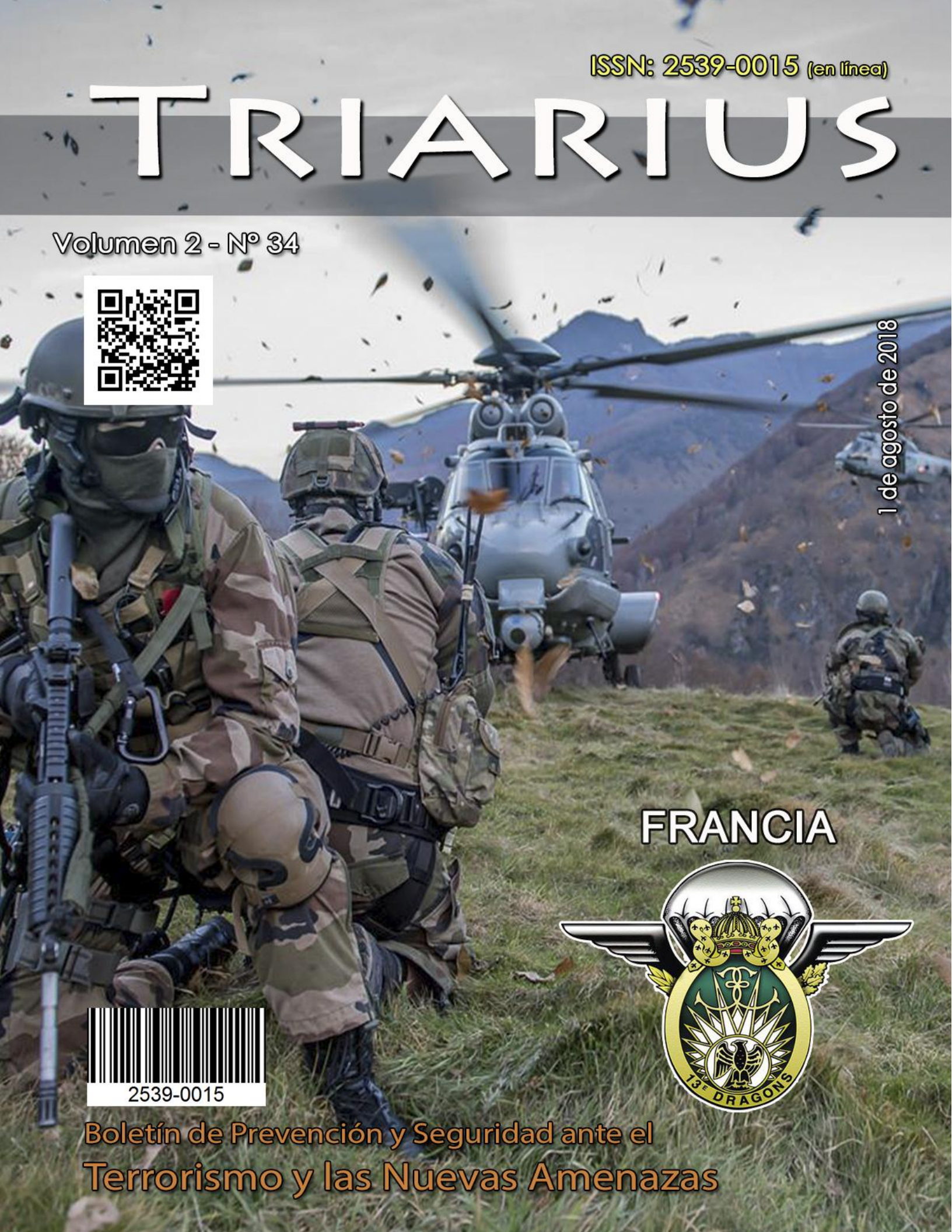
ISSN: 2539-0015 (en línea)

# TRIARIUS

Volumen 2 - Nº 34



1 de agosto de 2018

## FRANCIA

2539-0015

Boletín de Prevención y Seguridad ante el

## Terrorismo y las Nuevas Amenazas

ISSN: **2539-0015** (en línea)
Medellín - Colombia
Volumen **2** - Número **34**
1 de agosto de **2018**

**Editor**
Douglas Hernández

**Analistas Triarius**
Ulises León Kandiko, Francisco Javier Blasco, Haylyn Hernández, Alfredo Campos, Douglas Hernández,

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

**Información de Contacto:**

**Douglas Hernández**
Medellín, Colombia
Móvil: (+57) 321-6435103
director@fuerzasmilitares.org
hernandez.douglas@hotmail.com



# Editorial

Nos complace anunciar que hemos firmado convenios de cooperación con tres organizaciones que en nuestro ámbito revisten un carácter estratégico. Ellas son el Security College US (SCUS) de los Estados Unidos, el Master Security Consulting (MSC) de Colombia, y el Learning Institute for Security Advisor (LISA) de España, todas dedicadas a la asesoría en temas de seguridad y especialmente a la formación del talento humano con los más altos estándares. Invitamos a nuestros lectores a conocerlos y a inscribirse en alguno de los programas que ofrecen y que sin duda contribuirán a su mejoramiento profesional. Bajo los convenios mencionados, los suscriptores de TRIARIUS recibirán descuentos especiales. Estamos contribuyendo de distintas maneras a la seguridad mundial.

En este número traemos para ustedes, un interesante artículo Kandiko, quien desde Argentina profundiza en el tema de las ciberamas, teniendo en cuenta algunas premisas básicas. La primera, que la ciberguerra es una realidad, la segunda, que la ventaja tecnológica de una potencia, en caso de guerra se vuelve una vulnerabilidad debido a la ciberdependencia (concepto que por primera vez se toca en esta revista), y en tercer lugar, que las ciberarmas son de bajo costo y alto impacto. Nuestro experto en el quinto dominio de la guerra, realiza un ejercicio práctico para determinar si un país debe desarrollar ciberarmas, tomando como ejemplo a Nueva Zelanda. A partir de este ejemplo cada uno podrá desarrollar un ejercicio similar para su propio país.

A paso seguido el coronel Blasco, desde España, realiza un análisis muy preciso sobre el reciente acercamiento entre Estados Unidos y Corea del Norte, dándonos luces sobre las implicaciones geopolíticas que tiene este proceso por demás complejo y lleno de incertidumbre. Luego, Haylyn Hernández, analista colombiana, hace un repaso de la situación en la ciudad de Medellín, presentándonos el marcado contraste que se presenta en esta ciudad, llena de innovaciones urbanísticas, pero al mismo tiempo tan violenta. Llama poderosamente la atención una cita que allí se realiza y que afirma que las ciudades se están convirtiendo en algo más importante que los Estados.

El analista español Alfredo Campos, nos lleva a revisar la compleja situación de la República Centroafricana, un país convulsionado por hechos violentos de distinto tipo e intensidad, y donde las potencias y algunos organismos internacionales hacen presencia intentando estabilizar la situación, y en no pocos casos sacar algún provecho. En medio de todo ello, ¼ parte de la población ha huido, lo que da cuenta de la magnitud del problema.

Otro artículo de Kandiko, se enfoca la ciberinteligencia (CybInt), en este trabajo el analista aborda las similitudes y diferencias entre la inteligencia tradicional y aquella que se desarrolla o debería desarrollarse en el ciberespacio, atendiendo a sus particularidades. En esta aproximación al problema se cuestiona la viabilidad del ciclo de inteligencia tradicional en el quinto dominio, y se muestra una de las alternativas al mismo.

Finalmente, y en el interés de contribuir al fortalecimiento de las habilidades gerenciales de directores o comandantes de unidades militares o policiales, se presenta un artículo que aborda el tema de la gerencia estratégica del capital intelectual, y presenta algunas herramientas que podrían ser tenidas en cuenta para este propósito.

¡Conocer para vencer!

*Douglas Hernández*

Editor

Este boletín tiene versión en inglés.

# TRIARIUS 34, Contenido:




TRIARIUS

Queremos establecer que dentro de las "nuevas amenazas" que debemos afrontar en la modernidad, están los problemas medioambientales. El cuidado de la naturaleza es algo fundamental para la supervivencia de nuestra especie. No es una moda, ni siquiera es una opción, ahora es algo de vida o muerte. En este orden de ideas, queremos incluir en esta revista artículos que aborden los problemas medioambientales y propongan estrategias de solución. Invitamos a nuestros lectores a hacer aportes en este sentido.

En portada, miembros del ***13 Regimiento de Dragones Paracaidistas del Ejército Francés***. Por favor vea la reseña de esta unidad al final de la revista.

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

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

SHIELDAFRICA
Abidjan 2019

# Ciberarmas: poderío militar y diplomacia para países emergentes y estados pequeños

Por Ulises León Kandiko (Argentina)

El asunto de la Ciberguerra viene siendo un tema de interés en los últimos años especialmente en los países más desarrollados. Asimismo, y en paralelo a la gran cantidad de Ciberataques que se vienen produciendo, aparece el tema no menor de las Ciberarmas. Si bien la Ciberguerra parece más tema de países desarrollados, las cuestiones relativas a la adquisición de armas cibernéticas por parte de Estados pequeños han recibido poca atención. Si bien individualmente son débiles, los Estados pequeños son numerosos. Comprenden más de la mitad de los miembros de las Naciones Unidas y siguen siendo importantes para las consideraciones geopolíticas. De la mano de ello, estos Estados se enfrentan a elecciones de inversión en seguridad cada vez más difíciles ya que el equilibrio entre la seguridad global, el dominio regional y los intereses nacionales se evalúa constantemente, un claro ejemplo sucede en los países menos favorecidos, donde incluso los temas de Seguridad Interior se mezclan con los recursos de la Defensa Nacional. Un factor cada vez más relevante en estas elecciones es el aumento de los costos de las plataformas militares y las percepciones que la guerra cibernética puede proporcionar una capacidad ofensiva barata y efectiva para ejercer influencia estratégica sobre los rivales geopolíticos. Recordemos en este punto, que muchos analistas señalaron que la verdadera preocupación de Trump en la cumbre con Kim Jong-un era la amenaza Cibernética más que el programa nuclear de Korea del Norte.

Si bien las operaciones ofensivas y defensivas tienen características propias, en la actualidad del 5to dominio podemos decir que el balance de poder entre la ofensa y la defensa aún no se ha determinado. Además, la naturaleza indirecta e inmaterial de las Ciberarmas hace estimar que no alteren los principios fundamentales de la guerra y no puedan ganar conflictos militares sin ayuda. Por el contrario, es probable que las Ciberarmas sean más efectivas cuando se usan como un multiplicador de fuerza y no solo como una capacidad de interrupción de la infraestructura. La consideración de la ciberdependencia, es decir, la medida en que la

economía, los ejércitos y el gobierno de un Estado dependen del ciberespacio, también es muy relevante para esta discusión. Dependiendo de la resiliencia de la infraestructura, una ventaja tecnológica estratégica puede convertirse en una desventaja significativa en tiempos de conflicto. La capacidad de amplificar las capacidades militares convencionales, explotar las vulnerabilidades en la infraestructura nacional y controlar el espacio de ciberconflicto es, por lo tanto, un aspecto importante para cualquier doctrina guerrera. La integración de estas capacidades en las estrategias de defensa es la fuerza motriz en la investigación y el desarrollo de las Ciberarmas.

**La naturaleza de la guerra cibernética**

La guerra cibernética es cada vez más reconocida como el 5to dominio de la guerra. Su creciente importancia es sugerida por su prominencia en la estrategia nacional, la doctrina militar y las inversiones significativas en capacidades relevantes. Las características críticas de la Ciberguerra se pueden resumir en tres puntos [i]:

1. La guerra cibernética involucra acciones que tienen un efecto político o militar.
2. Implica el uso del ciberespacio para ofrecer efectos cinéticos directos o en cascada que tienen resultados comparables a las capacidades militares tradicionales.
3. Crea resultados que causan o son un componente crucial de una amenaza grave para la seguridad de una nación o que se llevan a cabo en respuesta a dicha amenaza.

En cuanto a las Ciberarmas, las mismas se definen como las capacidades de la Ciberguerra armada que tienen los que tienen experiencia y recursos necesarios para entregarlas e implementarlas.

En este dominio incipiente todo es dable a debatir, sin embargo, son muchos los especialistas que consideran a las operaciones ofensivas como dominantes en el 5to Dominio [ii]. Los ataques se pueden lanzar instantáneamente, y hay un rápido crecimiento en el número de redes y activos que requieren protección. Después de todo, el ciberespacio es un entorno rico en objetivos basado en estructuras de red que privilegian el acceso a la seguridad. Dificultades técnicas y legales considerables, así como represalias precisas y proporcionales, hacen que la atribución precisa de ciberataques sea un proceso tenso. También existe el bajo costo de crear Ciberarmas -el código es barato- y cualquier arma liberada en Internet puede ser modificada para crear la base de nuevas capacidades ofensivas[iii]. Todo esto significa que el espacio de batalla está abierto, es accesible, casi anónimo y con un costo de entrada que parece asequible para cualquier Estado-Nación.

Sin embargo, las estrategias que dependen demasiado del dominio ofensivo en la Ciberguerra pueden ser prematuras. Por ejemplo, la dependencia cibernetica (infraestructura crítica) es crucial para las ventajas estratégicas que las Ciberarmas pueden proporcionar. La incertidumbre rige porque la naturaleza de doble uso de las Ciberarmas les permite ser capturadas, manipuladas y puestas en contra de sus creadores. Igualmente importante es la práctica del "dominio de escalada" [iv]. Como lo muestra una política estadounidense aún no probada, la represalia por el ciberataque puede ser aplicada por capacidades militares más destructivas [v]. Y aunque la velocidad de un ataque cibernético puede ser casi instantánea, la preparación para sofisticados ciberataques es considerable. El ataque de Stuxnet requirió los recursos de un Estado tecnológicamente sofisticado para proporcionar el espionaje expansivo, las pruebas industriales y la entrega clandestina que fueron tan vitales para su éxito. Lo anterior demuestra que el verdadero costo de las armas cibernéticas avanzadas no radica en su creación, sino en su focalización y despliegue, que reducen su capacidad de redistribución para enfrentar futuras amenazas imprevistas.

Una de las limitaciones, que en ciernes está siendo corregida, está dada por su falta de fisicalidad (efecto físico concreto), aunque podremos ver como Triton están cambiando eso. Como piezas de código informático, generan efecto militar solo mediante la explotación de vulnerabilidades creadas por la dependencia del ciberespacio. Pueden atacar plataformas e infraestructuras vulnerables manipulando los sistemas informáticos o actuando como un multiplicador de la fuerza a los activos militares tradicionales. Esto puede conducir a la interrupción y el control del espacio de batalla, así como a la provisión de inteligencia adicional cuando se despliegan las cargas útiles. Sin embargo, estos efectos son siempre secundarios: las Ciberarmas per se aún no pueden afectar directamente el campo de batalla sin un dispositivo para actuar, ni ocupar y controlar el territorio.

En última instancia, el debate sobre el equilibrio de poder en la Ciberguerra y el poder relativo de las Ciberarmas se decidirá por evidencia empírica relacionada a dos factores:

La cantidad de daño causado por el compromiso de ciber-plataformas dependientes.

Hasta qué punto las principales interrupciones de la infraestructura erosionan la fuerza de voluntad

política y son explotables por las capacidades militares convencionales.

Por el momento, hay una creencia en que los conflictos no se ganarán solo en el ciberespacio y que esto se aplica tanto a los pequeños Estados como a las grandes potencias.

**Usos de las Ciberarmas por Países Emergentes y/o Estados pequeños**

Para ser digno de inversión, un arsenal de Ciberarmas debe proporcionarle a los Estados una ventaja política o militar sobre (o al menos la paridad) sus adversarios. Para juzgar si un pequeño Estado se beneficia lo suficiente como para justificar su adquisición, debemos entender cómo se pueden usar estas capacidades. Una lista no exhaustiva de posibles usos de Ciberarmas incluye la guerra, la coacción, la disuasión y la diplomacia de defensa. Su efecto más prominente probablemente será la alteración y / o manipulación de las capacidades militares de comando, control, comunicaciones, computación, inteligencia, vigilancia y reconocimiento (C4ISR) y la degradación de las redes de apoyo civil. Los ataques contra la infraestructura civil siguen siendo los más factibles, y los ataques a plataformas militares automáticas son posibles y cada vez más probables. El uso efectivo de las Ciberarmas como herramienta coercitiva se ve limitado por el tamaño relativo y la dependencia cibernética de un oponente y conlleva el riesgo de que las armas actúen de forma imprevista. Ambas dependencias se comparten cuando las Ciberarmas se utilizan como elemento de disuasión. Esto se debe a la naturaleza peculiar del dominio cibernético, donde tanto la coacción como la disuasión se basan en el mismo reconocimiento agresivo hacia adelante de la red de un adversario. La diplomacia de defensa puede actuar como elemento de disuasión, pero solo es efectiva si las capacidades militares relevantes son creíbles y demostrables.

**Poseer o No Poseer Ciberarmas, he ahí el dilema.**

A la hora de evaluar esta situación son múltiples los factores a analizar, pero aquí se verá en forma analítica una posible forma de evaluación para esta toma de decisiones tan peculiar. En concreto, el modelo propuesto es una base para un estudio comparativo e integral Estado por Estado. El mismo rinde su valor máximo cuando se han analizado numerosos Estados. Esto permite que surjan posibles patrones de proliferación y que se presente una imagen más clara del paisaje de amenazas. El esquema del proceso básico para el análisis se proporciona en el cuadro siguiente:

**Tabla 1.** Matriz de riesgo costo-beneficio de ciberarmas

Matriz de riesgo costo-beneficio de Ciberarmas (caso modelo Nueva Zelanda)

| | GUERRA | COERCION | DISUACION | DIPLOMACIA DE DEFENSA |
|---|---|---|---|---|
| BENEFICIO | Habilidad para complementar las capacidades Militares de sus Aliados. | Habilidad limitada de coercion con Ciberarmas. | Capacidad limitad de disucación con Ciberarmas. | Buena capacidad de discuación a través de la Diplomacia. |
| | Capacidad ofensiva económica. | | | |
| FACTIBILIDAD | Los aliados pueden brindar oportunidades de adquisicon favorables. | Existen recursos técnicos y de inteligencia apropiados. | Existen recursos técnicos y de inteligencia apropiados. | Existen recursos técnicos y de inteligencia apropiados. |
| | Existen recursos técnicos y de inteligencia apropiados. | | | |
| RIESGOS | La adquisición puede resultar en una reducción de fondos para otras capacidades militares. | La oposición nacional a la adquisición de nuevas armas ofensivas. | La adquisición puede resultar en una reducción de fondos para otras capacidades militares. | La adquisición puede resultar en una reducción de fondos para otras capacidades militares. |
| | La oposición nacional a la adquisición de nuevas armas ofensivas. | Identidad de seguridad no reconciliable con acciones militares coercitivas. | La adquisición de Ciberarmas puede reducir la reputación internacional. | La adquisición de Ciberarmas puede reducir la reputación internacional. |
| | La adquisición de Ciberarmas puede reducir la reputación internacional. | La adquisición puede resultar en una reducción de fondos para otras capacidades militares. | El alto nivel de dependencia cibernética aumenta la vulnerabilidad a las represalias. | El alto nivel de dependencia cibernética aumenta la vulnerabilidad a las represalias. |
| | La explotación de Ciberarmas depende de las fuerzas aliadas. | La adquisición de Ciberarmas puede reducir la reputación internacional. | La falta de amenazas identificadas reduce la capacidad de apuntar y desarrollar Ciberarmas disuasorias. | |
| | El alto nivel de dependencia cibernética aumenta la vulnerabilidad a las represalias. | El alto nivel de dependencia cibernética aumenta la vulnerabilidad a las represalias. | | |

Cada paso se explica por una declaración de propósito y se demuestra a través de un estudio de caso. El tema del estudio de caso es Nueva Zelanda, elegido debido a su membresía en la red de inteligencia Five Eyes y porque se autoidentifica y se percibe como un Estado pequeño. Idealmente, cada paso del marco lo completaría un grupo que represente una variedad de perspectivas de las fuerzas militares, entidades gubernamentales, y especialidades académicas.

Paso uno: identifique las características fundamentales de los estados pequeños. El propósito es identificar las características clave del Estado dentro de tres categorías: cuantitativo, conductual e identidad. Cuantitativo se refiere a medidas tales como la superficie territorial, la población y el producto bruto interno (PBI). Comportamiento se refiere a métricas cualitativas sobre el comportamiento de un Estado, tanto a nivel nacional como dentro del sistema internacional. La identidad se refiere a métricas cualitativas que se centran en cómo un Estado percibe su propia identidad. Este artículo propone que las métricas de cada categoría pueden ser utilizadas libremente por analistas informados adecuadamente para asignar una categoría de tamaño a cualquier Estado en particular. En cambio, la definición y categorización se logran mediante la posesión de un número suficiente de características superpuestas -algunas cuantitativas, algunas de comportamiento y otras basadas en la identidad. Cuantitativamente, Nueva Zelanda tiene una población pequeña (aproximadamente 4.5 millones), un pequeño PBI (aproximadamente u$s 197 mil millones), y una pequeña área de tierra [vi]. Está geográficamente aislada, sin fronteras con otros países. En el ámbito del comportamiento, Nueva Zelanda practica una política exterior multilateral centrada en las instituciones. Es un miembro fundador de las Naciones Unidas y fue elegido miembro del Consejo de Seguridad para el período 2015-2016 después de postularse en una plataforma de defensa de otros Estados pequeños. Participa en múltiples alianzas y tiene un interés especial en la seguridad del Pacífico Sur [vii]. Con respecto a la identidad, la autoidentidad de Nueva Zelanda enfatiza los valores de equidad, independencia, no agresión, cooperación y reconocimiento de su estatus como un Estado pequeño [viii]. Su identidad de seguridad está impulsada por la falta de una amenaza percibida que permite a Nueva Zelanda tomar decisiones de seguridad basadas en los principios y no en la practicidad [ix]. Esto quedó demostrado por la prohibición de barcos con armas nucleares y nucleares en aguas de Nueva Zelanda, y su subsecuente exclusión informal de aspectos del Tratado de Seguridad de Australia, Nueva Zelanda y Estados Unidos. Sin embargo, a pesar de la menor seguridad, la opinión interna apoyó firmemente la política antinuclear que, junto con el apoyo a la no proliferación y el desarme, ha fortalecido los elementos pacifistas de la identidad nacional de Nueva Zelanda.

Paso dos: identifique la disponibilidad de recursos y la alineación de políticas para el desarrollo, despliegue y explotación de Ciberarmas. El objetivo es identificar cómo el uso de Ciberarmas se alinearía con las políticas de seguridad y defensa actuales; si el Estado tiene la capacidad militar para explotar las vulnerabilidades causadas por el despliegue de Ciberarmas, y a su vez tiene la inteligencia y los recursos técnicos necesarios para atacar, desarrollar y desplegar Ciberarmas.

En los documentos clave de defensa de Nueva Zelanda, las referencias al dominio cibernético mencionan principalmente la defensa contra los ciberataques, con solo dos referencias a la aplicación de la fuerza militar al ciberespacio. No se menciona la adquisición de Ciberarmas. La política de defensa de Nueva Zelanda se ha centrado en las contribuciones militares a una Nueva Zelanda segura, un orden internacional basado en normas y una economía mundial sólida. Debido a que la probabilidad de amenazas directas contra el país y sus aliados más cercanos es baja, se ha enfocado en el mantenimiento de la paz, el alivio de desastres, la asequibilidad y la patrulla marítima. El ejército de Nueva Zelanda es pequeño (11.500 efectivos, incluidos reservistas) con capacidades ofensivas limitadas y escasa financiación (solo el 1,1% del PBI). En consecuencia, el ejército de Nueva Zelanda no tiene la capacidad de explotar las vulnerabilidades causadas por el uso exitoso de Ciberarmas.

Nueva Zelanda es miembro de la red de inteligencia Five Eyes y, por lo tanto, puede acceder a una inteligencia más sofisticada que la mayoría de los Estados pequeños. Esto se puede utilizar para aumentar su capacidad de atacar y desplegar Ciberarmas. Tiene una moderna capacidad de inteligencia de señales, alojada por el Buró de Seguridad de Comunicaciones del Gobierno civil, que también tiene la responsabilidad de la ciberseguridad nacional. Es muy probable que tenga la capacidad técnica para adaptar las Ciberarmas existentes o desarrollar otras nuevas, especialmente si cuenta con la ayuda de sus aliados. Sin embargo, debido a restricciones fiscales, cualquier financiamiento adicional para Ciberarmas probablemente tendrá que provenir del presupuesto de defensa existente y, por

lo tanto, resultará en compromisos con otras capacidades [x].

Paso tres: examinar la dependencia cibernética de los Estados pequeños. El propósito es examinar la dependencia en el ciberespacio por sus capacidades militares e infraestructura crítica, así como su dependencia cibernética relativa cuando se compara con potenciales adversarios geopolíticos.

Nueva Zelanda tiene una dependencia cibernética de moderada a alta, y el gobierno, el sector empresarial y la sociedad civil dependen cada vez más de los servicios y plataformas en línea. Esta dependencia aumentará. Por ejemplo, la adquisición de nuevas capacidades C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance)para aumentar la adopción militar de principios de guerra centrados en redes crearía nuevas vulnerabilidades. La ciberdependencia de Nueva Zelanda se ve incrementada aún más por la limitada experiencia en ciberseguridad. No tiene oponentes militares obvios, por lo que su nivel relativo de ciberdependencia es difícil de calcular.

Paso cuatro: analizar el comportamiento del Estado frente a los modelos de seguridad de la competencia. El propósito es analizar cómo el comportamiento del Estado se alinea con cada modelo de seguridad competidor y cómo la adquisición y el uso de Ciberarmas pueden apoyar o restar valor a este comportamiento. Los arsenales de Ciberarmas se utilizan para alcanzar objetivos políticos y militares. Estos objetivos dependen del comportamiento y la identidad de un Estado, los cuales son difíciles de cuantificar. Sin embargo, es posible cierto grado de cuantificación mediante el uso de modelos de seguridad conceptuales. Una síntesis de las recientes becas de seguridad en pequeños Estados genera cuatro modelos: el primero centrado en alianzas, el segundo en cooperación internacional y el tercero y cuarto en identidad, diferenciado por enfoques competitivos (colaboración e influencia, y autonomía defensiva) [xi]. El modelo centrado en alianzas presenta pequeños Estados con razones persuasivas para adquirir armas cibernéticas. Esto se aplica tanto para equilibrar el comportamiento (es decir, unirse a una alianza en contra de un Estado amenazante) y por efecto arrastre (es decir, entrar en una alianza con un Estado amenazante) [xii]. Los recursos militares adicionales proporcionados por una alianza presentan mayores oportunidades para la explotación de vulnerabilidades causadas por Ciberarmas. Las Ciberarmas pueden ser una contribución razonablemente rentable para una alianza; una gran potencia podría incluso proporcionar oportunidades de adquisición preferencial para un aliado favorecido.

Nueva Zelanda mantiene una estrecha alianza militar con Australia y es miembro de los Cinco Arreglos de Defensa de Poder. También ha firmado acuerdos de ciberseguridad con la Organización del Tratado del Atlántico Norte y el Reino Unido. Las alianzas anteriores se han centrado en la seguridad y la defensa mutua en lugar de las capacidades ofensivas. Nueva Zelanda, sin embargo, tiene una política de complementar las capacidades de defensa de Australia. Esto podría lograrse mediante la adquisición de Ciberarmas, siempre que esté estrechamente coordinado e integrado con el ejército australiano. Por lo tanto, este modelo evalúa la alineación del comportamiento del Estado como media / alta y el apoyo de Ciberarmas como medio / alto.

El modelo de cooperación internacional supone que los Estados pequeños pueden ejercer influencia fortaleciendo las organizaciones internacionales, fomentando enfoques cooperativos para la seguridad y creando leyes y normas para restringir a los Estados poderosos. Los Estados pequeños que actúen bajo este modelo favorecerán los métodos de influencia diplomáticos e ideológicos. Como tal, es menos probable que adquieran Ciberarmas. En cambio, es más probable que intenten regular las Ciberarmas de manera similar a las restricciones sobre armas biológicas y químicas o al dirigir los esfuerzos para incorporarlas explícitamente en las leyes internacionales de guerra.

Nueva Zelanda generalmente tiene un enfoque de política exterior multilateral y es miembro de múltiples organizaciones internacionales. Tiene una larga historia de defensa del desarme y el control de armamentos, lo que entra en conflicto con la adquisición de nuevas categorías de armas ofensivas. Este modelo evalúa la alineación del comportamiento del Estado como alto y el apoyo de Ciberarmas como bajo.

Ambos modelos centrados en la identidad (colaboración e influencia versus autonomía defensiva) se centran en el análisis de la "identidad de seguridad" de un Estado pequeño. Esto se desarrolla a partir de percepciones de "comportamiento pasado, imágenes y mitos vinculados a él que han sido internalizados durante largos períodos de tiempo por la élite política y la población del Estado" [xiii]. Esta identidad puede basarse en una serie de factores dispares, como las amenazas de seguridad en curso, las percepciones de carácter nacional y la conciencia histórica. La identidad de seguridad de un Estado puede

conducirlo hacia una preferencia por cualquiera de los modelos de seguridad centrados en la identidad mencionados anteriormente. Con respecto a la colaboración y la influencia, la identidad de Nueva Zelanda logra un equilibrio entre practicidad y principio. Se esfuerza por ser un Estado moral e imparcial que promueve lo que considera valores importantes, como los derechos humanos y el estado de derecho [xiv]. Sin embargo, aún desea trabajar de una manera constructiva que le permita aportar soluciones prácticas a problemas difíciles. La adquisición de Ciberarmas es poco probable que avance en este modelo. Por lo tanto, este modelo evalúa la alineación del comportamiento del Estado como medio y el apoyo a las Ciberarmas como bajo.

A pesar de su comportamiento multilateral, Nueva Zelanda conserva cierta autonomía defensiva y se enorgullece de mantener puntos de vista independientes sobre los principales problemas. Su aislamiento y la ausencia de amenazas importantes le han permitido conservar cierta autonomía en su política de defensa y mantener un pequeño ejército. Su naturaleza independiente y pacifista sugiere que la adquisición de Ciberarmas podría ser controvertida. Por lo tanto, este modelo evalúa la alineación conductual del Estado como medio y el apoyo a las Ciberarmas como bajo / medio.

Paso cinco: Analice los beneficios, la viabilidad y el riesgo para cada categoría de uso de Ciberarmas. El objetivo es identificar primero los beneficios, la viabilidad y el riesgo de adquirir Ciberarmas en función de cada categoría de uso potencial, como se muestra en la tabla 1. A continuación, esta información se analiza en función del uso de Ciberarmas para diferentes modelos de seguridad. como se muestra en la tabla 2. Esto da como resultado una clasificación de los beneficios, la viabilidad y el riesgo de cada combinación de uso de Ciberarmas y modelo de seguridad de Estado pequeño. Esto es seguido por una recomendación general o predicción para la adquisición de Ciberarmas bajo cada modelo de seguridad y categoría de uso de Ciberarmas.

Paso seis: recomendar o predecir la estrategia de adquisición de Ciberarmas. El objetivo es resumir los hallazgos clave, recomendar si un Estado pequeño debe adquirir Ciberarmas y predecir la probabilidad de tal adquisición. Los hallazgos clave para el caso que se usó de modelo son que es poco probable que Nueva Zelanda obtenga beneficios significativos de la adquisición de Ciberarmas. Esto se debe a sus capacidades militares limitadas, su enfoque multilateral extranjero, su amplia participación en organizaciones internacionales y su identidad de seguridad pacifista. Los factores que podrían cambiar esta evaluación y aumentar los beneficios de la adquisición de Ciberarmas incluirían un mayor enfoque en las alianzas militares, la aparición de amenazas más obvias para Nueva Zelanda o sus aliados cercanos, o una identidad de seguridad cambiante.

El producto que entrega esta matriz tiene una utilidad considerable como una herramienta de apoyo a la decisión. Cuando es utilizado por un Estado pequeño como un insumo en un proceso de toma de decisiones estratégicas, su resultado puede ser incorporado en la capacidad de defensa relevante y los documentos de política. Si se recomienda la adquisición de Ciberarmas, su resultado podría utilizarse para informar documentos estratégicos, doctrinales y de planificación específicos. También proporciona una base para que se analicen las capacidades potenciales de las Ciberarmas bajo un modelo estándar de adquisición.

**Tabla 2.** Matriz de adquisición de Ciberarmas

| MODELO DE SEGURIDAD | BFR | GUERRA | COERCION | DISUCACION | DEFENSA DIPLOMATICA | GENERAL |
|---|---|---|---|---|---|---|
| ALIANZAS | Beneficios | Mediio | Bajo | Bajo | Medio | Medio |
| | Factibilidad | Medio | Medio | Medio | Medio | Medio |
| | Riesgo | Alto | Muy Alto | Alto | Bajo | Alto |
| | Recomendación / Prediccion | Para prox. Inv. | No | no | Para prox.Inv. | Para prox.Inv. |
| COOPERACION INTERNACIONAL | Beneficios | Bajo | Bajo | Bajo | Medio | Bajo |
| | Factibilidad | Medio | Medio | Medio | Medio | Medio |
| | Riesgo | Alto | Alto | Alto | Bajo | Alto |
| | Recomendación / Prediccion | No | No | No | Para prox.Inv. | No |
| IDENTIDAD Y NORMAS: COLABORACIÓN E | Beneficios | Bajo | Bajo | Bajo | Medio | Bajo |
| | Factibilidad | Medio | Medio | Medio | Medio | Medio |
| | Riesgo | Alto | Alto | Alto | Bajo | Alto |
| | Recomendación / Prediccion | No | No | No | Para prox.Inv. | No |
| IDENTIDAD Y NORMAS: AUTONOMIA DEFENSAIVA | Beneficios | Bajo | Bajo | Bajo | Bajo | Bajo |
| | Factibilidad | Medio | Medio | Medio | Medio | Medio |
| | Riesgo | Alto | Alto | Alto | Bajo | Bajo |
| | Recomendación / Prediccion | No | No | No | No | No |

Alternativamente, la matriz permite a una variedad de actores determinar la probabilidad de adquisición de Ciberarmas por parte de Estados pequeños, podría usarse como una herramienta para desarrollar inteligencia predictiva. Además, cuando la matriz se utiliza en un número suficiente de Estados pequeños, podría usarse como base para hacer predicciones más amplias con respecto a la proliferación de Ciberarmas. Esto sería particularmente efectivo en áreas geográficas con una gran concentración de Estados pequeños. Para los Estados más poderosos, esto podría indicar oportunidades para una mayor cooperación de Ciberguerra con aliados geopolíticos, tal vez incluso se extienda a la venta de armas o la diplomacia de defensa. Por el contrario, la matriz podría proporcionar a las organizaciones no gubernamentales y académicos oportunidades para rastrear la proliferación de Ciberarmas y aumentar la visibilidad del fenómeno entre las organizaciones internacionales, los formadores de políticas y el público en general. Estos resultados brindan beneficios significativos al amplio espectro de actores que buscan estabilidad e influencia dentro del orden internacional.

**1D34S F1N4L3S**

La evolución de los campos de batalla y sus dominios no se dieron en forma sencilla ni inmediata a las evoluciones industriales o tecnológicas, ante la aparición de cada dominio el que precedía se rehusaba a ceder espacio. La virtud está en poder aprender del pasado, ya lo decía el viejo Nicolás Maquiavelo “Todo aquel que desee saber qué ocurrirá, debe examinar qué ha ocurrido, todas las cosas de este mundo, en cualquier época, tienen su réplica en la Antigüedad”, negarnos a la existencia del 5to dominio de guerra, al uso de Ciberarmas y a que tendrán efecto físico es no querer reconocer lo que sucederá, en breve. Hace poco, el Presidente de USA Donald Trump ordenó al Pentágono tomar la iniciativa en la creación de la 6ta Rama de las Fuerzas Armadas Estadounidenses, es decir el Space Force, podrán tildarlo de aventurero, pero lo cierto es que la historia será su juez.

El modelo acá expuesto, posee asimismo un potencial de predicción significativo: cualquier habilidad para pronosticar la adquisición de Ciberarmas de Estado por Estado y así monitorear la proliferación de las mismas sería de un gran beneficio geopolítico. Además, las grandes Potencias no deben ignorar el impacto estratégico que los Estados pequeños podrían tener en este ámbito. No es menos cierto y valedero recordar en ese sentido a los Estados pequeños, que sus rivales geopolíticos pueden desplegar Ciberarmas como un medio para promover intereses nacionales en esta esfera de influencia.

El Ciberespacio es hecho por el hombre, es un entorno altamente evolutivo, tecnológicamente configurado y no completamente tangible, que requiere que sea estudiado, evaluado, analizado y sometido a una continua investigación para poder dominar este nuevo dominio, habrá que transitar muchas millas o terabytes para lograrlo, de eso no hay dudas. Esta comprensión del 5to dominio va más allá de los aspectos tecnológicos y requiere la integración de las capacidades y estrategias

cibernéticas en las doctrinas de defensa existentes. El marco aquí expuesto es solo una mirada, no pretende ser una guía, solo dar ideas para asistir en este proceso, desde la decisión estratégica hasta la obtención y la integración doctrinal y operacional.

**Referencias y Notas**


[i] Raymond C. Parks y David P. Duggan, "Principios de guerra cibernética", IEEE Security and Privacy Magazine 9, no. 5 (septiembre / octubre de 2011), 30; Andrew M. Colarik y Lech J. Janczewski, "Desarrollo de una gran estrategia para la guerra cibernética", séptima conferencia internacional sobre seguridad y garantía de la información, diciembre de 2011, 52; Shakarian, Shakarian y Ruef.

[ii] Fred Schrier, Documento N. ° 7 sobre guerra cibernética, control democrático de las fuerzas armadas trabajando (Ginebra: Centro de Ginebra para el Control Democrático de las Fuerzas Armadas, 2015), disponible en <www.dcaf.ch/content/download/67316/.../ OnCyber warfare-Schreier.pdf>; John Arquilla, "Veinte años de guerra cibernética", Journal of Military Ethics 12, no. 1 (17 de abril de 2013), 80-87.

[iii] P.W. Singer y Allan Friedman, Ciberseguridad y Ciberguerra: Lo que todos deben saber (Oxford: Oxford University Press, 2014).

[iv] Thomas G. Mahnken, "Cyberwar and Cyber Warfare", en America's Cyber Future, ed. Kristin M. Lord y Travis Sharp (Washington, DC: Centro para una Nueva Seguridad Estadounidense, 2011), disponible en <www.cnas.org/sites/default/files/publications-pdf/CNAS_Cyber_Volume%20II_2.pdf>.

[v] Departamento de Defensa (DOD), The DOD Cyber Strategy (Washington, DC: DOD, Abril de 2015), disponible en <www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf>.

[vi] Estadísticas de Nueva Zelanda, "Índice de estadísticas clave de Nueva Zelanda", disponible en <www.stats.govt.nz/browse_for_stats/snapshots-ofnz/index-key-statistics.aspx#>.

[vii] El Ministerio de Asuntos Exteriores y Comercio de Nueva Zelanda, "Relaciones Exteriores", marzo de 2014, está disponible en <http://mfat.govt.nz/Foreign-Relations/index.php>.

[viii] Ibidem.

[ix] Doctrina de la Fuerza de Defensa de Nueva Zelanda, 3rd ed. (Wellington: sede de la Fuerza de Defensa de Nueva Zelanda, junio de 2012), disponible en <www.nzdf.mil.nz/downloads/pdf/public-docs/2012/nzddp_d_3rd_ed.pdf>.

[x] Libro Blanco de Defensa 2010 (Wellington: Ministerio de Defensa, noviembre de 2010), disponible en <www.nzdf.mil.nz/downloads/pdf/public-docs/2010/defence_white_paper_2010.pdf>.

[xi] Joe Burton, "Estados pequeños y seguridad cibernética: el caso de Nueva Zelanda", Political Science 65, no. 2 (2013), 216 - 238; Paul Sutton, "El concepto de pequeños Estados en la economía política internacional", The Round Table 100, no. 413 (2011), 141-153.

[xii] Joe Burton, "Estados pequeños y seguridad cibernética: el caso de Nueva Zelanda", Political Science 65, no. 2 (2013), 216 – 238.

[xiii] Jean-Marc Rickli, "Políticas militares de los pequeños Estados europeos después de la guerra fría: de estrategias territoriales a estrategias de nicho", Cambridge Review of International Affairs 21, no. 3 (2008), 307-325.

[xiv] Jim McLay, "Nueva Zelanda y las Naciones Unidas: Small State, Big Challenge"
27 de agosto de 2013, disponible en <http: // nzunsc. govt.nz/docs/Jim-McLay-speech-Small-State-Big%20Challenge-Aug-13.pdf


Fuente de la Imagen:
https://www.armytimes.com/resizer/M1idu3KQK7r5YGY2ngP5hurPqis=/1200x0/filters:quality(100)/arc-anglerfish-arc2-prod-mco.s3.amazonaws.com/public/NXP3Q667XZHG3BQ5PZ43GROJQM.jpg

# Corea del Norte y Estados Unidos se “besan” por primera vez

Por Francisco Javier Blasco, Coronel retirado

Escribo este trabajo de primeras impresiones sobre los acuerdos de mínimos alcanzados en la tan esperada Cumbre entre Donald Trump (EEUU) y Kim Jong-un (República Popular Democrática de Corea -RPDC- más bien conocida como Corea del Norte -CN-) celebrada en la ciudad Estado de Singapur, bajo todo tipo de cautelas, prevenciones y medidas de seguridad, para dar pasos significativos hacia la desnuclearización de CN y su integración en la normalidad internacional.

Cumbre, cuya celebración ha estado varias veces en el candelero y de la que en referencia a su duración y resultados aparentes se ha esperado y augurado tanto y nada al mismo tiempo. Un aparente y dado por acierto en la marcha de política y geoestratégia común que la Comunidad Internacional (CI) se ha apresurado -incluso por anticipado- a apuntar en el haber de Trump aunque, en realidad y como todo en la arena internacional, tiene varios actores principales, muchos secundarios y de cuyos beneficiarios serán varios países si es que posiblemente disfrutan de ellos.

Llevo muchos años oficial y particularmente tratando de desgranar, entender y explicar cómo ha sido posible lograr el éxito del Programa nuclear de Corea del Norte con tan escasos medios económicos, bajo tanta presión y restricción, pocos o muy escasos recursos técnicos y naturales para la obtención y producción de uranio enriquecido, su verdadera razón de ser y los fines últimos del mismo. He escrito no pocos informes clasificados para mis superiores y mucho sobre el tema en fuentes abiertas, siendo el último de ellos el que figura en mi blog cronológicamente sobre el tema [1].

En todos ellos, y con mayor o menor intensidad y grado de desarrollo, han venido apareciendo una serie de puntos comunes, que configurados adecuadamente, conforman lo que desde hace tiempo, he venido a denominar la Estrategia de CN y de su hereditaria dinastía reinante. En resumen, dichos puntos decisivos y secundarios se concentran en lo siguiente:

- La búsqueda permanente de la garantía de seguridad personal del Régimen norcoreano;
- Lograr el respeto a CN como nación soberana y al mismo nivel del resto de países con armas nucleares;
- Recibir garantías de no agresión exterior lo que implica una continuidad en sus formas y modos de gobierno;
- La desnuclearización total y definitiva de la Península de Corea como fin último y garantía de seguridad;
- Un gran número de importantes compensaciones económicas, aún por determinar y muy difíciles de cuantificar final y oficialmente.

Para lograr estos objetivos CN ha precisado de: una mano férrea sobre su población a la que se le ha sometido a todo tipo de penurias y persecuciones sin parangón en la era moderna; un potente apoyo económico, militar y técnico -de beneficios mutuos a priori y posteriori- de China y en algunos casos de Rusia; una fe y ansiedad ciegas en lograr el éxito del programa para dejar de ser considerado uno de los grandes parias del mundo; saber tensar y mucho la cuerda sin dejar que nunca se rompiera y el encontrar al egocéntrico adecuado para que, en el momento culminante de su exacerbado afán de protagonismo y total culto a su persona, fuera capaz de saltarse a torera todo protocolo, asesoramiento juicioso y no tuviera en cuenta los riesgos de una negociación que puede ser tan peligrosa para ellos y sus socios del lugar, como espectacular en la esfera interna e internacional.

Trump lleva meses enfrentándose, despreciando, vejando y amenazando a todos sus vecinos, aliados y colegas o no en todo tipo de foros, alianzas, tratados, acuerdos y convenios en los que figura en cabeza o, incluso, fueron fruto de iniciativas norteamericanas. Casi no queda ninguno en pie, ha roto o desvencijado todos los moldes y ha echado por tierra, lustros y lustros de esfuerzos y negociaciones de sus predecesores en el cargo y de la imponente y avasalladora maquinaría diplomática y comercial de EEUU. Es especialista en salir de sus reuniones insultando, de forma precipitada y dando un tremendo portazo – véase el último ejemplo hace poco tras la reunión del G-7 en Canadá-.

Desde su nombramiento como Presidente de EEUU y líder de la CI ha vilipendiado y despreciado especialmente a Kim-Jong-un con todo tipo de motes, insultos y calificativos despectivos. Ha amenazado varias veces al país con su destrucción y repetido en ocasiones su intención de anular esta cumbre incluso a escasas horas antes de su celebración. Como gran estratega y experto del dialogo, basaba ayer mismo la duración y efectivad de la misma en el olfato personal y sobre todo en su primera impresión.

Sin embargo o pese a todo ello, otro ególatra y despiadado dirigente que no solo menosprecia a las personas, sino que las persigue y las hace desaparecer por cualquier motivo o razón, y que se siente venerado por su “amado pueblo”, ha resistido y superado todos los escollos e insultos anteriores y no solo le ha estrechado la mano esta mañana a Trump, sino que ha hablado con él mucho más del tiempo previsto e, incluso y fuera de todo cálculo según lo previamente filtrado, ha compartido mesa y mantel durante varias horas con él.

Todos sabemos que, debido a los grandes escollos y dificultades en el “lenguaje y pretensiones" de ambos países, llevar a cabo determinadas relaciones productivas y adecuados avances en las mismas entre las respectivas comisiones, no es nada fácil; y mucho menos, sentar a sus "especiales" líderes a la misma mesa con un detallado programa lleno de puntos de calado, debidamente tasados y acotados en el fondo y forma y con un tiempo límite para su aplicación. Además, no hay que menospreciar la mutua desconfianza entre ambos, por motivos bien patentes y en base al nulo o muy limitado mantenimiento, abandono o rotura prematura de acuerdos alcanzados entre los dos países recién o pretéritamente.

No se fían por razones obvias y principalmente porque Kim entiende o debe tener presente que acuerdos o promesas similares -en los que se garantizaba la supervivencia personal a otros sátrapas y proliferadores en armas de destrucción masiva como Sadam Husein o Gadafi, si aquellos abandonaban todas sus prácticas y programas- no se respetaron por mucho tiempo tras creérselos y desmantelar aquellos sus respectivas instalaciones. Ambos tuvieron que sufrir en propias carnes unas despiadadas persecuciones y muertes nada dignas a manos de sus “garantistas de por vida” los norteamericanos. Esto en el plano personal; porque no debemos olvidarnos de la reciente denuncia y abandono unilateral por parte de EEUU del acuerdo sobre el programa nuclear de Irán.

En función de todo lo anterior y por la dificultad y complejidad que encierra el tema y sus derivadas en el acuerdo y por la escasa preparación previa y duración de la Cumbre, es muy normal que solo se haya podido alcanzar y hacer público un poco desarrollado acuerdo de mínimos que yo lo calificaría de “buenas intenciones” y un tanto de venta de humo a raudales. Poco ha sido lo alcanzado, dado lo no mucho publicado. A estas horas y como informe preliminar, baste con lo más detallado que he encontrado en la prensa española sobre el tema [2]. En dicho artículo, a su izquierda y en recuadro, se pueden ver plasmados los cuatro puntos principales alcanzados y firmados en el acuerdo. Hace falta una gran dosis de buena voluntad para interpretar algo más de lo que en ellos se dice.

Quedan muchos flecos pendientes. Flecos, nada nimios como son: los plazos para su puesta en práctica y finalización; fases y pasos intermedios; situación final a alcanzar; compensaciones económicas, sociales y técnicas; grado, autoridad y políticas de integración peninsular en su caso; acciones a tomar en lo referente al restablecimiento

del respeto a los derechos humanos en CN; papel y punto de implicación que deben adoptar los países vecinos afectados, preferentemente China, Japón y Corea del Sur; plazos y condiciones para el levantamiento de las sanciones y restricciones; internacionales y bilaterales; nivel y plazos para el necesario desmantelamiento parcial de las enormes fuerzas militares norcoreanas y el papel de futuro referente a la presencia, despliegue, continuidad y actividad combinada y conjunta de las fuerzas norteamericanas con las de sus aliados en despliegues permanente y ejercicios militares puntuales.

Muchos puntos, al parecer no tocados, o simplemente mencionados sin profundizar. De un valor e importancia tal que el fallo o la falta de acuerdo en, muchos por no decir todos ellos, puede dar al traste con toda esta parafernalia al puro estilo de los grandes imperios en los momentos en los que el Emperador de turno recibía con todo boato, antes de mandar acuchillar, a su hasta hace nada preocupante amenaza o terrible enemigo.

Hoy podemos dormir todos algo más tranquilos, aunque la vigilia o duermevela no debe abandonarse. Algunos como en CN se verán menos presionados, al menos inicialmente, otros como los chinos ven, por fin y tras casi 70 años, como las botas y las armas nucleares norteamericanas se alejan de sus fronteras y que como consecuencia del tremendo consumo de adrenalina por parte de sus vecinos y, en consecuencia, el potencial aumento de la despreocupación militar norteamericana en dicha zona, sus rutas, conquistas y nuevos despliegues por el Mar del Sur de China están hoy ya, menos amenazadas y serán más rápidas.

Los surcoreanos en gran medida y los japoneses en su parte alícuota deberán decidir si prosiguen en su carrera de rearme a ultranza o, por el contrario, dedican sus esfuerzos en mejorar otros aspectos de sus economías.

Solo me resta, entender, que es lo que ha ganado Trump y EEUU en este paripé de abrazos y casi besos. Tras el fulgurante efecto castillo de fuegos de artificio -al más puro estilo socialista en España- al aprovechar con cierto efecto el inicial éxito en situaciones desesperadas, pero que en realidad nunca han amenazado a su patria; perderá presencia en la zona lo que rápida y fácilmente se traducirá en menor prestigio y muy probablemente venderá muchas menos armas sofisticadas en una zona que, estaba en ello, y a la que pretende conquistar económica y políticamente ¿Acaso busca ahorrar esfuerzos y volverlos a enfocar en Oriente Medio? ¿Es solo cuestión de marketing interno y compensatorio externo tras una larga lista de meteduras de pata y despropósitos internacionales? ¿O solo pretende despistarnos y lo que persigue es acercarse y mucho más a los chinos, rusos, iraníes e indios [3]? Pronto lo veremos, seguro.

**Referencias**

[1] https://sites.google.com/site/articulosfjavierblasco/corea-del-norte-algo-deja-vu
[2] https://elpais.com/internacional/2018/06/12/actualidad/1528766187_744971.html
[3] https://www.efe.com/efe/espana/mundo/china-presume-de-unidad-con-rusia-india-o-iran-frente-a-la-division-del-g7/10001-3643910

Fuente de la Imagen:
https://img.kyodonews.net/english/public/images/posts/710ac39eef20bca3eb59b18a4bd584b5/cropped_image_l.jpg

# La realidad de Medellín: entre la innovación y la violencia

Por Haylyn Andrea Hernández Fernández (Colombia)

La globalización y el rápido crecimiento demográfico han sido determinantes para los modelos que organizan los procesos de urbanización del siglo XXI, en consecuencia, el desarrollo de las ciudades y su importancia en la arena internacional ha ido en aumento, incluso llegando a tener un protagonismo crucial que desborda las tradicionales concepciones estado-céntricas. Al respecto, la socióloga Saskia Sassen, cree que "las ciudades van a ser más importantes que los Estados", afirma que hay una especie de geopolítica urbanizada, que se concentra en vectores o ejes. Más importante que Estados Unidos, en términos de geopolítica mundial, será el eje de Washington, Nueva York y Chicago, para el caso de China, va a ser Hong Kong, Shanghái y Pekín, y para Turquía Ankara y Estambul, se vuelven más importantes que el país en sí (Armada, 2013).

Para el caso colombiano, una ciudad que marca la diferencia por su innovación y vanguardia es Medellín. En 2017 la agencia de innovación australiana 2ThinkNow reconoció a Medellín como una de las ciudades más innovadoras del mundo, la única de Colombia que ha logrado ingresar a este índice, esto es una muestra del potencial de la ciudad, lo que permite atraer inversión y talento. La capital antioqueña está en la categoría 'HUB', la segunda más avanzada, después de 'Nexus', que es liderada por Londres; las ciudades 'HUB' son territorios desafiantes, centros de actividad de innovación, ejes con influencia en segmentos sociales y económicos claves (El Tiempo, 2017).

No obstante, la cosmopolita metrópoli tiene otra cara que mostrar en materia de seguridad. Medellín cerró el 2017 con 577 homicidios, 33 más que en 2016, 318 de los casos fueron atribuidos por las autoridades al enfrentamiento entre grupos delincuenciales (Restrepo, 2018). De acuerdo con hipótesis de la Policía Metropolitana y la Alcaldía, los últimos homicidios violentos registrados, que se caracterizaban por ser casos de personas torturadas y abandonadas en bolsas plásticas, se deben a la captura de Juan Carlos Mesa Vallejo, alias 'Tom, o Carlos Chatas', uno de los más sanguinarios cabecillas de la 'oficina de Envigado'.

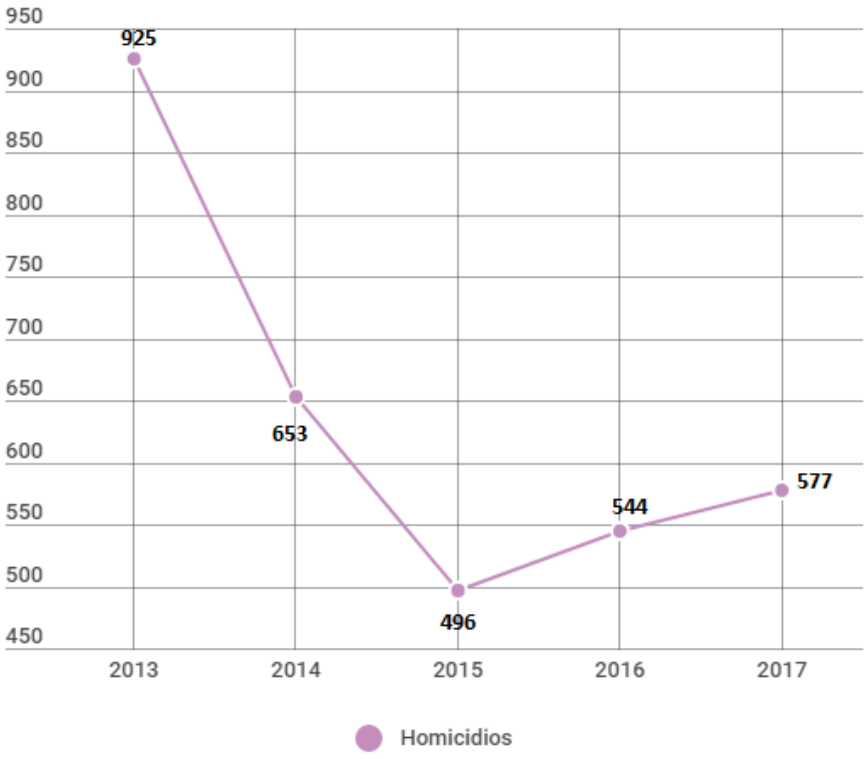



**Figura 1. Evolución histórica de homicidios.** Adaptado de: Restrepo, V. (2018, enero 1). Medellín cerró el año con 577 homicidios.

Según el último informe del Consejo Ciudadano para la Seguridad Pública y Justicia Penal, una organización civil mexicana que cada año elabora un listado con las 50 urbes más violentas del mundo, América Latina es la región que alberga el mayor número de ciudades violentas: 17 están en Brasil, 12 en México, 5 en Venezuela, 3 en Colombia y 2 en Honduras (BBC Mundo, 2018). Si bien Medellín presenta un aumento en el número de homicidios en los últimos dos años, por tercer año consecutivo estuvo fuera del listado de las ciudades más violentas del mundo, cuando por más de 15 años encabezó esta lista. Las ciudades colombianas incluidas en el ranking son Cali, Palmira y Cúcuta con los puestos 28, 37 y 50 respectivamente.

Por otro lado, la Encuesta de Percepción Ciudadana 2017 del programa Medellín Cómo Vamos, evidencia que la percepción de seguridad de los ciudadanos disminuyó 4 puntos porcentuales con respecto al año anterior, el 69% afirma sentirse seguro. Dentro de los problemas más graves que se mencionan con respecto a la seguridad lo encabeza la drogadicción con un 33%, las pandillas o combos 25% (al mando principalmente de la Oficina de Envigado y del Clan del Golfo, que se enfrentan por el control del crimen organizado en la ciudad), atracos callejeros 16%, tráfico de drogas 9%, entre otros (Medellín Cómo Vamos, 2017).

En este sentido, la ciudad de la eterna primavera presenta una realidad ambivalente, por un lado, es un gran referente mundial de planificación urbana, y por el otro, sigue siendo epicentro de criminalidad y violencia a pesar de no estar en el listado de las ciudades más violentas del mundo.

> La ciudad crece demográfica, económica y políticamente como un ejemplo de una ciudad exitosa, mientras que continúa constituyéndose como un epicentro de la criminalidad y la violencia, alcanzando cifras que la han situado dentro de las ciudades más violentas del mundo, debido al desarrollo de diversas actividades criminales, que van desde la microextorsión hasta el tráfico de drogas, armas y demás actividades propias del crimen organizado transnacional (Patiño Villa et al., 2015, p. 14).

Carlos Patiño expone que, pese a ser una de las pocas ciudades que ha destinado tantos recursos públicos para el desarrollo del urbanismo social y ejecutar proyectos integrales, la violencia y criminalidad persisten. La paradoja continúa: mientras existen ambiciosos planes de políticas públicas para combatir los problemas sociales, los índices de inseguridad y violencia colectiva todavía son elevados (2015, pp. 177-178).

En la actualidad operan estructuras ilegales responsables de homicidios, microtráfico, extorsión, desplazamientos y demás actividades criminales que alteran la seguridad. De acuerdo con cifras de la Dirección de Investigación Criminal e Interpol para el periodo del 01 de enero al 30 de abril de 2018, se han presentado 180 casos de homicidios (Policía Nacional de Colombia, 2018), por su parte, el Sistema de Información para la Seguridad y Convivencia -SISC- de la Alcaldía de Medellín, registra 199 personas asesinadas, 39 más que en el mismo período del año pasado. La tendencia, hasta ahora, es al alza: 9 de las 16 comunas y dos de los 5 corregimientos tienen aumento en esa estadística (Restrepo, 2018).

Precisamente la Comuna 13 ha sido escenario de un constante asedio criminal con balaceras, muertos, heridos, quema de buses y escuelas vacías por el accionar de las organizaciones delincuenciales, lo cual generó una respuesta institucional con la presencia de 320 policías y militares para controlar la situación, en el corregimiento de Altavista también se ha dado un refuerzo a la seguridad. Según el secretario de Seguridad, Andrés Tobón, la comuna 13, Robledo y Altavista son de gran interés para las organizaciones criminales porque constituyen un corredor estratégico para el transporte de armas y estupefacientes (El Tiempo, 2018).

Además de la ofensiva entre combos y grupos criminales que se disputan el control territorial, esta situación tiene un trasfondo y es el enfrentamiento entre las organizaciones y el gobierno local, esto debido a la guerra que declaró el alcalde Federico Gutiérrez, contra dichas estructuras criminales.

En la última rendición de cuentas del alcalde el pasado mes de marzo, se destacó la captura de 10 líderes de las Organizaciones Delincuenciales Integradas al Narcotráfico -ODIN- en 15 meses: alias ‘Jumbo’, ‘Soto’, ‘Camellete’, ‘Queso’, ‘Abelito’, ‘Mateo’, ‘El Chivo’, ‘Camilito’, ‘Tom’ y ‘Elkin Triana’(Alcaldía de Medellín, 2018). Gutiérrez ha calificado estas capturas como un logro de la ciudad ya que fueron producto de la acción conjunta de la Policía, Fiscalía, Ejército y la administración.


**Figura 2. Capturas relevantes 2016-2017.** Adaptado de: Alcaldía de Medellín. (2018). 2016-2019 Segundo informe de gestión. Audiencia Pública de Rendición de Cuentas.

Como consecuencia del aumento de la violencia, también se debe contemplar la posibilidad del desgaste del 'Pacto del fusil' de julio del 2013, el cual se dio como un acuerdo de no agresión, cooperación en actividades ilícitas y establecimiento de división de los territorios de la ciudad entre la Oficina de Envigado y el Clan del Golfo, autodenominado Autodefensas Gaitanistas de Colombia. Así que la relativa estabilidad de las estructuras criminales, gracias a la tregua, puede estar llegando a su fin debido a las capturas, ya que se están generando vacíos significativos de poder que están reactivando una guerra urbana que profundiza la desestabilización de la ciudad.

Aun así, parece no ser suficiente que el alcalde se atribuya como personal el combate de las organizaciones criminales. El revés que sufrió la administración con el entonces secretario de seguridad y hombre de confianza, Gustavo Villegas, capturado en julio de 2017 por su supuesta conexión con la Oficina de Envigado, y las conversaciones entre alias Pichi, jefe de la banda la Terraza, y Carlos Pesebre, líder de la organización Pesebre, quienes desde la cárcel de Cómbita estarían promoviendo un plan conjunto para desestabilizar Medellín (Semana, 2018), son muestra de las trabas que se han presentado en la gestión del alcalde, quien debe frenar la oleada criminal y mostrar resultados contundentes para hacerle frente al desafío que le impone la ilegalidad y las organizaciones criminales.

Las autoridades aseguran que los recientes hechos violentos no obedecen a la expansión de grupos criminales, sino a una reacción de estos ya que están desesperados con las capturas de los cabecillas. La Defensoría del Pueblo, además, asegura que el fenómeno se ha generado por cuenta de los cambios y la reconfiguración de las alianzas entre estructuras ilegales y la disputa de dos organizaciones por el monopolio de las economías ilícitas.

> De un lado el grupo ilegal posdesmovilización de las AUC: Autodefensas Gaitanistas de Colombia, pretende mantener el control sobre corredores de movilidad de economías ilegales, asegurando la lealtad de grupos armados locales que operan en el territorio, a través de la imposición de mandos foráneos y la intimidación de la población civil; y del otro, organizaciones criminales de incidencia territorial limitada, pero articuladas a estructuras de mayor capacidad armada y económica de la llamada Oficina de Envigado, pretenden disputar el control de dichos corredores de movilidad. (Defensoría del Pueblo Colombia, 2018)

Hasta este punto es claro que la dinámica evidencia que las organizaciones criminales tienen la capacidad de reinventarse con el fin de evadir los controles institucionales, lo que implica para el Estado estar a la delantera para impedir que se fortalezcan y trasciendan en el tiempo.

La situación es compleja y no se resuelve únicamente con medidas tradicionales de seguridad ciudadana, ya que en la población hay un sentimiento de incertidumbre que pone en entredicho la capacidad del Estado para controlar las organizaciones criminales y la legitimidad de las instituciones de seguridad y justicia que algunas veces son cooptadas por la corrupción, se deben tomar decisiones y ejecutar acciones estructurales que abarquen por completo el territorio, con el fin de tener una paridad visible entre la innovación y la seguridad.

**Referencias**


Alcaldía de Medellín. (2018). 2016-2019 Segundo informe de gestión. Audiencia Pública de Rendición de Cuentas. Recuperado a partir de https://www.medellin.gov.co/irj/go/km/docs/pccdesign/medellin/Temas/PlanDesarrollo/rendicion/Shared%20Content/2018/RENDICION%20DE%20CUENTAS%202017.pdf

Armada, A. (2013). «Las ciudades van a ser más importantes que los estados». Recuperado a partir de http://www.abc.es/20120612/sociedad/abci-ciudades-importantes-estados-201206112005.html

BBC Mundo. (2018, marzo 7). Estas son las 50 ciudades más violentas del mundo (y 42 están en América Latina). Recuperado a partir de http://www.bbc.com/mundo/noticias-america-latina-43318108

Defensoría del Pueblo Colombia. (2018, abril 24). Alterta Temprana de Inminencia No. 041-18. Recuperado a partir de https://verdadabierta.com/wp-content/uploads/2018/04/AT-N%C2%B0-041-18-ANT-Medelli%CC%81n.pdf

El Tiempo. (2018, abril 30). Persiste la violencia en Robledo, segunda comuna con más homicidios. Recuperado 24 de mayo de 2018, a partir de http://www.eltiempo.com/colombia/medellin/persiste-la-violencia-en-robledo-segunda-comuna-con-mas-homicidios-211808

El Tiempo. (2017, febrero 28). Medellín recibe nuevo reconocimiento como ciudad innovadora. *El Tiempo*. Recuperado a partir de http://www.eltiempo.com/colombia/medellin/medellin-recibe-nuevo-reconocimiento-como-ciudad-innovadora-62420

Medellín Cómo Vamos. (2017, noviembre 1). Presentación: Encuesta de Percepción Ciudadana, Medellín 2017. Recuperado 24 de mayo de 2018, a partir de https://www.medellincomovamos.org/download/presentacion-encuesta-de-percepcion-ciudadana-medellin-2017/

Patiño Villa, C. A., Zambrano Pantoja, F. R., Montenegro Lizarralde, F., Viviescas Monsalve, J. F., González Borrero, J. I., Montoya Pino, A. P., … Romero Quiñones, M. C. (2015). *Medellín: territorio, conflicto y Estado. Análisis geoestratégico urbano*. Bogotá, D.C., Colombia: Editorial Planeta Colombina S.A.

Policía Nacional de Colombia. (2018). Homicidios 2018. Recuperado 24 de mayo de 2018, a partir de https://www.policia.gov.co/observatorio/estudio_criminologia

Restrepo, V. (2018, mayo 3). ¿Cómo le ha ido al alcalde de Medellín con la seguridad? Recuperado 24 de mayo de 2018, a partir de http://www.elcolombiano.com/antioquia/seguridad/seguridad-en-medellin-balance-del-alcalde-EX8642789

Restrepo, V. (2018, enero 1). Medellín cerró el año con 577 homicidios. Recuperado 23 de mayo de 2018, a partir de http://www.elcolombiano.com/antioquia/seguridad/homicidios-en-medellin-durante-2017-FD7948557

Semana. (2018, abril 27). Bajo el asedio criminal: ¿qué está pasando en Medellín? Recuperado 24 de mayo de 2018, a partir de https://www.semana.com/nacion/articulo/crisis-criminal-en-medellin-y-la-comuna-13/565134

# LISA Institute
## Security Education

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

REINVENTANDO LA FORMACIÓN EN
## SEGURIDAD e INTELIGENCIA

Fórmate Online con Expertos.
Cuando quieras. Donde quieras.

CURSOS CON INSCRIPCIONES ABIERTAS

**INTELIGENCIA**

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

**TERRORISMO**

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

# 15%

Código de Descuento: *TRIARIUS15*

(Promoción válida hasta fin de existencias)

***Inscríbete ahora en www.LISAINSTITUTE.com***

# En el Reino de los Señores de la Guerra

Por Alfredo Campos (España)

"¡Perded toda esperanza los que entráis!"
(De Infierno Canto III, Sentencia 7-9, La Divina Comedia, Dante Alighieri)

En el corazón del continente, África tiene una herida por la que se desangra desde hace más de 5 años, y esa herida se llama República Centroafricana. La precaria situación de seguridad de la incipiente nación favorece la inestabilidad permanente, lo que supone un obstáculo enorme de cara a cualquier iniciativa que busque consolidar estructuras estatales más allá de su capital Bangui, así como para su propio desarrollo económico. Pero el conflicto centroafricano constituye además un mal endémico regional: la posición geográfica central de la República que comparte fronteras con países que afrontan graves problemas de seguridad: Chad, Sudán, Sudán del sur, República Democrática del Congo y Camerún; la convierten en un territorio estratégico para la región, corredor clave para combatientes y mercenarios.

La República Centroafricana ostenta el dudoso honor de iniciar el descenso más rápido a los "infiernos" para convertirse en el país más pobre del mundo, desde luego es uno de los más inestables, a merced de innumerables señores de la guerra que han hecho del conflicto permanente y la actuación criminal su lucrativo modo de vida. Los grupos criminales campan a sus anchas, bandas que se han gestado al calor de la depredación de las sucesivas élites políticas y a una ausencia casi total del aparato del estado en la mayor parte del país. Los líderes de los grupos armados, con el fin de legitimar su actuación, han alimentado un artificioso conflicto religioso entre cristianos y musulmanes, y disputas entre comunidades que incluso llegaron a la limpieza étnica. Mientras tanto, estos grupos sacan partido de negocios criminales tales como el contrabando de diamantes o la explotación ilegal de otros recursos naturales, llegando a convertir la violencia en un negocio rentable.

Desde el punto de vista humanitario, esta situación genera una catástrofe sin precedentes que a finales de 2017 ya había provocado la huida de 1,1 millones de personas; una cuarta parte de la población total. Dicha crisis amenaza con extenderse por toda la región y cronificarse en el tiempo. Con el presente artículo trato de desentrañar las claves de un conflicto tan complejo como dinámico e imprevisible.

**Antecedentes Históricos**

El territorio que ocupa la actual República Centroafricana históricamente albergaba el sultanato esclavista de Dar al-Kuti que ya en el siglo XIX fue

sustituido por la dominación francesa. Los nuevos administradores coloniales favorecieron algunos grupos étnicos sobre otros: como sucedió con las poblaciones ribereñas del sur como los Ngbaka (Mbaka), los Yakoma y los Ubangi, a partir de los cuales formaron las élites dominantes en el país, en detrimento de otras comunidades del norte que se han sentido desde entonces discriminadas.

La República Centroafricana, denominada Ubangi-Shari durante la colonización, consiguió su independencia de la metrópolis francesa en 1960. No obstante, nunca ha dejado de permanecer en la órbita de ese difuso espacio del continente africano de especial interés geoestratégico para el país galo llamado Françafrique. El país se encuentra en una posición clave en el continente ya que se extiende a lo largo de dos líneas de fractura del continente: una que separa el mundo árabe con el africano y otra que delimita las zonas de expansión del cristianismo y otras religiones animistas del islam. Si trazamos una línea imaginaria entre territorios de población mayoritaria de una de estas religiones mencionadas, seguiría una ruta que va desde África occidental, atravesando Nigeria, pasando por el extremo norte de República Centroafricana, Sudán del Sur, bordeando Etiopía por su extremo sur para terminar en Somalia. Por ello, no sorprende que a lo largo de esta línea desplieguen su actividad muchos grupos armados como Boko Haram o Al Shabah y algunos otros más que utilizan el elemento religioso como factor identitario y motivador de su lucha armada.

El primer presidente de la joven nación fue David Dacko, quien llegó al poder a través de un golpe de estado respaldado por Francia. Posteriormente, en el año 1965 Dacko fue derrocado por su primo; el coronel Jean-Bedel Bokassa que gobernó de manera dictatorial, proclamándose incluso emperador y convirtiéndose al islam para obtener el favor del líder libio Muammar el Gadafi. El mandato del infame dictador Bokassa se caracterizó por los graves abusos y violaciones de derechos humanos y en el año 1979, Francia ya había rebajado bastante su apoyo al dictador, lo que se materializó en un golpe de estado en su contra, reponiendo en el poder a Dacko nuevamente. En 1981, el general André Kolingba se alza al poder mediante un nuevo golpe. Nuevamente, Francia tuteló el proceso transicional desde el presidente Kolingba a Ange-Félix Patassé.

En mayo de 2001, Patassé sofocó un intento de golpe de estado con el apoyo de combatientes del líder rebelde de República Democrática del Congo Jean-Pierre Bemba y milicianos libios. La represión posterior fue de tal magnitud como para ser calificada de crimen de guerra. El posterior gobierno del militar François Bozizé fue apoyado por la antigua colonia francesa y coincidió con un período de inestabilidad, favorecido por la complicada situación regional en los países vecinos de Chad, Sudán y República del Congo, hasta la firma del acuerdo de paz en Birao el 13 de abril de 2007. Bozizé resulta elegido nuevamente en unas elecciones que son calificadas de pantomima por la oposición.

En el año 2013, se produce el enésimo golpe de estado. Un grupo de rebeldes se había unido desde el año 2012 en una coalición denominada Séléka ( “alianza” en el idioma local Sangho) con la religión musulmana y la etiqueta de minoría oprimida por la mayoría cristiana como factor identitario. Séléka estaba formada por combatientes musulmanes con fuertes vínculos transfronterizos con Chad y Sudán (mercenarios chadianos y sudaneses, éstos últimos dirigidos por el general Moussa Asimeh, acusado de genocidio por crímenes en Darfur) de la región fronteriza del noreste de República Centroafricana. Desde su origen, no obstante, se reveló que poco más que el ansia de poder y riqueza y un fuerte deseo de venganza motivaba la unidad de los líderes de este grupo. De hecho, posteriormente este grupo va a experimentar numerosas divisiones en los años 2013-14. Bozizé cae en marzo de 2013 y parte hacia el exilio, momento a partir del cual la República Centroafricana se ve inmersa en una espiral de caos y anarquía que llega hasta nuestros días.

La actuación de la coalición séléka recibió una amplia condena por parte de la comunidad internacional. Además, la nueva administración se planteó revisar los contratos de explotación minera firmados por el anterior mandatario con compañías chinas y sudafricanas. Como respuesta a la insurgencia de los Séléka, se forman las milicias antibalaka (“anti machete” o antibalas de AK 4” – “anti-balles-AK” en lenguas locales). Tienen la creencia generalizada de que los amuletos y objetos que portan les protegen de las balas para combatir a los primeros y a las comunidades musulmanas en general. En sus inicios, estas milicias se organizan en la capital Bangui, en el año 2013 en torno a grupos de milicianos cristianos y animistas motivados por la agitación del imaginario histórico popular de respuesta frente a las expediciones esclavistas de los musulmanes del noreste así como a la frustración por su prevalencia en los sectores del comercio y la minería. La agitación del factor identitario religioso alcanza su punto álgido bajo el mandato del derrocado presidente Bozizé, que lideraba una iglesia evangélica durante su mandato y posteriormente fue uno de los principales patrocinadores del movimiento anti-balaka desde el exilio. Aunque el elemento

religioso no parece estar en la raíz del conflicto centroafricano, una consecuencia directa de dichas tensiones ha sido los elevados niveles de violencia sectaria que se han producido durante la guerra.

**El conflicto deriva en la anarquía**

El actual conflicto que asola la República Centroafricana tiene unos contornos que reflejan la competición por acceder a los recursos naturales, el control del comercio y las redes financieras y la identidad nacional y étnica. Antes del conflicto, la población centroafricana se distribuía aproximadamente entre el 85% de población cristiana y animista y el 15% de población musulmana.

**División étnica de la República Centroafricana.**

Como indiqué anteriormente, François Bozizé es derrocado en el año 2013 por la alianza séléka, que controla el país llegando a las puertas de Bangui. Bozizé se ve obligado a firmar un acuerdo de paz cuya duración es exigua ya que el 24 de marzo de 2013, séléka aúpa al militar Michel Djotodia al poder. El gobierno de Bangui era incapaz de mantener el orden más allá de la capital y se sucedían los ataques a la población cristiana y a las iglesias, lo que llevó al presidente Djotodia a ordenar la disolución del grupo armado séléka, aunque muchos comandantes de esta milicia ignoraron la medida demostrando la falta de autoridad del líder de la coalición sobre éstos dado que operaban con bastante autonomía debido a su origen sudanés o chadiano. Por otro lado, tanto Djotodia como la coalición séléka que lideraba, desde su llegada al poder, demostraron carecer de agenda más allá de derrocar al presidente Bozizé y depredar los recursos naturales del país.

Como ya es sabido, esta situación provoca la reacción de los antibalaka, originariamente nacidos en la década de los 90 para proteger a la población de bandidos y delincuentes, y el estallido de la violencia entre ambos grupos, que ven en esta situación una oportunidad única para instrumentalizar las diferencias religiosas en su provecho. La violencia sectaria causa miles de muertos y provoca el desplazamiento de más de un millón de personas a lo largo del país. Como telón de fondo de este conflicto fratricida está la explotación de áreas ricas en recursos minerales, qué es la verdadera razón de ser del conflicto que se revela más intenso en estas regiones.

Los séléka son obligados a abandonar Bangui ante el empuje de las milicias antibalaka en enero de 2014. En su lugar, ocupan sus reductos en el norte y noreste del país donde obtienen recursos de la explotación de las minas de oro y diamantes. Por su parte, los antibalaka se asientan en la región suroeste donde hay importantes minas de diamantes. Ambos grupos utilizan la limpieza étnica contra los miembros de la comunidad rival, produciéndose masacres de cristianos o musulmanes en función del territorio y qué grupo lo controla.

La presión internacional obliga a Djotodia a dimitir en enero de 2014 y es sustituido por la dirigente Catherine Samba-Panza que ocupa el cargo de presidente de manera transitoria. El panorama no obstante es desolador: unas Fuerzas Armadas inoperantes cuyos miembros además en no pocos casos tienen nexos con los grupos armados irregulares. En medio de la anarquía, la seguridad de la población queda en manos de diferentes misiones internacionales que menciono más adelante.

El 23 de julio de 2014, los grupos armados antibalaka y antiguos séléka (más adelante hablaré de la evolución de estos grupos, firman un acuerdo de cesación de hostilidades, aunque siguen actuando con gran intensidad en buena parte del país y son los responsables de un buen número de atroces violaciones de derechos humanos cometidas contra la población civil y episodios de limpieza étnica, lo que ha profundizado la brecha y la animadversión entre las diferentes comunidades que pueblan el país. El conflicto que estalló en 2013, en muchas ocasiones lo que ha venido es a reactivar viejas tensiones subyacentes, relacionadas con la competición por el uso de los recursos, como por ejemplo la existente entre las comunidades de granjeros y los ganaderos trashumantes del grupo Mbororo (subgrupo de los peul o fulani); que ha resultado en violencia y desplazamiento para los miembros de este último grupo a manos de los antibalaka; lo que a su vez ha causado que algunos hayan terminado uniéndose a las filas de los grupos ex-Séléka.

**El papel de las misiones internacionales y los actores regionales**

Con la llegada al poder de Djotodia se marca el punto de partida de las misiones internacionales, debido a la falta de control de éste sobre el territorio y las enormes dimensiones que estaba alcanzando la crisis humanitaria. El 5 de diciembre de 2013, las Naciones Unidas aprueban la Resolución 2127/2013, autorizando el despliegue de la Misión Internacional de Apoyo a la República Centroafricana (MISCA), apoyada por una fuerza militar francesa. Esta misión de apoyo recibió el nombre de Operación Sangaris.

A su lado, la misión EUFOR RCA se constituye de manera temporal el 10 de febrero de 2014 para prestar apoyo temporal a las misiones ya citadas, estabilizar algunos de los sectores más peligrosos de

la capital y dar el relevo al despliegue de Naciones Unidas (MINUSCA). En esta misión, unidades del ejército y la Guardia Civil de España tuvieron un papel destacado.

Unos 9.000 soldados aproximadamente se revelaban claramente insuficientes para mantener el orden en un país del tamaño de Francia y de población muy dispersa. Rápidamente se tomó conciencia por parte de todos los actores implicados; República Centroafricana, Unión Africana y Naciones Unidas, de la necesidad de un enfoque integral en el mantenimiento de la paz en el que la protección de los civiles fuese la principal prioridad. La Resolución 2149/2014 del Consejo de Seguridad habilita el lanzamiento de la Misión Multidimensional Integrada de Estabilización de las Naciones Unidas en la República Centroafricana MINUSCA, autorizando el despliegue de un máximo de 12.000 efectivos. Para expertos en la región como el teniente coronel Jesús Díez Alcalde, la misión nació en 2014 marcada desde un primer momento como insuficiente para frenar el caos y la violencia que se había ya extendido a lo largo de todo el país; con la grave amenaza de cronificar la situación de la división del país por razones sectarias y el imperio de los grupos armados y los señores de la guerra.

Casi cuatro años después, la situación no es muy halagüeña y la tarea de la MINUSCA puede calificarse haciendo un símil cinematográfico de "Misión Imposible". La Misión ha sido renovada por la Resolución 2387 (2017) del Consejo de Seguridad, ampliando el mandato de la misma hasta el 15 de noviembre de 2018. Pese a que a lo largo de 2017 se han producido tímidos avances en el despliegue de la autoridad del estado a lo largo del país, la violencia persiste de manera generalizada. La culpa de ello es achacable en gran medida al empleo de una retórica incendiaria, la estigmatización étnica y la manipulación religiosa por parte de políticos y medios de comunicación, creando un caldo de cultivo propicio para la reactivación del conflicto. Si bien ha disminuido la violencia entre comunidades, los enfrentamientos entre grupos armados y milicias de autodefensa han aumentado en los últimos tiempos, especialmente en las áreas donde se producen movimientos migratorios estacionales. Queda claro que la carrera por dominar territorio y acceso a los recursos naturales es el principal factor causante de la violencia entre los diferentes grupos armados.

Al oeste del país, coincidiendo con la reapertura de los corredores de trashumancia, la fuerzas antibalaka se han enfrentado a grupos de pastores de etnia fulani en la prefectura de Mambéré-Kadéi después de que miembros de este grupo saquearan poblaciones cerca de Gamboula asesinando a civiles. La MINUSCA ha tenido éxito en terminar con la presencia de grupos armados como 3R en Bocaranga y el Movimiento Patriótico por Centroáfrica MPC en Bang (luego me referiré más en detalle a estos grupos), logrando que los primeros firmaran un acuerdo con las milicias antibalaka locales en Bouar, para terminar con la espiral de violencia en la región.

En el lado negativo, surgen nuevos grupos como escisiones de los ya existentes como el Movimiento Nacional para la Liberación de Centroáfrica (MNLC), surgido del MPC, en pugna con otros grupos para hacerse con el control del territorio y las rutas de comercio en la esquina oeste del país. En otras prefecturas como la de Ouham más al este, los combates entre las milicias antibalaka y los grupos ex-séléka provocaron la destrucción de poblaciones e importantes movimientos de desplazados. No son pocos los grupos que aún hoy en día sabotean los tímidos intentos de restablecer la autoridad del estado. Además, en la esquina este operan otros grupos armados desde la vecina Uganda como la milicia del Lord´s Resistance Army (LRA), que constituyen una serie amenaza para la población civil.

Paradógicamente, la situación en la capital Bangui es de relativa estabilidad pese a los rumores de que podría estar gestándose una insurrección armada. El año 2017 ha sido además el año más funesto para los miembros de las misiones de mantenimiento de la paz con 13 personas muertas en diferentes circunstancias.

Paralelamente, se desarrolla una operación de entrenamiento militar europea denominada EUTM RCA para apoyar a las Fuerzas Armadas de la República Centroafricana. España ha participado desplegando 30 militares pertenecientes al ejército europeo.

Al mismo tiempo, las fuerzas especiales estadounidenses desembarcaron en el país en diciembre de 2011, estableciendo una base en el extremo sureste como parte de una misión para neutralizar al rebelde de origen ugandés Joseph Kony, líder del "Ejército de Resistencia del Señor". La República Centroafricana se encuentra incluida en un grupo de 10 países de la región África Central cuyo ámbito se engloba en la actuación del Comando Africano (AFRICOM) con sede en Stuttgart (Alemania). Las tropas se establecieron en la ciudad de Obo con apoyo de militares locales y fuerzas armadas de Uganda. Aunque la misión fue declarada finalizada sin éxito, se desconoce a día de hoy si continúa presente algún contingente de tropas norteamericanas en la región.

Frente al despliegue de Europa y Estados Unidos, Rusia y China pugnan por hacerse hueco en una región tan complicada como codiciada por sus abundantes recursos minerales. En 2017 la ONU autorizó una excepción a Rusia para proporcionar armas y personal militar al gobierno de Bangui, fundamentalmente para colaborar en el sostenimiento del asediado gobierno central y sus débiles fuerzas armadas. Esta posición privilegiada ha permitido a Putin firmar acuerdos bilaterales con el gobierno encargándose actualmente un contingente de tropas rusas de la seguridad del actual presidente Touadera. Rusia exhibe músculo en lo que constituye la primera misión africana con botas sobre el terreno de la región, accediendo así a puestos influyentes en la administración del país centroafricano. China, por su parte, no se queda atrás y ha hecho acto de presencia en la región con su "diplomacia de talonario", llegando en los últimos meses a importantes acuerdos económicos en materia militar, de condonación de deuda bilateral y capacitación de funcionarios. La disposición de Rusia y China para "ayudar" a la endeble administración centroafricana no ha hecho más que levantar suspicacias para Francia y otros países europeos sobre las verdaderas intenciones de este apoyo, con la sospecha de que pueda ser como contrapartida a la obtención de concesiones mineras o relaciones comerciales privilegiadas. La propia MINUSCA no ha estado exenta de polémica ya que se han sucedido las denuncias sobre abusos sexuales y otro tipo de violaciones de derechos humanos cometidos por miembros de la misión.

Por último, no hay que perder de vista el papel desempeñado por actores regionales y en este sentido no podemos dejar de mencionar a Chad, el gigante del norte que tuvo un papel determinante en la caída de Bozizé. Comparte unos 1.200 km de frontera con la República Centroafricana, a través de la que se produce un importante volumen de intercambios comerciales. Factores como que los principales grupos de oposición al presidente chadiano Idriss Deby vinieran del norte de República Centroafricana o el avance de la desertificación, que provoca que los ganaderos trashumantes que atraviesan la frontera (segunda fuente de ingresos en importancia para Chad), cada vez tengan que viajar más al sur, condicionan las relaciones entre ambos países y son generadoras de conflictos. Adicionalmente, se ha denunciado en ocasiones ciertas "simpatías" desde el lado chadiano hacia los grupos séléka y ex-séléka, lo que dificulta el papel de mediador que puede desempeñar en la región. De lo que no hay duda es que República Centroafricana supone una preocupación de primer orden para Chad, ya que el país depende casi en exclusiva de los ingresos petroleros generados en los pozos que se localizan a lo largo de la frontera entre ambos países, teniendo en cuenta que los yacimientos se extienden dentro del territorio del país centroafricano.

**Una mirada a los grupos armados y señores de la guerra**

Anteriormente ya indiqué que la dinámica militar del conflicto en República Centroafricana es mucho más compleja de la ya superada rivalidad entre los grupos séléka y anti-balaka. Desde hace algunos años, el país ha asistido a la proliferación de grupos armados, así como su división en grupos más pequeños para actuar en un plano más local, y así tener un control efectivo sobre los recursos de la zona. Esta fragmentación y dispersión de grupos armados dificulta aún más una posible solución del conflicto ya que incluso grupos tradicionalmente antagónicos, han establecido alianzas estratégicas superando la antigua línea divisoria trazada entre los séléka y anti-balaka.

**Zona de influencia de los grupos armados.**

Según el periodista freelance Philip Kleinfeld, los principales grupos son los siguientes:

- Frente Popular para el Renacimiento en la República Centroafricana (FPRC), grupo ex-séléka procedente de la línea "dura", liderado por Nourredine Adam y el anterior líder de la coalición Michel Djotodia. Han establecido alianzas con algunos elementos de las milicias antibalaka.
- Unión para la Paz en la República Centroafricana (UPC), grupo ex-séléka liderado por Ali Darassa cuyo antiguo cuartel general se ubicaba en Bambari. Reivindican representar los intereses de la comunidad fulani/peuhl en el país. A lo largo del año 2017, combatieron contra el FPRC.
- General Ali Darassa de la Unión para la Paz en la República Centroafricana.
- Reunión Patriótica para la Renovación de África Central (RPRC), grupo ex-séléka que se forma en la región diamantífera de Bria en 2014. Liderado por el antiguo comandante séléka Zacharia Damane y el ex parlamentario Gotran Djono Ahaba. En el grupo tiene una importante presencia e influencia el grupo étnico Gula.
- Movimiento Patriótico de África Central (MPC), otra facción ex-séléka formada en 2015 como una disidencia del FPRC. El

grupo de fracciona a su vez a mediados de 2017, naciendo un nuevo grupo denominado MPC Siriri.

- Revolution and Justice (RJ), formado a finales de 2015 en el noroeste bajo el liderazgo de Armel Ningatoloum Sayo. El grupo ha sostenido recientemente combates con el Movimiento Nacional para la Liberación de la República Centroafricana (MNLC) en torno a la población de Paoua, lo que ha provocado importantes desplazamientos de refugiados hacia Chad. El MNLC está liderado por el autoproclamado general Ahamat Bahar; ex-Seleka, ex-FPRC y ex-MPC. Se sospecha que el MNLC recibe un importante apoyo de las comunidades nómadas fulani provenientes de Chad.
- Return, Reclamation, Rehabilitation (3R), liderado por el general Sidiki Abas, con base en la región noroeste del país, cerca de la frontera con Camerún. Este grupo está prácticamente dominado por combatientes del grupo fulani/peuhl.
- Anti-balaka, grupo de milicias cristianas y animistas con estructuras locales diseminadas a lo largo del país. Las principales facciones se encuentran lideradas por Patrice-Edouard Ngaissona y Maxime Mokom, cuyo grupo recibe el apoyo del anterior presidente Francois Bozizé y se alió con el ex-séléka FPRC desde el año 2015.
- Grupos de autodefensa, una nueva generación de milicias surgió a lo largo del año 2017 bajo esta denominación en la región sudeste. Lejanamente conectados con los grupos anti-balaka, han lanzado ataques tanto a las comunidades musulmanas como a los miembros de las misiones de Naciones Unidas.

**La violencia se renueva en 2017**

En fechas más recientes, a principios de 2016 en la República Centroafricana se celebraron elecciones y se verificó la transición desde un gobierno interino que había gobernado el país desde 2014. Faustin Archange Touaderá fue elegido presidente del país, en un marco de una fuerte dependencia de los fondos internacionales y una autoridad estatal que se difumina cuanto más nos alejamos de la capital Bangui. Esa estructura estatal aún es muy frágil y pocos pasos se han dado en la dirección de alcanzar la ansiada estabilidad. Como vimos anteriormente, el movimiento séléka se ha escindido en facciones que incluso combaten entre ellas, atacando a civiles pertenecientes a comunidades étnicas de grupos rivales. Todas las partes, incluídas las Fuerzas Armadas, tienen nexos con el crimen organizado y utilizan la extorsión en sus áreas de control.

Este cóctel de administración débil, violencia sectaria y competición por los recursos naturales entre los diferentes señores de la guerra, ya había causado más de 600.000 desplazados internos y más de 500.000 refugiados en los países vecinos según ACNUR a finales de 2017. Además, más de la mitad de la población total se encuentra en estado de necesidad de ayuda humanitaria. Estas cifras son escandalosas si las ponemos en perspectiva con la de la población total de República Centroafricana: aproximadamente 4.600.000 personas, lo que nos ofrece una ligera idea del sufrimiento al que se encuentra sometida la población civil.

El foco del nuevo estallido de violencia iba a ser la localidad de Bangassou, una ciudad ribereña del sureste, de unos 30.000 habitantes a orillas de río Bomu. No sería por falta de alertas, ya que a principios de 2017 comenzaron a producirse reclutamientos de jóvenes y presencia de militantes del UPC (milicia ex-séléka liderada por Ali Darassa), aprovechando el repliegue de las tropas norteamericanas y ugandesas de la región este. Paralelamente, una nueva generación de grupos cristianos y animistas denominados de “autodefensa” comenzaron a proliferar en la ciudad, ante los insistentes rumores de la presencia del grupo UPC en la región. Tampoco ayudaba demasiado la animosidad de estos grupos de autodefensa hacia las tropas de la MINUSCA desplegadas en la zona, marroquíes de religión musulmana, existiendo la creencia de que estaban confabulados por las milicias ex-séléka y particularmente con la UPC. El conflicto estaba servido.

En el trasfondo de la llegada de la guerra a Bangassou, región antes relativamente tranquila, se esconden complejas dinámicas. Por un lado, la escisión en dos facciones de uno de los grupos séléka más grandes: FPRC (liderado por Nourredin Adam y Michel Djotodia) y UPC; formados por combatientes de la comunidad nómada fulani. Ambos grupos se disputaban el control de los recursos mineros del país; en un intento de arrebatar las zonas mineras controladas por la UPC, el FPRC se alió con algunas facciones antibalaka, provocando la erupción de un fuerte sentimiento anti-fulani en las poblaciones locales. La ONU decide desalojar al líder de la UPC, Ali Darassa, de su bastión de Bambari en febrero de 2017 para evitar un baño de sangre, ya que las tropas

del FPRC avanzaban. Esta decisión, lo único que provocó es trasladar el problema más hacia el sur, donde las poblaciones locales estaban ya muy sensibilizadas contra la presencia de los combatientes de la UPC en la región. La violencia se desató entre los milicianos de la UPC y los grupos de autodefensa, teniendo lugar una "cacería" de musulmanes en el área.

En medio de todo este horror, se producen episodios que invitan a la esperanza. El obispo de Bangassou, el español Juan José Aguirre, se ofreció como escudo humano a miles de musulmanes que se habían refugiado en una mezquita, protegiéndose de la violencia antibalaka. A dicha mezquita se habían desplazado vecinos del barrio de Tokoyo, de mayoría musulmana, aconsejados por el contingente de la ONU. Previamente, unos 1500 milicianos antibalaka habían orquestado un plan para asesinar a todo aquel sospechoso de ser musulmán. El ataque y posterior cerco a la mezquita se saldó con cientos de muertos, hasta que todos los refugiados del interior pudieron ser evacuados. Pese a lo heroico del gesto, no pudo impedir que muchos musulmanes hayan tenido que emprender la huida hacia regiones del norte del país.

**Cuando la guerra resulta un negocio rentable**

La República Centroafricana es uno de los países más pobres del mundo. Todo ello a pesar de sus abundantes reservas mineras y forestales. El desplazamiento forzoso consecuencia del conflicto ha afectado gravemente a la producción agrícola y ganadera del país, desembocando en una crisis alimentaria sin precedentes. Se estima que unos tres millones de personas viven en extrema pobreza. El éxodo sur-norte de las castigadas comunidades musulmanas, que anteriormente controlaban las redes comerciales a lo largo del territorio, ha contribuido al colapso económico del país.

En este contexto, ha florecido todo un sector de redes de economías ilícitas que bien puede denominarse "economía de los señores de la guerra". Los grupos armados obtienen cuantiosos beneficios de las extorsiones y los impuestos al comercio ilegal de oro y diamantes. El pillaje y el robo tampoco es infrecuente por parte de las milicias. Algunos grupos como el LRA, se han lucrado de la caza ilegal de elefantes para traficar con marfil en el mercado asiático.

Pese a ser un importante productor mundial de diamantes, en 2013 le fue prohibida su venta bajo el Proceso de Kimberley; certificación internacional que buscar regular el comercio de este mineral precioso para evitar que los llamados "diamantes de conflicto" terminen en el mercado internacional. Dicha prohibición fue levantada parcialmente en el año 2016. Pese a las buenas intenciones de esta iniciativa, no hay otro ámbito donde sea más visible que la violación grave y sistemática de los derechos humanos pueda proceder de grandes multinacionales antes que del propio estado. En este sentido, el reciente artículo de la profesora Tania García Sedano para el Instituto de Estudios Estratégicos es muy ilustrativo.

Las regiones diamantíferas son muy codiciadas por los grupos armados, determinando en muchas ocasiones el curso de sus movimientos estratégicos y acciones militares. Esto se puede comprobar fácilmente si superponemos los mapas de ámbito de actuación de los grupos armados y el de distribución de los recursos naturales en el país, arrojando sorprendentes coincidencias.

**Recursos naturales de la República Centroafricana.**

La República Centroafricana no parece disponer de reservas de petróleo, aunque el anterior presidente Bozizé concedió algunas licencias de exploración en el norte, en la frontera con Chad, a compañías chinas. La revuelta séléka propició la revisión de dichos contratos.

Otra importante fuente de riqueza minera del país la constituye las reservas de uranio. Recientemente, en Francia se investiga un caso de corrupción promovido por el gigante francés del uranio, Areva, a través de una filial canadiense, Uramin, para que mediara con el ex-presidente Bozizé en un conflicto referente a una licencia de explotación minera en Bakouma. El uranio de las minas centroafricanas es codiciado igualmente por otros países como Reino Unido o Sudáfrica.

En tiempos más recientes, China ha demostrado tener gran interés en la explotación de los recursos naturales de la región, lo que podría generar una competición entre grandes potencias que sirva de retroalimentación del propio conflicto.

**Conclusiones**

En el conflicto de República Centroafricana, pese a haber entrado en una fase de menor intensidad, no parece que se atisbe su finalización a medio plazo. En el centro del conflicto confluyen varias dinámicas muy poderosas que propician su continuidad.

Para la analista Nathalia Dukhan, el país aparte de ser uno de los más pobres del mundo es uno de los más inestables. A esta situación se ha llegado en parte debido a la depredación de las élites políticas sucesivas que han gobernado el país y al síndrome del "estado fantasma" que ha facilitado la proliferación

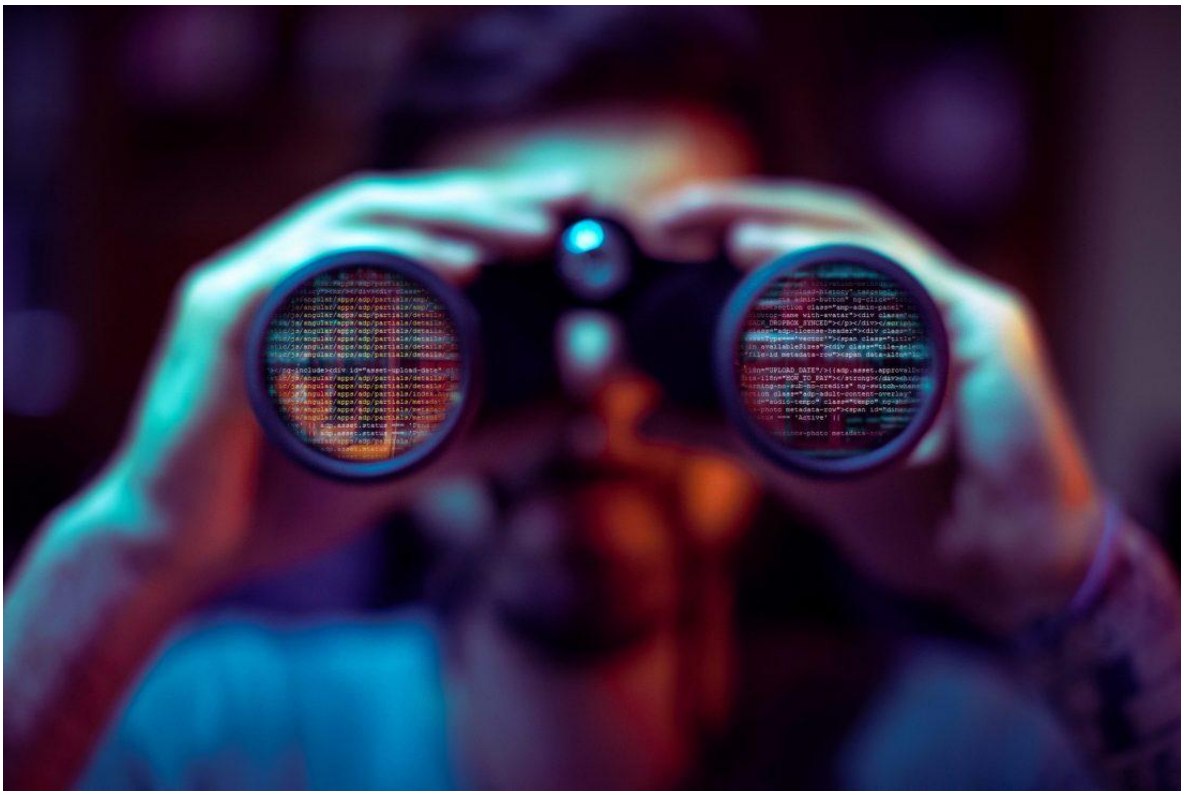
de grandes grupos criminales que han convertido la violencia en un negocio ciertamente rentable.

Como cobertura de su actividad criminal, estos grupos han agitado el fantasma de las diferencias religiosas y étnicas, alimentando las tensiones entre comunidades, hasta el punto de llegar a la limpieza étnica. Ya indicaba la periodista Trinidad Deiros allá por 2014 en un artículo publicado por el Instituto de Estudios Estratégicos, que lo que estaba sucediendo en aquel país era un conflicto religioso “inventado”. El verdadero origen del conflicto puede encontrarse en la pugna de los diferentes grupos por hacerse con el control de los recursos, aprovechándose de las tensiones preexistentes, pugna que se vuelve más feroz si cabe ante circunstancias naturales como el avance de la desertificación, provocando conflictos entre grupos sedentarios y ganaderos trashumantes como ya vimos.

La reciente irrupción en escena de las potencias internacionales, con intereses y agendas encontradas, tampoco parece ser un factor que ayude a la estabilización del país ya que podría ser aprovechado por los diferentes bandos en conflicto para buscar su propia supervivencia y alcanzar mayores cuotas de poder. La actual situación de caos y violencia llevará años para revertirla y habrá que dar muchos pasos en la dirección correcta. Parece que en el actual contexto, éste no es el caso.

# Ciberinteligencia: Reinventando la rueda

Por Ulises León Kandiko (Argentina)



Como en muchas oportunidades he dicho, hoy día a todo componente tecnológico se le suele anteponer el término Ciber seguido luego del tema de interés, en este caso la Ciber-Inteligencia. Sin embargo y parecido a otras nociones relacionadas con el ciberespacio, no hay ninguna definición cristalizada de "Ciberinteligencia", ni siquiera hay suficientes estudios centrados en cómo se elabora, si bien encontrarán varios artículos sobre el particular, no hay aún hoy una doctrina cabalmente aceptada.

Al respaldar la idea de que las organizaciones deben pasar de la seguridad reactiva a la proactiva, posturas de gestión y oponerse a la actitud de interpretar la ciberseguridad principalmente como "Medidas tomadas después del evento" y "defensa perimetral estática", diferentes representantes de la comunidad de ciberseguridad ahora están patrocinando la adopción de conceptos, herramientas y prácticas para la elaboración y el intercambio de inteligencia global sobre amenazas cibernéticas. Esta inteligencia debería permitir a sus consumidores comprender el funcionamiento, las tácticas, y contextos estratégicos de las amenazas (agentes, capacidades, motivaciones, objetivos, impacto, y consecuencias no solo desde una perspectiva técnica); prever sus desarrollos a corto, mediano y largo plazo; y tomar decisiones preventivas.

Si se integra en sus procesos de toma de decisiones relacionados con la seguridad, debería permitir a las organizaciones asumir acciones "predictivas y anticipatorias en lugar de orientadas hacia el pasado", en un formato "dinámico más que estático" y "ágil y adaptable vs. las posturas rígidas y conformadas" hacia los peligros relacionados con el ciber. La inteligencia descrita anteriormente a menudo se etiqueta como "Ciberinteligencia" (CYBINT). En general, se usa CYBINT para transmitir la idea de un conocimiento amplio y mejor calificado de reales o potenciales eventos relacionados con el ciberespacio que pueden poner en peligro una organización.

Si uno mira las políticas o mecanismos relevantes que se han implementado recientemente (especialmente Europa), así como otra documentación emitida por organizaciones privadas o públicas y de orden académico, la Ciberinteligencia no siempre se define de forma exhaustiva y las definiciones varían [i]. A pesar del creciente uso de esta u otras expresiones similares por parte de académicos, los medios y profesionales, el

pensamiento actual sobre el tema es limitado y no está bien desarrollado. Una investigación más profunda del tema, tanto sea desde un punto de vista teórico como práctico, falta.

Por el contrario, tanto académicos como profesionales del ámbito de la Seguridad Nacional de los Estados Unidos de Norteamérica (USA), tienen reflexiones sobre la Ciberinteligencia relativamente algo más avanzadas. Esta podría ser la consecuencia de la adopción anterior de conceptos, prácticas y soluciones tecnológicas relacionados con la CYBINT basados en los organismos de Gobierno de USA, similar situación se puede apreciar en Rusia y China.

**Buscando una definición, terminología o noción.**

Tristemente en el lenguaje cotidiano CYBINT suele utilizarse principalmente como un envoltorio o una expresión. ¿Qué es CYBINT más exactamente? Se debe entender como producto y proceso, ¿es inteligencia "desde", "dentro", " o "para" el ciberespacio o alguna combinación de los mismos? ¿Cuáles son las principales fuentes de CYBINT? ¿Cómo está hecho? ¿El ciclo de inteligencia "tradicional" es aplicable a la CYBINT? ¿Cuáles son los problemas asociados con el creación y uso compartido de CYBINT? Tratar de dar una respuesta a algunas de estas interrogantes podría llevarnos a comprender la CYBINT.

Por ejemplo, la falta de una comprensión uniforme del término "cyber" dificulta cualquier intento de proponer una noción integral y uniforme de CYBINT. De hecho, mientras es más o menos indiscutible al establecer qué inteligencia (como producto y proceso) es definirlo en relación con el dominio cibernético es un desafío. Uno puede preguntarse, sin embargo, en qué medida estos conceptos son aplicables a un dominio que difiere de los dominios tradicionalmente conocidos. Cyber es, de hecho, hecho por el hombre, un entorno altamente evolutivo, tecnológicamente configurado y no completamente tangible, que, tal vez, necesita ser interpretado a través de diferentes paradigmas. Sus interacciones con el dominio físico / real aún no se ha entendido completamente.

Además, la CYBINT es una práctica relativamente nueva, que está lejos de ser completamente probada, evaluada y desarrollada. No hay suficiente experiencia compartida sobre cómo funciona y sobre las mejores capacidades para llevarla a cabo de manera efectiva. Esto dificulta cualquier intento de aparecer con un modelo interpretativo completo para CYBINT.

Dependiendo del alcance de las actividades de recopilación de información, los medios empleados para llevarlos a cabo y el propósito final al que sirven, en realidad hay dos maneras de mirar o interpretar la CYBINT. Una forma es pensar en la CYBINT como inteligencia "De" cibernético; es decir, el conocimiento producido a través del análisis de cualquier información valiosa recolectado "dentro" o "a través" del ciberespacio. Esta es la CYBINT stricto sensu. Desde esta perspectiva, "cibernético" se refiere tanto al dominio donde se obtienen los datos como a en otras palabras, ese vasto repositorio digital de información susceptible de ser recuperado y procesado; y las herramientas / técnicas / medios a través de los cuales se recopilan estos datos (por ejemplo, a través de tecnologías y técnicas de explotación de redes informáticas). De acuerdo con esta interpretación, CYBINT puede, en principio, apoyar la toma de decisiones en cualquier dominio y no solo para contrarrestar las amenazas cibernéticas. Puede soportar una amplia variedad de misiones en el gobierno, la industria y la academia, incluida la formulación de políticas, la planificación estratégica, negociaciones internacionales, gestión de riesgos y comunicación estratégica en áreas más allá de la ciberseguridad. En otras palabras, la CYBINT puede operar "de manera independiente y no necesariamente es para apoyar una misión de ciberseguridad". Sin embargo, dado que la CYBINT a menudo se discute en relación con la ciberseguridad o la prevención y respuesta a las amenazas cibernéticas, estos son los objetivos primarios, pero, nuevamente, no exclusivos de este tipo de inteligencia.

Otra forma de interpretar la CYBINT es considerarla como inteligencia "para" la cibernética; esa es, visión que se deriva de una actividad de inteligencia de fuente completa que ocurre dentro y fuera del ciberespacio. Es la CYBINT lato sensu. En este sentido, la inteligencia "para" lo cibernético también puede incluir (o basarse en) inteligencia "desde" la cibernética. Puede extraer de cualquier disciplina de la inteligencia que le proporcione conocimiento crucial, independientemente de la fuente, método o medio empleado para elaborarlo. Como tal, la CYBINT puede resultar de la combinación de inteligencia de código abierto (OSINT), inteligencia de señal (SIGINT), Inteligencia geoespacial (GEOINT), Social Media Intelligence (SOCMINT) e Inteligencia humana (HUMINT). Desde este punto de vista, la CYBINT es menos una disciplina en sí misma que una práctica analítica basada en información / inteligencia recogida también a través de otras disciplinas y destinada a informar a los tomadores de decisiones sobre cuestiones relacionadas con las actividades en el dominio del

ciberespacio. Lo que califica este tipo de inteligencia como "cyber" es el propósito para el cual es elaborado: para apoyar la toma de decisiones sobre cuestiones relacionadas con el ciberespacio.

Las dos perspectivas discutidas sobre CYBINT "desde" y "para" a menudo se condensan en un solo concepto integral. Esto también se debe al hecho que la inteligencia "para" el ciber en realidad incorpora el ciber "de" uno. El resultado es una noción más amplia de CYBINT que incluye la recopilación, procesamiento, evaluación, análisis, integración e interpretación de la información que está disponible "dentro", "a través de", y / o en el ciberespacio "externo" para mejorar la toma de decisiones sobre amenazas relacionadas con el ciberespacio.

En cuanto a la información para la creación de CYBINT, esto puede variar desde la red de datos técnica (por ejemplo, datos de hardware y software), datos sobre organizaciones hostiles y sus capacidades, actividades cibernéticas en curso, a potencialmente cualquier información relevante sobre eventos geopolíticos. El tipo de datos así como su clasificación no son funcionales a la definición de CYBINT. Los datos pueden ser información en bruto o ya procesada; pueden ser obtenido legalmente o mediante acciones ilegales de intrusión / explotación de fuentes abiertas, propietarias o de otro tipo de fuentes clasificadas. Como lo sugiere la literatura, se necesitan múltiples fuentes de información para desarrollar una comprensión más holística del entorno de amenaza y producir una CYBINT integral. El aspecto más importante de los datos es que debe ser de alguna manera validado. Cuando se analiza, la información debe permitir a los responsables de la toma de decisiones identificar, rastrear y predecir capacidades, intenciones y actividades cibernéticas que ofrecen cursos de acción. Esta es la característica principal de la CYBINT; es decir, el objetivo habilitante de proporcionar a sus consumidores con conocimiento de actividades potencialmente hostiles que pueden ocurrir en el dominio cibernético o puede ser perpetrada a través o en contra del ciberespacio, lo que les permite diseñar medidas preventivas (proactivas) o contrarias (reactivas).

Dependiendo de su alcance o nivel de acción, la CYBINT puede ser estratégica, táctica, u operacional. No hay una interpretación uniforme de lo que los diferentes niveles de CYBINT deben ser. De acuerdo con la literatura disponible, la CYBINT estratégica se centra en el largo plazo. Por lo general, revisa las tendencias en las amenazas actuales y emergentes y examina oportunidades para contener estas amenazas. Sirve a procesos aplicables a la toma de decisiones destinados a lograr la misión de una organización y determinar su dirección y objetivos. La CYBINT estratégica cubre el panorama de amenazas, marca las tendencias (políticas, sociales y económicas) que afectan a la organización e identifica a los actores amenazados, sus objetivos y cómo pueden intentar alcanzarlos; es rico en información contextual. CYBINT táctica se refiere a lo que sucede en la red. También examina la fuerza y las vulnerabilidades de una organización, y las tácticas, técnicas y procedimientos (TTP) empleados por actores de la amenaza. Debido a su naturaleza y alcance, tácticamente CYBINT corresponde en general a la inteligencia de amenazas cibernéticas. Generalmente de naturaleza más técnica, informa los pasos y acciones centrados en la red que la organización puede tomar para proteger los activos, mantener continuidad y operaciones de restauración. En lo que se refiere a la CYBINT operativa, consiste en el conocimiento de amenazas inminentes o directas a una organización. Permite y mantiene las operaciones y salidas diarias. En este nivel, la CYBINT mira a la organización en sus procesos internos y vulnerabilidades.

Vale la pena dejar bien aclarado que la distinción descripta entre los niveles de CYBINT es principalmente académica. En la práctica, no existe una demarcación clara desde un nivel de inteligencia hasta otro; con frecuencia se superponen o se combinan. Además, el significado de estratégico, táctico y operativo es probable que varíe entre las organizaciones debido a su tamaño, complejidad, misión y atributos relacionados. Independientemente de cualquier demarcación clara entre los niveles, la capacidad de una organización para considerar todos estos niveles y el arte de inteligencia que le permite comprender los desafíos y oportunidades que es probable que encuentre en el corto, mediano y largo plazo es bastante importante.

**El proceso de la ciberinteligencia: Modelos alternativos vs. Tradicionales**

El proceso al que todos se refieren no es otro más que el conocido “Ciclo de Inteligencia” [ii], el que ha sido estudiado y cuestionado varias veces por profesionales y académicos hasta el punto que se han propuesto y discutido modelos alternativos. La "validez / aplicabilidad" del ciclo de inteligencia tradicional también se cuestiona en el contexto de la CYBINT. Como un eminente experto señaló, "a medida que la inteligencia crece en forma cada vez más digitalizada y cibernética (en su materia, sus

métodos y sus formas), una comprensión más clara de que la inteligencia y su ciclo es en realidad un dispositivo heurístico bastante anticuado, más que una dimensión constructiva de la inteligencia como tal, puede liberar a los interesados para que piensen sobre la inteligencia en formas más innovadoras" [iii]. Esta opinión es compartida por otros académicos y expertos, los que consideran al Ciclo como lineal y reiterativo, ya que el mismo no enfatiza la interrelación natural de las actividades (planificación, recopilación, procesamiento, etc.) mientras que el proceso de CYBINT consiste en su relevancia mutua; en otras palabras, no capturar sus interdependencias e influencias mutuas.

En realidad, aquellos que critican el ciclo, se basan en argumentos que se hacen para describir la inadecuada representatividad del ciclo de inteligencia en general, independientemente de la CYBINT. Por lo tanto, uno puede cuestionar más en profundidad si un ad hoc el modelo interpretativo es necesario para explicar el proceso de CYBINT; o, en otras palabras, el por qué el proceso CYBINT es tan peculiar y diferente de los procesos incrustados en otras disciplinas de Inteligencia que requiere ser descrito a través de un modelo alternativo y particular para la CYBINT. Proporcionar respuestas concretas a las preguntas anteriores requeriría una clara comprensión exhaustiva y completa de CYBINT como concepto y más aún como una práctica. Tal entendimiento es difícil de alcanzar debido a la falta de suficiente reflexiones y experiencia en CYBINT. Por lo tanto, en la etapa actual, la definición de modelo interpretativo representa sobre todo una especie de ejercicio intelectual o una prueba cuyos resultados deben ser validados progresivamente. No obstante, algunos argumentos parecen apoyar bien la definición de un modelo ad hoc para explicar el proceso CYBINT.

Tautológicamente hablando, la característica principal de la CYBINT radica en el hecho de que es "cibernética"; es decir, es conocimiento sobre cuestiones relacionadas con la cibernética. CYBINT involucra el análisis de la información recopilada del ciberespacio y de otras fuentes para lograr fines relacionados con el ciberespacio. En el nivel muy básico, el adjetivo "cibernético" se refiere a un dominio creado por el hombre, altamente evolutivo, con forma tecnológica y no totalmente tangible. En este dominio, la información se genera, procesa, disemina, comparte, almacena, altera, es consumida y destruida por una multitud de actores a una velocidad increíble. El impacto de toma de decisiones específicas sobre cuestiones relacionadas con el ciberespacio y sus efectos tanto en lo virtual como en lo los dominios físicos son difíciles de prever. Esto afecta la forma en que la CYBINT es elaborada y consumida. Desafía las funciones básicas del proceso de inteligencia cuando se aplica a la ciberesfera, a saber, la recopilación, evaluación, análisis, integración, interpretación de información y difusión de inteligencia.

Con respecto a la recopilación y evaluación, la CYBINT también se basa en la información entregada por fuentes no controladas, como Internet. Esta información debe ser filtrada, evaluada y (de alguna manera) validada. El filtrado es primordial para seleccionar solo elementos significativos de información del ciberespacio. La evaluación es a menudo un desafío debido a la alta volatilidad, el anonimato y la incertidumbre de los datos disponibles en el ciberespacio y la heterogeneidad de las fuentes de datos. Para validar los datos, se convierte en primordial para corroborar la información derivada de una fuente con la derivada de otras fuentes, y es mejor si al menos uno de los primeros está controlado. Filtrado, evaluación y la validación tiene como objetivo mitigar la llamada "anarquía de la información" generada por el alto volumen de datos disponibles junto con la falta de control sobre ellos. Dado que el proceso de elaboración de CYBINT también puede recurrir a la información / inteligencia producida a través de otras disciplinas, la integración de todos los conocimientos relevantes en un único producto consistente puede ser desafiante. Esto se debe a los diferentes formatos, naturaleza y grado de incertidumbre de la información e inteligencia obtenida del ciberespacio (por ejemplo, información u otros datos técnicos provenientes de las redes sociales, foros web, etc.) confrontado con otras fuentes "no virtuales". El grado de incertidumbre también afecta a la interpretación de la información procesada; es decir, el juicio y las deducciones basadas en él, que generalmente se agregan en el producto cibernético final. Dicha incertidumbre también debería ser transmitida claramente al consumidor de CYBINT, que debe ser consciente de su principal límite en términos de precisión.

Otro aspecto relevante a considerar al definir cualquier modelo interpretativo para el proceso CYBINT es el marco de tiempo ajustado que a menudo se requiere para ejecutar funciones de inteligencia. Esto exige que las funciones ocurran simultáneamente o que se tomen atajos en su ejecución. En otras palabras, las funciones no se ejecutan en un círculo, sino que establecen un "canal de red "entre ellos.

Según parece, podríamos estar ante la necesidad de contar con un ciclo de inteligencia propio para la

CYBINT, o al menos revitalizado. Al mirar la literatura, un equipo de expertos y académicos que trabajan en el Software and Engineering Institute (SEI) de la universidad Carnegie Mellon propuso su propio modelo hace un par de años. El modelo SEI difiere del ciclo de inteligencia tradicional debido a la terminología adoptada, no es lineal y lógicamente estricto o consecuente de las funciones en que consiste el proceso, el desglose de las funciones de análisis en dos funciones especializadas (el análisis técnico o funcional y el análisis estratégico) y la capacidad de conjugar la ciberseguridad técnica "estrecha" y los propósitos de prevención de ciberamenazas "más amplios" a los que la CYBINT puede servir dentro de una organización. Tal como está representado, el modelo propuesto acomoda la interpretación de la CYBINT como una práctica analítica que depende de la información / inteligencia recopilada también a través de otras disciplinas y que está destinado a informar a los tomadores de decisiones sobre cuestiones relacionadas a las actividades en el dominio cibernético. El modelo SEI consta de cinco funciones:

1. La determinación del "entorno" que establece el alcance del esfuerzo de CYBINT e influye en la información que se necesita para lograrlo;
2. La "recopilación de datos" o la exploración de fuentes de datos y la recopilación y el filtrado de información a través de herramientas de uso intensivo de mano de obra;
3. El "análisis funcional", que es el rendimiento de análisis técnico y personalizado (generalmente en apoyo de una misión de ciberseguridad) destinado a derivar el "qué" y el "cómo" de las amenazas informáticas;
4. El "análisis estratégico" que implica la revisión, integración con información contextual, y una mayor elaboración de la funcional CYBINT con el objetivo de responder las preguntas "quién" y "por qué"; y
5. El "Informe y comentarios"; es decir, la diseminación de la CYBINT a los tomadores de decisiones y la recopilación de comentarios.

Las principales dependencias e influencias mutuas entre las funciones descritas son las siguientes: la recopilación de datos debe basarse en la determinación del medio ambiente, que está influenciado por las decisiones tomadas por la organización sobre la base de CYBINT consumida. La inteligencia resultante del análisis funcional puede informar decisiones sobre acciones a tomar a nivel de la red técnica de una organización que, a su vez, impactan en la determinación del ambiente interno; lo mismo pasa para la inteligencia resultante de la función estratégica, que afecta tanto a la interna y ambiente externo. La función estratégica también representa la inteligencia resultante del análisis funcional, que es más consumible por los encargados de la toma de decisiones que pueden no tener un fondo técnico. Desde esta perspectiva, es una especie de complemento que contribuye a cerrar la brecha de comunicación entre los analistas y los principales tomadores de decisiones. Los últimos proporcionan retroalimentación sobre la inteligencia recibida con el fin de dar forma analítica, ajustar la dirección de la organización y, por lo tanto, influir en el entorno. Cuestionar la "validez" del modelo de SEI está más allá del alcance de este artículo. El modelo fue diseñado y propuesto como resultado del trabajo empírico que mapeó y evaluó prácticas actuales en la CYBINT de USA. También tiene un alcance normativo; sugiere cómo el proceso debería funcionar para ser efectivo.

**1D34S F1N4L3S**

Tener una comprensión clara de CYBINT es importante. Puede ayudar a las partes interesadas relevantes a ser coherentes cuando promueven programas o toman acciones relacionadas con la CYBINT a nivel político, legal, operativo y de otro tipo. Tal comprensión debe ser premisa sobre la definición de un marco conceptual sólido de CYBINT. La adopción de dicho marco también representaría un elemento fundamental para desarrollar la CYBINT como una disciplina; es decir, un área específica de estudio o trabajo en inteligencia. A pesar que la mayoría de la literatura considera que la CYBINT es una ya establecida o próximamente establecida disciplina, no parece ser el caso.

En otras palabras, CYBINT no debe considerarse una disciplina porque aún no ha sido suficientemente definida teóricamente ni puesta en práctica en profundidad. Además, como se describió a lo largo de este artículo, la naturaleza de la CYBINT y su proceso de elaboración hace que sea menos una disciplina que una práctica analítica, que se basa en información / inteligencia recogida también a través de otras disciplinas. Por supuesto, nada impide que la CYBINT se establezca como una disciplina que emplea recursos técnicos o humanos específicos a través de las diferentes funciones de su proceso de elaboración.

A título personal creo que la CYBINT terminará siendo una disciplina mucho antes de lo que se cree, el uso de un ciclo propio obedece más a la particularidad del ciberespacio en el que la inmediatez

y la interconexión conviven simbióticamente haciendo que el ciclo clásico quede algo desfasado conceptualmente. El ciberespacio como se ha dicho acá, es hecho por el hombre, un entorno altamente evolutivo, tecnológicamente configurado y no completamente tangible, que, tal vez, necesita ser interpretado a través de diferentes paradigmas, es por esta razón que desde el campo militar es conocido como el 5to dominio, un nuevo escenario de batalla donde lo virtual también suele convivir con lo físico y por ello a mi entender requerirá de una atención especial, no comprender la importancia de contar con Ciberinteligencia a nivel Estratégico es perder una batalla antes de iniciar la contienda.

**Notas y Referencias**

[i] Acá algunos de los documentos que dan cuenta de ello. Ver, por ejemplo, Mario Caligiuri, Cyber Intelligence. Tra libertà e sicurezza (Roma: Donzelli, 2016); Mario Caliguiri, "Cyber Intelligence, la Sfida dei Data Científico, "junio de 2016, https://www.sicurezzanazionale.gov.it/sisr.nsf/ approfondimenti / cyber cyber intelligence-la-sfida-dei-data-scientist.html; Antonio Teti, "Ciber Inteligencia" e Cyber Espionaje.

[ii] Si bien hay diferentes representaciones del ciclo de inteligencia, las más comunes comprenden cinco funciones distintas: planificación y dirección, recopilación, procesamiento, análisis y diseminación. En el ciclo de inteligencia, vea Mark Phythian, ed. Comprender el ciclo de inteligencia (Londres y Nueva York: Routledge, 2013). En particular, vea a Philip H.J. Davies, Kristian Gustafson, e Ian Ridgen, "El El ciclo de inteligencia ha muerto, viva el ciclo de inteligencia, "en Comprender el Ciclo de inteligencia, p. 56.

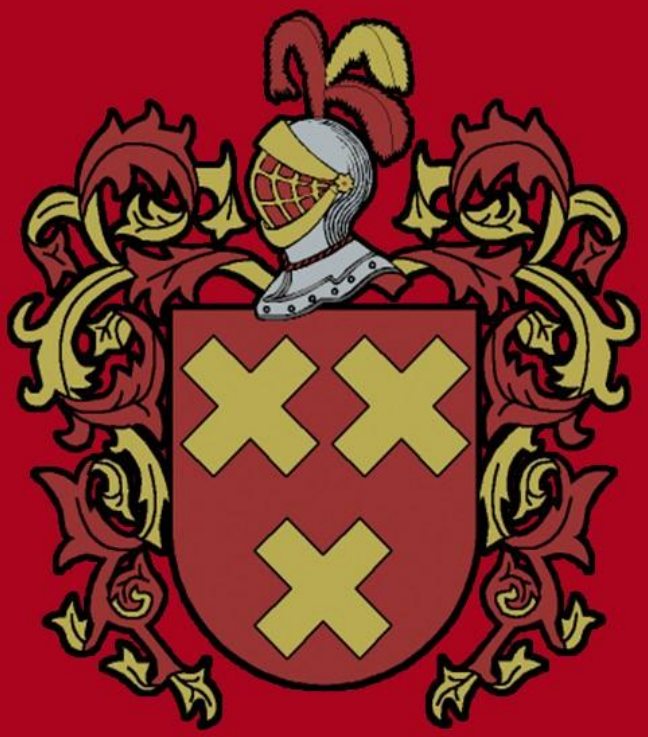
[iii] Michael Warner, "El pasado y el futuro del ciclo de inteligencia", en Understanding the Intelligence Cycle, p. 19.

Fuente de la Imagen:
https://www.pandasecurity.com/spain/mediacenter/src/uploads/2017/10/iStock-610855316-1100x733.jpg

AIG

American Intelligence Group

ANIVERSARIO NÚMERO 15



www.fuerzasmilitares.org

2003-2018

15

¡Siempre en Vanguardia!

# Gerencia Estratégica del Capital Intelectual

Por Douglas Hernández (Colombia)

En este escrito se pretende hacer una reflexión sobre las posibilidades que ofrece la gerencia estratégica del capital intelectual, y como pueden contribuir a ello técnicas administrativas y gerenciales modernas como el Coaching, el Empowerment, el ADN Organizacional y el Benchmarking. Por supuesto, estamos pensando en cómo trasladar estos elementos propios del sector empresarial, al sector de la seguridad y la defensa, aprovechando todas las cualidades y experiencias exitosas que se han logrado en el primero, para potenciar el segundo y tornarlo más eficiente. Como paso previo, lo procedente es establecer algunas definiciones sobre las que basar la reflexión.

El capital intelectual es un intangible propio de todas las organizaciones, está formado por el capital estructural, que tiene que ver con aspectos como las patentes, el goodwill, y otros activos intangibles similares; el capital humano, que tiene que ver con los saberes y las capacidades de los empleados, y el capital relacional, que se refiere a la manera como la organización se relaciona internamente, con su entorno y con el mercado.

Por otro lado, una definición que parece bastante acertada sobre la gerencia, es la aportada por Chirinos, citado por Hernández y Gómez (2010):

> La gerencia es el arte y ciencia de trabajar con y a través de un equipo de personas hacia el logro de los objetivos de una organización. Esto implica construir un cuerpo de conocimiento sobre dicha actividad, y que la actividad del gerente involucre relación con otras personas para lograr los objetivos de la organización. (p.628)

Un gerente es -en términos generales-, el encargado de dirigir y gestionar los asuntos de una empresa u organización, además de coordinar los recursos internos, representar a la compañía frente a terceros y controlar las metas y objetivos. Más concretamente, debe cumplir con cuatro funciones de manera simultánea:

- Planear: establece cursos de acción para lograr los objetivos organizacionales, teniendo en cuenta los recursos disponibles.
- Organizar: es el deber de disponer en tiempo y espacio los recursos humanos, materiales, y financieros, necesarios para lograr los objetivos.
- Dirigir: principalmente se refiere a sus dotes de liderazgo, y a su capacidad para la toma de

decisiones, influyendo constantemente en la marcha de los procesos.

- Controlar: se refiere a mediciones cualitativas y cuantitativas de los procesos y de la ejecución de los planes que se hayan trazado.

Estas cuatro funciones son comunes a los gerentes, directores, o comandantes de unidades militares, policiales, de inteligencia, y antiterroristas, de todo el mundo. En ese orden de ideas, proporcionar elementos que contribuyan a mejorar el desempeño de estos actores, contribuirá a que el personal y los recursos bajo su mando sean empleados más eficientemente, y se logren mejores resultados en la lucha contra el crimen, el terrorismo y la las nuevas amenazas.

La gerencia estratégica, es aquella que está basada en un pensamiento holístico, que abarca múltiples aspectos propios de la organización, del entorno y del mercado, y que además se proyecta hacia el futuro. Hay niveles gerenciales enfocados en el cumplimiento de objetivos cualitativos y/o cuantitativos de muy corto plazo o de poco impacto, se trata de asuntos cotidianos de la empresa u organización. El gerente de producción debe garantizar la manufactura de un número determinado de unidades, en un plazo determinado, con una calidad específica, y empleando para ello una maquinaria, un personal y unas materias primas específicas. Y así una y otra vez. No es competencia de este gerente si lo producido se vende o no, ni cuáles son las características del mercado, o de la competencia, ni mucho menos qué pasará dentro de 5 años con todas estas variables. Esta persona no cumple funciones gerenciales estratégicas.

Por el contrario, en una reunión de gerencia, el gerente general recibe informes de los gerentes de producción, finanzas, logística y administración, y en función de ello, y de su valoración del mercado, de manera prospectiva toma decisiones que afectan a toda la empresa, hoy y en el futuro, en aras de alcanzar objetivos en el corto, mediano y largo plazo. Debiendo los demás gerentes ejecutar las directrices estratégicas que emanan de la gerencia general. En el contexto de la seguridad y la defensa, las decisiones de orden estratégico se toman en los altos niveles de comando, siendo más claro establecer responsabilidades, debido a que la estructura organizativa es eminentemente vertical

En el marco del capital intelectual, hay que hacer claridad en cuanto a que a diferencia de los demás activos, su cuantificación es muy difícil, habida cuenta de que se trata de intangibles. Pero a pesar de ser intangibles existen, y afectan de una u otra manera la marcha de la organización y la posibilidad de alcanzar o no alcanzar los objetivos organizacionales. Por tanto, el capital intelectual también debe ser gerenciado.

Se ha establecido ya que el capital intelectual está conformado por capital estructural, el capital humano y el capital relacional. Es necesario hacer notar que el capital humano parece ser el determinante de los otros dos, y por lo tanto la mejora en esa variable influirá muy seguramente en los demás, y estos en su conjunto permitirán una mejora en toda la organización.

En este orden de ideas, en este escrito nos enfocaremos en el capital humano, y en cómo gerenciarlo de manera estratégica.

El capital humano es entonces el conjunto de conocimientos, habilidades, destrezas y talentos que posee una persona y la hacen apta para desarrollar actividades específicas en la organización.

Lógicamente, para cada cargo se requieren conocimientos, habilidades, destrezas y talentos específicos. Pero también hay una serie de conocimientos, habilidades, destrezas y talentos que todos deben poseer y que contribuirán a crear, sostener y mejorar las relaciones interpersonales. Grosso modo, podemos establecer que es necesario definir descripciones de cargo para cada trabajador, donde se especifique que es lo que se espera de él/ella en desempeño de sus funciones específicas -aquello por lo cual le pagan-, pero también es necesario una descripción general de cómo debe ser el perfil de un empleado de esa empresa u organización. De esta forma, para gerenciar apropiadamente debemos tener:

- Compendio de descripciones de cargo.
- Perfil de un empleado de la empresa u organización, que se elabora en función de, y a su vez fortalece a:
    - Filosofía Institucional.
    - Valores Institucionales.
    - Relaciones interpersonales deseadas.
    - Valores Sociales/Familiares.
    - Actitudes frente a asuntos de interés para la organización, por ejemplo, el medio ambiente.

Existen dos grandes campos de actuación para la gerencia estratégica del capital intelectual:

- Los conocimientos, habilidades, destrezas y talentos específicos, que los trabajadores ya poseen, que están orientados al cumplimiento de sus labores cotidianas, y que pueden ser incrementados y mejorados.

- La actitud con que el trabajador aborda todo lo atinente a su dimensión laboral, lo que resulta absolutamente determinante en cuanto a los resultados que aportará a la organización.

Es claro que una persona con un alto coeficiente intelectual, perfectamente formado en las mejores universidades del mundo, con estudios de posgrado, y con una vida familiar ejemplar, puede resultar siendo un empleado improductivo e incluso nocivo para la empresa u organización, si no tiene la actitud adecuada, por el contrario, una persona promedio, con estudios regulares, e incluso adscrito a una familia disfuncional, puede llegar a ser un empleado ejemplar, si su actitud conduce a ello. De acuerdo con esta reflexión a priori, resulta fundamental mejorar la actitud del personal, como estrategia base para lograr que estén dispuestos a dar el máximo de sus capacidades, lo mejor de sí mismos.

Para lograr un cambio de pensamiento, y en consecuencia un cambio de actitud, alineando los objetivos personales de los empleados con los objetivos organizacionales, pueden emplearse algunas herramientas gerenciales modernas.

En este orden de ideas, estos son algunos elementos a tener en cuenta:

1. El trabajo con las personas siempre es de largo plazo, se trata de procesos.
2. La planeación estratégica es también de procesos.
3. El Benchmarking, el Empowerment, el Coaching y el ADN Organizacional, tienen carácter estratégico, por los importantes cambios que se generan a partir de ellos.
4. Las mejoras en el Capital Intelectual, pueden abordarse desde la Gestión del Conocimiento.
5. Desde la Gestión del Conocimiento, podría intentarse crear una comunidad de aprendizaje en la organización, al tiempo que se aplican de manera sucesiva, las cuatro estrategias.
6. Trazados los objetivos estratégicos de la organización, a 5, 10 o 15 años, en el marco de la filosofía y los valores corporativos, pueden aplicarse las estrategias en este orden: (a) ADN Organizacional - formando y fortaleciendo a la gerencia, (b) Coaching - liderado por gerentes que acompañan y hacen crecer al capital humano, (c) Empowerment - equipos empoderados de su misión y funciones, y (d) Benchmarking - La organización asumen nuevos retos, con entusiasmo, eficiencia y flexibilidad.
7. De acuerdo a lo anterior, se pueden aprovechar todas las ventajas de cada una de esas estrategias, aplicándolas de manera sucesiva, y no avanzando a la siguiente, hasta que la etapa anterior se encuentre consolidada.
8. Creo que una organización que se avoque a la mejora continua de su capital humano, y planifique en el nivel estratégico, tiene múltiples y mayores posibilidades de sobrevivir y prosperar, que aquellas que no lo hacen.

Estas son solo algunas ideas para el debate. En el área gerencial no todo está dicho, y lo que funciona en una organización puede no funcionar en otras. En ese orden de ideas la flexibilidad es una característica que debe poseer un gerente moderno, para poder operar en el complejo entorno de la transmodernidad.

Precisamente para aportar más elementos, es importante hacer algunas precisiones sobre las herramientas gerenciales a las que nos hemos referido unos párrafos atrás.

**El ADN Organizacional**

En esta interesante estrategia gerencial, se hace una analogía de la empresa u organización, con los seres vivos (realmente dotados de ADN). El material genético les permite a los seres vivos evolucionar, reaccionar a su entorno y adaptarse a los cambios. Lozano, O., Gómez, H., y Rositas, I. (s/f). señalan los elementos de “ADN” que la empresa necesita para evolucionar y reaccionar ante las oportunidades del entorno, estos son: *cultura y liderazgo, competencias organizacionales, estructura organizacional y gestión*. Señalando además que esos cuatro elementos son interdependientes entre sí, y por lo tanto deben ser mutuamente congruentes. Estos autores señalan:

> Empezamos por analizar a la organización desde la perspectiva de cada uno de estos elementos. Esto nos permite conocer a profundidad la situación actual de la empresa, plantear hacia dónde se quiere llegar, entender lo que hay que cambiar, diseñar cómo se va a lograr el cambio, y establecer un método de gestión para hacerlo de forma sustentable a través del tiempo. Cada elemento del ADN contribuye al proceso de cambio de una organización, desde el primer contacto al cambio hasta la internalización por completo.
>
> Estos elementos se ejecutan mediante un plan de acción que permite a la organización fusionarse haciendo partícipe a la organización de lo que la dirección entiende y desea (Comunicación), integrando y comprometiendo a la gente en un mismo asunto (Involucramiento), desarrollando habilidades

> para construir una aptitud (Capacitación) y construir un todo (Inclusión).

La estructura como la entienden Lozano, et al (s/f), consiste en la división funcional del trabajo en diferentes roles, así como de una autoridad asociada a los puestos, entre los que se presentan interacciones horizontales y verticales. Por otro lado, la gestión se refiere a la toma de decisiones en una empresa. Estas decisiones también tienen una jerarquía (afirmación cónsona con nuestras tesis iniciales). Hay que determinar quién toma qué decisiones tratando de obtener cuáles resultados. Según estos autores, la variable que diferencia las decisiones es el tiempo. En este sentido, una decisión estratégica está proyectada a un tiempo más largo (años tal vez), mientras que una decisión operativa, tiene que ver con el resultado del día, con el corto plazo.

Los conocimientos y habilidades que posee el personal es lo que se entenderá como competencias, mientras que por cultura y liderazgo se entenderán los comportamientos de las personas de una empresa, dentro y fuera de ella.

La gerencia traza un norte, una estrategia, y luego la organización sigue a la estrategia. Cuando la estrategia y la organización no están alineadas, se produce confusión y resultados fallidos. Las decisiones gerenciales deben entonces perseguir esa alineación, teniendo en cuenta los cuatro factores del ADN organizacional.

En cuanto a cultura y liderazgo, se deben priorizar la comunicación eficiente y la transparencia y disponibilidad de la información, para facilitar de esta manera el trabajo en equipo. En cuanto a competencias organizacionales, es importante definir claramente los perfiles de cargo, los roles y funciones, y capacitar a las personas para cumplir de mejor forma los roles y funciones asignados, trabajando de manera armónica con sus compañeros y formando equipos. En cuanto a estructura organizacional, es necesaria la definición precisa de la estructura que sustenta el rol, así como la asignación de responsabilidades directas para cada proceso y función. Finalmente, en cuanto a la gestión, los gerentes deben entrenarse para tomar decisiones oportunas, acertadas y que se traduzcan en resultados que conduzcan al logro de los objetivos organizacionales.

**El Coaching**

El coaching ha sido definido a lo largo del tiempo de muchas maneras, pero en esa diversidad hay unos elementos esenciales a tener en cuenta. Según la *International Coaching Community* (s/f), esta herramienta persigue:

> Ayudar a una persona a cambiar en la forma en que lo desea y ayudarle a ir en la dirección que quiere ir, (…) apoya a una persona en cada nivel a convertirse en quien quiere ser, (…) fomenta la conciencia, en quien quiere ser y permite el cambio. Desbloquea el potencial de una persona para maximizar su rendimiento. El Coaching ayuda a aprender en lugar de enseñar.
>
> El coach ayuda al cliente para lograr su mejor versión de sí mismo y para producir los resultados que quiere en su vida personal y profesional. El Coaching asegura que el cliente puede dar lo mejor, aprender y desarrollarse en la forma que desee. (s/p)

De manera adicional, la misma fuente establece diferencias conceptuales entre el Coaching y otras herramientas, que guardan cierta relación, pero definitivamente no son lo mismo. Estas diferencias se establecen con la tutoría, la consejería, la terapia, la formación, la consultoría y la enseñanza.

Concretamente y según García-Allen (s/f), el coaching es:

> (…) una metodología que consigue el máximo desarrollo profesional y personal de las personas y que influye en la transformación de éstas, generando cambios de perspectiva, aumentando la motivación, el compromiso y la responsabilidad. Por tanto, el Coaching es un proceso sistemático que facilita el aprendizaje y promueve cambios cognitivos, emocionales y conductuales que expanden la capacidad de acción en función del logro de las metas propuestas.

Este autor nos señala además que existen diferentes tipos de Coaching, estableciendo las siguientes tipologías:

- Coaching Personal (también llamado Life Coach).
- Coaching Organizacional, que se subdivide en Empresarial y Ejecutivo, y
- Coaching Deportivo.

El coaching personal, se refiere al desarrollo de habilidades para la vida diaria. En estos procesos, se trabaja a partir de los proyectos de vida y las estrategias necesarias para lograr los cambios que permitan alcanzar los objetivos que las personas se han trazado.

El coaching ejecutivo está dirigido a los altos ejecutivos de la organización. Busca desarrollar el liderazgo, las habilidades de dirección y de comunicación interpersonal.

El coaching empresarial está dirigido a empresas y organizaciones de manera global y no solo a los ejecutivos. En su desarrollo se incluyen temas como

relaciones interpersonales entre trabajadores, el trabajo en equipo, la productividad, la satisfacción de los clientes, y particularmente el empoderamiento (Empowerment).

Estos son los tres tipos de coaching que interesa reseñar en este escrito, pues como ya se habrá apreciado, ciertamente permiten influir sobre el capital humano de las organizaciones.

Finalmente, según el método que se emplee para adelantar el coaching (individual o grupal), tendremos los siguientes tipos:

- Coaching Ontológico: Persigue mejorar la forma en que los individuos se expresan.
- Coaching Sistémico: considera a la persona como parte de un sistema. Identifica el impacto que tienen los actos de la persona en su entorno.
- Coaching con Inteligencia Emocional: Persigue la autoregulación de las emociones a través del autoconocimiento.
- Coaching Coercitivo: Pretende motivar al individuo y fomentar su sentido de pertenencia a un grupo. Ha creado gran controversia por utilizar estrategias radicales y agresivas. Se le conoce también como "Sanando tu vida", "Coaching inside", "Liderazgo transformacional", "Samurai game" o "Ingeniería de lo imposible".
- Coaching PNL (Programación Neurolingüística): Ayuda a modificar conductas, a través del análisis de la forma como la persona interpreta y afronta la realidad (lo visual, lo auditivo y lo kinestésico).
- Coaching Cognitivo: busca la transmisión eficaz de conocimientos.

**El Empowerment**

Podemos observar que los nombres en inglés de algunas técnicas gerenciales se conservan sin traducir, este es el caso del Empowerment. Quizá se considere que así comercialmente su impacto psicológico será mayor, o que dicha técnica tendrá mayor credibilidad al ser algo "importado". Johnson (s/f), nos dice al respecto que:

> Empowerment quiere decir potenciación o empoderamiento que es el hecho de delegar poder y autoridad a los subordinados y de conferirles el sentimiento de que son dueños de su propio trabajo.
>
> En inglés "empowerment" y sus derivados se utilizan en diversas acepciones y contextos, pero en español la palabra se encuentra en pugna con una serie de expresiones que se aproximan sin lograr la plenitud del sustantivo. Se homologan "empowerment" con "potenciación" y "to empower" con "potenciar", mientras que caen en desuso expresiones más antiguas como "facultar" y "habilitar". (s/p)

Esta herramienta -que se considera estratégica- provee elementos para fortalecer los distintos procesos al interior de las empresas, permitiéndoles desarrollarse en mejores condiciones. Surge de la Calidad Total, y se aplica en los modelos de mejora continua y reingeniería. Además de dar sentido al trabajo en equipo y fortalecer el liderazgo, "permite que la calidad total deje de ser una filosofía motivacional, desde la perspectiva humana y se convierta en un sistema radicalmente funcional." (Johnson, s/f:s/p).

En el proceso de capacitación para promover el surgimiento y desarrollo del Empowerment en la organización, se debe prestar atención a la capacidad para:

- Apoyar a sus compañeros.
- Participar en reuniones.
- Organizarse.
- Comunicar ideas.
- Ayuda en toma de decisiones.
- Evaluar Diferencias.
- Controlar conflictos.
- Resolver Problemas.

Estas habilidades para la solución de problemas, contribuirán decididamente a la conformación de equipos autodirigidos, los cuales proporcionan los siguientes beneficios:

- Mejor comunicación entre empleados y gerentes.
- Mayor compromiso de los empleados.
- Cambio de actitud positivo, pasando de "tener que hacer" una cosa a "querer hacerla".
- Proceso más eficiente de toma de decisiones.
- Aumento de la Satisfacción.
- Calidad Mejorada.
- Costos de Operación Reducidos.
- Una organización más rentable.

**El Benchmarking**

Esta herramienta, también llamada *Comparación Referencial*, es una práctica no solo bastante popular sino también efectiva. Consiste en comparar el propio negocio con las empresas de la competencia, así como con otras empresas -incluso de otros sectores-, con el fin de detectar y analizar sus estrategias ganadoras, y de ser posible, aplicarlas en el propio negocio. Obviamente, lo mismo aplica para las organizaciones militares, policiales, de inteligencia o antiterroristas.

David T. Kearns, citado por Entrepeneur (2012), quien fuera director de Xerox Corporation, fue uno de los iniciadores de este concepto y lo definía como “el proceso continuo de medir productos, servicios y prácticas, contra competidores más duros o aquellas compañías reconocidas como líderes en la industria”.

Hay cinco pasos básicos para aplicar de forma eficiente esta herramienta:

1. Conócete a ti mismo. La organización debe realizar un análisis DOFA, junto con un análisis de rendimiento. En este punto se debe realizar una planeación sobre qué es lo que realmente se espera obtener del proceso de Benchmarking, y cuál será el método para recopilar la información tanto propia como de las otras empresas, además de determinar un presupuesto y un cronograma. En un número anterior de esta misma revista se da un ejemplo de cómo elaborar una matriz DOFA.
2. Conoce a tu competencia. Es muy importante tener claro en qué sector se trabaja y cuáles son las empresas líderes en dicho sector. Adicionalmente se pueden seleccionar empresas o individuos que adelanten buenas prácticas de negocio que sirvan de ejemplo.
3. Encuentra sus fortalezas. Una vez elegidas las otras empresas en las que se enfocará la investigación, se recurre a múltiples vías para obtener información sobre esas organizaciones, intentando detectar cuáles son sus fortalezas y cuáles sus debilidades. Enfocando las prácticas que los hacen líderes del sector.
4. Aplícalo a tu empresa. La información recabada en los puntos anteriores, debe ser analizada, evaluando cuales prácticas pueden ser efectivamente incorporadas a la propia organización, aun con adaptaciones. Los cambios organizacionales que se vayan a ejecutar, deben ser profusamente socializados con los empleados.
5. Avaluación. Es fundamental evaluar constantemente el resultado de los procesos organizacionales, y en particular cuando se implementan nuevas prácticas o estrategias.

Estos cinco puntos deben repetirse contantemente, pues es necesario estarse renovando para adaptarse a los cambios en el contexto y en el mercado.

**A modo de conclusión**

Suele suceder que lo cotidiano nos absorbe y las urgencias del día a día no nos permiten dedicar mucho tiempo a lo importante. Grosso modo, podemos afirmar que, en cuanto a las actividades organizacionales, lo necesario para el mero funcionamiento sería lo táctico, y lo pensado o previsto para el largo plazo sería lo estratégico.

En este orden de ideas, un gerente puede "gerenciar" el día a día y ser bueno en ello, hasta que las circunstancias internas, del entorno, o del mercado, se vuelven difíciles de manejar o adversas a los intereses organizacionales, y entonces se echará en falta el no haber gestionado pensando en el futuro. Por supuesto que nadie puede predecir el futuro, pero hay métodos que permiten proyectar escenarios -como la prospectiva, a través de la cual podemos prepararnos para el cambio de circunstancias, o podemos obrar de manera proactiva para cambiar circunstancias.

De esta forma, y en el contexto del capital intelectual (estructural, humano y relacional), debemos tener políticas, planes y metas, tanto de orden táctico como estratégico. Herramientas como el Benchmarking, el Empowerment, el Coaching y el ADN Organizacional, nos permiten mejorar el capital intelectual desde lo humano, con impacto en lo estructural y lo relacional. Está claro que estas herramientas son aplicables al sector de la seguridad, la defensa y la inteligencia.

**Referencias**


Entrepeneur (2012). Qué es el Benchmarking. Recurso en línea, consultado el 11 de julio de 2018. Disponible en: https://www.entrepreneur.com/article/265507

García-Allen, J. (s/f). Los 6 tipos de Coaching: los distintos coaches y sus funciones. En Psicología y Mente. Recurso en línea, consultado el 20 de julio de 2018. Disponible en: https://psicologiaymente.com/coach/tipos-de-coaching

Hernández, J. y Gómez, D. (2010). Una aproximación al concepto de gerencia y administración aplicado a la disciplina de enfermería. Recurso en línea, consultado el 13 de julio de 2018. Disponible en: http://www.redalyc.org/pdf/1277/127715324027.pdf

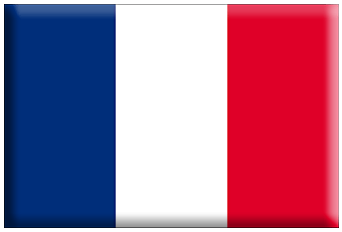
International Coaching Community (s/f). ¿Qué es Coaching?. Recurso en línea, consultado el 18 de julio de 2018. Disponible en: https://internationalcoachingcommunity.com/es/que-es-coaching/

Johnson, Y. (s/f). Concepto de Empowerment. Recurso en línea, consultado el 15 de julio de 2018. Disponible en: https://www.gestiopolis.com/concepto-de-empowerment/

Lozano, O., Gómez, H., y Rositas, I. (s/f). ¿Qué es el ADN organizacional? Recurso en línea consultado el 10 de julio de 2018. Disponible en: https://www.forbes.com.mx/brand-voice/que-es-el-adn-organizacional/


**Francia**

## 13 Regimiento de Dragones Paracaidistas



El 13 ° Regimiento de Dragones Paracaidistas (en francés: 13 e Régiment de Dragons Parachutistes , 13 e RDP) es una unidad especial de reconocimiento del ejército francés. Es uno de los tres regimientos pertenecientes al Comando de Fuerzas Especiales del Ejército Francés, que a su vez está bajo el comando del COS (Comando de Operaciones Especiales). Tiene su base en Martignas-sur-Jalle.

**Reseña Histórica**

Es una unidad de mucha tradición, de las más antiguas de Francia. Fue creado por el Marqués de Barbezières en Languedoc en 1676 como Regimiento de Dragones (caballería montada). Luego en 1791 se le nombró como 13 Regimiento de Dragones. En 1936 el regimiento se transformó en un cuerpo blindado, para luego en 1952 convertirse en una unidad de reconocimiento con capacidad aerotransportada.

En 1956 el regimiento estuvo integrado a la 25 División de Paracaidistas, creada en ese año. En 1957 se transfirió a la 10 División de Paracaidistas durante la guerra de Argelia. Posteriormente fue parte de la 11 División de Intervención Ligera. El 13 e RDP se transformó en una unidad de reconocimiento de largo alcance. Durante la Guerra Fría, la misión principal del 13 e RDP era proporcionar inteligencia para el 1er Ejército, mientras que cada compañía del 1er Regimiento de Paracaidistas de Infantería de Marina 1 er RPIMa proporcionaría inteligencia para un Cuerpo de Ejército.

En abril de 1960, el ejército francés en Alemania decidió formar una compañía experimental de inteligencia de largo alcance, la 7ma compañía de Comandos, basada en trabajos anteriores en Indochina y Argelia. La séptima compañía desarrolló procedimientos de supervivencia y reconocimiento para operar detrás de las líneas

enemigas. Estos métodos y procedimientos y el personal son absorbidos por el 13 e RDP. Esto llevó al 13 e RDP a partir de 1963 formalmente a la tarea con sus misiones actuales de la 'Patrulla de reconocimiento de largo alcance'.

Finalmente, en 1968, el ejército francés presentó un plan para la conversión del regimiento completamente a su nueva tarea. A la espera de la creación del nuevo 1er Ejército en 1972, EMA decidió implementar este plan, reestructurando el regimiento. El 13 e RDP se pone a disposición del ejército para ser utilizado en Alemania en caso de guerra. El Regimiento estaba inicialmente subordinado al BGRE (Brigada de inteligencia militar y guerra electrónica del ejército francés). Hoy en día, el 13 e RDP es parte del Comando de Operaciones Especiales Francés.

Desde el final de la Guerra Fría, el 1er Regimiento de Paracaidistas de Infantería de Marina 1 e RPIMa se convirtió en una unidad de acción directa, mientras que el 13 e RDP se especializó en operaciones de reconocimiento / vigilancia en ambientes hostiles, reuniendo inteligencia para operaciones especiales. En cierto modo, son similares al papel del Destacamento de Vigilancia de Largo Alcance del Ejército de los EE. UU.

El 13 e RDP participó en la Guerra del Golfo. Esto se destacó cuando tres operadores fueron capturados por los iraquíes a fines de 1990. El 13 e RDP estaba, junto con otras unidades francesas, fuertemente involucrado en la Guerra de Kosovo y utilizó tácticas y tecnología para forzar a los blindados serbios a combatir al Ejército de Liberación de Kosovo y otras fuerzas aliadas al aire libre, lo que facilitó su destrucción por los bombardeos aliados, particularmente por la Fuerza Aérea de los Estados Unidos y la Royal Air Force. El 13 e RDP también contribuyó a la captura de Momčilo Krajišnik en 2001.

**Misión**

La misión del regimiento es adquirir inteligencia humana en cualquier momento y en cualquier ambiente hostil (acuático, alta montaña, bosque ecuatorial, desierto), detrás de las líneas enemigas, usando pequeñas unidades autónomas y discretas, capaces de posicionarse muy cerca para adquirir inteligencia y transmitirla a las fuerzas

aliadas. Las tropas están entrenadas para utilizar en sus misiones medios improvisados, pero también la más alta tecnología.

Las habilidades de alto nivel del 13 e RDP es reconocimiento especial, hace que a menudo sea solicitado su apoyo por otras fuerzas. El Groupe d'Intervention de la Gendarmerie Nationale mantiene una estrecha relación con el 13 e RDP para entrenar a sus gendarmes en el reconocimiento avanzado, y para operaciones de rescate de rehenes en entornos hostiles. Las Équipes d'Observation en Profondeur (EOP, equipos de control de avanzada) de los regimientos de artillería franceses utilizan los procedimientos operativos estándar del 13 e RDP. El Regimiento también colabora con la Direction générale de la sécurité extérieure (DGSE, Servicio de Inteligencia francés).

**Organización**

El Regimiento se compone actualmente de siete escuadrones, entre ellos tres escuadrones de "búsqueda" o inteligencia, que proporcionan los equipos de reconocimiento del Regimiento. Dos escuadrones de comunicaciones de largo alcance, que proporcionan un enlace de comunicaciones seguro entre los equipos de reconocimiento desplegados y las oficinas centrales superiores, y dos escuadrones de entrenamiento, que son responsables de proporcionar cursos de capacitación internos y certificar nuevos miembros de la unidad.

El 13 e RDP está equipado con material estándar del ejército francés, pero tiene acceso a armas y equipos especializados cuando es necesario.

GESTIÓN DE RIESGOS
WWW.MASTERSECURITYCONSULTING.COM


## MITIGA RIESGOS EN TU ORGANIZACIÓN

# ANTES, DURANTE Y DESPÚES

### IMPLEMENTA CONTROLES QUE REDUZCAN LOS RIESGOS

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

**MAS QUE CONSULTORES, SOMOS TUS ASESORES DE CONFIANZA**

**PREGUNTA POR LOS PAQUETES EMPRESARIALES Y KIT PYME TOTAL**

contáctanos info@mastersecurityconsulting.com
+57 3165479295