ieee.es
Instituto Español de Estudios Estratégicos

Documento
Marco

06/2015 26 de febrero de 2015

*Alfonso Arias Gómez de Liaño**

LA SEGURIDAD EN LAS OPERACIONES EN LOS MEDIOS DE COMUNICACIÓN (OPSEC IN MASS MEDIA)

LA SEGURIDAD EN LAS OPERACIONES EN LOS MEDIOS DE COMUNICACIÓN (OPSEC IN MASS MEDIA)

Resumen:

Es imperativo desarrollar un programa OPSEC. La seguridad en Operaciones constituye un elemento esencial de la planificación y desarrollo de una operación. Ejemplos históricos así lo demuestran siendo numerosos los casos en los que no observar este protocolo ha mermado notablemente e incluso llevado al fracaso la misión.

Las medidas de seguridad deben establecerse a priori. El avance de la tecnología permite transmitir información en tiempo real a cualquier parte del mundo. Según se ha podido comprobar, una vez se vierte la información en internet, es imposible eliminarla por completo, de tal modo que cualquier medida que se adopte con posterioridad llega tarde.

Se recomienda elaborar protocolos escritos y campañas de difusión de medidas de seguridad. La fuga de información no siempre es voluntaria. Informes analizados reflejan que en numerosas ocasiones de manera involuntaria se revelan datos sensibles que pueden comprometer la discreción del operativo, siendo preciso con ello establecer los mecanismos necesarios de protección.

Es preciso revisar con frecuencia todo el proceso. Se consigue así que las medidas de seguridad se adapten a las nuevas realidades y se detecten a tiempo los posibles errores que se hayan cometido.

Abstract:

It is of most importance to develop an OPSEC program. Security Operations is an essential part of planning and development any operations. Historical examples shown that failures in observing OPSEC protocol have led to defeat or, at least, a loose of efficiency.

Security measures must be set up prior in order to be fully operational. Technology advances allow transforming any data into information and sharing it throughout the world in a matter of seconds, without being able to remove it once done. Any measure launched after the disclosure of information through internet has shown to be ineffective.

It is highly recommendable to fulfill and elaborate written protocols and make sure everyone gets the security measures. Informs shown information leaks are not always voluntary or consciously, but it can be very common in unaware personnel who might transmit critical data risking therefore the mission.

NOTA:** Las ideas contenidas en los ***Documentos Marco son de responsabilidad de sus autores, sin que reflejen, necesariamente, el pensamiento del IEEE o del Ministerio de Defensa.

It is also highly recommended to review frequently the whole process, updating the security measures to the real needs in each moment as well as detecting and solving any mistakes or potential failures.

Palabras clave:

OPSEC, seguridad en operaciones, información, operaciones, seguridad .

Keywords:

Operations security, information, data treatment, operations, security.

INTRODUCCIÓN

En plena guerra franco prusiana, tras la batalla de Gravelotte-Saint Privat, el mariscal francés Mac Mahon trataba de reunir lo que quedaba del ejército galo en Bazaine para evitar que los prusianos marcharan sobre París. Sin embargo el mariscal de campo von Moltke estaba al tanto, con lo que pudo concentrar su ataque, obligando a que sus enemigos se retiraran a Sedán, siendo allí donde dos meses después harían prisionero a Napoleón III rindiéndose la capital el 28 de enero de 1871. Esta guerra que duró un año fue tremendamente costosa para Francia, que perdió 138.000 combatientes mientras que los prusianos apenas pasaron de 28.000 y fue precisamente porque los alemanes conocían en todo momento los movimientos del ejército. En contra lo que cabía esperar, tales previsiones no se debían a la labor de inteligencia militar o de algún desertor, sino que era la prensa parisina la que hacía eco de todos los movimientos que su ejército realizaba.

Este ejemplo pone de manifiesto que si bien la comunicación es clave en toda operación, es imprescindible llevar a cabo una serie de medidas de seguridad con el fin de evitar que estos sucesos se repitan. El papel de los medios de comunicación es imprescindible para mantener a la sociedad informada de las acciones que van sucediendo, así como de las medidas que el Estado va tomando. Sin embargo, esta información, al ser accesible por cualquier persona, puede ser analizada por el adversario extrayendo información crítica de tal modo que anule la eficacia del cometido.

La trascendencia es aún mayor, cuando los avances tecnológicos permiten difundir mensajes de forma muy variada y a un inmenso número de consumidores, siendo inviable en muchas ocasiones limitar el mismo al ámbito territorial de un país.

Este artículo tiene por objeto analizar el equilibrio entre información y seguridad operacional, entendida como una relación de mutuo entendimiento y coexistencia de tal modo que, respetándose el derecho a saber, no se perjudique el cometido en cuestión. Con el fin de alcanzar dicha meta, se va a seguir la siguiente estructura:

En primer lugar se analizará todo lo relativo a la seguridad en operaciones, incluyendo unos conceptos previos, que permitan tener un entendimiento común de los términos implicados, tomando para ello como referencia lo que nuestra doctrina entiende como tal, seguido del pensamiento estadounidense y por último, como ente homogeneizador, la OTAN.

Seguirá el planteamiento teórico en el cual se desarrollará el proceso y la estructura encargada de hacerla funcionar, apoyándose en ejemplos para una mejor comprensión.

La segunda parte analiza la situación con los medios, de tal modo que se propondrán una serie de medidas inspiradas en lo dispuesto en otros países, con una especial dedicación a la principal fuente de información de operaciones: el reportero de guerra.

Por último, se planteará la revisión continua del proceso, haciendo hincapié en la necesidad de ser actualizado periódicamente, y lógicamente en los casos de fallos. Igualmente se planteará el exceso de celo como contraposición a la información absoluta, siendo ambos no deseables.

PRIMERA PARTE: SEGURIDAD EN OPERACIONES

Conceptos Previos

El término Seguridad en Operaciones (OPSEC por sus siglas en inglés) es complejo, pues encuadra una gran cantidad de funciones. Existen así mismo numerosas doctrinas que enfatizan o limitan de distinta forma las funciones a desarrollar, si bien cada vez más tienden a normalizarse, sobre todo al amparo de la cooperación internacional derivado de la OTAN. Este mecanismo de protección es desarrollado en el nivel operacional, de tal modo que será el comandante jefe de la fuerza el máximo responsable, incluyendo la acción de todos los miembros componentes de la misma.

Doctrina Española

En el panorama nacional, ya la Doctrina para el Empleo de las Fuerzas Terrestres[1] incluía bajo el apartado *"*Las actividades conjuntas" del capítulo 8 una definición de OPSEC como "el proceso por el que se proporciona la adecuada seguridad a una operación militar mediante el uso de medidas pasivas o activas para negar al enemigo el conocimiento de nuestros dispositivos, capacidades e intenciones*"*. La nueva Doctrina en vigor[2]se refiere como tal "precaverse contra la acción del enemigo" añadiendo lo anteriormente mencionado, e introduce un elemento nuevo: "La seguridad no implica una excesiva precaución". Como se desarrollará más adelante, un exceso en las medidas de vigilancia puede contrarrestar la operatividad necesaria de la operación.

La publicación doctrinal sobre la Protección de la Fuerza[3]sostiene que la seguridad en las operaciones tiene como fin "la aplicación de medidas activas o pasivas para negar al enemigo el conocimiento de nuestros dispositivos, capacidades o intenciones, protegiendo así toda la información relativa a una operación militar:

[1]*PD1-001: Doctrina para el empleo de la Fuerza Terrestre*
[2]*PD1-001 Doctrina para el empleo de la Fuerza Terrestre, 3.3.e Seguridad,* 2011
[3]*PD3-302 Protección de la Fuerza,* 2010

• Las medidas activas tienen como finalidad desorganizar o destruir las capacidades ISR del adversario.

• Las medidas pasivas buscan la protección de la información –que tratarán de obtener las capacidades ISR del adversario para elaborar su inteligencia– mediante la adopción, entre otras, de medidas de seguridad de protección, con la finalidad de proteger los soportes y sistemas de información y telecomunicaciones, el personal, material, instalaciones y actividades dentro de una operación."

La importancia es tal que de ello depende el éxito de la operación, recomendando la DO2-004 en el apartado 14.12 que "cuando la protección no sea posible o la información pueda haber sido comprometida, deberán introducirse en los planes previstos las correcciones necesarias para paliar las consecuencias e incluso, en caso necesario, detener la operación.

En conclusión puede decirse que entendemos OPSEC como un proceso o método adscrito a INFOOPS dedicado a negar información vital al enemigo a través de los mecanismos establecidos. No es por tanto una lista o una serie de instrucciones, sino un proceso que opera continuamente allí donde se desarrolle una operación.

Doctrina Estadounidense

La doctrina de las Fuerzas Armadas de Estados Unidos fue la primera en recoger este concepto a raíz de la Guerra de Vietnam, donde se puso de manifiesto el grave riesgo que entrañaban la información obtenida por el enemigo que llevaba en numerosas ocasiones al fracaso de las operaciones cuando no a un mayor número de bajas.

La Publicación Conjunta de Seguridad en Operaciones[4]establece en el apartado 3 del capítulo I que el propósito de OPSEC es reducir la vulnerabilidad de las fuerzas estadounidenses, la coalición y de las fuerzas combinadas de la explotación de información crítica realizada por el enemigo. OPSEC se aplica a todas las actividades preparatorias, logísticas o fuerzas empleadas durante toda operación. No es extraño que coincida con la doctrina española, al ser fuente de inspiración de la misma. Así mismo se remarca claramente que se trata en todo momento de un proceso de identificación de información crítica constante, por lo que no debe limitarse a un plan de acción previo a la operación sino que durante el transcurso de la misma operará de manera asociada a la acción principal. (*the purpose of OPSEC is to reduce the vulnerability of US, coalition, and combined forces from successful adversary exploitation of critical in formation. OPSEC applies to all activities that prepare, sustain, or employ forces during all operations.)*

[4]*Joint Publication 3-13-3 Operations Security; Chap 1.3,* 2006

La Publicación Conjunta 3-13-1 de Doctrina Conjunta para C2W[5]en el capítulo II ya introducía la OPSEC como un mecanismo cuya misión era forzar al enemigo a tomar decisiones sin la información necesaria o con una información errónea (decepción). La JP 3-13-3 incorpora ese concepto y añade más características al decir que OPSEC se ocupa de identificar, controlar y proteger información desclasificada asociada con operaciones y acciones militares *(is concerned with identifying, controlling, and protecting unclassified evidence that is associated with military operations and activities*).

La Doctrina INFO-OPS de Operaciones de Información[6] considera el OPSEC como una parte esencial de la misma indicando que "la negación efectiva dejará a los oponentes vulnerables para nuestras capacidades ofensivas. OPSEC es el método básico de negación no letal. Se aplica a través de todo el espectro del conflicto". Remarca por tanto que la Seguridad en Operaciones contempla un panorama más amplio que el español al introducir cualquier campo dentro del conflicto y no sólo las operaciones en sí. El capítulo III incorpora esta idea como parte de la Protección de la Fuerza, llegando por tanto del comandante (jefe de operación, no el rango) al soldado al afirmar que "todos los soldados ejecutan medidas OPSEC. Esto incluye un amplio espectro de actividades, desde mantener la discreción con familiares y amigos hasta el enmascaramiento del equipo".

En conclusión, puede afirmarse que el concepto estadounidense de Seguridad en Operaciones va un paso más allá que la concepción española al introducir todos los aspectos relativos al combate y no solo las acciones propias derivadas directa o indirectamente de la operación. Así mismo remarca que se trata de un proceso y no una operación en sí mismo y que involucra a todos los miembros destinados en la zona. Introducen OPSEC dentro de INFO-OPS y describen las características como la negación de información crítica al enemigo, especificando que pueden recurrirse para tal cometido a operaciones de decepción.

Doctrina OTAN

La Alianza Atlántica opera de igual modo que una organización supranacional como puede ser la Unión Europea de tal modo que la legislación española debe operar de acuerdo a la normativa comunitaria. En otras palabras, la doctrina española sobre OPSEC debe casar con la establecida por la OTAN.

[5] *Joint Publication 3-13-1 Joint Doctrine for C2W,* 1997
[6] *FM 3-13 Information Operations doctrine INFO-OPS,* 2003

Se entenderá por OPSEC el "proceso por el que se proporciona la adecuada seguridad a una operación militar o ejercicio mediante el empleo de medidas activas o pasivas para negar al enemigo el conocimiento de los despliegues, capacidades e intenciones propias"[7].

Al mencionar acciones activas se refiere a destrucción física, contramedidas electrónicas (ECM) y operaciones de decepción y psicológicas (PSYOPS). Serán pasivas la seguridad personal, física, documental, enmascaramiento y ocultación.

La base doctrinal de la OTAN introduce junto con OPSEC la Seguridad de Comunicaciones (COMSEC), la Seguridad Informática (COMPUSEC), la Seguridad de Transmisión (TRANSEC) y el Control de Emisiones (EMCON) en un panorama más amplio conocido como INFO-OPS[8]. Tal y como hace Estados Unidos en su concepción de Seguridad de las Operaciones, incluye la decepción como mecanismo necesario y añade que tan importante es durante las operaciones como en los ensayos de las mismas.

Resulta interesante la matización que hace la doctrina Operaciones Conjuntas[9] al decir que deberá establecerse un equilibrio entre OPSEC y operatividad. Es decir, introduce por primera vez la idea de un exceso de seguridad como factor limitador del funcionamiento eficiente del ejército.

A efectos de este documento, se entenderá OPSEC como un proceso asociado a una operación u operaciones destinado a detectar la información crítica, evaluar vulnerabilidades y aplicar medidas tanto activas como pasivas con el fin de negar información crítica al enemigo.

Proceso OPSEC

A día de hoy, la Seguridad de las Operaciones se entiende como un proceso que consta de cinco fases:

1. **Identificación de Información Crítica:** supone determinar los factores clave de la inteligencia, aquellos datos que revelan operaciones, detalles o en definitiva asuntos que, de ser públicos, anulan el efecto o, cuanto menos, lo reducen. Por ejemplo, la pregunta parlamentaria solicitando información sobre los inhibidores que usaba el Ejército en el Líbano, a raíz de un atentado que costó la vida a seis militares[10]:

[7] *AAP-06 Operations Security*, 2008
[8] *AJP-01Allied Joint Doctrine,* 2010
[9] *AJP-3 Allied Joint Operations,* 2011
[10] Rosa Díez González, *Pregunta al Gobierno para la que se le Solicita Respuesta por Escrito,* http://www.upyd.es/fckupload/file/preguntas%20parlamento/Cuerpos%20y%20fuerzas%20seguridad/Preg_Gob_escrito%2008-09-16%20Inhibidores.pdf. Visitado el 13/10/2014

En septiembre de 2008 el grupo parlamentario UPyD registra una pregunta parlamentaria sobre la eficacia de los inhibidores usados en distintas misiones en el extranjero. Al ser formulada en el pleno del congreso, dicha respuesta iba a ser de conocimiento público. En ellas se registraban preguntas del tipo ¿dónde se instalan los inhibidores? o ¿qué frecuencia protegen?

En esta situación el error es en la fase inicial, de identificación de información crítica, pues la respuesta a esas preguntas (de forma cierta, se entiende) conllevó a relevar al adversario vulnerabilidades críticas de Protección a la Fuerza de tal modo que el gobierno, quien responde, no pareció calificar adecuadamente la información solicitada. El error volvió a cometerse en 2013 cuando Unión, Progreso y Democracia volvió a plantear la pregunta en la Comisión de Defensa

2. **Análisis de Amenazas: se sirve de la Inteligencia y Contrainteligencia para responder a preguntas tales como:**
    a. Quién es el adversario.
    b. Qué objetivos tiene.
    c. Cuál es el curso de acción estimado del enemigo (OCOA por sus siglas en inglés, *Oponent Course of Action)*.
    d. Qué información dispone.
    e. Que capacidades tiene.

Es quizá la parte más compleja, pues a menudo no se cuenta con toda la información o incluso pueden darse casos de adversarios no conocidos. En el Caso Gara, el 17 junio de 2014 el periódico publicaba en portada una información asegurando que el Ministerio del Interior había comunicado a "periodistas cercanos" su intención de hacer una redada contra el aparato económico de ETA haciendo especial hincapié en los abogados de la banda[11]. Citaba a su vez nombres propios de los objetivos que iban a verse afectados incluyendo que iba a ser inminente.

En el proceso OPSEC parece lógico pensar que lo que falló fue el análisis de las amenazas, pues no se tuvo en cuenta que un periodista ante todo desea "vender" la información, más aún si es en exclusiva. Puede no obstante deberse a un fallo en las medidas adoptadas, dependiendo una u otra del conocimiento del riesgo que suponía revelar la operación a personas que no necesitaban saberlo de antemano.

[11] S. E. *Gara da el soplo de una inminente operación contra abogados etarras.*http://www.abc.es/espana/20140618/abci-operacion-abogados-gara-201406172118.html. Visto el 13/10/14

3. **Análisis de Vulnerabilidades: se centra en las operaciones o ejercicios y debe responder a:**
    a. Indicadores de información crítica.
    b. Qué indicaciones puede obtener el adversario.
    c. Qué indicadores puede usar.

    Sirva de ejemplo la destrucción de helicópteros de ataque AH-64 "Apache", del ejército de Estados Unidos, en 2007[12]: los sucesos ocurren cuando unos soldados suben a internet unas fotos de la nueva dotación de vehículos aéreos en una base de Irak apareciendo en los metadatos las coordenadas geográficas de la misma. El resultado de dicha filtración involuntaria fue la pérdida de cuatro unidades al ser utilizada la información por fuerzas insurgentes que utilizaron para un ataque con morteros.
    En este caso, el fallo se produce en el análisis de vulnerabilidades, pues no se informó debidamente a la tropa de los riesgos que suponía no desactivar el GPS en los terminales móviles cuando se toman fotos en operaciones, pues adjuntan en los metadatos la citada información desvelando con absoluta precisión la localización real de la instantánea.

4. **Valoración de Riesgos:** consiste en determinar el grado de protección deseable y qué daños serían aceptables. Este aspecto es quizá el más sensible, pues obliga al mando a tomar decisiones sobre qué proteger y qué dejar al descubierto. Se trata de conjugar los medios disponibles para reunir los requisitos necesarios de seguridad. Se apoya por tanto y de manera esencial en el análisis de vulnerabilidades ya que cuanto mejor sea menores riesgos se correrán. Debe tenerse en cuenta que los medios son limitados y a menudo los riesgos sobrepasan las medidas técnicas, por lo que es preciso un cierto grado de decisión política entendida como priorización y protección de elementos. Si proteges todo, no proteges nada, que diría Federico el Grande.

5. **Aplicación de las Medidas OPSEC:** se centra fundamentalmente en
    a. Evitar la detección de indicadores.
    b. Decepción, es decir, confundir al enemigo.
    c. Adoptar más de una medida por vulnerabilidad.

[12] *5 Social Networking Tips for Military Members,* https://www.usaa.com/inet/pages/advice-security-socialnetworkingmilitary?SearchRanking=1&SearchLinkPhrase=advice%20security%20social%20networking. Visto el 13/10/2014

La estrategia a seguir las adopta el mando y debe centrarse en minimizar lo predecible, proteger los indicadores propios y ocultar las capacidades y objetivos.
En el caso del revelado de operación por parte del Gabinete de Comunicación del Ministerio del Interior previa a una operación contra ETA, en enero de 2014 el Ministerio del Interior a través de su cuenta de twitter en la que relataba una operación contra la banda armada ETA antes de que ésta se llevase a cabo. En este caso, realmente lo que falló fue la aplicación de las medidas de seguridad de operaciones y no el proceso en sí, pues fue un desliz en el tiempo y no en la forma o contenido, es decir, se adelantó un acontecimiento que más tarde sería público. Se refleja por tanto cómo aun poniendo todos los mecanismos de protección con un correcto proceso OPSEC, puede fallar por el error humano. No es preciso por tanto revisar todo el proceso, sino vigilar con mayor ahínco para evitar errores futuros.

No debe olvidarse que es un proceso continuo, es decir, constantemente se vuelve al principio y se repite ya que surge nueva información en formatos diferentes y a cada medida el adversario aplicará una contramedida o buscará otra forma de acceder a ella.

Es muy difícil establecer que el éxito de una misión se ha debido a una buena OPSEC, pues de igual modo que ocurre con muchas otras profesiones de carácter defensivo, sabemos cuándo fallan, pero no cuándo aciertan.

En cuanto a los errores, la mayor parte de las ocasiones los fallos en OPSEC traen consigo el fracaso de la operación o, al menos, una pérdida de la eficacia inicial esperada. Sin embargo no hay que olvidar que puede también acarrear un mayor número de bajas. Sirva la referencia histórica como ejemplo de sucesos que aun estando bien planeados y contar con la ventaja cambia totalmente el escenario con un adversario al tanto de los detalles de la operación.

La seguridad operacional es, según puede deducirse de lo expuesto, una doctrina fundamental en todo funcionamiento militar pudiendo además incorporarse a la vida civil tanto a nivel institucional como a nivel empresarial. Su ausencia e inobservancia o su funcionamiento incorrecto no sólo llevará a una pérdida en la eficacia de la operación sino que puede llevar consigo un mayor coste siendo más dramático cuando involucra vidas humanas.

El proceso OPSEC, compuesto por las fases de Identificación de Información Crítica, Análisis de Vulnerabilidades, Valoración de Riesgos y Aplicación de Medidas es una labor que compete en última instancia al oficial encargado de la operación, pero que debe en todo momento involucrar a todo el personal de las Fuerzas Armadas así como aquellas personas que por su función o profesión tengan conocimiento de los detalles críticos. En otras

palabras, tiene una dimensión vertical, implicando tanto a mandos como a tropa; así como horizontal, pues no debe olvidar que el riesgo no viene únicamente de puertas adentro sino que una palabra inoportuna o un desliz informativo pueden acarrear graves consecuencias.

Pese a que la doctrina OPSEC ha evolucionado mucho y se cuenta a día de hoy claramente instaurada en el seno de las Fuerzas Armadas, en mi opinión debe entrar a valorar los riesgos adyacentes a la misión u operación. Esto es, a los medios de comunicación tanto a nivel profesional como a nivel individual/particular al tener un gran poder de difusión.

Responsabilidad de OPSEC

Todo plan tiene siempre un responsable, alguien entre cuyas funciones está la de organizar y hacer efectivas las medidas necesarias para pasar de la teoría a la práctica. En el caso OPSEC las funciones se distribuyen a distintos niveles. De acuerdo con el teniente coronel Fernando Ruano[13] nos encontramos:

- **Director de Operaciones:**
  - Es el responsable último de OPSEC.
  - Designa al personal encargado de OPSEC.
  - Dirige y orienta todo el proceso para el Estado Mayor.
  - Coordina a los niveles inferiores con el fin de adecuar las medidas y asegurarse que el proceso se está realizando correctamente.
  - Nombra a un oficial OPSEC de enlace para los distintos ejercicios u operaciones que se realicen.
- **Jefe de la Fuerza Conjunta:**
  - Apoya el planteamiento OPSEC de los comandantes en misión.
  - Coordina a los subordinados en las funciones OPSEC cuando afecten a varias misiones u operaciones.
  - Determina la información crítica que luego trasladará a los subordinados.
  - Establece las medidas a adoptar para proteger esa información.
  - Edita un anuario revisando el proceso realizado y analiza las enseñanzas aprendidas de los éxitos y fracasos.
  - Instruye en la importancia de OPSEC a los niveles inferiores.
- **Oficial de Programa OPSEC:**
  - Desarrolla y distribuye el material necesario para instruir en OPSEC.
  - Dirige el programa OPSEC.
  - Asesora al mando sobre aquellas materias que puedan precisar OPSEC.
  - Coordina los informes de inteligencia y contrainteligencia.

[13]Tcol Fernando Ruano, *Proceso OPSEC,* OE.55.1.01 OPSEC, 2014

- Coordina el apoyo a la protección a la fuerza, antiterrorismo y seguridad.
- Determina información crítica que sea preciso proteger.
- Coordina la información OPSEC a incluir como crítica cuando se establezcan operaciones conjuntas cívico-militares.
- Incorpora escenarios y simulacros periódicamente a fin de evaluar la preparación.

- **Centro de Inteligencia de las Fuerzas Armadas (CIFAS) y Centro Nacional de Inteligencia (CNI):**
  - Es ante todo un órgano de apoyo para el correcto funcionamiento del proceso.
- **Elementos de Seguridad:**
  - HUMINT
  - OSINT
  - COMSEC
  - SIGINT
  - IMINT

SEGUNDA PARTE: POSIBLES MEDIDAS QUE GARANTICEN EL EQUILIBRIO OPSEC-INFORMACIÓN

Medios de Comunicación

El llamado cuarto poder es frecuentemente olvidado en materia de seguridad de tal modo que es frecuente ver ejemplos de pequeños deslices que acaban en portadas. No debe olvidarse nunca que un medio de comunicación en su mera esencia busca trasladar información a la mayor cantidad de gente posible usando para ello la información más interesante. Los medios además suelen hacerse eco de los fracasos, de las carencias y en general de todo aquello que desvirtúe en gran medida a un servicio, institución o individuo. Rara vez pueden encontrarse noticias que hagan referencia a un éxito, cuando sea algo activo, o a que “todo va bien” en caso de ser pasivo o defensivo.

Recuérdese al mariscal de campo von Moltke, que tuvo conocimiento del movimiento de las tropas enemigas por la prensa de su capital, o las campañas propagandísticas realizadas durante la Segunda Guerra Mundial. A día de hoy los medios cobran aún mayor difusión gracias a internet, con lo que el riesgo de obtener dicha información es nulo.

En un Estado de Derecho como el español, tal y como sucede en las democracias occidentales, llevar un control previo o veto sobre las publicaciones sean del tipo o ideología

que sean (salvo casos ilícitos contemplados en la legislación penal) no es aceptable. Esta situación dificulta la labor OPSEC, pero se incurriría en una paradoja al hacer lo contrario, pues se destruiría aquello que se defiende en última instancia.

Casos como los mencionados arriba, entre otros, ponen de manifiesto la necesidad de tomar medidas para evitar que los fallos cometidos vuelvan a producirse. Realmente conviene centrarse en los supuestos en los que falla alguna parte del proceso, no cuando falla el individuo, pues eso es inevitable.

Dos profesiones entran en aparente colisión: la del oficial u agente encargado de la Seguridad de las Operaciones, uno de cuyos cometidos es velar por la protección de la información crítica de una misión u operación a fin de que el adversario no acceda a ella; y de otro lado la del periodista, cuya función es la de investigar toda aquella información que sea de interés público. No es realmente una colisión, ya que no es función del militar ocultar información que sea de interés al público, pero si hay información sensible que debe salvaguardarse para evitar que el enemigo la conozca. Se trata por tanto de conjugar la balanza de tal modo que ni se caiga en el extremo del absoluto secretismo, más propio de dictaduras, ni se produzca la situación surrealista de acceso absoluto a la información clasificada. Como reza el refrán, uno es esclavo de sus palabras y dueño de sus silencios.

Como regla general opera la concienciación: mejor prevenir que curar. La única medida que puede adoptarse, aparte de revisar continuamente el proceso, es la de instruir a los medios de comunicación de la necesidad de aun conociendo dicha información, no publicarla a fin de no arriesgar vidas humanas a cambio de una mayor audiencia. Debe hacerse notar claramente que dichos datos son igualmente accesibles al enemigo en un mundo globalizado y que por tanto vulnerarían irremediablemente la Seguridad de las Operaciones. Se trataría por tanto de buscar extender la cultura OPSEC más allá de lo estrictamente operacional con el fin de establecer mayores controles antes de que la información sea pública.

Desde el punto de vista legal, el Código Penal actual contempla como delito dos acciones:

- Art. 197-198 del Código Penal: regula el descubrimiento de secretos como la obtención de información secreta sin autorización u consentimiento del afectado, especificando en el art. 197.3 los supuestos de vulneración del secreto en procesos.
- Art. 199-200 del Código Penal: contempla como hecho ilícito el que distribuya o difunda información reservada que conociera con motivo del ejercicio de su profesión, sin consentimiento del afectado.
- Capítulo III del Libro II del Código Penal Militar: bajo el nombre de revelación de secretos o informaciones relativas a la seguridad nacional y defensa nacional castiga

tanto la tenencia ilícita de información confidencial como los casos en los cuales se revela de manera involuntaria.

Pese a ser una medida a "toro pasado" no deja de ser relevante su carácter disuasorio, presente siempre en toda norma penal.

En los países de nuestro entorno como puede ser Estados Unidos, Reino Unido o Francia la legislación correspondiente tanto civil como militar sin que existan diferencias notables salvo la pena concreta. Se enfoca no obstante en un control a los artículos de prensa que parten de fuentes oficiales apoyándose en la censura previa amparada en la protección de la fuerza.

En el caso británico, por ejemplo, las medidas empiezan a incorporarse de manera prioritaria tras la guerra de los Balcanes, donde las fuerzas serbias conocían los movimientos de las tropas a través de información desclasificada. Sin embargo todo indica a que prefieren usar un sistema puntual más allá de establecer un protocolo concreto. Así pues, según refleja Greg Williams[14], en un caso escenario se habría aplicado un doble control en los artículos de prensa a fin de evitar revelar información que pudiera ser crítica siendo responsable el oficial OPSEC y así mismo revisar toda información desclasificada por si pudiera estar erróneamente catalogada o pudiera transmitir información sensible.

Redes Sociales, Blogs y Páginas Web en general

En muchos casos la información llega primero por redes sociales que en los propios periódicos, precisamente porque cualquier persona puede publicar en ellos lo que desee y es además muy accesible para el público en general. Esta ventaja es a su vez un inconveniente ya que resta credibilidad por su falta de profesionalidad de tal manera que muchas noticias que a menudo ante noticias que parecían increíbles o falsas el público esperaba a una confirmación por parte de los medios de comunicación.

En estos momentos Defensa está desarrollando la Doctrina Conjunta de Protección a la Fuerza, con el ánimo de reunir en un único documento las directrices operantes en las Fuerzas Armadas. Este nuevo texto incorporará, previsiblemente, un apartado destinado al estudio de la Seguridad en las Operaciones. Mientras tanto, se deberá acudir a las publicaciones oficiales que tanto el Ejército de Tierra como el Aire han desarrollado.

En Estados Unidos tienen por cada cuerpo un manual que permite informar a los soldados sobre medidas de seguridad generales conciliando su vida digital con la seguridad

[14] Greg Williams, *Operations Security,* http://www.iwar.org.uk/iwar/resources/call/opsec.htm. Visitado el 13/10/2014

operacional. Tomando por ejemplo el Manual de Redes Sociales de los Marines[15] dedica en apenas 48 páginas a recorrer los aspectos más relevantes sobre la materia tratando desde usuarios ocasionales que publican información o comentarios a un perfil más avanzado dedicado a blogs y páginas web.

Una de las primeras ideas es que el marine es la cara del cuerpo, es decir, que representa lo que hay dentro. Hacen especial hincapié en la necesidad de mantener la reputación (la imagen del cuerpo) e insiste además en la importancia de mantener la confianza pública. Son muy conscientes que cuando se critica algo no es lo mismo desde dentro que desde fuera, cobrando mayor relevancia en el primer aspecto. Respetan claramente la libertad de expresión recogida en su Constitución, pero debe relegarse al plano personal. Dicho de otro modo, cuando escribe sobre cualquier aspecto militar como marine, debe hacerlo respetando unos principios generales de seguridad. Así mismo incluye una guía sobre los puntos claves en cualquier publicación y cómo evitar revelar información sensible.

Otro aspecto interesante es que configura a los propios miembros de las Fuerzas Armadas como vigilantes en el sentido de informarles sobre qué hacer en caso de encontrar en internet información que pueda ser sensible.

Con carácter general rige además la *Marine Corps Order 3070.2* que regula el programa OPSEC y entra más a fondo en los conceptos y aspectos que comprenden la disciplina. Por tanto la idea es hacer un manual breve y sencillo con los aspectos más importantes a los que se van a enfrentar con base en la ordenanza o doctrina que regula la seguridad operacional.

No debe olvidarse que a veces el desliz no viene provocado por un miembro del cuerpo, sino que es su familia y allegados quienes publican algo que revele información no autorizada conforme a las reglas OPSEC. En su voluntad de mostrar su apoyo, reconocimiento o afecto pueden poner en riesgo la seguridad, como podría ser dar detalles sobre la localización o la vuelta a casa. Se establece para ello un sencillo decálogo sobre qué publicar y qué no publicar a fin de ser comprensivos tanto con la libertad de expresión como con la seguridad operacional.

Relaciones Personales o Informales

La guardia debe mantenerse en todo momento, pues en un bar o en la calle en general no se sabe siempre con quien se habla y, sobre todo, quien está escuchando. Sobra decir que es de sentido común no tratar temas sensibles en ambientes no aptos para ello, pero pueden no obstante revelarse en información inofensiva a primera vista aspectos que puestos en

[15] *Marines Social Media Handbook,* 2011

conjunción con otros permitan rellenar el hueco que deja la información clasificada, siendo ejemplo de la teoría del mosaico como más adelante se detallará.

Realmente en este caso rigen las reglas generales de comunicación en redes sociales, blogs y páginas web, con la salvedad de que debe hacerse mayor enfoque en el estado del transmisor. En el caso de las redes sociales, por ejemplo, se tiene normalmente mayor tiempo de reflexión que cuando se está cara a cara. A menudo, movidos por sentimientos se hacen comentarios que más tarde se lamentan siendo ya imposible su retirada.

La primera actividad, como ya se ha mencionado, es introducir los mecanismos de protección establecidos para las redes sociales, pues operan de igual manera. Resulta interesante el caso estadounidense, pues una vez más, el propio Estado se encarga de cubrir las relaciones fuera del ámbito militar. En este caso, el "Military OneSource" cumple dicha función, estando adscrito al Departamento de Defensa, al publicar en su página web una guía dirigida a la vida social tanto del funcionario como de su familia. Llama la atención que se centra no sólo en la protección de la información crítica como también en aspectos o detalles aparentemente inocuos pero que analizados por un experto puede suponer información relevante que en conjunto con otras llene el vacío de información que precisa. Esto, que se conoce como teoría del mosaico, será analizado más adelante.

Bajo el título de "Safety Away from Home"[16] el Departamento de Defensa de Estados Unidos dedica una serie de párrafos a las medidas de seguridad a adoptar para proteger información crítica, como por ejemplo, nunca discutir los detalles de una operación o de desplazamientos programados en público. Se especifica además claramente el elemento esencial del espacio, es decir, no se trata de no transmitir esta información a personas desconocidas, sino que también incide en la necesidad de evitar estos asuntos en espacios públicos, aunque sea con miembros de la misma unidad.

Se recomienda además mantener un estado de alerta constante sobre personas que puedan romper el protocolo de OPSEC, ya sea voluntaria o involuntariamente, con lo que se crea una especie de concienciación social del problema.

Pasando al punto de vista civil, esto es, a familiares y amigos del militar, se establece una comunicación en doble sentido oficial y privado, de tal modo que la información es accesible tanto en páginas del Estado como en otras de carácter particular o empresarial dirigidas a un público concreto. En la misma página mencionada se establece un listado de asuntos que no deben, bajo ningún concepto, ser tratados con nadie. Por supuesto dejar por escrito, ya sea de forma tradicional o digital, cualquier información relevante, como pueda ser el destino

[16] *How to Keep Your Family Safe Through Operations Security.* http://www.militaryonesource.mil/deployment?content_id=270487 Visitado el 21/11/2014.

concreto, asuntos relativos a la moral de la tropa, etc. quedan totalmente prohibidos, por su grave riesgo en caso de caer en manos equivocadas.

En páginas web dirigidas al público civil y de carácter privado[17] se encuentra igualmente esta información, bien porque existe una mayor concienciación sobre el asunto o en otros casos porque se hacen eco de recomendaciones realizadas a través de las instituciones estatales.

Tener respuestas preparadas frente a posibles preguntas que puedan "incomodar" resulta también muy útil, pues como refieren muchas de ellas, abordar con naturalidad temas sensibles, respetando la información crítica, dota de seguridad y transparencia, con lo que evita sospechas y preguntas inquisitivas de aquellas personas especialmente curiosas. Es además especialmente recomendado para los introvertidos o en general aquellos que tengan dificultades a la hora de improvisar.

En opinión del autor de este texto, se enfoca demasiado en las medidas de seguridad en detrimento del material que el adversario busca. Por regla general se trata de dar instrucciones concretas para casos concretos, que una vez estos varían pierden eficacia, y dado que el personal afectado no tiene conocimiento sobre la "teoría" queda indefenso frente a los posibles nuevos intentos de obtener información que el adversario realice.

Si bien esto trae consigo una mayor facilidad para el usuario final en tanto que tiene que cumplir con unas reglas, no prepara de cara al imprevisto. Desconocer el porqué de las normas a menudo relaja a los individuos afectados en su cumplimiento, pues se desconoce la importancia real que tienen y además quedan obsoletas en el momento en que las circunstancias cambian.

Se puede citar a modo de ejemplo el *Marines Social Media Handbook*, donde se ponen sobre el papel una serie de reglas concretas al medio sobre el cual tratan de proteger, de tal modo que el lector o el destinatario de ese documento las aplicará como aplica una orden, sin entender realmente el proceso que hay detrás y sin saber adaptarse a las nuevas necesidades conforme nueva información vaya cayendo en sus manos.

No se trata obviamente de que conozcan la información o detalles en cuanto a quién puede estar interesado en hacer daño a la misión. Tampoco se busca romper la disciplina imperante y necesaria en las operaciones. Pero si entienden el fondo del asunto, el porqué es tan importante no revelar esa información así como quién puede estar interesado en la misma logrando con ello no solo una mayor concienciación sino que a instancias propias sean capaces de adoptar medidas más allá de las establecidas.

[17] Operation Military Family. *Operations Security and Personel Security.* http://operationmilitaryfamily.com/opsec-and-persec/ Visitado el 21/11/2014

Relaciones Institucionales

La comunicación es necesaria ya que sin ella no existe operatividad posible. El mando necesita transmitir las órdenes a los subordinados de manera eficaz y rápida, por lo que entra en juego de un lado la rapidez en transmitir el mensaje y de otro la seguridad del canal Esto supone una inversión en cuanto a prioridades, ya que la inversión en uno de ellos avoca necesariamente a una reducción del contrario. Dicho de otro modo, si se prefiere priorizar al máximo la seguridad, nos encontraremos con que la velocidad de transmisión de la información sea tremendamente lenta hasta el punto de llegar tarde; sin embargo, elegir la velocidad sobre la seguridad, puede implicar que el adversario pueda acceder fácilmente al contenido del mismo y por tanto anular el objetivo buscado con la operación. A día de hoy se cuentan con medios suficientes para asegurar una comunicación segura. Sin embargo en algunas circunstancias puede obviarse estas medidas por comodidad. En ese sentido, tomando como referencia Reino Unido, Greg Williams[18], manifiesta la obligatoriedad de usar medios seguros en toda comunicación, sea o no clasificada. Hace además alusión al "*need to know*" que más adelante se analizará.

Bajo este amparo puede caer igualmente la información facilitada de manera oficial a los medios de comunicación, sea del tipo y origen que sean. En el caso español el gran problema es que rara vez ofrecen su versión las personas al cargo o que desempeñen las funciones afectas, de tal modo que son antiguos miembros o en general cualquiera dispuesto a hablar quien transmite información sin que esta haya sido autorizada o revisada. Puede ocurrir por tanto que o bien la información esté falseada o que revele información sensible. Existen aun así las ruedas de prensa y preguntas parlamentarias cuando sean precisas que relegan en la discreción del orador el evitar responder a preguntas comprometidas. En Estados Unidos existe un miembro de una unidad o cuerpo que actúa como portavoz en las redes sociales, páginas web y blogs que transmite de una manera personal la información que estime oportuno, siempre respetando las normas marcadas, así como la información ofrecida con carácter general por los mandos. En estos casos existe un procedimiento concreto para solicitar una entrevista con las personas autorizadas y en muchas ocasiones éstas se contestan por escrito, facilitando así un mejor mecanismo de control.

Resulta interesante además el caso británico, donde se establecen unos Elementos Esenciales de Información Amistosa[19], (*Essential Elements of Friendly Information, EEFI* por

[18]Greg Williams, *Operations Security,* http://www.iwar.org.uk/iwar/resources/call/opsec.htm. Visitado el 13/10/2014
[19]Greg Williams, *Operations Security,* http://www.iwar.org.uk/iwar/resources/call/opsec.htm. Visitado el 13/10/2014

sus siglas en inglés*)* que dan una serie de consignas generales sobre qué se puede contar y qué no, en relación a misiones concretas.

Especial Referencia al Reportero de Guerra

La relación entre los medios de comunicación y los conflictos bélicos ha estado siempre presente. Cuando Cayo Julio César realizaba sus hazañas en las Galias, mandaba informes a Roma para que estos engrandecieran su prestigio. Aquí yace el primer escollo que ha de abordar cualquier reportero, la descripción de los hechos. En este caso, el objeto de los despachos mandados no era la guerra en sí, sino cómo había contribuido el ingenio militar del general a ganarla. Igualmente, los cónsules romanos y en general cualquier oficial o magistrado imperial debía rendir cuentas ante el Senado, órgano que reflejaba el parecer del pueblo y que de algún modo permitía conocer los asuntos oficiales. Posteriormente lo expresado en estas audiencias era pregonado al pueblo en las plazas en una suerte de "diario" verbal, pero poco a poco, lo que en un principio trataba de engrandecer a los personajes públicos, fue convirtiéndose en un medio de supervisión y aprobación social.

La figura del reportero de guerra, concebido como un periodista dedicado en concreto y casi en exclusiva a relatar los acontecimientos de una contienda, nace a finales del s. XIX cuando William Randolph Hearst destacó a un corresponsal en La Habana con la función de relatar todos los detalles de la guerra hispanoamericana.

No es hasta la Guerra de Vietnam cuando surge el gran hito del corresponsal de guerra, donde Estados Unidos otorgó una gran cantidad de permisos para que los medios pudieran informar de lo que observaran en el campo de batalla. Pese a la falta de medios y a la inexistencia de la televisión en el terreno, el público pudo leer relatos de primera mano, comentando el día a día de las tropas, apoyado puntualmente por fotos. Éstas, no obstante, fueron suficientes para que la gente viera el horror de la guerra, el enorme coste humano y la incapacidad estadounidense de ganar la guerra. La falta de preparación tanto de los profesionales de la información como del público pudo en gran medida mermar el apoyo a una guerra que ya en un primer momento no había gozado de gran popularidad. Todo ello promovió una enorme oposición a la contienda que obligó a Estados Unidos a retirarse finalmente de Vietnam.

El s. XXI y las nuevas tecnologías han permitido que a día de hoy se vea con gran claridad lo que está ocurriendo en cada conflicto mundial, gracias a sus impactantes imágenes. Esto, sumado a una sociedad cada vez más concienciada con el entorno global, que busca una información más completa, en el mismo escenario en que se producen. El periodista, que busca satisfacer la demanda de su público con el objetivo de saltar a los medios y labrarse

una carrera, se ve obligado a adentrarse en la zona de conflicto, poniendo en riesgo su vida y la de aquellos que le rodean.

Según afirma Plate[20], existen dos clases de periodistas: los primeros, que son expertos en la materia, que mantienen contacto con sus homólogos en el país y conocen al menos los datos más esenciales del país; y el segundo grupo, de pseudoperiodistas, que acuden al lugar del desastre sin conocer realmente dónde se encuentran y sin saber qué sucede realmente. Son estos últimos los que más peligro tienen, pues tal como afirma el mencionado autor, están presionados por sus jefes en sus países para obtener historias sensacionalistas que justifiquen los gastos.

Como relata el periodista Hernán Zin[21], "mucha gente cree que por ir a la guerra ya tienen que publicarte". Los grupos terroristas ven en estos “lobos solitarios” el objetivo perfecto, pues son un blanco fácil, casi siempre desarmado y con claros visos de no ser un problema durante el cautiverio.

Si bien la función de los profesionales de los medios de comunicación es esencial para relatar lo que sucede en los conflictos, denunciar los abusos y explicar a su público el cometido de las fuerzas armadas, no debe olvidarse que suponen un riesgo añadido al desarrollo operacional, pues obliga al personal militar y diplomático a prestar parte de su tiempo y recursos en su protección casi en exclusiva cuando se produce algún secuestro.

Debe recordarse que la entrada a un país en guerra sigue siendo un asunto de extranjería, por lo que el país de destino debe autorizar la entrada, sin embargo muchas veces la negativa del gobierno o la falta del mismo obligan a estos profesionales a buscar medios alternativos -menos seguros- de acceder de manera ilegal al país. Sirva de ejemplo el caso de Bünyanim Aygün[22], reportero turco que fue secuestrado por milicianos del ISIS cuando intentaba acceder a Siria a invitación de sus futuros secuestradores para realizarles una entrevista. Igualmente los enemigos actuales a los que hacen frente las potencias occidentales ya no son gobiernos y países en sí, sino grupos terroristas de grandes envergaduras capaces de poner en juego la seguridad internacional.

El caso de Espinosa y García Vilanova, ambos corresponsales españoles, fue traumático para ellos, su familia y en general la sociedad española, que exigía una acción del gobierno que permitiera su pronta vuelta a casa. En la mayoría de casos, pese a no existir confirmaciones

[20] Cristoph Plate, *Los informes de los periodistas no pueden evitar los conflictos,* https://www.icrc.org/spa/resources/documents/misc/5tdp95.htm. Visitado el 21/11/2014
[21] Hernán Zin, *Los corresponsales de guerra no son Indiana Jones,* http://www.elmundo.es/television/2014/04/26/535bc5b0e2704ef7118b457a.html. Visto el 13/10/2014
[22] Lluís Miquel Hurtado, *Secuestrado en Siria el fotoperiodista turco Bünyamin Aygün,* http://www.elmundo.es/internacional/2013/12/18/52b19e0a268e3ec44b8b4576.html. Visto el 13/10/2014.

oficiales, los secuestros acaban con el pago del rescate por parte de los gobiernos, siendo excepcional las operaciones de rescate, pues su riesgo es excesivamente elevado (un fracaso automáticamente supone la ejecución del rehén así como otras medidas que los secuestradores adopten a modo de represalia)[23].

Pese a que podría considerarse "rentable" el pago de estos rescates que visto desde los fríos números no es más que un precio desorbitado por la noticia, el dinero que obtienen de estos son fuente primaria[24] que financia sus actividades terroristas dotándoles de una mayor operatividad así como "dinero fácil" al existir un riesgo bajo.

Todo esto supone un mayor riesgo a la seguridad, pues el periodista en busca de la noticia puede caer imprudentemente en “trampas” que acaben con su secuestro, obligando a activar un plan especial para su rescate. Así mismo, pueden encontrarse en posesión de información sensible tales como localizaciones de campamentos, metodología operativa, vulnerabilidades de complejos, etc. que caiga automáticamente en manos de sus secuestradores.

Así mismo el periodista entra en contacto con información directa, no existiendo ningún tipo de control o filtro sobre la misma, con el riesgo de que descubra información reservada. Tómese como ejemplo el reportero, que en una entrada ilegal a un país en conflicto, se tope con un despliegue sorpresa de fuerzas aliadas en preparación de una operación. La falta de conocimiento de la situación que se está desarrollando frente a él junto con las nuevas tecnologías que le permiten transmitir una noticia en el acto, puede desbaratar el factor sorpresa que buscaba la acción militar.

El corresponsal de guerra no es por tanto parte del problema o de la solución, sino que es el individuo quien a través de sus decisiones contribuye a la seguridad o la pone en riesgo.

Las medidas al respecto parten de una decisión política. Esto es, decidir si se desea primar la información sobre la seguridad o al revés. Tomando de ejemplo Estados Unidos, el Departamento de Defensa permite incrustar (*“embedded”)* reporteros en unidades de combate. Pese a ser una decisión interesante desde el punto de vista informativo, las cifras desaconsejan tal opción, pues la ratio de bajas es del 0.43% frente al 0.07% del personal militar[25].

---

[23] EFE, *El rescate de Denis Allex acaba en desastre,* http://www.abc.es/internacional/20130112/abci-muere-rehen-frances-somalia-201301121047.html. Visto el 13/10/2014

[24] BG Ricardo Charry Solano, *Los rescates como financiamiento al terrorismo,* http://www.cemil.mil.co/?idcategoria=349445. Visto el 14/10/2014

[25] M. A. Ballesteros. *Los reporteros de guerra.*http://elpais.com/diario/2003/05/19/sociedad/1053295204_850215.html. Visto el 30/10/2014

Según lo expuesto, todo parece indicar que debe priorizarse la seguridad frente a la información, no ya solo por salvar vidas, sino por evitar que información sensible pudiera caer en manos de individuos no autorizados. Esto no debe entenderse como censura u ocultación de actividades, pues no tiene como fin ocultar las acciones llevadas a cabo, sino más bien ofrecer dicha información a través de canales seguros que garanticen la integridad física de los periodistas así como evitar la fuga de información crítica.

Por todo ello, se recomienda establecer cursos orientativos para cada operación que pongan al personal afectado en conocimiento de las medidas de seguridad necesarias para un desarrollo seguro de la profesión de los involucrados. El conocimiento de las zonas seguras, de los grupos o facciones en conflicto así como toda aquella información que pueda poner en corriente a los periodistas antes de embarcarse en su labor puede ser crucial a la hora de prevenir tanto las bajas como los secuestros.

Así mismo, sería interesante valorar la adopción de medidas que desincentiven las prácticas furtivas de periodismo consistente en la entrada ilegal a países en guerra, poniendo por ejemplo ruedas de prensa en lugares seguros donde puedan ver satisfechas todas sus preguntas siempre y cuando no afecten al desarrollo de OPSEC como medida proactiva; y la concienciación sobre los peligros del secuestro y su elevado coste de resolución, como medida preventiva.

Estas medidas deben ser también bilaterales ya que en definitiva el periodista tiene una labor que realizar. Si se les involucra en el desarrollo de las medidas de seguridad, que al fin y al cabo ellos son los primeros interesados, se logrará un mayor compromiso y sobre todo poder atender sus necesidades en la medida de lo posible.

La seguridad es una labor de todos, involucra y afecta a cada individuo tanto colectivamente como individualmente, pues como se suele decir, la fortaleza de una cadena la determina el eslabón más débil.

Need to Know & Duty to Share

Aquellas personas que prestan servicios en OPSEC o en general en cualquier organización o institución con información clasificada precisan para acceder a la misma de unas credenciales, conocidas en el argot como *security clearance*. Se trata de un estatus alcanzado cuando tras una investigación el sujeto en cuestión reúne los requisitos necesarios para poderle ser confiados materiales reservados. Es algo así como un “pasaporte” que permite acceder a áreas restringidas precisamente como mecanismo de seguridad.

Si bien esta credencial da acceso a un sinfín de información, surge un nuevo obstáculo que viene a regular el acceso a la misma, pues a mayor número de personas que conozcan el

secreto, mayor riesgo de fuga hay. Como dice Richard A. Best[26] "tener una *security clearance* no es, por supuesto, suficiente para tener acceso a la información sensible; es preciso que a su vez exista la necesidad de conocer" (*Having a clearance is not, of course, sufficient to gainaccess to sensitive information; there must also be a need to know*). De este modo quien opere OPSEC en el Líbano no tiene necesidad de conocer lo que su homólogo haga en Mali, pues aun teniendo el mismo rango y nivel de seguridad, no precisa de su información para funcionar en su puesto. Puede ponerse a modo de ejemplo el Caso Snowden, donde tenía acceso a una gran cantidad de información clasificada sin que la mayor parte de ésta fuera necesaria o útil a su labor como analista.

Junto a este concepto nace el *Duty to Share (o Need to Share)* como respuesta a los sucesos del 11 de septiembre de 2001 en Nueva York. Las dos investigaciones parlamentarias realizadas por Estados Unidos trajeron consigo, tal y como señala en el mismo documento Richard A. Best, resultados asombrosos: toda la información necesaria para parar o al menos reducir los daños de los atentados estaba diseminada entre las distintas agencias de inteligencia si bien por exceso de celo o por carencias colaborativas no permitieron reunir todas las piezas y ver el puzle.

Es por ello que se reforma todo el protocolo añadiendo la otra cara de la moneda al *Need to Know*. Si un agente o agencia tenía conocimiento de una información que podía interesar a otro departamento, éste debía dar traslado de la misma a su destinatario final. En otras palabras, buscar un interés nacional más allá del de la propia organización.

Aplicado a OPSEC supone un contrapeso a la mencionada necesidad de saber que permite operar como una verdadera fuerza conjunta. Tomando el ejemplo anterior, si bien no precisa de toda la información el oficial de OPSEC en el Líbano, quizá si precise conocer de los medios que dispone o en general la fase de análisis de las amenazas cuando un adversario sea común porque opere en ambos países.

Quizá dicha cooperación necesaria sólo sea aplicable en el análisis de amenazas, pues la información crítica sería puntual de cada operación, de igual modo que las vulnerabilidades (salvo el uso conjunto de un procedimiento o herramientas) y las medidas a adoptar. Si puede no obstante ser de interés la creación de un protocolo frente a vulnerabilidades comunes o trabajar en escenarios a fin de ofrecer una guía no vinculante que permita cuanto menos inspirar o preparar al oficial OPSEC para el desempeño de sus funciones de campo.

En conclusión a este apartado, debería en mi opinión reforzarse esta idea proveniente del mundo anglosajón con el fin de crear una verdadera fuerza conjunta que si bien guarde sus

[26] Richard A. Best Jr. *Intelligence Information: Need to Know vs. Need-to-Share,* http://fas.org/sgp/crs/intel/R41848.pdf. Visitado el 13/10/14

secretos lógicamente en el amparo de OPSEC, tenga en cuenta que su labor realizada no solo puede proteger la misión u operación en su territorio, sino que puede conocer o dar a conocer información relevante a otros oficiales de OPSEC que traiga consigo un mejor análisis de amenazas. Aplicando el proceso OPSEC se podrán detectar los riesgos y establecer medidas que contrarresten las vulnerabilidades, como puede ser la información susceptible de ser intercambiada o no.

Teoría del Mosaico

Esta idea parte de información que por sí sola carece de interés estratégico, pero que añadida a un conjunto de ellas o mediante la elaboración de inteligencia sobre ellas puede rellenar el espacio creado por una información clasificada.

El concepto nace nuevamente en Estados Unidos dentro de la política de inteligencia como escudo a la filtración de determinada información que aun siendo aparentemente inocua, en un conjunto y siendo el observador una persona cualificada podía desvelar información sensible, tal y como opina David E. Pozen[27], permitiendo al gobierno, a través de sus agentes, bloquear la publicación de los datos.

Tómese como ejemplo la publicación de detenciones realizadas en el marco de una operación anti-terrorista. El hecho aparentemente no reviste de interés desde el punto de vista OPSEC, pues la operación ha concluido. Sin embargo tal hecho puede revelar una campaña dirigida a contrarrestar la fuerza de dichos grupos de tal modo que ponga en alerta a los objetivos de otras organizaciones. Puede incluso, extrapolándose un poco, animar a bandas armadas más pequeñas al entender que los recursos están centrados en las grandes organizaciones y por tanto sus crímenes van a quedar impunes.

En el ámbito militar estricto, podría servir la publicación de maniobras conjuntas en un escenario concreto que se asemeje a un país hostil, conjuntamente con acuerdos en materia militar. Estos ejemplos meramente teóricos en la práctica son pequeños detalles irrelevantes que permiten llegar a esas conclusiones y por tanto poner en riesgo todo el plan.

Resulta muy difícil encontrar una solución adecuada a este problema. Realmente siempre existe este riesgo, ya que incluso la teoría del mosaico no siempre se ha probado eficaz y roza además con prácticas ilegales como la censura previa.

En mi opinión, la teoría del mosaico debe únicamente invocarse cuando realmente sea la única forma que disponga el adversario para conocer de la información crítica debiendo adecuarse la técnica y el tiempo a la información revelada. Puede así mismo generarse un

[27] David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act,* http://www.yalelawjournal.org/pdf/358_fto38tb4.pdf. Visitado el 13/10/2014

mayor ruido con respecto a otras operaciones, dotándoles de mayor relevancia de la que realmente tienen, o incluso valorar la posibilidad de utilizar la información como decepción.

TERCERA PARTE: REVISIÓN CONTÍNUA Y EXCESO DE CELO

Revisión Continua

Un buen protocolo, por muchos riesgos que haya evitado o por la falta de los mismos debe ser revisado periódicamente de cara a analizar nuevamente el proceso. No existe un tiempo o un periodo de vigencia, pero puede observarse que, cuanto más precisa es la medida o más concreta la información, mayores cambios sufre. No es lo mismo la información crítica del funcionamiento de un arma, o de una unidad, que tiende a ser estable en el tiempo, como los detalles sobre las maniobras que se van a realizar en un momento dado, que se consume en el mismo momento en que estas se realizan.

La información crítica, las amenazas y los riesgos van cambiando, con lo que lógicamente las medidas deberán adaptarse a las nuevas necesidades. Por poner un ejemplo, las diversas doctrinas que contemplan OPSEC en líneas generales suelen tener una vigencia de entre uno y cinco años. Las medidas concretas sobre misiones por regla general se adoptan *ad hoc* de manera verbal o con breves notas, precisamente para no dejar rastro. Su corta duración, que va asociada tanto a la misión como a la información, en ocasiones no permite revisiones, si bien son siempre recomendables en la medida de lo posible.

Aun con todo el proceso OPSEC bien realizado y la adopción de las medidas oportunas, existen los fallos (generalmente cadenas de fallos) que derivan en fracasos operacionales y en algunos casos pérdidas de vidas humanas. Una vez finalizada la crisis es preciso revisar las causas que llevaron a esa situación y será muy importante ver exactamente si lo que falló fue el proceso, las medidas adoptadas o fallos individuales, pues un fracaso bien analizado y contrarrestado puede suponer mayores éxitos en el futuro o que, cuanto menos, no se vuelva a repetir.

Es muy importante realizar un análisis objetivo que cuente tanto con la participación de aquellos que estuvieron a cargo como un punto de vista externo que permita dar un enfoque distinto y más centrado. Una vez realizado deberán depurarse las responsabilidades correspondientes en su justa medida, es decir, aceptando que la gente comete fallos. Así mismo, en opinión del autor, un fallo salvo casos de excepcional gravedad en los cuales se deriva incluso responsabilidades criminales, y siguiendo la máxima de “se aprende más de los errores que de los aciertos” el responsable no queda incapacitado para el desempeño de sus funciones sino que todo lo contrario tiene una experiencia preciosa a explotar y que muy

probablemente le permita no solo evitar con mayor ahínco fallos futuros sino que podrá prever otros futuros.

Exceso de Celo

El análisis post-crisis que sucedió a los ataques terroristas del 11 de septiembre de 2001 en Estados Unidos reveló que las agencias de inteligencia tenían en conjunto la información necesaria para prevenir o al menos reducir el efecto de la operación. "La virtud está en el término medio" que diría Aristóteles.

El exceso de celo o la falta de comunicación entre las agencias fue lo que en gran medida motivó el fallo de seguridad que costó la vida a tres mil personas, como refiere la comisión de investigación llevada a cabo con posterioridad a fin de evitar que los sucesos volvieran a producirse. Pese a tratarse de información clasificada, si ha podido saber que las tres grandes agencias involucradas en el desastre fueron la CIA, la NSA y el FBI, cuya relación se detalla a continuación.

Perter Bergen[28] informa que en la primavera de 2001 la CIA tenía información relativa a Bin Laden sobre “múltiples operaciones” y “ataque inminente” sin que compartiera dichos datos con otras agencias. Así pues, no informó al FBI sobre al menos dos de los secuestradores de los aviones. Tampoco les informó de Mihdhar y Hazmi, dos sospechosos de terrorismo.

Los entonces sospechosos, con su nombre real, conocido por la CIA, pudieron alquilar apartamentos, obtener el carnet de conducir e incluso aprender a volar en California, pero sus nombres no fueron transmitidos a las autoridades locales, con lo que tuvieron total capacidad operativa para atentar contra el Pentágono matando a 189 personas.

Como posteriormente reconocería el Inspector General de la CIA[29], “haber informado al FBI así como una buena coordinación entre ambos podría haber resultado en una correcta vigilancia a al-Mihdhar y a al Hazmi. Potencialmente se había podido obtener información sobre el motivo del entrenamiento de vuelo, su financiación y conexiones con los otros involucrados en los ataques del 11 de septiembre de 2001.” *("informing the FBI and good operational follow-through by CIA and FBI might have resulted in surveillance of both al-Mihdhar and al-Hazmi. Surveillance, in turn, would have had the potential to yield information on flight training, financing, and links to others who were complicit in the 9/11 attacks.")*

[28] Peter Berger, *Would NSA surveillance have stopped 9/11 plot?* http://edition.cnn.com/2013/12/30/opinion/bergen-nsa-surveillance-september-11/. Visitado el 21/11/2014
[29] *OIG Reporto n CIA Accountability With Respect to the 9/11 Attacks.* http://www.washingtonpost.com/wp-srv/politics/documents/cia_accountability_report_082107.pdf. Visitado el 23/11/2014

El entonces director del FBI, Robert Mueller, manifestó su opinión al respecto[30], indicando que, de haber transmitido la información disponible de la CIA a la NSA, se podría haber realizado una operación de vigilancia telefónica con los medios que disponen. En concreto, referenciando a servicios de inteligencia de Oriente Medio que habían localizado un piso franco de los terroristas en Yemen, "se entendió que esa casa tenía un teléfono, pero no podían saber quién llamaba al mismo. Se descubrió después que había sido al-Mihdhar, desde San Diego en Estados Unidos. Si se hubiera montado el programa a tiempo, se podría haber detectado el número particular de San Diego" *("They understood that that al Qaeda safe house had a telephone number, but they could not know who was calling into that particular safe house. We came to find out afterwards that the person who had called into that safe house was al-Mihdhar, who was in the United States in San Diego. If we had had this program in place at the time, we would have been able to identify that particular telephone number in San Diego."*)

Como reconoce Bergen, de acuerdo con la conclusión extraída de todos los análisis post crisis que se realizaron, el principal error fue la falta de comunicación de la información relevante por parte de la comunidad de inteligencia de Estados Unidos. De hecho, el principal problema de los oficiales de contra-terrorismo no es la falta de información sino la falta de comunicación entre sus homólogos, pues existe un término medio que respeta OPSEC y a la vez permite un buen funcionamiento de los organismos, especialmente si existen varios dedicados a funciones similares.

Estados Unidos, con el fin de evitar que los mismos errores se cometieran en un futuro, fomentó la cooperación interinstitucional favoreciendo así una respuesta más eficaz. La ley de Reforma de la Inteligencia y Prevención del Terrorismo[31] creó en 2004 el despacho del Director Nacional de Inteligencia como jefe y coordinador de las dieciséis agencias de inteligencia, siendo además el principal asesor del Presidente en el Consejo de Seguridad Nacional y en el Consejo de Seguridad Interior.

*Alfonso Arias Gómez de Liaño**
Alumno en prácticas en el IEEE

i

NOTA:** Las ideas contenidas en los ***Documentos Marco son de responsabilidad de sus autores, sin que reflejen, necesariamente, el pensamiento del IEEE o del Ministerio de Defensa.

[30] *Oversight of the Federal Bureau of Investigation.* http://www.fas.org/irp/congress/2013_hr/fbi-hjc.pdf. Visitado el 23/11/2014

[31] *Intelligence Reform and Terrorism Prevention Act of 2004.* http://www.gpo.gov/fdsys/pkg/PLAW-108publ458/pdf/PLAW-108publ458.pdf. Visitado el 23/11/2014