U N I V E R S I D A D A U T Ó N O M A D E M A D R I D

La_SEI
School of Economic Intelligence & International Relations
Escuela de Inteligencia Económica y RRII
Universidad Autónoma de Madrid

Enero 2022

Volumen 9
ISSN 2660-7352
Editados por la Escuela de Inteligencia Económica y RRII
Editor Jefe / *Chief Editor*: Ángel Rodríguez García-Brazales

REPORTS DE INTELIGENCIA ECONÓMICA Y RELACIONES INTERNACIONALES

La contrainteligencia como protección a la organización

José Manuel Veiga Torres

Todas las organizaciones, ya sean empresas privadas u organizaciones públicas, se enfrentan a multitud de amenazas que afectan al normal funcionamiento de la organización. La continuidad del negocio debe ser una de las prioridades de cualquier entidad. Entender a qué nos enfrentamos, cuáles son nuestras vulnerabilidades y cómo las podemos hacer frente, debe ser la finalidad de cualquier departamento que se dedique a proteger a una organización de las amenazas, ya sean estas internas o externas. Contar con un sistema holístico que incorpore aspectos de contrainteligencia y seguridad, permitirá tener herramientas suficientes como para afrontar con confianza los retos que se presentan para que una organización esté protegida.

Universidad Autónoma de Madrid UAM

La SEI
School of Economic Intelligence & International Relations
Escuela de Inteligencia Económica y RRII
Universidad Autónoma de Madrid

Título: *La contrainteligencia como protección a la organización*

Autor: José Manuel Veiga Torres [1]

Volumen nº: 9

ISSN 2660-7352

Reports de Inteligencia Económica y Relaciones Internacionales

Editor Jefe: Ángel Rodríguez García-Brazales

Editada por la:

Escuela de Inteligencia Económica y Relaciones Internacionales
Universidad Autónoma de Madrid
Campus de Cantoblanco
C/. Francisco Tomás y Valiente, nº 11, Edificio C, planta 3ª
28049 MADRID (SPAIN)

[1] Comandante del Ejército de Tierra. E-mail: josemanuelv8518@gmail.com

Contenidos

1. Introducción

El ser humano siempre ha tenido necesidad de protegerse, de mantenerse seguro ante los peligros. Empezaron utilizando cuevas para estar a salvo de las inclemencias meteorológicas, de los animales depredadores o de otros grupos rivales. Posteriormente, y a medida que el hombre comenzaba a utilizar la tierra para cultivar y se establecía en los valles, empezó a utilizar empalizadas temporales con los medios naturales de los que disponía.

Cuando las sociedades evolucionaban se hacían sedentarias y se establecían comunidades más complejas, en ese momento, el ser humano empezó a construir muros más sólidos, primero de adobe y madera y después de piedra. A medida que pasaba el tiempo las murallas se transformaron en fortificaciones que aumentaban su complejidad para hacerlas inexpugnables al enemigo, o al menos, retrasar su penetración para propiciar una mejor defensa. Además, establecían puestos avanzados en atalayas para saber lo antes posible cuando se acercaba el enemigo.

Toda esta estructura defensiva se completaba con fuerzas de reacción, que en un primer momento respondían a los ataques desde el interior de las fortalezas, cuando los atacantes se concentraban en las murallas o sus proximidades. Si tenían la posibilidad de ser advertidos con antelación, por medio de puestos avanzados, atalayas o incluso espías, podían hacer frente al agresor antes de que éste llegara a las puertas de la ciudad o fortaleza. En ocasiones, intentaban engañar al atacante para que plantara batalla en un terreno que favoreciera al defensor, o los canalizaban para conseguir una posición dominante.

En definitiva, el ser humano ha buscado proteger a su clan, tribu, poblado, ciudad o estado de la acción de amenazas para poder continuar con su actividad como sociedad. Esta lección histórica nos muestra el camino que todas las organizaciones y empresas deben seguir, precisamente para eso, para permitir la continuidad de la actividad, en este caso, como organización.

Desde el punto de vista histórico se identifica que la protección de las comunidades se articula en acciones defensivas y ofensivas. **Las acciones defensivas** tienen las finalidades de hacer ver al agresor, por medio de gruesos y altos muros, que el ataque sería muy costoso y no merecería la pena intentarlo. También permitiría identificar cuándo se está produciendo un ataque, y finalmente, posibilitaría la derrota del agresor una vez el ataque ha comenzado. Esto es, **disuasión, detección y neutralización**.

Por otra parte, **las acciones ofensivas** tenían como finalidades identificar lo más temprano posible, antes de que se materializarse el ataque, las intenciones del atacante, posibilitar su derrota lo más alejado posible de nuestra fortaleza y hacer que éste tome decisiones que nos favorezca en la defensa. Esto es, **detección, neutralización y decepción**. Estas acciones ofensivas eran las que marcaban la diferencia y se constituían en la clave del éxito de la protección.

Para estandarizar el significado de estos cuatro términos que constituyen la piedra angular sobre la que se va a construir la protección de las organizaciones, conviene acudir al Diccionario de la Real Academia Española (RAE):

- **Disuadir**: inducir o mover a alguien a cambiar de opinión o a desistir de un propósito.

- **Detectar**: descubrir la existencia de algo que no era patente.
- **Neutralizar**: contrarrestas el efecto de una causa por la consecuencia de otra diferente u opuesta; o en una segunda acepción: anular, controlar o disminuir la efectividad de algo o de alguien considerados peligrosos.
- **Decepción**: engaño, a su vez, engaño es hacer creer a alguien que algo falso es verdadero.

Son los elementos de disuasión, detección, neutralización y decepción, agrupados en acciones defensivas y ofensivas la base del modelo de contrainteligencia que identifica Hank Prunckun (Prunckun, 2019). Prunckun limita la contrainteligencia a contrarrestar la intención del adversario o del personal propio de hacerse con información de la organización. Sin embargo, este artículo pretende ampliar este concepto.

Para desarrollar un modelo holístico de protección es necesario contemplar otras amenazas, no solo contra los accesos a la información propia, sino toda aquella actividad que busque impedir o limitar la capacidad de nuestra organización de desarrollar su actividad normal (Blanco Iñigo, 2018), defendiendo sus propios intereses frente a los esfuerzos de otros por conseguir los suyos (Sanchez Gamboa, 2016), esto es, defender su capacidad de operar con normalidad, libre, o al menos con riesgos controlados.

Además de estos cuatro términos vamos a introducir un quinto elemento, prevención, íntimamente ligado a la disuasión y detección (van Genderen, 2018). La RAE define prevención como preparación y disposición que se hace anticipadamente para evitar un riesgo o ejecutar algo.

2. Desarrollo del modelo holístico de contra-inteligencia

Se parte de la base de que la finalidad buscada es proteger la capacidad operativa o de operar de una organización, ya sea esta una empresa, una organización pública o un ente privado. Una vez en este punto nos debemos preguntar ¿qué puede perjudicar el normal funcionamiento de una organización? cuestión que nos lleva a dos respuestas, por un lado, causas naturales o accidénteles, en el que no hay un actor malicioso. Y, por otro lado, actores internos o externos que intenten impedir o dificultar el normal funcionamiento de la organización u obtener una ventaja explotando su conocimiento. El desarrollo de este concepto de contrainteligencia se centra principalmente en los riesgos derivados de la actividad de actores maliciosos.

Siguiendo el hilo conductor de las preguntas, la siguiente que nos hacemos es ¿cómo pueden actuar estos actores internos o externos para conseguir tales fines? La respuesta la tenemos en las diferentes amenazas comúnmente aceptadas en ámbitos tanto militares como civiles, públicos o privados**;** empleando la violencia, de carácter terrorista o no, el espionaje, el sabotaje, la subversión, las acciones criminales y los ataques reputacionales. Y claro está, hoy en día, los actores que representan una amenaza no se limitan al entorno físico, también actúan en el entorno cibernético. Del mismo modo, las amenazas ciber no viven solo en el ciberespacio, hay personas, organizaciones o entidades detrás de ellas que viven en el entorno físico, y normalmente, tienen intereses también en el entorno físico. El uno no se puede entender sin el otro y el otro sin el uno.

La respuesta a la pregunta ¿cómo podemos contrarrestar esta amenaza? nos dará la clave del modelo. A la amenaza se le combate, como se ha visto en la introducción, con una serie de acciones defensivas y ofensivas con las siguientes finalidades: disuasión, detección, neutralización y decepción. La primera y la última son netamente defensiva y ofensiva respectivamente, mientras que la detección y neutraliza-

ción pueden ser defensivas y ofensivas, dependiendo de si se realizan antes o después de que se materialice la amenaza. Al igual que la amenaza, las acciones para contrarrestarla deben desarrollarse en los entornos físico y ciber.

Es necesario resaltar que aplicar únicamente un enfoque defensivo no es suficiente. La estructura de contrainteligencia debe de ser ofensiva, proactiva (Diaz-Caneja, 2021). Las acciones ofensivas deben ser siempre la primera regla de cualquier decálogo de contrainteligencia (Olson, 2019).

Una vez determinada qué tipo de acciones se pueden emplear surge la pregunta ¿cómo podemos aplicar estas acciones en nuestra organización? Para responder a esta pregunta debemos pasar por un proceso de planeamiento y análisis que, con el conocimiento previo de nuestra propia organización, las amenazas existentes y las organizaciones adversarias o competidoras, nos permita determinar qué acciones, cuándo, dónde y de qué manera las podemos aplicar.

Específicamente se realizarán dos tipos generales de planeamiento y análisis diferentes, uno para las acciones de disuasión, detección y neutralización y otro para las acciones de decepción.

Para las acciones de disuasión, detección y neutralización, y sus medidas preventivas asociadas, se realizará el planeamiento en cuatro fases principales con sus correspondientes análisis:

1. Determinar los elementos a proteger.
2. Realizar un análisis de la amenaza.
3. Llevar a cabo un análisis de las vulnerabilidades propias.
4. Efectuar un análisis y valoración de riesgos.

El resultado del planeamiento y análisis servirá para:

- Asesorar acerca de las medidas de seguridad a implementar en la organización.
- Asesorar a la dirección sobre las amenazas a las que se enfrenta la organización.
- Dirigir y priorizar el esfuerzo en las tareas de obtención y elaboración de inteligencia sobre la amenaza.
- Servir de base para la elaboración de un plan de continuidad de negocio.

Respecto a la decepción, el planeamiento sigue cuatro fases principales (Rogert M. & William L., 2019):

1. Determinar la situación final deseada que se pretende alcanzar con la decepción.
2. Identificar las decisiones y acciones que el adversario debe tomar y realizar para llegar a esa situación final deseada.
3. Crear una historia o escenario ficticio en el que el oponente debe creer para poder tomar las decisiones identificadas en el punto anterior.
4. Identificar los elementos de información y los canales por los que esa información debe circular para que guíen al adversario a creer la historia.

El resultado de este planeamiento y análisis servirá para apoyar las operaciones y funcionamiento de la organización, permitiendo mantener la seguridad operacional y alcanzar la sorpresa, ya sea para anular la acción de una amenaza a la seguridad o los intentos de un adversario de alcanzar una ventaja competitiva sobre nuestra organización o productos.

3. Desarrollo de las acciones de contrainteligencia

Una vez determinado el marco general del modelo de contrainteligencia, llega el momento de establecer qué actividades concretas se deben desarrollar para responder a las finalidades de disuasión, detección, neutralización y decepción.

La disuasión se consigue principalmente por medio de la adopción de **medidas de seguridad preventivas**, ya sean estas físicas, del personal, de la información, de la organización, etc. También se consigue manteniendo un elevado grado de concienciación entre el personal en relación a las amenazas y las normas de seguridad a cumplir.

La detección por medio de la implementación de las medidas de seguridad preventivas, en su aspecto defensivo, y la **obtención y análisis de información sobre las intenciones y capacidades de la amenaza**, en su aspecto ofensivo.

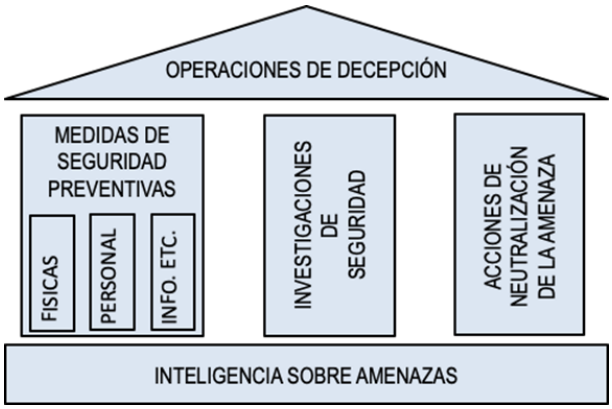
La neutralización por la ejecución de los planes y mediadas de seguridad preventivas, en su aspecto defensivo. En el aspecto ofensivo por las **investigaciones de incidentes de seguridad**, tanto de origen interno como externo, y la ejecución de acciones específicas de **neutralización de la amenaza**, como los enlaces con las Fuerzas y Cuerpos de Seguridad o acciones de contrapropaganda o contrainfluencia negativa.

La decepción se consigue por medio de **operaciones de decepción**. Éstas se deben desarrollar en coordinación con diferentes aéreas de la organización, pero es en la estructura de contrainteligencia donde reside el conocimiento de su planeamiento y la inteligencia básica y actual para su desarrollo.

En la base de todas estas actividades mencionadas se encuentra la **inteligencia sobre las amenazas**. Elemento indispensable sin la cual no se pueden desarrollar de forma eficiente el resto de actividades, a la vez, el resto de actividades alimenta el ciclo de inteligencia sobre las amenazas.

El resultado práctico de este modelo es una organización de contrainteligencia con cinco funciones principales, tal y como viene reflejado en la figura 1. En el que la inteligencia sobre las amenazas es la base y el primer elemento a establecer, sobre él, se erigen los tres principales pilares de la protección de la organización; las medidas de seguridad preventivas, las investigaciones de incidentes de seguridad y las acciones específicas para neutralizar la amenaza. Como elemento más elevado por su complejidad y carácter ofensivo se sitúan las operaciones de decepción.

Figura 1. Esquema de modelo holístico de contrainteligencia
(*Fuente: Elaboración propia*)



Es precisamente el orden expuesto el que se debe seguir y priorizar a la hora de implementar un sistema de contrainteligencia, llegando solo a la decepción cuando se tenga una estructura de contrainteligencia madura.

4. Conclusiones

Se puede llegar a definir la contrainteligencia, en su sentido más amplio y rompiendo un poco la clásica percepción que se tiene de ella, como la actividad encaminada a **proteger**, tanto en el entorno físico como en el ciberespacio, **la capacidad de operar** de una organización de la acción de organizaciones e individuos que intenten impedir o dificultar su normal funcionamiento, así como obtener una ventaja explotando su conocimiento por medio de acciones de violencia, espionaje, sabotaje, subversión, actividades criminales y ataques reputacionales. La protección se consigue con una adecuada combinación de acciones defensivas y ofensivas de disuasión, detección, neutralización y decepción.

La aplicación organizativa y funcional práctica de esta definición sería una estructura que desarrolle las cinco actividades principales expuestas: inteligencia sobre las amenazas, medidas de seguridad preventivas, investigaciones de incidentes de seguridad, neutralización de la amenaza y operaciones de decepción.

La puesta en práctica de este modelo en el que se combinan tradicionales aspectos de contrainteligencia y seguridad, permitiría afrontar con una visión holística el reto de mantener protegida una organización, esto es, y como define la Real Academia Española el verbo **proteger**: «Resguardar a una persona, animal o cosa de un perjuicio o peligro, poniéndole algo encima, rodeándolo». En este caso, resguardamos una organización o empresa de la materialización de la amenaza poniendo encima una serie de medidas y actividades para mantearla segura.

5. Referencias

Blanco Iñigo, P. (2018). Necesidades del consumidor de inteligencia. En J. del Toro Jimenez, M. Bernardino Gonzalez, J. Villena Romera, & G. Diaz Matey, *La Inteligencia Empresarial en España* (págs. 113-125). Madrid: Borrmart.

Diaz-Caneja, J. (21 de junio de 2021). *Contrainteligencia en apoyo a la seguridad de la empresa*. Recuperado el 15 de setiembre de 2021, de Inteligencia más Liderazgo: https://inteligenciayliderazgo.com/contrainteligencia/contrainteligencia-y-seguridad-empresarial/

Olson, J. M. (2019). *To catch a spy. The art of counterintelligence.* Washington, DC: Georgetown University Press.

Prunckun, H. (2019). *Counter-intelligence theory and practice.* Londres: Rowman & Littlefield.

R. C., & W. M. (2019). *Deception, Counterdeception and Counterintelligence.* Thousand Oaks, California: SAGE Publications.

Sanchez Gamboa, J. (2016). Ideas fundamentales sobre inteligencia. En J. Sanchez Gamboa, V. Diaz Blanco, J. Diaz-Caneja Greciano, & I. Martin Barbero, *Inteligencia. Un enfoque integral* (Vol. Monografia 148, pág. 23). Madrid: Ministerio de Defensa de España.

van Genderen, D. (2018). *Counterintelligence for Corporate Enviroments, Volume II.* Nueva York: Business Expert Press

Reports de Inteligencia Económica y Relaciones internacionales

[ISSN 2660-7352]

PUBLICACIONES DE LA ESCUELA DE INTELIGENCIA ECONÓMICA DE LA UAM