Josep Baqués Quesada
Doctor en Ciencias Políticas y profesor de la Universidad de Barcelona

Moderador Área n.º 1

D. Carlos M. García-Guiu López
Tcol. director del Dpto. de Ciencias Jurídicas y Sociales de la AGM

14:00 h.: Descanso

17:00 h.: Lectura comunicaciones

19:00 h.: Actividad cultural

Martes, 1 de octubre

Área n.º 2: Amenaza híbrida y ciberdefensa

09:00 h.: **China y Rusia en las zonas grises del ciberespacio**
D. Guillem Colom Piella
Profesor de Ciencia Política en la Universidad Pablo de Olavide y codirector de THIBER

10:00 h.: **Guerra híbrida y ciberespacio**
D. Enrique Cubeiro Cabello
CN. jefe de Estado Mayor del Mando Conjunto de Ciberdefensa

11:00 h.: Descanso

11:30 h.: **Ciberterrorismo y hackivismo**
D. Luis Fernando Hernández García
Coronel jefe del Área Técnica de la Jefatura de Información de la Guardia Civil

12:30 h.: Moderador Área n.º 2

D. Eduardo Rodríguez Rosales
Tcol. profesor del Dpto. de Ciencias Jurídicas y Sociales de la AGM

14:00 h.: Descanso

16:00 h.: Lectura comunicaciones

18:00 h.: Actividad cultural

Miércoles, 2 de octubre

Área n.º 3: Amenaza híbrida y posverdad

09:00 h.: **Posverdad. Antecedentes y situación actual**
D. Emilio Andreu Jiménez
Corresponsal para Asuntos de Defensa de los Servicios Informativos de Radio Nacional de España. Presidente de la Asociación de Periodistas de Defensa

10:00 h.: **La ética militar en los conflictos del siglo XXI**
D. Juan Antonio Moliner González
GD (reserva) subdirector del Instituto Universitario «General Gutiérrez Mellado»

11:00 h.: Descanso

11:30 h.: **Cómo afrontan los medios de comunicación las *fake news***
D. Manuel Campo Vidal
Periodista y doctor en Sociología. Presidente de Next Educación

12:30 h.: Moderador Área n.º 3

D. Carlos M. García-Guiu López
Tcol. director del Dpto. de Ciencias Jurídicas y Sociales

14:00 h.: Descanso

16:00 h.: Lectura comunicaciones

18:00 h.: Demostración empresa ALTUS

Jueves, 3 de octubre

Área n.º 4: Otras amenazas híbridas

09:00 h.: **Riesgos nucleares**
D.ª Natividad Carpintero Santamaría
Secretaria general del Instituto de Fusión Nuclear Guillermo Velarde y académica de la Academia Europea de Ciencias

10:15 h.: **Amenazas económicas**
D. Valentín Martínez Valero
GD (retirado) ex director del Centro de Inteligencia de las Fuerzas Armadas (CIFAS)

11:15 h.: Descanso

11:45 h.: **La Geopolítica de los recursos energéticos**
D. Iván Martén Uliarte
Senior Fellow de ESADEGeo and Senior Partner Emeritus de BCG

13:00 h.: Moderador Área n.º 4

D. José Manuel Vicente Gaspar
Tcol. director del Dpto. de Técnica Militar de la AGM

14:00 h.: Descanso

20:00 h.: Concierto de la Unidad de Música de la Academia General Militar

Viernes, 4 de octubre

Área n.º 5: Europa, España y seguridad

09:00 h.: Mesa redonda: **Situación geopolítica. Entorno europeo**

Ponentes:

Mediterráneo. Una vuelta al horizonte
D. Juan A. Mora Tebas
Coronel (reserva) analista asociado Instituto Español de Estudios Estratégicos

Tráficos ilícitos y redes criminales
D.ª Sonia Alda Mejías
Investigadora principal. Directora del Observatorio de Tráficos Ilícitos y Redes Criminales del Real Instituto Elcano

Moderador Área n.º 5

D. Eduardo Rodríguez Rosales
Tcol. profesor del Dpto. de Ciencias Jurídicas y Sociales de la AGM

11:00 h.: Descanso

11:45 h.: **Incertidumbres y certezas, en el futuro de las Fuerzas Armadas**
D. Fernando Alejandre Martínez
General de ejército jefe de Estado Mayor de la Defensa (JEMAD)

12:00 h.: Despedida: Clausura

COMISIÓN ORGANIZADORA

COMISIÓN ORGANIZADORA

Presidencia

Excmo. Sr. D. CARLOS MELERO CLAUDIO
General director de la Academia General Militar

Excmo. Sr. D. JOSÉ ANTONIO MAYORAL MURILLO
Rector magnífico de la Universidad de Zaragoza

Dirección

Ilmo. Sr. D. MIGUEL ÁNGEL SANTAMARÍA VILLASCUERNA
Coronel director de la Cátedra Cervantes

Excma. Sra. D.ª PILAR ZARAGOZA FERNÁNDEZ
Vicerrectora de Transferencia e Innovación Tecnológica de la Universidad de Zaragoza

Secretaría Técnica

Sr. D. FRANCISCO JOSÉ TRUJILLO PACHECO
Comandante profesor del Dpto. de Humanística Militar

Sr. D. RUBÉN ENGUITA BASCUÑANA
Brigada jefe del Servicio de Publicaciones

Sr. D. JESÚS JAVIER BARRAGÁN PARACUELLOS
Brigada de la Jefatura de Apoyo y Servicios de la AGM

Sr. D. FERNANDO PÉREZ PELLICER
Capitán jefe de Ayudas a la Enseñanza

Sr. D. DAVID MATEO LLANAS
Cabo 1º de la Oficina del CCTV

Sra. D.ª ANA TABORDA GUERRA
Soldado del Servicio de Publicaciones

Sra. D.ª SARA BUÑUALES MARCO
Secretaria de la Cátedra Cervantes

Sra. D.ª ELISA ARNÉS ILLÁN
D.A.C. de la Academia General Militar

Sr. D. JOSÉ CARLOS MARTÍNEZ BENAYAS
C.A.C. de la Academia General Militar

Sr. D. JORGE ALCALDE SANZ
C.A.C. de la Academia General Militar

Sr. D. JOAQUÍN LÓPEZ MARTÍNEZ
C.A.C. de la Academia General Militar

Sr. D. JESÚS AGRELO BARROS
C.A.C. de la Academia General Militar

Mrs. GEORGIA CERVANTES
DC. de West Point (USA)

Mr. JACOB HARE
DC. de West Point (USA)

Mr. PETER KUSICK
CC. de West Point (USA

Mr. CLARK SCALIA
CC. de West Point (USA)

Mr. BENJAMIN SIEGEL
CC. de West Point (USA)

Mr. LUIGI GALZERANO
CC. de West Point (USA)

Mr. KING KEVIN
CC. de West Point (USA)

Mr. WALTER GEORGE
Cadet Saint-Cyr (Francia)

Sra. D.ª ÁNGELA GONZÁLEZ ESPACIO
Soldado de la Jefatura de Apoyo y Servicios

Sr. D. MIGUEL ÁNGEL ASENSIO BAUSET
Cabo de la Jefatura de Apoyo y Servicios

Sr. D. DAVID RODRÍGUEZ GÓMEZ
Cabo de la Jefatura de Apoyo y Servicios

Sr. D. DAVID ALONSO LUJÁN
Cabo de la Jefatura de Apoyo y Servicios

Vocales

Sr. D. JOSÉ MANUEL VICENTE GASPAR
Tte. coronel jefe del Dpto. de Técnica Militar

Sr. D. CARLOS MARÍA GARCÍA-GUIU LÓPEZ
Tte. coronel director del Dpto. de Ciencias Jurídicas y Sociales

Sr. D. EDUARDO RODRÍGUEZ ROSALES
Tte. coronel profesor del Dpto. de Ciencias Jurídicas y Sociales

Sr. D. JOSÉ RAMÓN ORTIZ DE ZÁRATE
Coronel director del Museo y de la Biblioteca

Sr. D. MIGUEL ÁNGEL SALAS HERREROS
Stte. Oficina PLMD S1

Sr. D. SALVADOR IBÁÑEZ SICILIA
Suboficial mayor

Sr. D. CARLOS JESÚS LOSTAO SEGARRA
Capitán jefe Habilitación de la SAECO

Sr. D. JOSÉ MARÍA JOVEN URIOL
Brigada de la SAECO

Sr. D. ANDRÉS COSIALLS UBACH
Profesor del Centro Universitario de la Defensa

Sra. D.ª CLAUDIA PÉREZ FORNIÉS
Directora de la Cátedra de Paz, Seguridad y Defensa de la Universidad de Zaragoza

Sr. D. JAIME SANAÚ VILLARROYA
Profesor titular de Economía Aplicada de la UNIZAR

Sr. D. JUAN FRANCISCO BALTAR RODRÍGUEZ
Vicedecano de Estudiantes y Rel. Institucionales de la Facultad de Derecho de la UNIZAR

Sr. D. NARCISO MANUEL LOZANO DICHA
Profesor Dpto. Dirección de Marketing e Investigación de Mercados de la UNIZAR

Sr. D. ALEJANDRO TOQUERO MATÉ
Periodista Área de Comunicación


EXCMO. AYUNTAMIENTO D
XXVII Curso Internacional de Defensa
Amenaza híbrida. La guerra

Publicaciones de Defensa

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL