Big Data aplicado a Defensa y Seguridad

Estado del Arte de las Tecnologías

Cátedra Isdefe-UPM

Octubre 2021 – Julio 2022

Índice

Índice de figuras

Índice de tablas

Alcance del documento

Este documento, tiene el propósito de dar una visión general de las aplicaciones del Big Data en el ámbito de la Defensa y la Seguridad. Para hacerlo, el documento ha sido estructurado mediante diversos capítulos o secciones.

El primer capítulo, es un capítulo introductorio al Big Data. En él, tras poner de manifiesto la importancia actual de los datos y presentar el concepto Big Data a partir de algunas de las definiciones utilizadas, se analiza con cierto detalle los distintos eslabones de la cadena de valor del dato en diferentes secciones: adquisición y tratamiento de datos, transmisión de datos, almacenamiento de datos, análisis de datos y finalmente la visualización de datos. A lo largo de las mismas, se revisan algunos de los elementos básicos asociados a estas tecnologías como son las fuentes de obtención de datos, sus tipos y características (volúmenes, velocidades, latencia…) y los procedimientos de análisis.

En el siguiente capítulo, "Estado del arte del Big Data en el ámbito de la Defensa y Seguridad" se enumeran y describen brevemente las distintas políticas y proyectos llevados a cabo por distintas instituciones y países en el ámbito de la Defensa y Seguridad empleando el Big Data. Obviamente no es un catálogo completo, pero si permite tener una visión general de la importancia que tienen estas técnicas y el interés por las mismas en los países más avanzados. Se finaliza el capítulo describiendo algunas de las principales actividades en este ámbito en nuestro país.

En el tercer capítulo, bajo el título "Aplicaciones del Big Data en Defensa y Seguridad" se realiza un análisis sistemático y pormenorizado de las principales las aplicaciones encontradas en una revisión exhaustiva de los publicado al respecto en fuentes abiertas. Se desglosan por campos de aplicación y se relacionan los artículos encontrados en cada uno de ellos. En cada apartado se introduce una descripción general de cómo se emplea el Big Data, su utilidad y se desarrollan con algo más de extensión algunas de las aplicaciones más características.

Finalmente, en el último capítulo, se presenta la estructura del mapa de conocimiento construido a partir de los trabajos realizados. Se ha completado la hoja Excel desarrollada hasta ahora en los diferentes trabajos de la Cátedra ISDEFE-UPM, incluyendo la línea de investigación Big Data. La hoja permite clasificar todas las fuentes de conocimiento por la tecnología implicada, en algunos casos desglosada en ámbitos más concretos, países, centros de investigación, autores, palabras clave y año. En todos casos se suministra el enlace al documento.

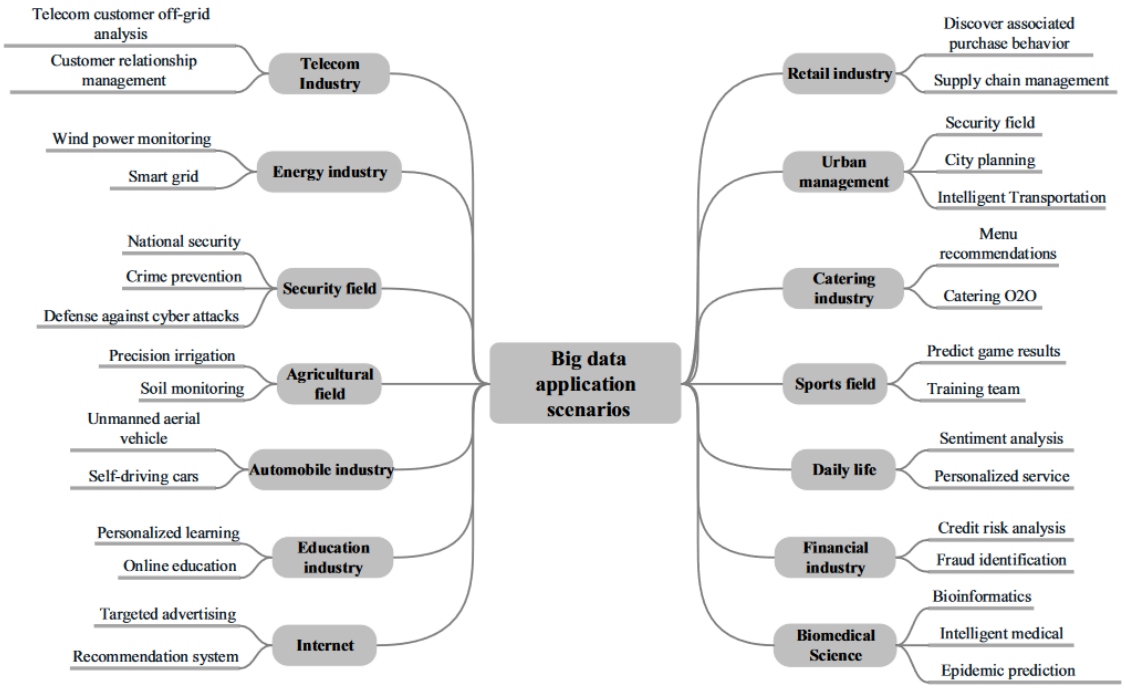
El trabajo incluye un anexo dedicado a resumir el seguimiento realizado sobre lo publicado en relación con el uso de técnicas de Big Data en el conflicto de Ucrania y la bibliografía empleada en el mismo.

1. Introducción al Big Data

En estos últimos años, los datos digitales han ido creciendo a un ritmo vertiginoso y debido a eso, cada día más algoritmos hacen uso de grandes cantidades de datos para aprender patrones complejos empleando "conocimientos ocultos" para predecir comportamientos y estimar información nueva difícil de extraer.

En la actualidad muchas aplicaciones hacen uso de los datos de los usuarios para proporcionarles nuevos contenidos personalizados. Por ejemplo, Amazon emplea los datos para recomendar nuevos productos, Netflix para proponer películas y series, Google para suministrar enlaces relacionados con las búsquedas realizadas, además de un gran número de otras aplicaciones y campos como son el médico, el entretenimiento, la seguridad, las finanzas, etc.

Asimismo, en el campo de Internet de las cosas, la tecnología de recopilación de datos mediante redes de sensores inalámbricos y los algoritmos de procesamiento de datos de Big Data pueden realizar aplicaciones prácticas como Internet de vehículos, arquitecturas informáticas novedosas, localización en interiores y detección de anomalías en las carreteras, etc.

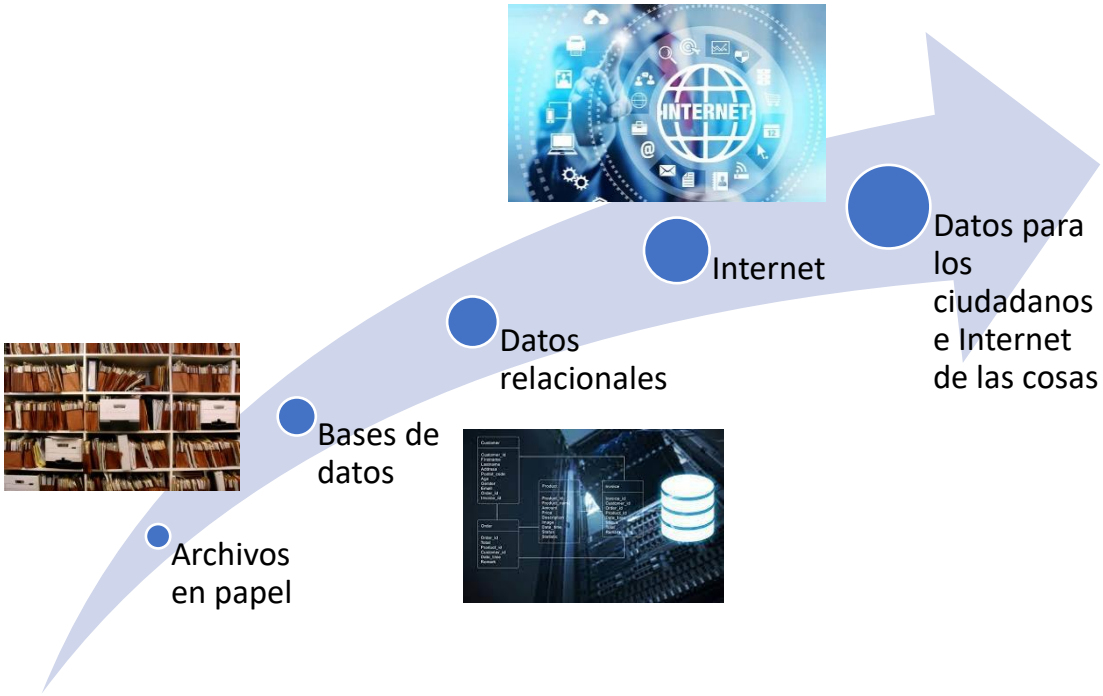


ESCENARIOS DE APLICACIÓN DEL BIG DATA [1]

El Big Data no es una tecnología en sí misma, sino un conjunto de distintas técnicas para obtener valor y beneficios de los grandes volúmenes de datos que se generan hoy en día.

1.1. Definición de Big Data

El concepto de Big Data es relativamente nuevo, pero los orígenes de los grandes conjuntos de datos se pueden remontar a las décadas de 1960 y 1970, en las cuales el mundo de los datos empezaba con la implementación de los primeros centros de datos y el desarrollo de las bases de datos relacionales. Se puede plantear la evolución de la gestión de la información en el siguiente gráfico.



EVOLUCIÓN DE LOS DATOS

Existen diversas definiciones de Big Data como las que se muestran a continuación, pero en general en todas ellas se menciona de alguna manera un gran volumen de datos.

- *McKinsey Global Institute (MGI) en Junio de 2011 [2]*

"conjuntos de datos cuyo tamaño va más allá de la capacidad de captura, almacenado, gestión y análisis de las herramientas de base de datos".

- *Gartner [3].*

"son activos de información de gran volumen, alta velocidad y / o gran variedad que exigen formas rentables e innovadoras de procesamiento de información que permitan una mejor comprensión, toma de decisiones y automatización de procesos".

- *Wikipedia [4]*

"Big Data o macrodatos es un término que hace referencia a conjuntos de datos tan grandes y complejos que precisan de aplicaciones informáticas no tradicionales de procesamiento de datos para tratarlos adecuadamente".

- *Oracle [5]*

"son datos que contienen una mayor variedad y que se presentan en volúmenes crecientes y a mayor velocidad".

- *O'Reilly Radar [6]*

"son datos que exceden la capacidad de procesamiento de los sistemas de bases de datos convencionales. Los datos son demasiado grandes, se mueven demasiado rápido o no se ajustan a las restricciones de las arquitecturas de su base de datos".

En la Real Academia Española (RAE), en su versión del diccionario de la lengua española, no existe una definición de Big Data, pero en el diccionario panhispánico del español jurídico se define Big Data [7] como:

"Conjunto de técnicas que permiten analizar, procesar y gestionar conjuntos de datos extremadamente grandes que pueden ser analizados informáticamente para revelar patrones, tendencias y asociaciones, especialmente en relación con la conducta humana y las interacciones de los usuarios."

Adicionalmente, la RAE en su cuenta oficial de Instagram especifica como alternativa a «Big Data», se puede usar «macro datos» para el conjunto ingente de datos e «inteligencia de datos» para la rama de la computación que estudia su gestión y análisis [8].

De acuerdo con Gartner [9], "el Big Data garantiza soluciones de procesamiento innovadoras para una variedad de datos nuevos y existentes para proporcionar beneficios comerciales reales. Pero el procesamiento de grandes volúmenes o una amplia variedad de datos sigue siendo simplemente una solución tecnológica a menos que esté vinculado a metas y objetivos comerciales."

El Big Data tiene cinco características que son conocidas como las cinco uves [10]:

- Volumen: los datos tienen que ser "grandes", y en este caso el tamaño se mide como volumen, por lo que la cantidad de datos importa.
- Velocidad: cada vez es mayor la velocidad a la que se crean nuevos datos gracias a los avances tecnológicos y la correspondiente necesidad de que esos datos se digieran y analicen casi en tiempo real.
- Variedad: hace referencia a los diversos tipos de datos disponibles.
- Veracidad: la autenticidad de los datos y cuánto se puede confiar en ellos.
- Valor: los datos en sí tienen un valor intrínseco, pero, no tienen ninguna utilidad hasta que dicho valor se revela.

En los últimos años, algunos expertos han ido expandiendo las cinco uves mediante la incorporación de más palabras para caracterizar el Big Data hasta alcanzar las 17 uves. En el artículo "The 17 V's Of Big Data" [11] identifican y definen las diecisisiete características de Big Data para manejar grandes conjuntos de datos de manera eficiente.

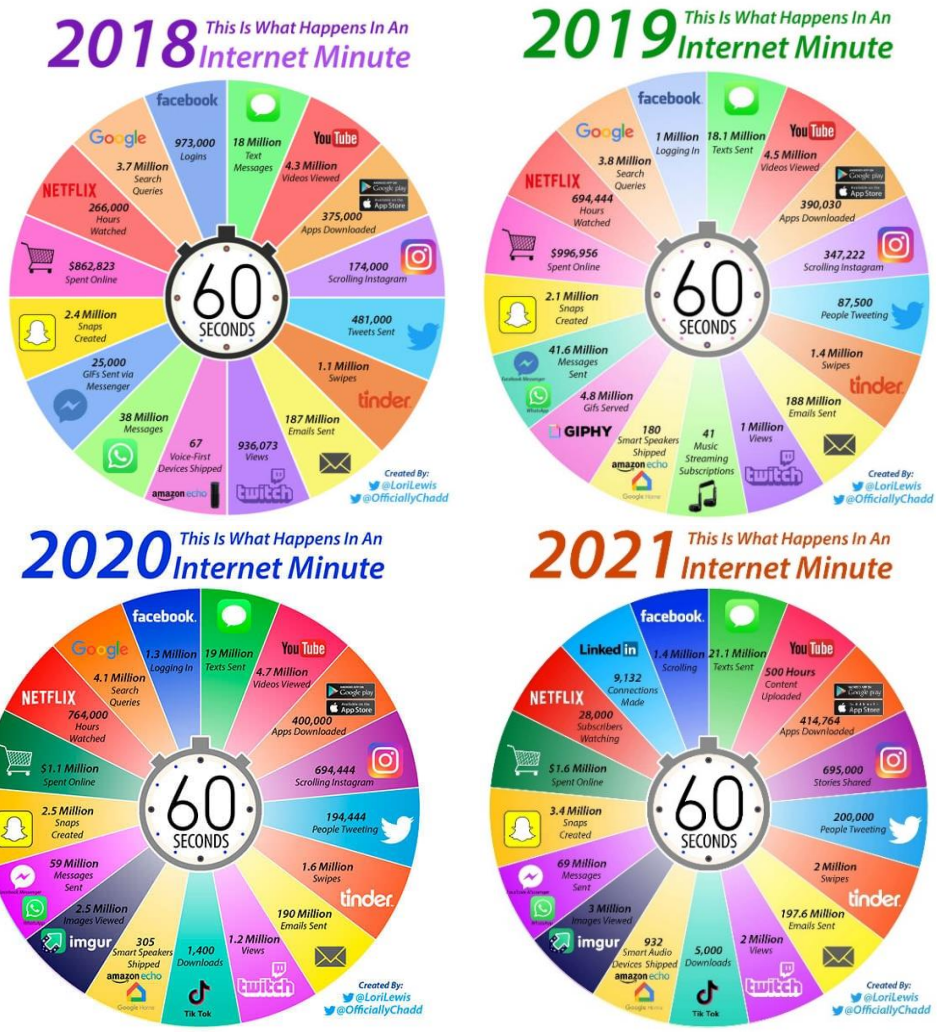
1.2. Adquisición de datos y tipos de datos

La frase "*data is the new oil*", es decir, *los datos son el nuevo petróleo* es quizás una de las frases más populares que destaca la importancia de los datos, debido a que cada día la creación de nuevos datos se dispara y es difícil de computar. Aunque conocer la cantidad de datos que se crean cada día no sirve de nada si no sabemos utilizarlos estratégicamente. Al igual que el petróleo, los datos en sí mismos tienen poco valor intrínseco, lo que realmente importa son los conocimientos prácticos que podemos aprender de él.

En 2013, alrededor del tiempo en que se aceleró el desarrollo de la tecnología de máquinas inteligentes, el mundo produjo 4,4 zettabytes de datos, pero para 2025 se espera que la tasa de producción anual sea de 163 zettabytes. Dónde el video e imágenes constituyen una gran parte de los nuevos datos digitales de los cuales más del 80% no está estructurado [12].

A principios de 2020, se estimó que la cantidad de datos en el mundo era de 44 zettabytes. Dicho número se logró al sumar la cantidad total de datos generados cada día por los sitios de redes sociales, instituciones financieras, instalaciones médicas, plataformas de compras, fabricantes de automóviles y muchas otras actividades en línea [13].

El uso del internet ha permitido que se generen en un minuto una inmensa cantidad de datos de distintos ámbitos, y dichos datos van creciendo con los años como se puede observar en los gráficos "This is What Happens in An Internet Minute" de diversos años.



GRÁFICOS DE 2018, 2019,2020 Y 2021 DE "THIS IS WHAT HAPPENS IN AN INTERNET MINUTE" [14]

Todos los días se crean aproximadamente 2,5 quintillones de bytes de datos, pero con la llegada del Internet de las cosas o *Internet of Things* (IoT), esta tasa de creación de datos será aún mayor al producirse un incremento de objetos y dispositivos conectados a Internet que generan datos sobre patrones de uso de los clientes y el rendimiento de los productos.

En la actualidad hay un gran volumen de datos procedente de distintas fuentes como son:

- Equipos electrónicos (cámaras, teléfonos móviles…)
- Sensores
- Geoespacial

- Redes sociales
- Correos
- Transacciones
- Web
- Etc.

Un dataset o conjuntos de datos es una colección de datos habitualmente tabulada. En el caso de los datos tabulados, las variables están organizadas por columnas y cada fila personifica a un miembro determinado del conjunto de datos.

En el contexto de Big Data, se entiende por dataset aquellos conjuntos de datos tan grandes que las aplicaciones de procesamiento de datos tradicionales no los pueden procesar debido a la gran cantidad de datos contenidos [15], como por ejemplo, un conjunto de imágenes de satélite en las que pueden aparecer buques [16].

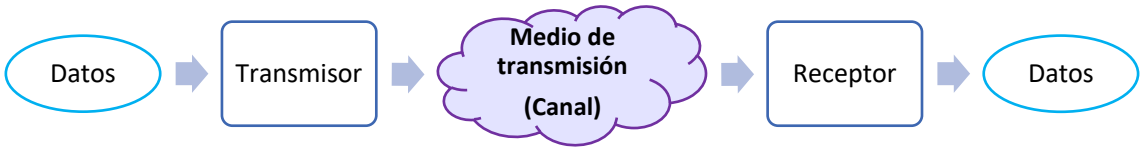
Distintos tipos de datasets pueden ser descargados de diversos centros institucionales (MIT, Standford, Oxford…), de grandes empresas (Google, Microsoft, Facebook, Twitter….) o en sitios web que ofrecen concursos (Kaggle, CrowdAnalytix, …) entre otros. También, se puede recolectar datos propios y crear un conjunto de datos personalizado para resolver problemas donde un conjunto de datos no está disponible o los conjuntos de datos no son suficientes para que los algoritmos funcionen eficientemente.

En función de la fuente de precedencia, existen innumerables tipos de dato como son:

- Datos numéricos
- Multimedia: imágenes, video, audio, texto, etc.
- Datos web
- Secuencias de clics
- Geográficos

1.3. Transmisión de datos

La trasmisión de datos puede ser llevada a cabo mediante diversos medios de transmisión, como es el aire, la fibra, o el cable.



ESQUEMA DE TRANSMISIÓN DE DATOS

La capacidad del canal es un parámetro que indica las posibilidades para transmitir información, que depende de la respuesta en frecuencia del medio de transmisión y del tipo de modulación de la señal empleada. La capacidad del canal se mide como una velocidad binaria en bits por segundo (bps), y viene limitada por el límite teórico de Shannon independientemente de la técnica de transmisión empleada.

Para un mismo canal, caracterizado por un cierto ancho de banda (BW) se pueden obtener diferentes velocidades binarias según la eficiencia espectral de la técnica de modulación de la señal empleada (BPSK, 16QAM, 32QAM, 16APSK,etc.).

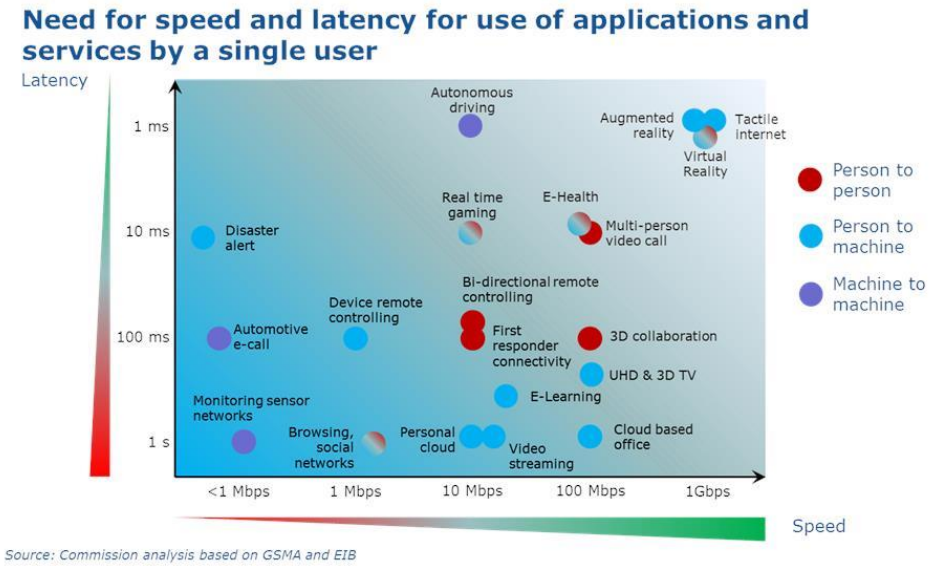
A la hora de la transmisión de datos, también hay que considerar la latencia del sistema de transmisión. La latencia se puede definir como el tiempo que tarda en transmitirse un paquete de datos desde que se solicitó hasta que es recibido. Dependiendo de la aplicación o servicio se requieren latencias bajas, especialmente en aplicaciones de tiempo real como la conducción autónoma, realidad virtual o de aplicaciones que requieran una interacción instantánea.

APPLICATIONS.

Big Data Applications	Time Requirement
Financial Market Trading and Surveillance	Milliseconds
Military Decision Making	Seconds
Intelligent Transportations	Seconds
Smart Grid	Seconds
Crowd Control	Seconds
Large-Scale Emergency Responses	Minutes
Early Warning for Natural Disasters	Minutes

REQUISITOS DE TIEMPO PARA DIFERENTES APLICACIONES EN TIEMPO REAL [17]

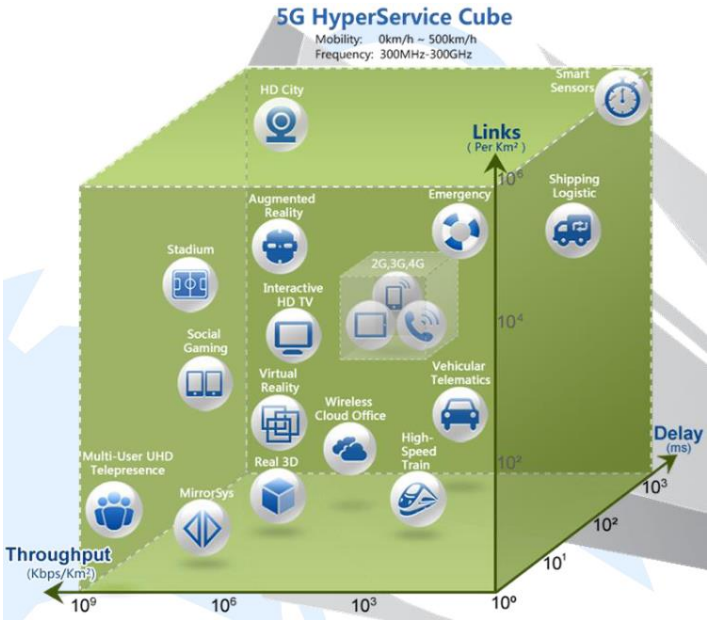
Adicionalmente, dependiendo de la red de acceso empleada para la transmisión de datos se conseguirá una mayor o menor velocidad de transmisión, que dependiendo de la aplicación se requerirá mayor o menor velocidad.



GRÁFICA DE VELOCIDAD VS. LATENCIA EN DISTINTAS APLICACIONES [18]

El gráfico anterior ilustra la necesidad de velocidad de conectividad a Internet y capacidad de respuesta para un solo uso de una aplicación o un servicio. Esta necesidad aumenta para los usos múltiples, que se han convertido en la norma, ya que un solo usuario suele tener usos simultáneos y una sola conexión suele servir a varios usuarios simultáneamente.

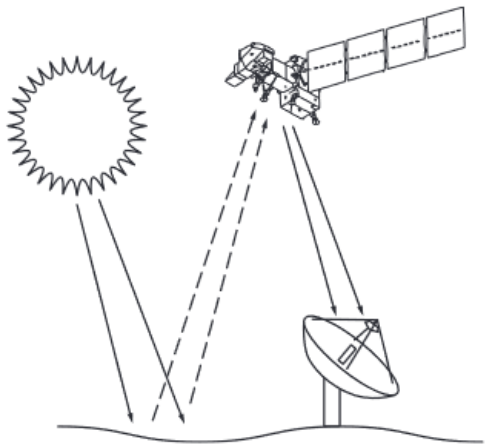
Asimismo, conviene resaltar con la implementación de redes 5G, se consigue una reducción en tiempos de latencia y un incremento de velocidad. En la siguiente gráfica se muestra el "5G HyperService Cube" [19] que ofrece una multi-visión general dimensional en términos de rendimiento, latencia y número de conexiones requeridas para los muchos tipos de servicios que necesitarán las redes 5G para ejecutarse.



5G HYPERSERVICE CUBE [19]

La latencia que se ha mencionado anteriormente se refiere a la de sistemas de comunicaciones, sin embargo existen otras latencias que no tienen que ver con el sistema de comunicaciones como tal, sino con los procedimientos de obtención de los datos. Es el caso de la latencia que se produce en la obtención de datos obtenidos por satélites para aplicaciones como la teledetección.

Los satélites que hay alrededor de la Tierra tiene distintos propósitos, pero algunos de ellos se encargan de obtener imágenes de la Tierra (teledetección) además de la recolección de otro tipo de datos obtenidos de los sensores que llevan a bordo. La información recolectada por los satélite es transmitida a distintas estaciones terrestres, pero el problema es que en el caso de algunos satélites y la tierra al encontrarse en constante movimiento el tiempo de visibilidad del satélite y la estación terrestre para poder descargar los datos es limitado, en promedio alrededor de unos 6 minutos.



LA ENERGÍA ELECTROMAGNÉTICA SE REFLEJA EN LA SUPERFICIE DE LA TIERRA Y LLEGA AL SENSOR DEL SATÉLITE, QUE RECOPILA Y REGISTRA INFORMACIÓN SOBRE ESA ENERGÍA, PARA LUEGO SER TRANSMITIDA A UNA ESTACIÓN RECEPTORA EN FORMA DE DATOS QUE SE PROCESAN EN UNA IMAGEN [20]

La NASA propone una definición para latencia de los datos satelitales, "se define como el tiempo total transcurrido entre el momento en que los datos son recopilados, adquiridos por un sensor satelital, aéreo o in situ, y cuando están disponibles para el acceso público a través de Internet" [21]. También propone las siguientes definiciones de latencia de datos satelitales:

Term	Latency	Purpose
Real-time	Less than 1 hour	These terms are often used to refer to data that are made available quicker than routine processing allows. They are used for a range of applied sciences, decision and tactical support, monitoring and early warning of events.
Near real-time (NRT)	1-3 hours	
Low latency	3-24 hours	
Expedited	1-4 days	
Standard routine processing	Generally, 8 – 40 hours but up to 2 months for some higher-level products	Standard products provide an internally consistent, well-calibrated record of the Earth's geophysical properties to support science.

TABLA 1: RESUMEN DE DEFINICIONES DE LATENCIA DE DATOS SATELITALES [21]

Obviamente, es necesario separar claramente los dos conceptos de latencia indicados en los párrafos anteriores.

1.4. Almacenamiento de datos

A la hora de almacenar grandes volúmenes de datos, se necesitan sistemas que sean capaces de gestionar dicha ingesta de datos. Para ello, existen centros de datos que son edificios que contienen varios servidores y dispositivos de comunicaciones que comparten requisitos y necesidades (energía, almacenamiento, red, seguridad). Google cuenta en la actualidad con 21 centros de datos conocidos [22], mientras que Facebook cuenta con 18 centros de datos [23], para el manejo y almacenamiento de todos los datos.

Se puede considera que los sistemas Big Data tienen una forma particular del almacenamiento y gestión de los datos obtenidos, gestionando la diversidad de tipos de datos a través de dos conceptos:

- Lago de datos (Data Lake): se almacenan todos los datos, estructurados y no estructurados, con distintos formatos y con distintas fuentes de origen, pudiendo considerarse datos "en crudo".
- Almacén de datos (Data Warehouse): almacena datos estructurados y procesados recibidos del Data Lake, de forma que puedan realizarse análisis posteriores de manera precisa y muy rápida.

CLOUD computing o computación en la nube, es otra opción para almacenamiento de grandes conjuntos de datos. En términos generales, la computación en la nube involucra almacenar y acceder a datos y programas desde fuentes externas que utilizan Internet en lugar de usar recursos locales como es un disco duro.

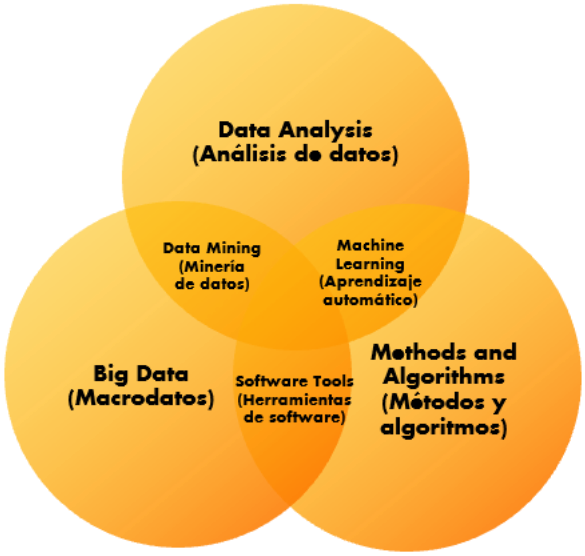
Una infraestructura que se suele emplear para almacenar datos y ejecutar aplicaciones en clústeres de hardware es Hadoop que es una estructura de software de código abierto. Además, proporciona almacenamiento masivo para cualquier tipo de datos, enorme poder de procesamiento y la capacidad de procesar tareas o trabajos concurrentes virtualmente ilimitados [24].

1.5. Análisis de datos

Lo primero que se necesita si se desea aprender de los datos, es un dataset con información útil para resolver un problema. Dependiendo del problema a resolver se necesitarán distintas fuentes de información. Por ejemplo, se puede realizar un análisis de sentimiento sobre los Tweets para clasificarlos en función de si son positivos, negativos o neutros. También, se puede efectuar la detección de objetos en imágenes y para ello se necesita un dataset compuesto por una gran cantidad de imágenes con los objetos presentados en el problema y sus etiquetas.

La ciencia de datos o Data Science, es considerado un campo multidisplinario centrado en extraer información (*insights*) de grandes volúmenes de datos para ayudar a tomar decisiones, mientras que el Big Data se centra en la ciencia que analiza enormes volúmenes de datos [25].

De acuerdo con IBM, la analítica de Big Data, en ingles conocido como Big Data analytics, es el proceso mediante el cual los ordenadores evalúan grandes colecciones de datos para permitir a los humanos ganar nuevos conocimientos que dan como resultado decisiones mejores y más rápidas ". La analítica de Big Data incluye capacidades como "análisis de texto, aprendizaje automático, análisis predictivo, minería de datos, estadísticas y procesamiento del lenguaje natural" [26].



RELACIÓN DE BIG DATA Y EL ANALÍSIS DE DE DATOS [25]

Para analizar grandes volúmenes de datos, además de tener equipos adecuados para procesar tal ingesta de datos como son los supercomputadores, se suele recurrir a técnicas de Machine Learning (Aprendizaje máquina o aprendizaje automático). Machine Learning (ML) es una rama de la inteligencia artificial (IA) y la ciencia de datos que se centra en el uso de datos y algoritmos para imitar la forma en que aprenden los humanos, mejorando gradualmente su precisión según la definición del IBM [27].

La IA se centró en sus comienzos en el empleo de redes neuronales inspiradas en el funcionamiento de las neuronas en el cerebro humano, con el fin de implementar una máquina tan inteligente como un ser humano en la década de 1980. Debido a las limitaciones en la potencia de procesamiento de los ordenadores, la IA estaba limitada a los laboratorios de investigación, pero cuando los grandes tecnológicos empezaron a construir superordenadores

con una mayor potencia de computación fue posible que la investigación de la IA sea posible a nivel mundial [28].

Se puede considerar que la IA es la capacidad que podemos dotar a una máquina para permitirla comprender o interpretar datos, aprender de los datos y tomar decisiones "inteligentes" basadas en conocimientos y patrones extraídos de los datos. Mientras, que el aprendizaje automático en su forma más básica es la práctica de usar algoritmos para analizar datos, aprender de ellos y luego hacer una determinación o predicción sobre algo en el mundo [29].

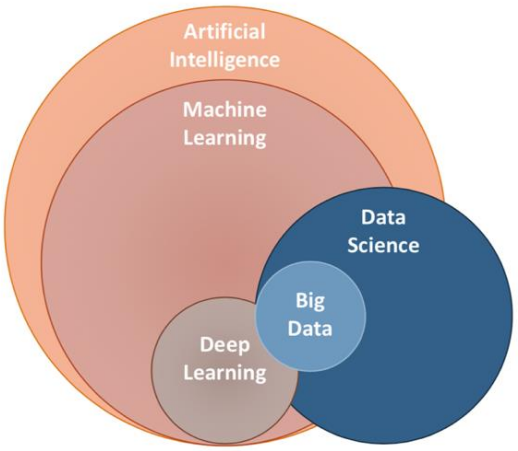
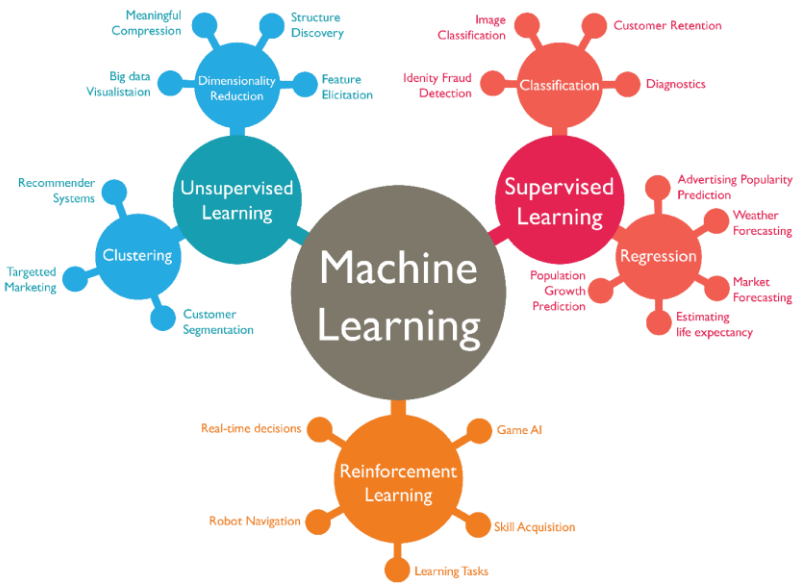


DIAGRAMA DE VENN PARA VISUALIZAR LA RELACIÓN ENTRE BIG DATA, DATA SCIENCE, IA, ML Y DL [28]

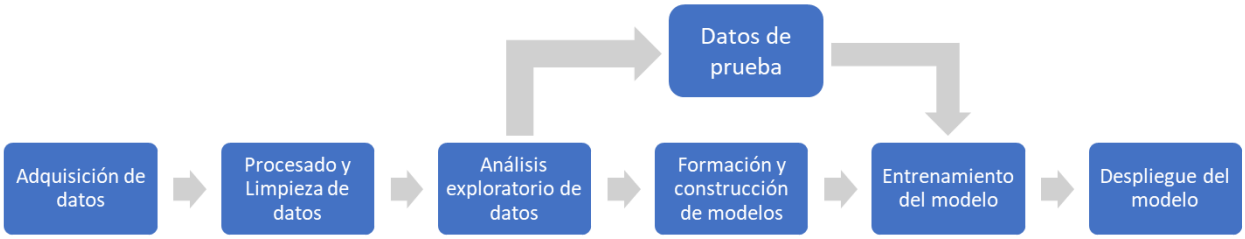
Machine Learning se puede dividir en aprendizaje supervisado (supervised learning), aprendizaje no supervisado (unsupervised learning) y aprendizaje reforzado (reinforcement learning).

- Aprendizaje supervisado: se utiliza un dataset con datos etiquetados, por etiquetados se refieren a un conjunto de datos (principalmente multimedia) cada uno con su correspondiente etiqueta / descripción. En aprendizaje supervisado se tiene variables de entrada (X) y una variable de salida (Y), y el algoritmo se usa para inferir el mapeo de la función de entrada con la salida. La entrada son una serie de vectores de datos y la salida es la etiqueta correspondiente estimada a partir del aprendizaje sobre los datos. El objetivo es aproximar la función de mapeo para cuando se tengan nuevos datos de entrada poder predecir la variable de salida. Los problemas se pueden resolver por clasificación (la salida es una categoría) o regresión (la salida es un valor real)
- Aprendizaje no supervisado: el dataset está compuesto por un conjunto de datos pero los datos no están etiquetados. El aprendizaje no supervisado se tienen datos de entrada (X) y no las variables de salida correspondientes. El objetivo es modelar la estructura subyacente o distribución en los datos para aprender más sobre los datos. Los algoritmos tratan de buscar patrones comunes en los datos para asociarlos o agruparlos (clustering).
- Aprendizaje reforzado: no hay un dataset previo pero se sabe el comportamiento y las reglas involucradas en el problema. Estos algoritmos interactúan con los entradas del entorno (estados) e intentan averiguar cuál es la mejor cuál es la mejor acción que realizar. Una vez Una vez que se decide una acción, una retroalimentación (recompensa / multa) se recibe.



VISIÓN GENERAL DE MACHINE LEARNING [21]

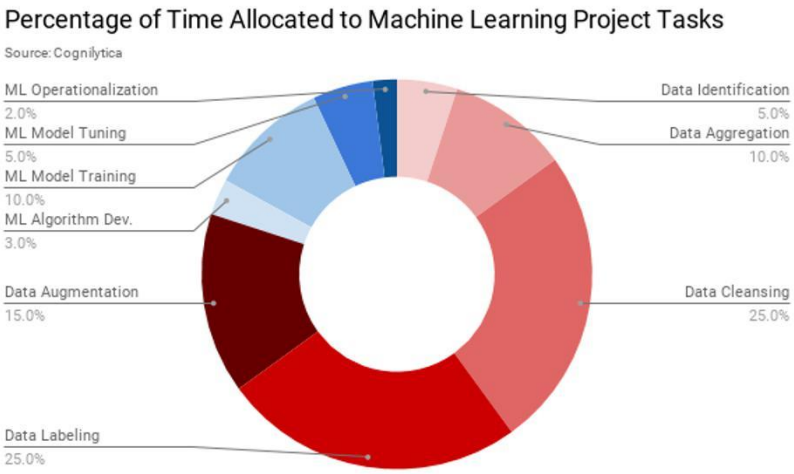
Habitualmente, los proyectos de Machine Learning suelen tener la siguiente estructura:



ETAPAS DE LOS PROYECTOS DE MACHINE LEARNING

1) Adquisición de datos: los datos que van a ser usados para entrenar el algoritmo se recolectan de conjuntos de datos existentes.
2) Procesado y Limpieza de datos: el procesado de datos consistes en convertir el "raw data" o datos en brutos al tipo de datos necesario para el algoritmo o sistema. Mientras que la tarea de limpieza está relacionada con inspeccionar los datos para asegurarse de que toda la información esté. En caso de que haya información vacía, es decir faltan valores, rellenarlos o eliminarlos.
3) Análisis exploratorio de datos: es un enfoque para analizar conjuntos de datos para resumir sus principales características, a menudo con métodos visuales. El análisis exploratorio de datos puede ayudar a visualizar lo que los datos pueden decirnos más allá del modelado formal o la tarea de prueba de hipótesis.
4) Pruebas y entrenamiento del modelo: operaciones que se realizan mediante un algoritmo de aprendizaje para aprender sobre los datos y probar si el modelo aprendido tiene la precisión necesaria para resolver el problema.
5) Despliegue del modelo: uso del modelo entrenado en su aplicación final para predecir nuevos valores o información.

Dentro de los proyectos de Machine Learning, el porcentaje de tiempo que se emplea en técnicas de aprendizaje máquina es inferior al que se emplea en la manipulación o procesado de datos, como se puede apreciar en la siguiente figura.



PORCENTAJE DE TIEMPO ASIGNADO A TAREAS DE APRENDIZAJE MÁQUINA (FUENTE: COGNILYTICA) [30]

A continuación, se va a explicar el procesado de distintos tipos de datos, y como se puede extraer información útil de ellos.

❖ Procesado de datos numéricos

Los datos numéricos tienden a ser los más fáciles de procesar o manipular, pues habitualmente no hay que hacer ningún tipo de pre procesado al menos que se deseé cambiar de tipo, por ejemplo pasar de "float" a entero.

De los datos numéricos, se puede obtener estadísticas descriptivas, como por ejemplo las mostradas a continuación.

TB prevalence, all forms (per 100 000 population per year)	Afghanistan	Albania	Algeria	American Samoa
count	18.000000	18.000000	18.000000	18.000000
mean	353.333333	36.944444	47.388889	12.277778
std	64.708396	6.915220	4.487091	9.886447
min	238.000000	22.000000	42.000000	0.000000
25%	305.000000	32.000000	44.000000	6.000000
50%	373.500000	40.500000	45.500000	9.000000
75%	404.500000	42.000000	50.750000	16.250000
max	436.000000	44.000000	56.000000	42.000000

ESTADÍSTICAS DE DATOS NUMÉRICOS

❖ Procesado de Imágenes

Una imagen puede verse como una matriz de números, la cual tiene distintos valores para representar los distintos pixeles de la imagen, por lo que se aplicar ciertas operaciones o funciones matemáticas.

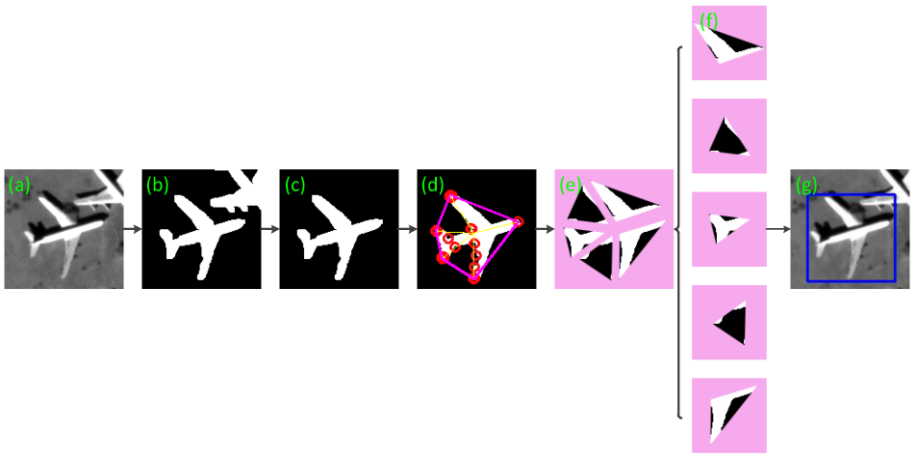
En el procesado de imágenes, las imágenes pueden estar comprimidas o no comprimidas, en función del formato del fichero de la imagen (jpeg, bmp, png, etc.), pero su tratamiento es el mismo.

Como se ha dicho, la imagen se puede ver como una matriz de números por lo que se consigue acceder a cualquiera de los valores de la imagen para obtener el valor de cierto pixel. También se puede aplicar transformaciones de rotación, traslación, cambiar el tamaño (aplicando distintas interpolaciones), voltear o recorte.

Adicionalmente, se puede aplicar aritmética, es decir, sumar o restar valores para aclarar o oscurecer la imagen. Asimismo, se pueden usar operaciones bitwise (bit a bit) para conseguir máscaras y aplicarlas a la imagen, o el uso de operadores como Sobel, Prewitt y Canny para la detección de bordes o esquinas.

Como las imágenes suelen estar en formato RGB, se puede obtener la información de cada uno de los canales por separado. También, se puede pasar la imagen a escala de grises y obtener información de su luminancia y sus dos crominancias, o trabajar con otros espacios de colores como HSV o Lab al tener distintas propiedades y, pueden ser más adecuados dependiendo de la aplicación.

De las imágenes se pueden obtener características como su histograma, estadísticas del canal de color (media, desviación estándar, sesgo y curtosis), patrones binarios locales (LBP) o el histograma de gradientes orientados (HOG).



BOSQUEJO ESQUEMÁTICO DEL PROCESO DE DETECCIÓN DE OBJETOS PARA UN EJEMPLO DE AVIÓN. EN LA FIGURA, (A) IMAGEN DE ENTRADA, (B) BINARIZACIÓN, (C) LAS REGIONES CONECTADAS EXTRAÍDAS, (D) DETERMINACIÓN DEL RECORRIDO CONVEXO DE ESQUINA, (E) EFECTO DE SEGMENTACIÓN, (F) MUESTRA CADA FRAGMENTO, Y (G) DA LOS RESULTADOS FINALES. [31]

Se puede considerar que a la hora de tratar los datos, en especial las imágenes, hay dos vertientes en función de su forma de ejecución:

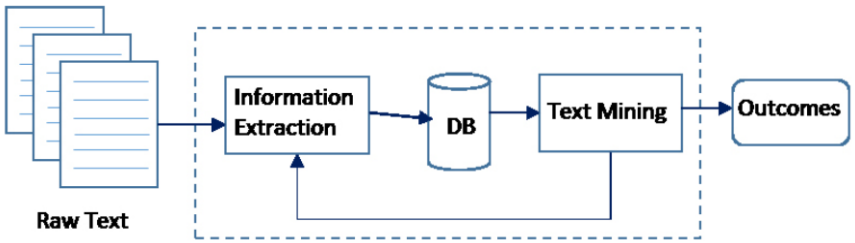
- Centrada en modelos: pruebas empíricas de diferentes diseños/arquitecturas. En este caso se tiente un descomunal espacio de arquitecturas bases posibles (backbones) pero está condicionado a tener grandes bases de datos. Suele ser la estrategia tomada por investigadores y gigantes tecnológicos.
- Centrada en datos: se ha de tener buenos datos y anotaciones, es decir, volumen, consistencia y calidad.

❖ Procesado de Texto

El procesado de texto entraría dentro de la minería de texto o el análisis de texto, que tienen como objetivo examinar automáticamente grandes colecciones de datos de texto no estructurados, con el fin de extraer información relevante o patrones. Se estima que más de un 80% de los datos de texto no son estructurados, incluidos correos electrónicos, noticias, artículos web, informes internos, artículos de investigación, entradas de blogs, etc.

El procesado de texto consistiría en estructurar el texto en bruto de entrada, mediante análisis, extracción de características, indexación, etc.. En el paper "Text Analytics: the convergence of Big Data and Artificial Intelligence" [32] plantean que una aplicación de análisis de texto típica consta de los siguientes pasos y tareas:

- Partiendo de una colección de documentos, una herramienta de minería de texto recupera un documento en particular y lo pre procesa verificando el formato y los conjuntos de caracteres.
- Lo siguiente sería una fase de análisis de texto, a veces repitiendo técnicas hasta que se extrae la información. La estrategia subyacente en todos los componentes es encontrar un patrón (ya sea de una lista o de un proceso anterior) que coincida con una regla, y luego aplicar la regla que anota el texto. Cada componente realiza un proceso particular en el texto, como: segmentación de oraciones (dividir el texto en oraciones); tokenización (palabras identificadas por espacios entre ellas); etiquetado de parte del discurso (sustantivo, verbo, adjetivo, etc., determinado por la búsqueda y las relaciones entre las palabras); análisis sintáctico superficial / fragmentación (dividiendo el texto por sintagma nominal, sintagma verbal, cláusula subordinada, etc.); reconocimiento de entidad nombrada (NER) (las entidades en el texto tales como organizaciones, personas y lugares); análisis de dependencia (cláusulas subordinadas, anáfora pronominal [es decir, identificar a qué se refiere un pronombre], etc.).
- El proceso resultante proporciona información estructurada o semiestructurada para un uso posterior, por ejemplo, creación de bases de conocimientos, o validación de algoritmos de aprendizaje automático.

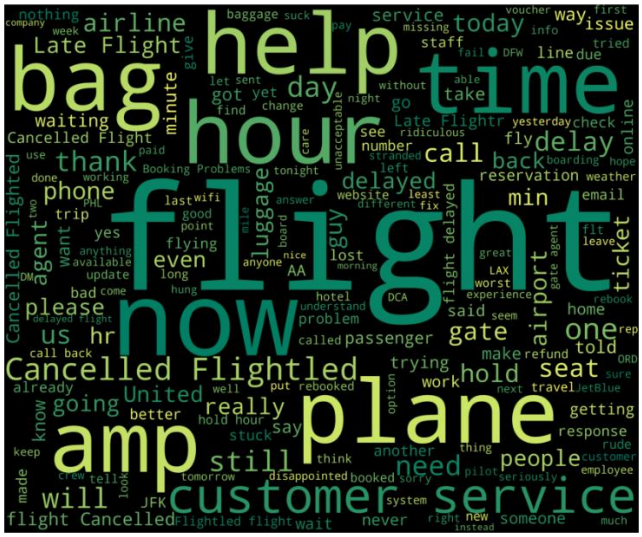


DESCRIPCIÓN GENERAL DE UN MARCO DE MINERÍA DE TEXTOS [32]

En el documento [32], también se mencionan algunas de las técnicas existentes para el análisis de texto como son la extracción de información, el seguimiento de temas, el resumen, la categorización, la agrupación en clústeres, el enlace de conceptos, la visualización de información, la respuesta a preguntas y el aprendizaje profundo.

Mediante el análisis de texto se podría realizar análisis de sentimientos, además de realizar contabilizar la frecuencia con que aparecen ciertas palabras o efectuar búsquedas de palabras significativas en el ámbito de la defensa y seguridad.

A continuación se muestra el resultado de algunas técnicas de procesado de texto.



USO DE WORDCLOUD PARA VER LA DISTRIBUCIÓN DE PALABRAS (IZQUIERDA) Y LA FRECUENCIA CON LA QUE SE REPITEN CIERTAS PALABRAS (DERECHA)

❖ Procesado de audio

El procesado de audio tiende a ser un procesado complejo, al ser un tipo de dato no estructurado, del cual se ha de obtener información. La señal de audio audible se encuentra entre frecuencias de 20 Hz y 20kHz, pero las personas tienden a ser más sensible a frecuencias entre 2kHz y 5kHz.

El cambio de presión en el aire en un cierto instante de tiempo genera una onda de presión sonora o acústica, que puede ser digitalizada. Para capturar dicha onda por un equipo electrónico, hay que muestrear la señal analógica para convertirla a digital.

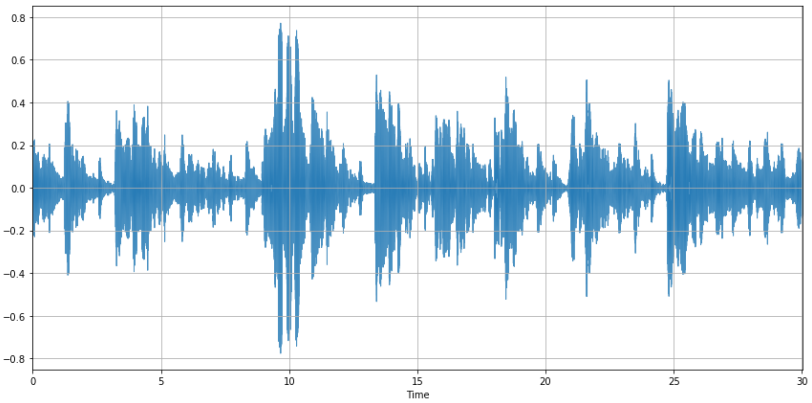
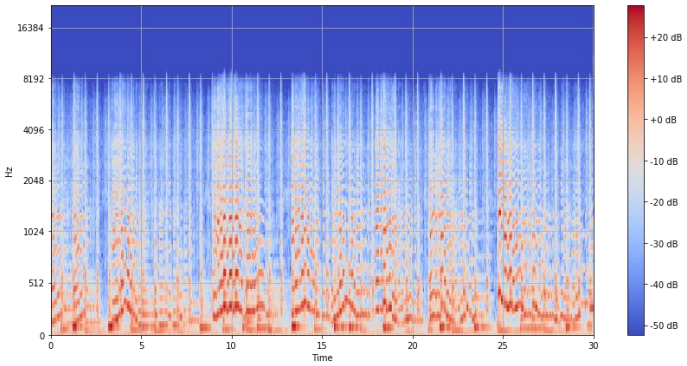


GRÁFICO DE TIEMPO VS. PRESIÓN

De la propia señal de audio se puede extraer las siguientes características:

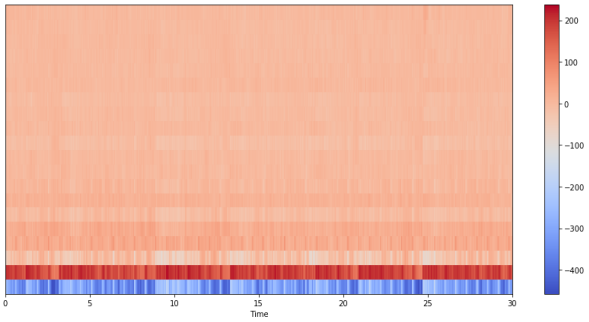
- Energía y valor cuadrático medio de energía (RMSE): la energía de una señal corresponde a su magnitud total. Para las señales de audio, eso corresponde aproximadamente a qué tan fuerte es la señal.
- Tasa de cruce por cero: indica el número de veces que una señal cruza el eje horizontal.

- Transformada de Fourier de corta duración (STFT): las señales de audio son altamente no estacionarias, por lo que la aplicación de la transformada de Fourier de corta duración es obtenida al computar la transformada para tramas sucesivos de la señal.
    - Espectrograma: en procesado de audio, a menudo solo nos preocupamos por la magnitud espectral y no el contenido de fase, por lo que se puede definir un espectrograma (magnitud al cuadrado de la STFT) como una representación que muestra la intensidad de las frecuencias a lo largo del tiempo. El espectrograma puede ser representado en escala normal o escala logarítmica (espectrograma de Mel), pues la percepción humana de la intensidad del sonido es de naturaleza logarítmica.



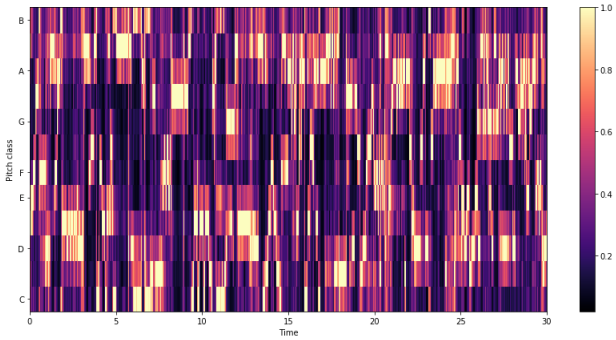
ESPECTOGRAMA

- Coeficientes cepstrales de frecuencia Mel (MFCC): son un pequeño conjunto de características (entre 10-20) que describen de manera concisa la forma general de una envolvente espectral. El primer MFCC, el coeficiente 0, no transmite información relevante para la forma general del espectro. Solo transmite un desplazamiento constante, es decir, agrega un valor constante a todo el espectro.



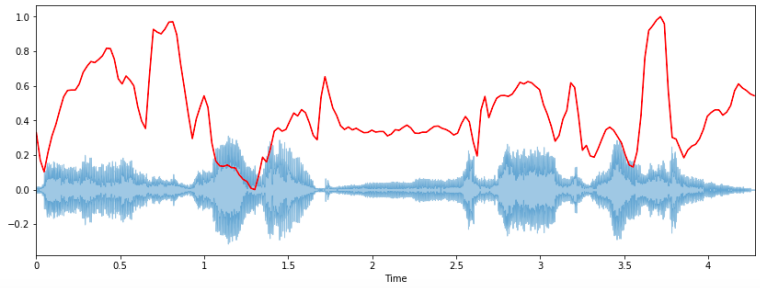
COEFICIENTES CEPSTRALES DE FRECUENCIA MEL (MFCC)

- Cromagrama: Las características de croma son una representación atrayente y poderosa para audio musical en la que todo el espectro se proyecta en 12 contenedores que representan los 12 semitonos distintos (o croma) de la octava musical. Dado que, en la música, las notas con una separación de exactamente una octava se perciben como particularmente similares, conocer la distribución del croma incluso sin la frecuencia absoluta (es decir, la octava original) puede brindar información musical útil sobre el audio.



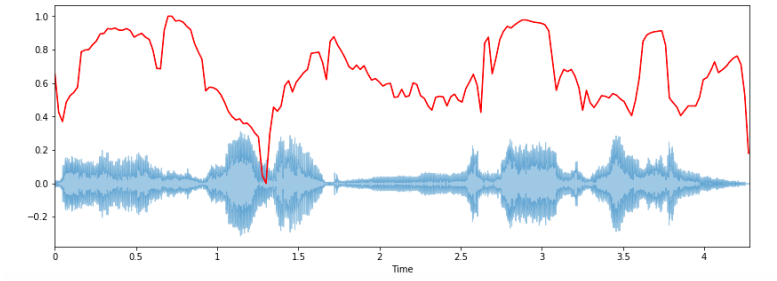
CROMAGRAMA

- Centroide espectral: indica en qué frecuencia se centra la energía de un espectro, es decir, dónde se encuentra el "centro de masa" de un sonido.



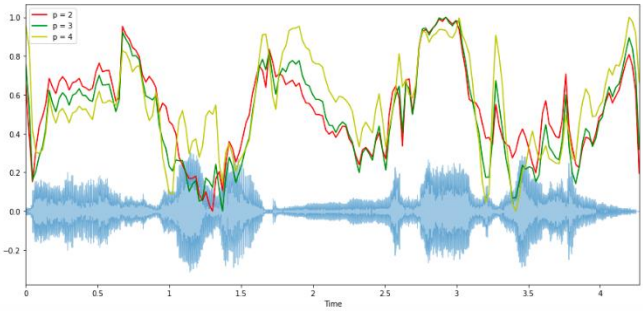
CENTROIDE ESPECTRAL

- Rolloff espectral: medida de la forma de la señal, representa la frecuencia a la que las frecuencias altas descienden a 0.



ROLLOFF ESPECTRAL

- Ancho de banda espectral: se define como el ancho de la banda de luz a la mitad del pico máximo (o ancho completo a la mitad del máximo [FWHM]).



ANCHO DE BANDA ESPECTRAL

De las características anteriores, se pueden obtener sus estadísticas (valor medio, desviación estándar, media, mínimo y máximo) para crear vectores de características y poder así clasificar distintos sonidos, por ejemplo, el sonido que hacen distintos aviones militares, o generar un motor de búsqueda de audio.

En lo mencionado anteriormente, se trabaja con una señal de audio en el dominio temporal o frecuencial, pero también se podría trabajar con un dataset en el cual distintas características de la señal de audio ya han sido extraídas como es el timbre, tono, instrumentalidad, acústica, etc. [33].

Adicionalmente, la señal voz podría pasarse a texto lo hablado, utilizando las herramientas adecuadas para ello, y así poder realizar posteriormente un análisis de texto para buscar frases o palabras concretas, por ejemplo, relacionadas con terrorismo, con ataques cibernéticos o migraciones.

❖ Procesado de datos espaciotemporales

La mayor parte de los datos espaciotemporales son registrados mediante el sistema de posicionamiento global (GPS). Sin embargo, los datos GPS brutos de dispositivos móviles, como son los teléfonos móviles en la vida diaria no siempre están marcados con el modo de viaje y no son adecuados para ingresarlos en los algoritmos, por lo tanto, el pre procesamiento de datos GPS sin procesar es esencial.

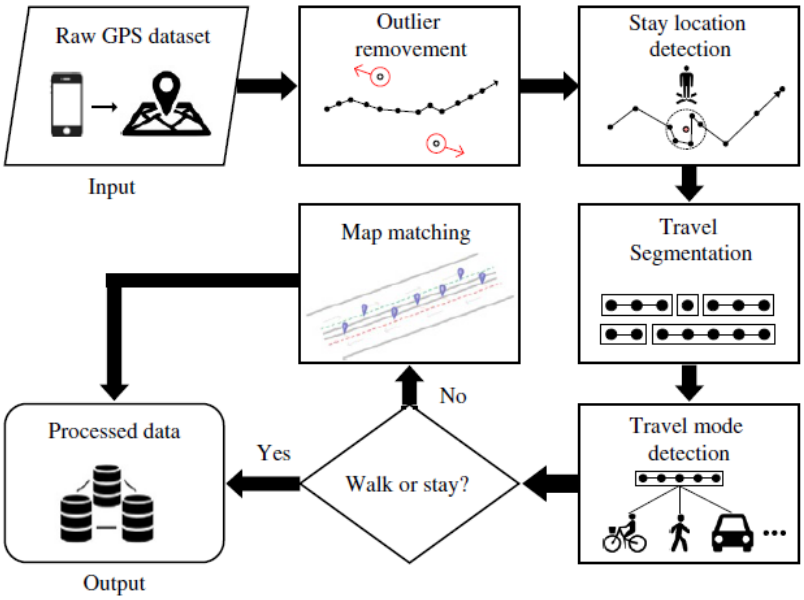
Los datos GPS en bruto habitualmente son registrados en forma de tupla:

$$(x, y, t)$$

Donde *x* se refiere a la longitud, *y* a la latitud, y *t* al correspondiente timestamp (marca de tiempo). Puede haber otras variantes de la tupla como añadir un número de identidad adicional que indica los individuos.

Normalmente, el gran conjunto de datos de la trayectoria del GPS tiene la escala miles de millones de este tipo de tupla, por lo que es complicado trabajar con el conjunto de datos sin procesar de este tamaño. Para comprender mejor el patrón de movilidad que se efectúa, se debe extraer información de alta dimensión.

En el capítulo dos bajo el título “Spatio-temporal data preprocessing technologies” del libro “Big Data and Mobility as a Service” [34], se plantea como parte del procesado de datos GPS el siguiente flujo de trabajo.



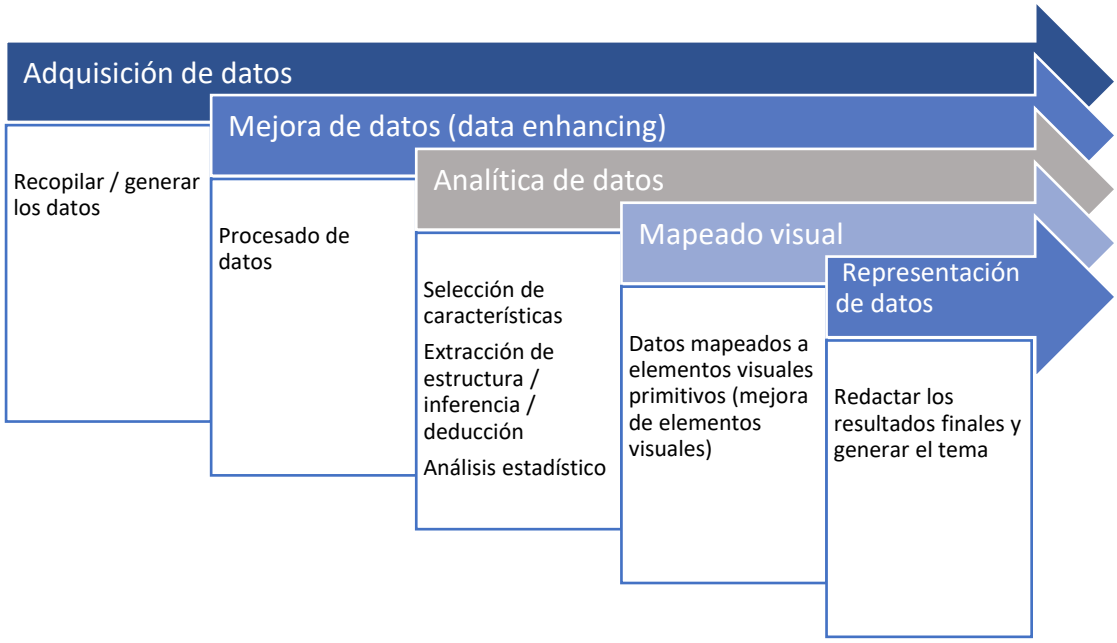
FLUJO DE TRABAJO GENERAL DE PRE PROCESAMIENTO DE DATOS GPS [34]

- Remover outliers (partes aisladas): eliminar los puntos GPS que no han sido registrados correctamente debido a la mala señal, error de computación o error del sistema.
- Detección de ubicación de estancia: puede ser utilizado para el análisis de patrones de vida, al detectar dónde y cuándo el usuario se queda en la trayectoria.
- Segmentación de viaje: ayuda principalmente a juzgar si el objetivo del estudio se mueve y, lo que es más importante, cuando cambian el modo de viaje a otro.
- Detección de modo de viaje: intentar averiguar el modo de viaje del segmento de viaje. Distintos modelos han conseguido distinguir el modo de viaje (andando, bus, coche, moto, etc.) con una probabilidad mayor al 85%.
- Mapeado de mapas: el método de coincidencia de mapas tiene como objetivo que el modo del viaje del segmento de viaje (moto, coche, tren, etc.) este en el área designada, por ejemplo, un automóvil debe viajar por carreteras en áreas urbanas.

1.6. Visualización de los datos

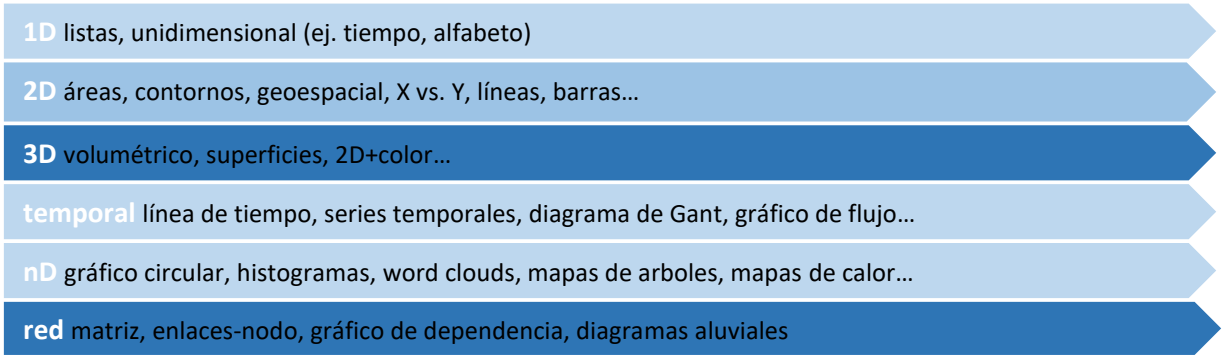
Los datos además de ser analizados también pueden ser visualizados, y para ello hay distintas formas de visualización en función del tipo de dato que se maneje y el problema a resolver.

Una definición de problema para la visualización de datos puede ser conectar las fuentes de datos y los tomadores de decisiones de maneras que se agilice la interpretación y la toma de decisiones basadas en las especificidades de la percepción humana. Se puede tener la siguiente canalización agrupando visualización y análisis.



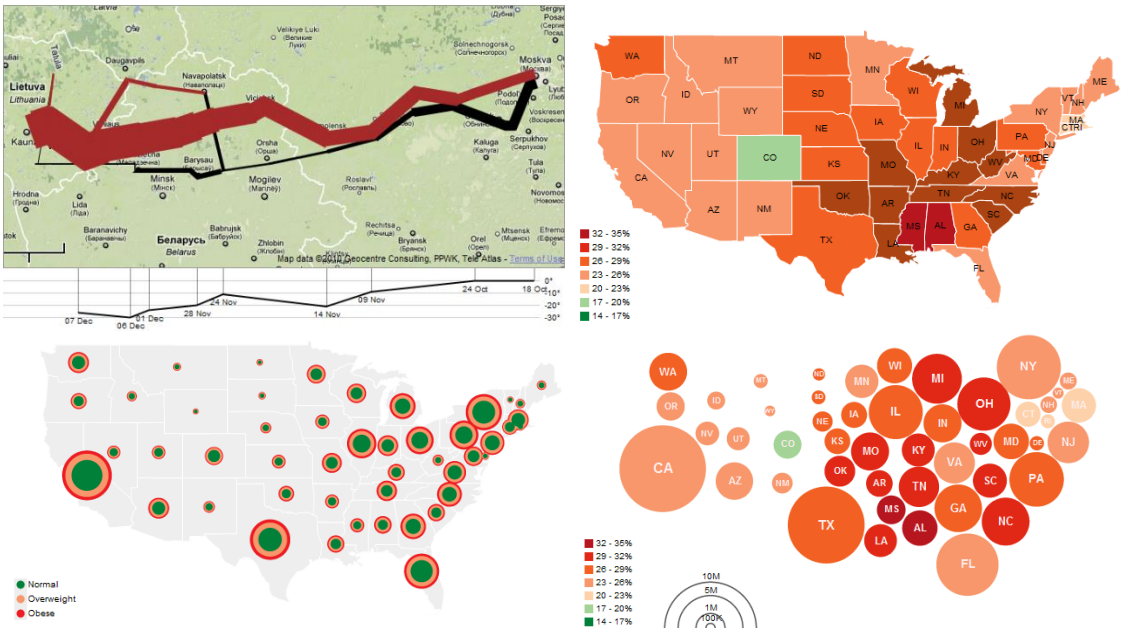
PASOS PARA LA VISUALIZACIÓN Y ANÁLISIS DE DATOS

Como ejemplo de algunos tipos de técnicas para visualización, se tienen los siguientes en función de sus dimensiones.



TÉCNICAS DE VISUALIZACIÓN DE DATOS EN FUNCIÓN DE SU DIMENSIÓN

Adicionalmente a las técnicas mencionadas arriba, en el artículo "A Tour Through the Visualization Zoo" [35], se proponen técnicas de visualización de mapas como son mapas de flujo (flow maps), mapas de coropleta (chropleth maps), mapas de símbolos graduados y cartogramas.



TÉCNICAS DE VISUALIZACIÓN DE DATOS EN MAPAS. ARRIBA A LA IZQUIERDA CORRESPONDE A MAPA DE FLUJO, ARRIBA A LA DERECHA CORRESPONDE A MAPA DE COROPLETA. EL DE ABAJO A LA IZQUIERDA ES UN MAPA DE SÍMBOLOS GRADUADO Y EL DE LA DERECHA UN CARTOGRAMA. [35]

2. Estado del arte del Big Data en el ámbito de la Defensa y Seguridad a nivel global

El Big Data ofrece alternativas para resolver problemas existentes o emergentes, además tiene la capacidad de influir en todos los aspectos de una organización, desde recursos humanos hasta capacitación, logística y gestión de instalaciones y operaciones diarias para la guerra.

El futuro espacio de batalla está construido no solo con buques, carros, misiles y satélites, sino también con algoritmos, redes y redes de sensores. Como en ningún otro momento de la historia, las guerras futuras se librarán en infraestructuras civiles y militares de sistemas satelitales, redes de energía eléctrica, redes de comunicaciones y sistemas de transporte, y dentro de redes humanas. Ambos campos de batalla, electrónico y humano, son susceptibles de manipulación por parte de algoritmos adversarios. [36]

En entornos electrónicos, los algoritmos ya se utilizan para monitorear y mantener el control sobre la mayoría de las áreas de infraestructura crítica (electricidad, agua, alimentos, finanzas, comunicaciones, etc.). También para entrar en las redes sociales y robar datos personales de trabajadores gubernamentales o de empresas, lo que proporciona un conocimiento valioso para que un adversario adapte una campaña de influencia encubierta contra cada líder militar o político individual.

En el ámbito de defensa y seguridad, el Big Data tiene por objetivo captar y explotar grandes cantidades el datos dispares con el fin de aunar sensorización, percepción y decisión en sistemas autónomos, con el objeto de aumentar así el entendimiento de la situación y el contexto del analista y del agente del orden o combatiente [37].

2.1. OTAN

En el año 2000, ya se planteó el uso de los datos en el ámbito militar en el congreso en Canadá bajo el nombre de Multimedia Visualization of Massive Military Datasets (Atelier OTAN sur la visualisation multimedia d'ensembles massifs de donnees militaires) [38], organizado por la OTAN (Organización del Tratado del Atlántico Norte) también conocida por su acrónimo en inglés como NATO. En dicho congreso se implantaron cinco talleres de trabajo distintos: visualización de operaciones, visualización para comando, visualización de redes, fusión de datos y matemáticas y técnicas.

En el 2018 se publicó el paper de posicionamiento, “Big Data and Artificial Intelligence for Decision Making: Dutch Position Paper” [39], se plantea que una de las principales misiones de la OTAN es la facilitar la colaboración entre estados miembros en este ámbito. Asimismo, la tecnología para Big Data e inteligencia artificial actualmente se está desarrollando a un ritmo rápido, con un gran impacto potencial en los procesos de toma de decisiones militares estratégicas, operacionales y tácticas. Como tal, los beneficios operativos militares pueden ser enormes y diversos, pero a su vez, también hay deficiencias y riesgos que deben evaluarse. Para las aplicaciones militares, existen requisitos importantes que pueden hacer que las tecnologías civiles sean inadecuadas o exigir cambios en las implementaciones dado que los sistemas tienen que funcionar en un contexto altamente desestructurado e impredecible, y con oponentes que deliberadamente intentan perturbarlos o engañarlos. Adicionalmente, los autores plantean la

adopción de la perspectiva del bucle OODA (Observe, Orient, Decide, Act) como marco básico para identificar y alinear tecnologías y temas de interés, dado que el ciclo OODA representa el ciclo de vida desde la adquisición de datos hasta la toma de decisiones y refleja cuán sofisticada debe ser una tecnología para proporcionar valor agregado. También, recomiendan iniciar una migración a una infraestructura habilitadora de Big Data, habilitada por diversas tendencias y tecnologías emergentes, incluidas las infraestructuras centradas en datos, la contenedorización y el desarrollo de (micro) servicios, para aprovechar al máximo las posibilidades de la inteligencia artificial y el Big Data.

The OODA perspective for structuring the topics and activities within themes	
OBSERVE (O)	**Link / overlap with Autonomy Theme**
– *Internet of Things* – *Data Collection Architectures* – *Social Media Analysis* – *Data Fusion* – *Interoperability*	– *Autonomy for Intelligence*
ORIENT (O)	**Link / overlap with Autonomy Theme**
– *Analytics and Statistical modeling* – *Anomaly and False data detection* – *Knowledge Abstraction*	– *Machine Leaning*
DECIDE (D)	**Link / overlap with Autonomy Theme**
– *Decision Support Mthods* – *Augmented/Virtual Reality* – *Modelling & Simulation for Decision Support* – *Predictive Analytics*	– *Training, Trust and V&V* – *Human-Machine Interfacing*
ACT (A)	**Link / overlap with Autonomy Theme**
– *Moral Decisions*	– *Autonomous Decision Making* – *Human-Machine Teaming* – *Modeling and Simulation of Autonomy* – *Legal, Ethics, Policy*

LA PERSPECTIVA DEL BUCLE OODA PARA ESTRUCTURAR LOS TEMAS Y ACTIVIDADES DENTRO DE LOS TEMAS [39].

El reporte técnico “NATO Guide to Data Collection and Management for Analysis Support to Operations” publicado en 2020 [40], presenta una revisión de los desafíos asociados con el recolección y gestión de datos militares (DC&M), un proceso genérico de DC&M para respaldar la planificación de DC&M interfuncional en un cuartel general militar y un resumen de las funciones y herramientas especializadas requeridas para respaldar el DC&M militar. En el informe se plantea que los algoritmos avanzados, como los desarrollados por Google o Amazon, hacen que Big Data esté disponible para todos en apoyo de su toma de decisiones diaria, pero los enfoques actuales para la recopilación y gestión de datos militares son inadecuados para proporcionar los conjuntos de datos confiables necesarios para lograrlo. Los datos en los sistemas militares a menudo se recopilan sobre la marcha sin tener en cuenta su reutilización y los analistas se ven obligados a dedicar una cantidad desproporcionada de tiempo a buscar y preparar datos para el análisis.

En el 2021, se publicó “NATO Decision-Making in the Age of Big Data and Artificial Intelligence” [41], que es el resultado de la séptima conferencia académica “NATO Decision-making: promises and perils of the Big Data age”, organizada por el Comando Aliado de Transformación de la OTAN (ACT), la Universidad de Bolonia y el Istituto Affari Internazionali (IAI) de Roma. Mediante la publicación se exploran tres aspectos amplios e interconectados con miras a la evolución futura de la OTAN. Primeramente, los retos organizativos que plantea el Big Data para la Alianza, que debe adaptarse para aprovechar al máximo sus potencialidades, pero también mitigar los riesgos que conlleva. En segundo lugar, las amenazas híbridas a la toma de decisiones de los Aliados a través del ciberespacio, por medio de las cuales, por ejemplo, la inteligencia artificial (IA) y Big Data permiten una guerra de información más efectiva por parte de actores hostiles. Finalmente, la adopción de la IA en el ámbito de la defensa es crucial, desde el equipamiento hasta los procedimientos, y la OTAN puede desempeñar un papel positivo en este sentido también en lo que respecta al diálogo con las empresas privadas.

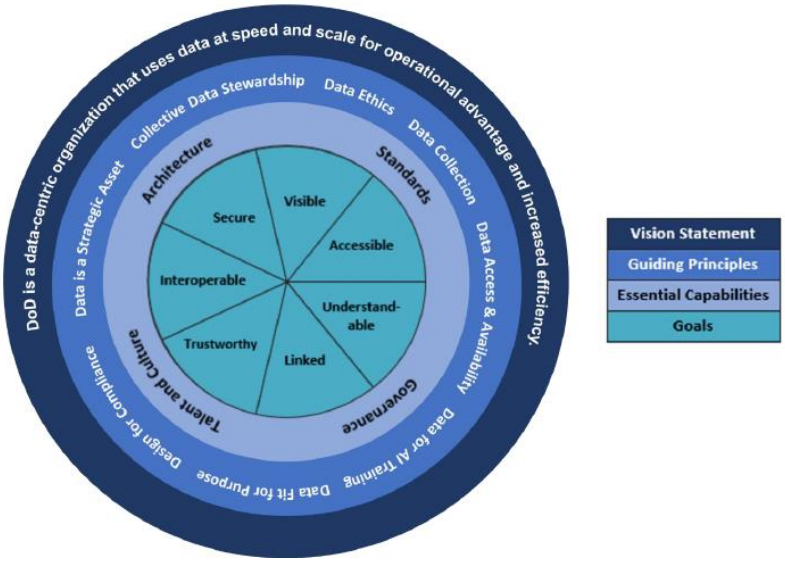
En la conferencia “Singapore Defence Technology Summit” llevada a cabo en octubre de 2021, el ministro de defensa de Singapur Ng Eng Hen dijo respecto a la inteligencia artificial en el entorno militar que tiene “gran impacto potencial de destrucción y disrupción en nuestro tiempo”, por lo que llamó a las tecnologías autónomas y la inteligencia artificial un "gran área para discutir", ya que los ejércitos buscan explotar el potencial de la inteligencia artificial para lidiar con grandes y complejas cantidades de datos mientras toman mejores y más rápidas decisiones. [42]

En el mismo mes de octubre, la OTAN propuso adoptar una estrategia de inteligencia artificial de 18 puntos, en la cual los principios del uso responsable de la inteligencia artificial en defensa serán "el núcleo" de dicha estrategia [43], como se menciona en el primer punto “La inteligencia artificial (IA) está cambiando el entorno global de defensa y seguridad. Ofrece una oportunidad sin precedentes para fortalecer nuestra ventaja tecnológica, pero también aumentará la velocidad de las amenazas que enfrentamos. Esta tecnología fundamental probablemente afectará el espectro completo de actividades realizadas por la Alianza en apoyo de sus tres tareas principales; defensa colectiva, gestión de crisis y seguridad cooperativa.”

2.2. Estados Unidos

Estados Unidos al ser una de las grandes potencias a nivel mundial, fue uno de los primeros en incorporar técnicas de Big Data en el ámbito de la defensa y seguridad, que fueron impulsadas por el Departamento de Defensa conocido por las siglas DoD (Department of Defense), que tiene como misión proporcionar las fuerzas militares necesarias para disuadir la guerra y garantizar la seguridad de la nación.

El DoD publicó en el 2020 , un informe con el nombre DoD Data Strategy [44], en el que reconoce que los datos son un activo estratégico que debe ponerse en funcionamiento para proporcionar una fuerza conjunta letal y eficaz que, combinada con la red de aliados y socios, mantenga la influencia estadounidense y promueva la seguridad compartida y prosperidad. La mejora en la gestión de datos mejorará la capacidad del departamento para luchar y ganar guerras en una era de competencia de grandes potencias, y permitirá a los operadores y a los responsables de la toma de decisiones militares aprovechar los datos para capitalizar las oportunidades estratégicas y tácticas que actualmente no están disponibles. Para ello traza un marco de estrategia en relación con los datos compuesto por visión, principios rectores, capacidades esenciales, metas y objetivos para el DoD.



MARCO DE ESTRATEGIA DE DATOS DEL DOD [44].

Como declaración de visión plantean que "*DoD es una organización centrada en datos que utiliza datos a velocidad y escala para obtener ventajas operativas y una mayor eficiencia*". Mientras que para sus principios rectores especifican los siguientes aspectos:

- Datos como un activo estratégico: los datos del DoD son un bien de gran interés y deben aprovecharse de una manera que brinde una ventaja militar inmediata y duradera.
- Administración de datos colectivos: el DoD debe asignar administradores de datos (establecen políticas que gobiernan el acceso, uso, protección, calidad y difusión de los datos.), custodios de datos (responsables de promover el valor de los datos y hacer cumplir las políticas) y un conjunto de gerentes de datos funcionales (implementan las políticas y administran la calidad del día a día) para lograr la responsabilidad durante todo el ciclo de vida de los datos.
- Ética de datos: DoD debe poner la ética a la vanguardia de todos los pensamientos y acciones en lo que respecta a cómo se recopilan, utilizan y almacenan los datos.
- Colección de datos: el desafío sigue siendo el mismo: descubrir y recopilar datos y agregar valor continuamente para informar mejor al tomador de decisiones, por tanto el DoD debe permitir la recopilación electrónica de datos en el punto de creación y mantener el pedigrí de esos datos en todo momento. En el momento en que se crean los datos, se deben etiquetar, almacenar y catalogar, del mismo modo, cuando los datos se combinan o integran, el producto resultante también debe recopilarse, etiquetarse, curarse y protegerse adecuadamente de inmediato.
- Acceso y disponibilidad de datos en toda la empresa: los datos deben estar disponibles para su uso por parte de todas las personas autorizadas y entidades que no son personas a través de los mecanismos adecuados.
- Datos para entrenamiento de inteligencia artificial: conjuntos de datos para entrenamiento de IA y modelos algorítmicos se convertirán cada vez más en los activos digitales más valiosos del DoD y se deberá crear un marco para administrarlos a lo largo del ciclo de vida de los datos que brinda visibilidad protegida y corretaje responsable.
- Datos adecuados para su propósito: Los datos "aptos para el propósito" son datos de calidad que se pueden descubrir y comprender fácilmente dentro del contexto de su uso previsto. El DoD debe considerar cuidadosamente cualquier inquietud ética en la

recopilación, el intercambio, el uso, la integración rápida de datos y la minimización de cualquier fuente de sesgo no intencional.

- Diseño para el cumplimiento: se debe implementar soluciones de TI que brinden la oportunidad de automatizar completamente el ciclo de vida de la administración de la información, proteger adecuadamente los datos y mantener la administración de registros de un extremo a otro.

La Agencia de Sistemas de Información de Defensa, conocido como DISA (Defense Information Systems Agency), es una agencia de apoyo al combate compuesta por militares, civiles federales y contratistas, que proporciona tecnología de la información y soporte de comunicaciones, y es un departamento del DoD. Dentro de su Plan Estratégico 2013-2018 [45], se hace referencia a la necesidad de DISA de proporcionar capacidades de Big Data a sus socios de misión dado que las competencias del Big Data se están volviendo esenciales para la guerra moderna, al igual que tecnologías de computación en la nube. La maduración de dichas tecnologías y la integración de las capacidades resultantes son clave para lograr los distintos objetivos; objetivo estratégico 1 desarrollar el entorno de información conjunta), objetivo estratégico 2 (brindar apoyo conjunto C2 y de liderazgo) y el objetivo estratégico 3 (operar y asegurar la empresa).

En su siguiente Plan Estratégico 2019-2022, tanto en la versión1 [46] como en la versión 2 [47], tiene 3 objetivos principales; operar y defender, adoptar antes de comprar y comprar antes de crear, y habilitar a las personas y reformar. Para ello la agencia plantea diversos objetivos estratégicos como son:

- Modernizar la infraestructura: mejorando la seguridad, la resistencia y la capacidad de las redes del DoD. Uno de los objetivos es estandarizar las configuraciones para un mayor rendimiento y asequibilidad, mientras que otro es consolidar y hacer converger los centros de datos, las redes, las mesas de servicio y los centros de operaciones de redes en un entorno seguro, integrado y mejorado.
- Optimizar para la empresa: optimizar las capacidades y los servicios empresariales para minimizar los costos y la complejidad al tiempo que brinda una experiencia de usuario consistente con alto rendimiento, disponibilidad y confiabilidad. Las soluciones empresariales permitirán que un usuario o dispositivo autorizado acceda a datos y servicios autorizados en cualquier momento y desde cualquier lugar.
- Fortalecer la ciberseguridad: El dominio cibernético actual es un espacio de batalla dinámico, complejo y disputado constantemente bajo el ataque de una variedad de adversarios altamente competentes. Para la defensa de estas amenazas se plantea mejorar la arquitectura defensiva con un enfoque en la defensa contra ataques tanto externos como internos, detectando el movimiento lateral e incorporando por completo capacidades de end point más robustas en una implementación defensiva sincronizada y estandarizada.
- Impulsar la innovación: adoptar tecnologías lideres en la industria pero manteniendo un equilibrio entre la seguridad y el acceso a requisitos del mundo real. Para ello plantea un marco de automatización (automatización de la nube, infraestructura como código, ciberseguridad y procesos de negocio); desarrollo, seguridad, operaciones / desarrollo ágil de software (alto grado de transparencia para reportar el estado de un sistema dado, fusionando datos a través de la inserción de tecnología, estandarización de datos, automatización de procesos y evolución cultural); compromisos de la industria; adquisición innovadora; identidad asegurada; convergencia móvil / escritorio; y gateway universal gateway (consistirá en toda la infraestructura empresarial necesaria para admitir servicios de comunicaciones terrestres, móviles y por satélite, como voz, video y datos, para todos los clientes de DoDIN en todo el mundo).

- Capacitar a las personas: dentro de uno de los aspectos de capacitar a las personas se plantea aprovechar las aplicaciones de productividad para recopilar, analizar y emplear datos de adquisición de talento para ayudar a los gerentes de contratación a tomar la mejor decisión de contratación.
- Reformar la agencia: como el DoD adopta una serie de iniciativas de gestión de datos, DISA busca construir una cultura que valore los datos como un activo estratégico, dado que cuando se recopilan y analizan cuidadosamente, los datos pueden catalizar la innovación e informar la prestación de servicios. DISA intentará establecer una junta de gobierno de datos y una evaluación de madurez en toda la agencia para desarrollar un plan de acción integral consiguiendo como estado final el desarrollo y uso de métricas para medir las aplicaciones, el servicio y el desempeño general de misiones.

El DoD plantea como capacidades esenciales para conseguir sus objetivos los siguientes aspectos:

- Arquitectura: habilitada por la nube empresarial y otras tecnologías, debe permitir la rotación de los datos más rápidamente de lo que los adversarios pueden adaptarse.
- Estándares: DoD emplea una familia de estándares que incluyen no solo enfoques comúnmente reconocidos para la gestión y utilización de activos de datos, sino también métodos probados y exitosos para representar y compartir datos.
- Gobernanza: la gobernanza de datos del DoD proporciona los principios, las políticas, los procesos, los marcos, las herramientas, las métricas y la supervisión necesarias para gestionar los datos de forma eficaz en todos los niveles, desde la creación hasta la eliminación.
- Talento y cultura: la fuerza laboral del DoD (miembros del servicio, civiles y contratistas en cada escalón) estará cada vez más empoderada para trabajar con datos, tomar decisiones basadas en datos, crear políticas basadas en evidencia e implementar procesos efectivos.

Para lograr convertirse en un departamento de defensa centrado en datos, el DoD tiene siete objetivos conocido como VAULTIS (Visible, Accessible, Understandable, Linked, Trustworthy, Interoperable, Secure):

1. Hacer los datos visibles: los consumidores pueden localizar los datos necesarios.
2. Hacer los datos accesibles: los consumidores pueden recuperar los datos.
3. Hace los datos comprensibles: los consumidores pueden reconocer el contenido, el contexto y la aplicabilidad.
4. Hacer los datos vinculables: los consumidores pueden explotar los elementos de los datos a través de relaciones innatas.
5. Hacer los datos confiables: los consumidores pueden confiar en todos los aspectos de los datos para la toma de decisiones.
6. Hacer los datos interoperables: los consumidores tienen una representación / comprensión común de los datos.
7. Hacer los datos seguros: los consumidores saben que los datos están protegidos contra el uso / manipulación no autorizados.

Ya por el año 2012 la Agencia de Proyectos de Investigación Avanzada de Defensa conocida como DARPA (Defense Advanced Research Projects Agency), tenía en marcha diversos programas que hacían uso de las técnicas del Big Data bajo la Iniciativa de Investigación y Desarrollo de Big Data que esperaba reforzar las herramientas y técnicas necesarias para

acceder, organizar y recopilar descubrimientos de grandes volúmenes de datos digitales. Entre los programas de Big Data de DARPA se encuentran [48]:

- Anomaly Detection at Multiple Scales (ADAMS): el programa analiza el problema de la detección y caracterización de anomalías en conjuntos de datos masivos. Las anomalías en los datos están destinadas a indicar la recopilación de información adicional procesable en una amplia variedad de contextos del mundo real. El dominio de aplicación inicial de ADAMS es la detección de amenazas internas, en el que las acciones anómalas de un individuo se detectan en un contexto de actividad rutinaria de la red.
- Cyber-Insider Threat (CINDER): tiene como objetivo desarrollar enfoques novedosos para detectar actividades consistentes con el ciber espionaje en redes informáticas militares. Como un medio para exponer las operaciones ocultas, CINDER aplicará varios modelos de misiones adversarias a la actividad "normal" en las redes internas. El programa también tiene como objetivo aumentar la precisión, la tasa y la velocidad con la que se detectan las amenazas cibernéticas.
- Insight: el programa aborda las deficiencias clave en los sistemas actuales de inteligencia, vigilancia y reconocimiento. La automatización y el razonamiento humano-máquina integrado permiten a los operadores analizar un mayor número de amenazas potenciales antes de situaciones sensibles al tiempo. Insight tiene como objetivo desarrollar un sistema de gestión de recursos para identificar automáticamente las redes de amenazas y las operaciones de guerra irregulares a través del análisis de información de sensores de imágenes y no imágenes además de otras fuentes.
- Machine Reading: persigue realizar aplicaciones de inteligencia artificial mediante el desarrollo de sistemas de aprendizaje que procesan texto natural e insertan la representación semántica resultante en una base de conocimiento en lugar de depender de los costosos y lentos procesos actuales para la representación del conocimiento que requiere de ingenieros expertos y del conocimiento asociado para elaborar la información a mano.
- Mind's Eye: busca desarrollar la capacidad de "inteligencia visual" en las máquinas. Mientras que el estudio tradicional de la visión artificial ha avanzado en el reconocimiento de una amplia gama de objetos y sus propiedades, lo que podría considerarse como sustantivos en la descripción de una escena, Mind's Eye busca agregar los fundamentos perceptivos y cognitivos necesarios para reconocer y razonar sobre los verbos en esas escenas. Juntas, estas tecnologías podrían permitir una narrativa visual más completa.
- Mission-oriented Resilient Clouds: aborda los desafíos de seguridad inherentes a la computación en la nube mediante el desarrollo de tecnologías para detectar, diagnosticar y responder a los ataques, construyendo de manera efectiva un "sistema de salud comunitaria" para la nube. El programa también tiene como objetivo desarrollar tecnologías para permitir que las aplicaciones y la infraestructura en la nube continúen funcionando mientras están bajo ataque. La pérdida de hosts individuales y tareas dentro del conjunto de nubes sería admisible siempre que se mantuviera la eficacia general de la misión.
- Programming Computation on Encrypted Data (PROCEED): pretende superar un desafío importante para la seguridad de la información en entornos de computación en la nube mediante el desarrollo de métodos prácticos y lenguajes de programación modernos asociados para el cálculo de datos que permanecen encriptados todo el tiempo que están en uso. Al manipular los datos cifrados sin descifrarlos primero, los adversarios tendrían más dificultades para interceptar los datos.
- Video and Image Retrieval and Analysis Tool (VIRAT): tiene como objetivo desarrollar un sistema para proporcionar a los analistas de imágenes militares la capacidad de explotar la

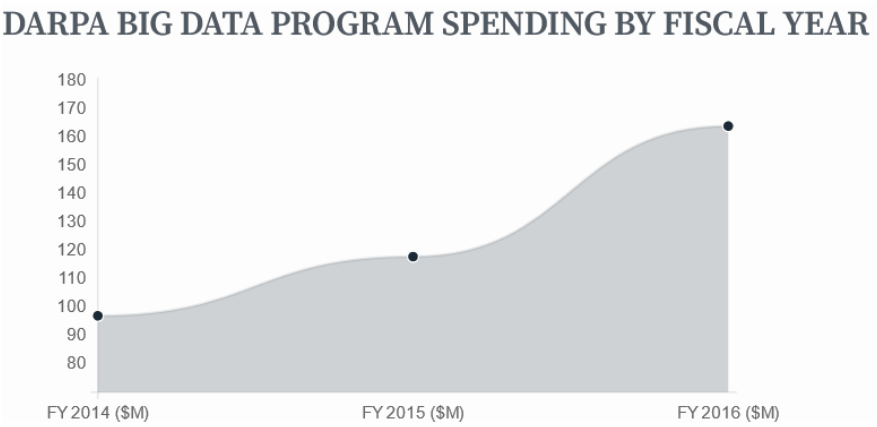
gran cantidad de contenido de video aéreo que se recopila. Si VIRAT triunfa, permitirá a los analistas establecer alertas para actividades y eventos de interés a medida que ocurren. VIRAT también intenta desplegar herramientas que permitan a los analistas recuperar rápidamente, con alta precisión y recuperación, contenido de video de bibliotecas de videos extremadamente grandes.

- XDATA: busca desarrollar técnicas computacionales y herramientas de software para analizar grandes volúmenes de datos semiestructurados y no estructurados. Los desafíos centrales que deben abordarse incluyen algoritmos escalables para procesar datos imperfectos en almacenes de datos distribuidos y herramientas efectivas de interacción persona-computadora que se pueden personalizar rápidamente para facilitar el razonamiento visual para diversas misiones. El programa prevé conjuntos de herramientas de software de código abierto para el desarrollo de software flexible que permiten el procesamiento de grandes volúmenes de datos para su uso en aplicaciones de defensa específicas.

En el 2017, DARPA en colaboración con Intel implementaron el programa Hierarchical Identify Verify & Exploit (HIVE), que tiene el potencial de superar el hardware actual utilizado para manejar Big Data hasta 1000 veces en rendimiento por vatio. HIVE quiere mejorar el análisis de gráficos en relación con Big Data aprovechando el aprendizaje automático y la inteligencia artificial para construir y procesar rápidamente no solo relaciones "uno a uno" o "uno a muchos", sino también árboles más complejos de relaciones indirectas, como el cambio patrones de compra de los usuarios de Amazon. [36]

Información sobre otros programas implementados por DARPA se puede encontrar en la referencia [37].

Considerando los diversos programas llevados a cabo por DARPA, una gran inversión se debe de realizar para poder ejecutarlos. De acuerdo al artículo publicado en 2015 por FCW “DARPA is spending big on Big Data” [49], el dinero invertido por DARPA en Big Data ha sido incrementado notablemente como se puede observar en el siguiente gráfico.

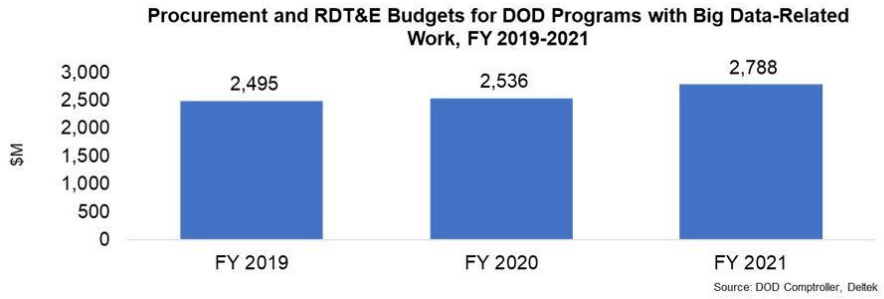


DINERO GASTADO EN LOS PROGRAMAS DE DARPA BIG DATA POR AÑO FISCAL [49]

En septiembre del 2018, DARPA anuncio una inversión de varios años de más de $ 2 mil millones en programas nuevos y existentes denominada campaña "AI Next", dado que DARPA visualiza un futuro en el que las máquinas son más que simples herramientas que ejecutan reglas programadas por humanos o generalizan a partir de conjuntos de datos seleccionados por humanos. DARPA imagina las máquinas como colegas más que como herramientas y teniendo eso presente, la investigación y el desarrollo de DARPA en simbiosis hombre-máquina establece

el objetivo de asociarse con las máquinas. Habilitar los sistemas informáticos de esta manera es de vital importancia porque los sistemas de sensores, información y comunicación generan datos a velocidades superiores a las que los humanos pueden asimilar, comprender y actuar. La incorporación de estas tecnologías en los sistemas militares que colaboran con los combatientes facilitará mejores decisiones en entornos de campo de batalla complejos y en los que el tiempo es crítico; permitir una comprensión compartida de información masiva, incompleta y contradictoria; y empoderar a los sistemas no tripulados para realizar misiones críticas de forma segura y con un alto grado de autonomía. [50]

En "Big Data in DOD's FY 2021 Procurement and RDT&E Budget Programs" [51], mencionan que la solicitud de presupuesto del DOD para el año fiscal 2021 para los programas de Adquisiciones y RDT&E con trabajo relacionado con Big Data totaliza $2.8B. En el siguiente grafico se muestra que los presupuestos totales para programas con trabajo relacionado con Big Data aumentarán aproximadamente un 10 % del año fiscal 2020 al año fiscal 2021, un crecimiento que es consistente con las tendencias recientes en el DOD.



PRESUPUESTOS TOTALES PARA PROGRAMAS CON TRABAJO RELACIONADO CON BIG DATA. [51]

Debido a las numerosas incursiones militares de Estados Unidos contra ISIS, los analistas de inteligencia militar y civil se encontraban abrumados por el gran volumen de datos de videovigilancia registrados, pues tenían que dedicar bastante tiempo a tareas administrativas, como ingresar datos manualmente en hojas de cálculo cada vez que encontraban algo de interés, en lugar de emplear tiempo analizando datos [52], por lo que Estado Unidos puso en marcha en el año 2017 el controvertido proyecto Maven, formalmente conocido en inglés como Algorithmic Warfare Cross-Functional Team (AWCFT). Dicho proyecto fue establecido con el propósito de acelerar la integración del DOD de Big Data y aprendizaje automático. El enfoque de Maven es aplicar algoritmos de visión por computación para etiquetar objetos identificados en imágenes o videos capturados por aviones de vigilancia o satélites de reconocimiento. El programa recibió atención nacional después de que Google Inc., una de las varias empresas de tecnología que participan en el programa, se retirara públicamente en medio del alboroto de los empleados sobre el "uso de armas" de la inteligencia artificial [53]. Maven hoy en día sigue en marcha, pues de acuerdo con el DoD "mejora el desempeño del equipo humano-máquina al fusionar inteligencia y operaciones a través de AI / ML y tecnología de realidad aumentada. Project Maven busca reducir el tiempo requerido para la toma de decisiones a una fracción del tiempo necesario sin AI / ML" [54].

2.3. China

China, ya por el año 2017 intentaba convertirse en una potencia global en la analítica de datos, pues durante el XIX Congreso del Partido en octubre de 2017, el presidente chino, Xi Jinping, dijo que China necesitaba "promover la integración más profunda de Internet, Big Data e inteligencia artificial con la economía real" [26]. Las fuerzas de seguridad pública de China han sido probablemente las más entusiastas en adoptar el análisis de Big Data, debido a la ausencia de restricciones legales al uso de datos personales por parte del gobierno para la seguridad pública, pudiendo realizar referencias cruzadas rápidamente de antecedentes penales con prácticamente cualquier otro dato considerado relevante para capturar a presuntos delincuentes. Además de apoyar directamente el estricto seguimiento y control de los ciudadanos chinos.

En el mencionado XIX Congreso del Partido, el presidente Xi Jinping señaló su intención de que el EPL (Ejército Popular de Liberación) se transforme completamente en "fuerzas de clase mundial" para 2050., por lo que, para cumplir ese objetivo a largo plazo, China considera que el análisis de Big Data es un recurso nacional vital, ya que el dominio de ello posicionará mejor a China para ganar futuros conflictos militares entre grandes potencias. Debido a eso definen *Big Data de defensa nacional* como los datos colectivos generados por las actividades militares, como la defensa de la soberanía nacional, la unidad, la integridad y seguridad, y recursos de datos generados por actividades políticas, económicas, científicas, diplomáticas, educativas y de otro tipo relacionadas con cuestiones militares [26].

Asimismo, China ha creado una agencia de tecnología militar avanzada similar a DARPA, conocida como Scientific Research Steering Committee (SRSC) para llevar a cabo investigaciones de vanguardia, y el desarrollo de la ingeniería para el campo de las armas y productos de uso civil entre otros aspectos [55].

Con el fin de aumentar la capacidad de defensa del país mediante el uso generalizado de la IA, investigadores chinos han desarrollado un submarino con IA [56]. Dicho submarino sería capaz de tomar decisiones sobre el cambio de rumbo o la profundidad para eludir los radares enemigos, determinar si tiene al frente a un buque civil o militar, y seleccionar la ruta óptima.

China lleva a cabo diversos programas de vigilancia como son los siguientes [57], [58]:

- The Golden Shield Project: El proyecto incorpora tecnologías que ahora son fundamentales para la vigilancia en China, como la censura en Internet y el reconocimiento facial y de voz. Inicialmente se implementó en dos fases principales: primero a través de bases de datos de población, sistemas de seguimiento de identidad y herramientas de vigilancia en Internet, luego a través de sistemas de cámaras de vigilancia.
- Safe Cities and Skynet: son dos programas similares que funcionan en conjunto y que con frecuencia se consideran sinónimos dentro de China. En 2003, se implementa Safe Cities que brinda alertas de desastres, gestión urbana y del tráfico y mantenimiento de la seguridad pública a través de tres sistemas entrelazados que cubren la defensa aérea técnica, física y civil. En cambio, Skynet fue lanzado en 2005 para "combatir el crimen y prevenir posibles desastres" a través de una red nacional de cámaras de televisión de circuito cerrado que proporcionan cobertura las 24 horas del día, los 7 días de la semana, de los principales distritos, calles, escuelas y áreas comerciales, y vigilancia cronometrada en las calles más pequeñas.

- Sharp Eyes: es uno de una serie de proyectos de vigilancia tecnológica superpuestos e intersectados construidos por el gobierno chino en las últimas dos décadas, con el objetivo de proporcionar una cobertura de vigilancia rural completa y en tiempo real para 2020. Ha tenido éxito principalmente en establecer una "gestión de red" impulsada por la comunidad, que divide las ciudades en unidades administrativas e integra datos para identificar y resolver problemas de gestión social. Pero el programa busca mejorar la integración de datos, ya que los datos de videovigilancia todavía están aislados y no existe un enfoque estándar de extracción de datos.

También lleva a cabo un proyecto conocido como “Predictive Policing” donde hace de la vigilancia predictiva, un enfoque basado en datos para la aplicación de la ley preventiva y anticipada.

Durante la pandemia del COVID-19, China fue uno de los países en los cuales sus cuerpos nacionales, emplearon Big Data para el control de la población y ganar la batalla al virus mediante la recopilación y utilización de los datos de ubicación de cientos de millones de teléfonos y dispositivos móviles con el fin de contener y frenar la propagación de COVID-19 [57], [59].

2.4. Europa

En Europa, existe la Agencia Europea de Defensa conocida como EDA, formada por distintos países de la Unión Europea, dónde se llevan a cabo distintos proyectos. La EDA tiene como objetivo apoyar a los estados miembros y al consejo en su esfuerzo por mejorar las capacidades de defensa europeas en el ámbito de la gestión de crisis y mantener la Política europea de seguridad y defensa tal como está ahora y como se desarrolla en el futuro. La EDA, hace un par de años promovió organizar la investigación y el desarrollo (I + D) de sus Estados miembros en el sector de la inteligencia artificial, desde la creación de un conjunto común de referencias y terminología de IA hasta la identificación de áreas lógicas para su colaboración transfronteriza.

Una primera fase fue desarrollar una comprensión común de la IA relacionada con la defensa pues, como plantea Ignacio Montiel, oficial de proyectos de EDA para investigación en tecnologías de la información, “Todos deben leer la misma 'partitura' para que todos se refieran y utilicen términos y definiciones de IA de la misma manera” [60]. Como el dominio de la IA es muy extenso precisaron elaborar una definición común, una taxonomía tecnológica relevante para la defensa, y un glosario de términos para producir un vocabulario claro para todos dentro de EDA, como una definición clara de IA (“IA es la capacidad proporcionada por algoritmos para seleccionar opciones óptimas o subóptimas de un amplio espacio de posibilidades, con el fin de lograr objetivos específicos mediante la aplicación de diferentes estrategias, incluida la adaptabilidad a las condiciones dinámicas circundantes y el aprendizaje de la propia experiencia, suministrada externamente o de datos autogenerados”), y de machine learning (“significa la capacidad de los algoritmos para "modelar sistemas aprendiendo de los datos que estos sistemas producen". Estos modelos identifican y extraen patrones, adquiriendo así su propio conocimiento e infiriendo de los datos cómo predecir el resultado de nuevas entradas no vistas anteriormente”).

Servicios y productos que empleen IA necesitaran estandarización y certificación si se emplean en el entorno militar, por lo que la EDA propuso a sus miembro crear un repositorio o lago de

datos, de datos operativos militares menos sensibles pero anónimos sobre vehículos, plataforma aéreas, etc. De esa forma es posible dar acceso a los datos a las organizaciones de investigación y tecnología, las pymes y la gran industria, pues con el repositorios de datos, una empresa podría acudir a EDA como tercero de confianza para vincular al innovador con el Estado miembro que controla y posee los datos operativos necesarios, y dar solución a la metodología tradicional como plantea Panagiotis Kikiras, jefe de unidad de EDA para tecnología e innovación, "Supongamos que tiene una empresa trabajando en mantenimiento predictivo para un tipo de helicóptero y ha desarrollado un gran algoritmo. ¿Cómo probarlo? Tradicionalmente, tendrían que acudir al fabricante o al usuario militar, donde puede ser difícil o lento obtener los conjuntos de datos adecuados para las pruebas y la validación." [60]

En el 2013, germino la iniciativa GISMO [61] que es una iniciativa conjunta entre la Agencia Europea de Defensa y el Centro de Satélites de la UE (SatCen). Tiene como objetivo el uso de la información geoespacial para el conocimiento del campo de batalla, el análisis de eventos y la toma de decisiones, todos cuyos elementos deben integrarse tanto como sea posible para la planificación de la misión y la reacción rápida. El trabajo llevado a cabo por GISMO da como resultado el actual GeohuB (Geospatial hub), una aplicación de software que permite a las unidades operativas de una sede compartir y mostrar información geoespacial en un modo fácil de usar que contribuye a realizar análisis de situación.

En septiembre del 2016, la EDA inicio el estudio "Big Data in Defence Modelling and Simulation" (BIDADEMS) con el objetivo de comprender mejor las metodologías y técnicas de Big Data y sus posibles aplicaciones en el dominio de la defensa, en particular para fines de modelado y simulación (M&S). En el dominio de M&S, el Big Data podría ayudar a proporcionar diseños de simulación militar simplificados, generar escenarios y entornos de simulación más realistas, mejorar la explotación de los resultados de la simulación o brindar nuevas oportunidades para el apoyo de M&S a las actividades de prueba y evaluación militares (T&E). El resultado del estudio es una Matriz de Evaluación que mapea las herramientas de Big Data a las áreas de M&S para facilitar futuros proyectos colaborativos de defensa en el desarrollo de la próxima generación de sistemas de simulación militar de una manera que optimice el uso de herramientas y procesos de Big Data [62]. Esas áreas son:

- Preparación del programa: desarrollo de conceptos operativos futuros y actividades de gestión de capacidades.
- Análisis operativo: técnicas analíticas utilizadas para informar la toma de decisiones de defensa.
- Desarrollo de sistemas: adquisición, desarrollo y despliegue de capacidades militares nuevas o mejoradas.
- Entrenamiento: desarrollo de doctrina en servicio, análisis para identificar brechas de entrenamiento, problemas de retención, métodos de entrenamiento alternativos y entrenamiento militar en vivo, virtual o constructivo.
- Apoyo a Operaciones: apoyo a la toma de decisiones para la planificación y realización de actividades operativas.

El proyecto BIDADEMS ha motivado al Grupo de Tecnología de Capacidad de 'Simulación' (CapTech) de la EDA a iniciar un nuevo estudio, MODSIMMET, que analizará cómo abordar escenarios muy complejos como la guerra híbrida con diferentes metodologías como la agricultura de datos y los juegos de guerra apoyados en Big Data y Artificial. Inteligencia.[63]

En el año 2019, la EDA lanzo el proyecto CLAUDIA (Cloud Intelligence for Decision Making Support and Analysis) [61]. La primera fase del proyecto se centró alrededor de un prototipo "SWAN" cuyo objetivo era demonstrar como la inteligencia artificial podría explotar la nube analizando datos de código abierto y generar inteligencia sobre las señales tempranas con respecto al posible actividad de guerra híbrida. Entre las tareas que SWAN demostró en febrero de 2021 fue la recopilación de datos de fuentes de noticias para identificar las noticias falsas. Según Ignacio Montiel-Sánchez, ex oficial de proyectos de la EDA para CLAUDIA y la investigación en tecnologías de la información, "Lo que esto mostró era que los datos de diversas fuentes ser procesados y analizados, utilizando el procesamiento del lenguaje natural para establecer los umbrales y advertencias como indicadores de posibles campañas híbridas de desinformación". En un principio, la base de datos de CLAUDIA no emplea datos militares dado que, se requeriría estructurar SWAN de manera que pudiera compartir esa información pues hubiese requerido de un entorno completamente clasificado, pero eventualmente la inteligencia militar podría incorporarse a la base de datos.

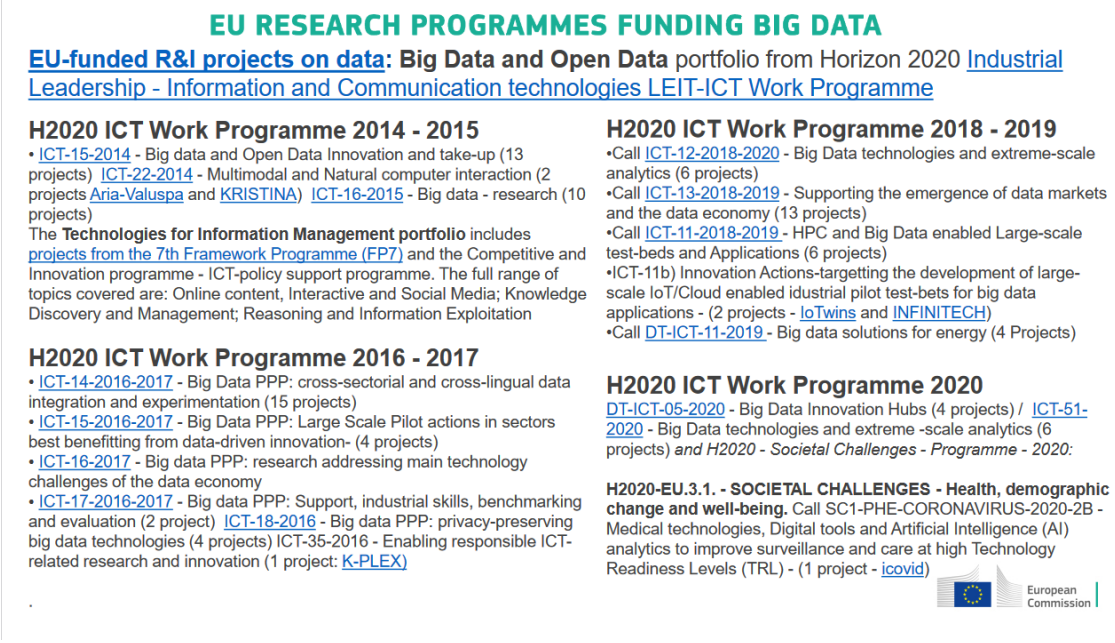
En ese mismo año, la EDA también promovió el proyecto CySAP-RRP [64] liderado por España en conjunto con Alemania e Italia. El proyecto tenía como objetivo establecer una capacidad operativa completa de conocimiento de la situación cibernética (CySA) para las fuerzas de defensa de la UE, además de la investigación esencial para ayudar a los tomadores de decisiones militares en el ciberespacio y sentar las bases de un sistema C2 para operaciones cibernéticas.

También en 2019, la EDA llevó a cabo en conjunto con la empresa española GMV e IPTC-UPM [65], [66] el proyecto ABIDE: Artificial Intelligence and Big Data for Decision Making in C4ISR, cuyos objetivos son la mejora del rendimiento de los sistemas C4ISR (Sistemas de Mando, Control, Comunicaciones, Computación, Inteligencia, Vigilancia y Reconocimiento) a nivel de la UE mediante la aplicación de técnicas de Big Data e inteligencia artificial al apoyo a la toma de decisiones de Defensa, la mejora de la calidad de la información y la identificación de formas de proporcionar una conciencia situacional compartida. El estudio se centró en los siguientes beneficios potenciales de la integración perfecta de fuentes de inteligencia: SIGINT (Inteligencia de señales), HUMINT (Inteligencia Humana) e IMINT (Inteligencia de imágenes), analizando el nivel de IA necesario para ayudar a los operadores a interactuar permanentemente con el sistema y reduciendo la carga de trabajo humano en el campo de la gestión de la información y restaurando el valor añadido humano siempre que sea necesario para la interpretación de la información.

La Comisión Europea financió con un presupuesto de cerca de 80 000 millones de euros el programa de investigación e innovación Horizonte 2020, durante los años 2014 a 2020 [67]. En dicho programa se llevaron diversos programas de investigación empleando el Big Data como SELMA (Stream Learning for Multilingual Knowledge Transfer), MARVEL (Multimodal Extreme Scale Data Analytics for Smart Cities Environments), MORE (Management of Real-time Energy Data), EVEREST (dEsign enVironmEnt foR Extreme-Scale big data analytics on heterogeneous platforms) o DAPHNE (Integrated Data Analysis Pipelines for Large-Scale Data Management, HPC, and Machine Learning) [68]. Cabe destacar que también se llevaron proyectos centrados en la gestión de fronteras como [69]:

- ITFLOWS (IT Tools and Methods for Managing Migration Flows): proporcionar predicciones precisas y soluciones de gestión adecuadas de los flujos migratorios en la Unión Europea en las fases de recepción, reubicación, asentamiento e integración de la migración, de acuerdo con una amplia gama de factores humanos y utilizando múltiples fuentes de información.

- MIRROR (Migration-Related Risks Caused by Misconceptions of Opportunities and Requirement): generar una mejor comprensión de cómo las personas (desde fuera de la UE) perciben a Europa como un destino para la migración.
- METICOS: tiene como objetivo introducir el análisis de Big Data en los sistemas de información de control fronterizo, con el fin de proporcionar un cambio radical hacia una gestión inteligente de fronteras más moderna y eficiente y hacia la obtención de la aceptación social y política de las tecnologías modernas de control de las fronteras de la UE, como las "soluciones sin puerta".
- PROFILE: proyecto de gestión de riesgos aduaneros para ayudar a las aduanas a enfocarse y controlar los movimientos transfronterizos de alto riesgo con mayor precisión y eficacia, actualizar las capacidades de análisis de datos de las aduanas, y redefinir la forma en que las aduanas utilizan la información para identificar riesgos.



PROYECTOS EN HORIZONTE 2020 QUE EMPLEAN BIG DATA [69]

En mayo de 2021, dos compañías francesas, Thales y Atos anuncian la creación de Athea, "una plataforma soberana de Big Data e inteligencia artificial para los actores del sector público y privado en los mercados de defensa, inteligencia y seguridad estatal interna" [70]. Thales por el año 2018 ya estaba tomando iniciativas de Big Data, pues de acuerdo con el Almirante Stephane Verwaerde, Asesor de Defensa (Marina) de Thales, "Hoy estamos aplicando las tecnologías disruptivas de la revolución digital (Inteligencia Artificial, Big Data, Conectividad y Ciberseguridad) para darles a nuestros clientes la ventaja sobre su enemigo en mar abierto, sin importar la situación que enfrenten y sin importar qué apoyo puedan necesitar por nuestra parte" [71].

En el reporte publicado por Market Research Future en febrero de 2021 bajo el título "Global Big Data Analytics in the Aerospace & Defense Market Research Report: Information by Solution, Technology, Application, Deployment Type, and Region (North America, Europe, Asia-Pacific, Latin America, and Rest of the World) - Forecast till 2027" [72], se prevé que la analítica de Big Data en el mercado aeroespacial y de defensa crezca a una tasa compuesta anual del 4,6% durante el período de pronóstico (2019 a 2024). En el reporte, según la aplicación, el análisis de Big Data en el mercado aeroespacial y de defensa se ha dividido en Defensa, aeroespacial

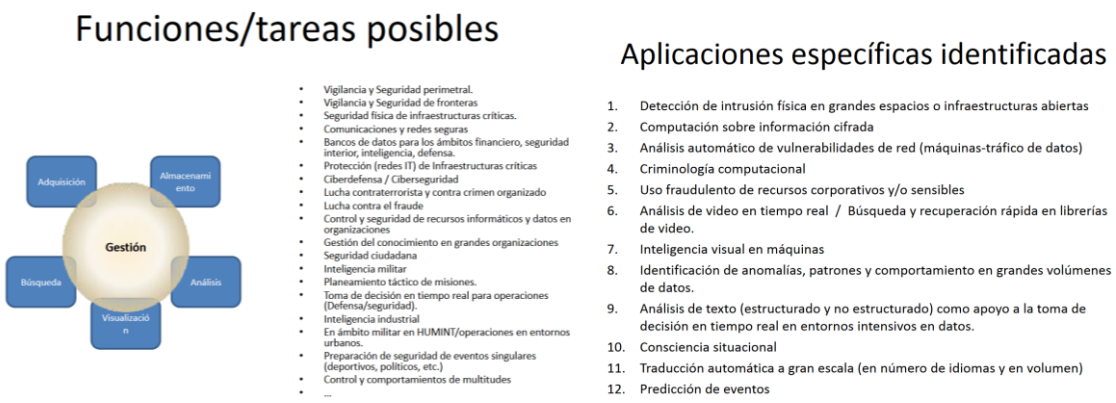
comercial y espacial. Organizaciones de todo el mundo, como son The Boeing Company, la Fuerza Aérea de los EE. UU., y Southwest Airlines, están extrayendo conocimientos de los datos para construir un futuro mejor. Adicionalmente, una gran cantidad de sensores y complejos sistemas digitalizados se utilizan en la última generación de aviones para recopilar exponencialmente más datos, y cada vuelo genera más de 30 veces la cantidad de datos que la generación anterior de aviones de gran tamaño. Se espera que para el 2026, la era de la información anual llegue a los 98 mil millones de gigabytes.

El Independiente organizó por cuarto año consecutivo en noviembre de 2021 el Congreso Internacional de Inteligencia Artificial en Alicante. Dicho congreso, tiene como título 'La Era de la Inteligencia Artificial: Un nuevo orden Mundial, desde el liderazgo tecnológico global de Estados Unidos a la transformación brutal de China ¿dónde queda Europa?' [73], que ha contado con invitados como Kai-Fu Lee, actual presidente de Sinovations Ventures, expresidente de Google China o David Carmona, director general de Inteligencia Artificial e Innovación en Microsoft Corporation. Este último destaca que "estamos en un momento muy interesante de la IA y es una ocasión para Europa liderar esa transformación porque la IA está pasando de ser usada en algunos escenarios y en algunas empresas a tener que ser usada en cualquier sector, en todas las hipótesis, en todas las compañías", pero para ello se necesita de más capital privado como hace EEUU. Carmona también menciona el tema de la protección de datos de los habitantes europeos a diferencia otras regiones como China o EEUU, lo cual provoca que Europa se quede más rezagada en la investigación y desarrollo de la tecnología, pero que una correcta regulación puede ayudar bastante y ser una oportunidad para diferenciarse del resto de regiones [74].

Obviamente la invasión de Ucrania por parte de Rusia con fecha de inicio el 24 de febrero 2022, está siendo un escenario privilegiado para el desarrollo de las técnicas y tecnologías objeto de este informe. En el *Anexo: Uso del Big Data en la invasión de Ucrania*, se ha realizado una descripción del uso de las mismas en dicha invasión.

2.5. España

En España, el día 30 de mayo del 2013, se llevó a cabo el seminario "Aplicaciones de Big Data en entornos de Defensa y Seguridad" [69], promovido por CESEDEN/IEEE en conjunto con la Fundación Círculo e ISDEFE. El seminario tenía como objetico la difusión de los resultados del Grupo de Trabajo de Big Data y sus aplicaciones en los entornos de Defensa y Seguridad. En dicho seminario se llevaron a cabo varias presentaciones, en las que se presentaba el paradigma del Big Data, la utilización de distintos tipos de fuentes de datos como son los sensores, las redes sociales o las imágenes, y las posibles aplicaciones del Big Data como se puede observar a continuación.



TRANSPARENCIAS OBTENIDAS DE LA PRESENTACIÓN "APLICACIONES DE BIG DATA EN DEFENSA Y SEGURIDAD" [75]

También, en una de las presentaciones, se planteó el uso del Big Data en las administraciones públicas [76]. El problema de la administración como fuente de Big Data es que coexisten datos confidenciales (datos sensibles de la administración y de los ciudadanos) y datos no confidenciales. De estos últimos existen grandes cantidades que puede ser explotados por terceros para el desarrollo económico del país, además de obtener los siguientes beneficios: mejoras en la eficiencia y eficacia, ayuda a la toma de decisiones, reducción del fraude y reducción del gasto público.

En Galicia, en el año 2017, se publicó un informe bajo el título "Oportunidades Industria 4.0 en Galicia" [77], en el cual se hacía planteaba el estado del arte del Big Data además de realizar un estudio a nivel tecnológico de diez sectores industriales considerados cómo estratégicos en Galicia; Aeronáutica, Agroalimentación y Bio, Automoción, Energías Renovables, Madera/Forestal, Metalmecánico, Naval, Piedra Natural, Textil/Moda, y TIC. En el informe, para el sector de automoción plantean como algunas aplicaciones del Big Data el mantenimiento predictivo de maquinaria, planificación y asignación óptima de recursos de producción, predicción de fallos en cadenas de producción, la seguridad en la planta o el análisis de riesgos y predicción de fallos. Mientras que para el sector naval, proponen optimización de fabricación de bloques en buques individuales o series de buques, sistemas autónomos o semiasistidos de fabricación y análisis modal de fallos en buques. En el sector aeronáutico las aplicaciones del Big Data planteadas son similares al de automoción, pero también se añade reducción del tiempo de pruebas de una aeronave y eficiencia del mantenimiento de las aeronaves mediante la integración de fuentes de datos dispares, como registros electrónicos de mantenimiento, datos paramétricos de aeronaves y datos operacionales creando así un conjunto de Big Data para análisis y optimización de toma de decisiones.

También en el 2017, hubo el Congreso Big Data Valencia organizado por Las Provincias, que fue un encuentro entre sectores clave y empresas líderes en la explotación de datos a gran escala. Entre los asistentes, se encontraba la entonces ministra de Defensa María Dolores de Cospedal, que mencionó "necesitamos sociedades más libres, no más amenazadas y hay que tener presente la capacidad actual para manipular y dirigir opiniones", y que para defenderse de las amenazas múltiples se "requieren también respuestas multilaterales" para que el entorno de la tecnología y el Big Data sean un foco de grandes oportunidades donde se sepa atajar las amenazas". Debido a que la cantidad de datos es ingente, su gestión no es sencilla, y se requiere de un tiempo limitado para su análisis e interpretación, se plantea si dichos datos pueden ser empleados para la defensa pues, las amenazas se encuentran camufladas ya que el nuevo campo

de batalla es complejo virtual e integral, pero Cospedal termina especificando “El rápido avance tecnológico hace desarrollar sistemas que nos permitan analizarlos e integrarlos para tomar las mejores decisiones. Convertir el Big Data en datos comprensibles y útiles es un desafío y adelantarnos a las amenazas un reto para defensa. Tenemos que estar preparados con todos los recursos que sean precisos” [78]. Además, Cospedal aseguró que “la facilidad con la que la información privada, o que creemos privada, se multiplica y almacena, ha de venir acompañada de una protección global y de una seguridad integral”, como se puede observar en el tweet publicado por la cuenta oficial del Ministerio de Defensa.

TWEET DEL MINISTERIO DE DEFENSA EN RELACIÓN CON EL USO DE DATOS Y SU SEGURIDAD [79]

En España, se han llevado a cabo distintos congresos, especialmente en Barcelona, sobre el tema del Big Data, pero lo que tiende a pasar es que no se consigue localizar mucha información sobre lo divulgado en ellos. En la séptima edición, del AI & Big Data Congress, llevada a cabo en octubre 2020, se resalta la capacidad de predicción que brinda la Inteligencia Artificial pues consigue establecer una ventaja competitiva para las empresas. Adicionalmente, el director del congreso que es a su vez director del Centre of Innovation for Data tech and Artificial Intelligence (Cidai) y la Unidad de Big Data & Data Science de Eurecat, Marc Torrent, enumeró los ámbitos de actividad donde se prevé una transferencia de la inteligencia artificial como son los siguientes; sector agrario, energía y sostenibilidad, lenguaje y habla, movilidad, salud y bienestar, educación, industrias culturales y basadas en la experiencia e industria 4.0. También, explicó los proyectos en los que está trabajando el Cidai entré los que se destacaron la aplicación del Deep Learning para diagnosticar tumores pulmonares, predecir la accidentabilidad para mejorar el control del tráfico, mejorar el reciclaje selectivo y aplicar Machine Learning en data sets encriptados manteniendo la privacidad de la información [80].

Durante tres días del mes marzo del año 2021, se realizaron varios webinar que formaban parte del Congreso Regulación y explotación del Big Data para los servicios públicos [81], en las que hubo más de 10 presentaciones relacionadas con mejores regulaciones y estrategias para la explotación pública de datos, la explotación de datos para la inspección y control de la ejecución de políticas públicas junto con inteligencia artificial, políticas urbanas y sostenibilidad y la explotación de datos para la inclusión, educación, salud y vivienda. Las distintas presentaciones se pueden encontrar en la referencia [82], de las cuales cabe destacar “Datos dinámicos y agregados para mejorar la visión de las administraciones públicas en materia de turismo y

gestión urbana". En dicha presentación se explica en clave general como el uso de distinto tipo de datos más concreto los datos generados por las tarjetas bancarias, mediante disociación de la identidad del usuario de tarjeta puede ser usado para crear información estadística y realizar diversos estudios como puede ser los patrones de los consumidores y las zonas dónde compran, o la monitorización del turismo doméstico o internacional. Aunque no se especifica en la presentación el uso de los datos de las tarjetas bancarias para defensa o seguridad, se podría considerar que de igual forma que se puede monitorizar el turismo domestico se podría monitorizar los tránsitos migratorios o la compra de ciertos productos que puedan ser usados como armas.

De acuerdo a un artículo web de Confilegal [83], en el que se valora el informe White Paper 'Big Data, Machine Learning y Business Intelligence', llevado a cabo por la consultora Nuvix Consulting, el Big Data se estanca en España dado que solamente un 6% de las empresas españolas hicieron uso de herramientas de Big Data, pese a su potencial. Las empresas que emplean técnicas de Big Data gestionan una inmensa cantidad de información valiosa procedente de clientes, proveedores y del contexto de su sector, convirtiendo los datos en conocimiento lucrativo para la compañía.

En otro artículo web, está vez publicado en infodefensa.com [84], se dice que el Centro Nacional de Inteligencia (CNI), que depende del Ministerio de Defensa, pretende "obtener nuevas capacidades de análisis de la información e incorporar tecnologías disruptivas como el Big Data o la inteligencia artificial a sus procedimientos de trabajo", así mejorando la eficiencia y al eficacia de sus tareas al implantar tecnología de última generación. La incorporación de la transformación digital aparece mencionada en el 'Proyectos tractores de Digitalización de la Administración General del Estado', pues se desea alcanzar una administración "guiada por los datos" y el despliegue de servicios digitales para ciudadanos, empresas y empleados públicos que sean fiables, eficientes y seguros.

Adicionalmente, en el "Plan de Acción del Ministerio de Defensa para la Transformación Digital" [85], se plantea la creación de Centro de Innovación para promover el uso de nuevas metodologías y tecnologías en el ámbito CIS/TIC. Dentro las nuevas metodologías y tecnologías destacan la Inteligencia Artificial que a su ver debe ser uno de los principales catalizadores de la Transformación Digital y de la optimización de los recursos. Dentro de las áreas más notorias de la IA, que debe analizar el centro, se encuentran: Big Data y análisis de datos, representación del conocimiento, aprendizaje y razonamiento automático, lógicas y ontologías, tratamiento de la incertidumbre, planificación y deducción automática, cooperación hombre-máquina, diseño de sistemas y asistentes cognitivos, modelado basado en agentes inteligentes, optimización heurística, procesamiento de flujo de datos, robótica, sistemas de recomendación, sistemas inteligentes de predicción, de teledetección y de tutorización, sistemas multiagente, toma de decisiones, procesamiento y generación del lenguaje natural, procesamiento y aprendizaje de estructuras en imágenes, visión por computador, etc. También en el documento del plan de acción se plantea la creación de una plataforma de Análisis Masivo de Datos e Información para analizar y explotar la información de manera más eficaz utilizando diversas capacidades como son Business Intelligence, Business Analytics, Big Data, Análisis Predictivo o búsquedas y análisis semánticos.

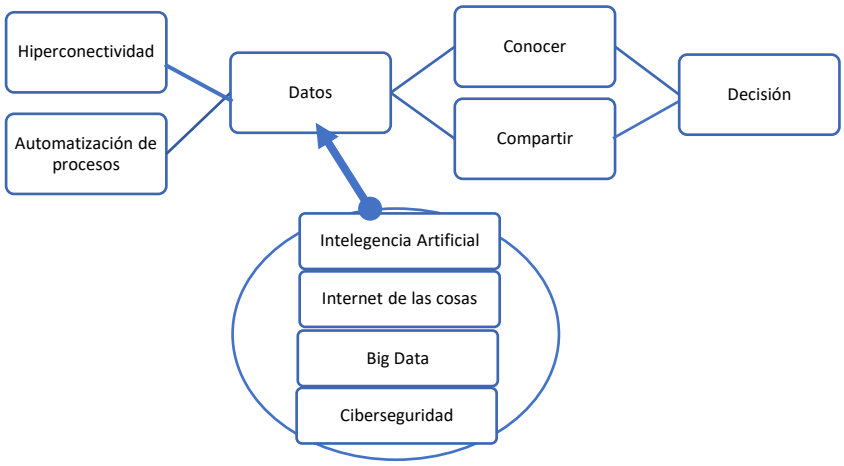
En el informe del Instituto Español de Estudios Estratégicos publicado en 2015 bajo el título "Despega la transformación digital del Ministerio de Defensa" [86], el autor plantea que la transformación digital para el Ministerio de Defensa deberá girar alrededor de una cuidadosa transición entre lo viejo y lo nuevo, el equilibrio en la gestión de riesgos, la creación de valor y

la sostenibilidad a largo plazo. Para ello, la información se ha convertido en el activo clave de cualquier tipo de organización profesional y, razonablemente, las tecnologías de la información han conseguido un valor valioso dentro de ellas. Dichas tecnologías están en constante cambio debido a la constante irrupción de nuevas tecnologías: Cloud Computing, movilidad, aplicaciones móviles, Big Data, Software como Servicio, Infraestructuras como Servicio, Internet de las Cosas, metodologías ágiles de desarrollo, etc.. Respecto al Big Data se dice que sus capacidades se han convertido en esenciales para la guerra moderna pues permite el despliegue de procesamiento de los datos, especialmente cuando los datos son demasiado grandes para pasar a través de redes existentes y emergentes, y faculta el análisis de las tendencias y la identificación de anomalías. Adicionalmente, en las transiciones desde una sociedad industrial o desde una sociedad de la información hacia una edad social, se demanda que las tecnologías de análisis de datos puedan interactuar con las tecnologías sociales, teniendo en cuenta que, con el internet de las cosas se intenta alcanzar una interconexión de distintos dispositivos o sensores que suponen una nueva fuente de datos integrados con las tecnologías Big Data en procesos como logística, seguridad de instalaciones, salud del combatiente, controles ambientales, etc.

Actualmente el MINISDEF está apostando por la aplicación de la IA a problemas de Defensa y de logística, mediante el empleo de los últimos avances en Big Data y aprendizaje automático con los proyectos [69]:

- SOPRENE (2018-2020) - MAPRE (2021-2023): Utilización de redes neuronales como método para mantenimiento basado en la condición en los buques de la Armada.
- MPC16 (2021): Mantenimiento predictivo de aviónica C16.
- SILPRE (2022): Mantenimiento predictivo plataformas terrestres.
- Proyecto MANPREDIC: Desarrollo de un demostrador TRL 6-7.
- DAQ Project: Instalación de dispositivos de datos (DAQ), comerciales, programables en vehículos tácticos blindados con arquitectura abierta (GVA). Integración con BMS y radio táctica. Descarga de datos, carga de modelos de fallo.
- Proyecto JALTEST GRP: Despliegue de la arquitectura GRP en el entorno del Ministerio de Defensa, llevando a cabo la gestión y almacenamiento completo de los datos GRP, aumentando el nivel de seguridad y confidencialidad de los datos.
- Análisis Peticiones Abastecimiento: Análisis y resolución de peticiones de abastecimiento que han sido retenidas en los Centros de Control.
- Auditorías de Almacén: Aumentar la fiabilidad del inventario de los almacenes del ET.

En el artículo “Evolución del Centro de Supervisión y Análisis de Datos de la Armada (CESADAR)” [87], de la Revista general de marina Vol. 275, MES 2 (Agosto-Septiembre) 2018, se plantea que con la cuarta revolución industrial, también conocida como Industria 4.0, los sistemas van a generar y emplear grandes flujos regulares de información compartidos a gran velocidad, permitiendo la toma de decisiones en emplazamientos distintos al de la fuente de la información. Para ello, los autores identifican como unidad fundamental, *el dato*, que sería la unidad de valor a proteger. En un sistema hiperconectado y automatizado, la producción de datos sería el primer eslabón de la cadena de valor, del los cuales se han de obtener conocimiento.



ENTORNO DE LA INDUSTRIA 4.0 [87]

La Armada, inicia la transformación digital con un gran valor de partida que son los datos de comportamiento de equipos y sistemas de plataforma naval desde 2010 en el Centro de Supervisión y Análisis de Datos de la Armada (CESADAR). CESADAR se encuentra ubicado en el Arsenal de Cartagena y fue creado con el fin de proporcionar un apoyo a las decisiones de mantenimiento de los equipos y sistemas de plataforma de los buques de la Armada, en concreto evitar averías catastróficas y permitir mayor eficiencia en el mantenimiento, y proporcionar a la Flota el mayor número posible de días de mar de calidad, entendiendo el término calidad como operatividad de equipos y sistemas. En la actualidad CESADAR consiste primariamente en la recolección de datos provenientes del Sistema Integrado de Control de Plataforma (SICP) y del Sistema de Mantenimiento Basado en la Condición (SMBC). Los datos SICP son una copia de la base de datos generada a bordo por los equipos de plataforma. En cambio, los datos SMBC son el conjunto de la información generada por el sistema de auscultación de vibraciones de motores conectados y no conectados automáticamente, los de comportamiento de motores alternativos, los de análisis de aceite y combustible, así como las termografías. Los datos de sensores conectados son enviados diariamente desde los buques a CESADAR central por satélite, si se encuentran navegando en las horas valle de utilización de la red. Cada buque envía conjuntos de datos diferentes debido a los sistemas conectados y a la tipología de sus datos.

ESQUEMA DEL SISTEMA CESADAR [87]

Los autores, mencionan que en el 2017 se llevó a cabo una auditoria de CESADAR para conseguir un diagnóstico objetivo y una propuesta de desarrollo en el contexto de las nuevas tecnologías y la irrupción de la Industria 4.0. De los resultados de la auditoria, se planteó diseñar un nuevo sistema escalable basado en técnicas de aprendizaje automático utilizando parte de la estructura y los datos recolectados hasta el momento, identificando cuatro fases:

— Fase 0: análisis del ciclo de vida del dato.
— Fase 1: visualización de datos (paneles de control inteligentes/dashboards).
— Fase 2: analítica en tierra, procesos de IA desarrollada/entrenada en CESADAR.
— Fase 3: analítica a bordo, cálculo de disponibilidad de equipos embarcados en tiempo real.

Adicionalmente, para seguir desarrollando el sistema futuro de CESADAR como proyecto se definen los siguientes objetivos:

— Principal objetivo: aprender junto a expertos en aprendizaje automático sobre las soluciones disponibles.
— Basarse en soluciones OpenSource y formar un equipo de desarrollo en CESADAR, dado que la Armada debe tener el control sobre un producto del cual es propietaria para no ser coartados por empresas externas.
— Análisis y evaluación de las distintas técnicas de aprendizaje automático o profundo y demostrar su efectividad utilizando datos ya recopilados.
— Diseñar un demostrador escalable que integre todas las fases del análisis (ingesta de datos, plataforma de análisis, analítica de datos y visualización) y escalable a otros sistemas embarcados. El demostrador deberá poder calcular disponibilidades de equipos en un rango de tiempo dado y probabilidad de ocurrencia a modos de fallo en período estipulado.

En otro artículo de la Revista general de marina Vol. 275, MES 2 bajo el título “La Maqueta Digital” [88], los autores plantean que en el sector naval el mundo físico se materializa en lo que llaman «buque inteligente», capaz de integrar datos de una amplia variedad de fuentes y procesar y transmitir la información obtenida para llevar a cabo las operaciones y el sostenimiento. Mientras, el entorno digital está representado por la nombrada «maqueta digital», que es una versión virtual del buque real, no se limita a un puro modelo 3D con la localización y dimensiones de sus equipos y sistemas, sino también integra toda su información funcional.

La normativa ISO 17599 establece diferentes niveles de maqueta digital en función de su grado de madurez, entre ellos constituye el denominado «gemelo digital» (digital twin). Los autores plantean que existen numerosas aproximaciones en cuanto a su definición, pero consideran que una maqueta digital ha alcanzado el grado de gemelo digital cuando el mundo virtual y el físico se conectan y son capaces de interactuar. Otra definición de gemelo digital se puede encontrar en [89], que es una representación digital de un objeto, proceso o servicio físico, es decir, una réplica virtual para poder ser utilizadas para hacer simulaciones antes de que se creen e implementen cambios en los objetos reales, con el fin de recopilar datos para predecir cómo funcionarán, reduciendo su mantenimiento y los costes asociados, además de prever posibles fallos y adelantarse a ellos.

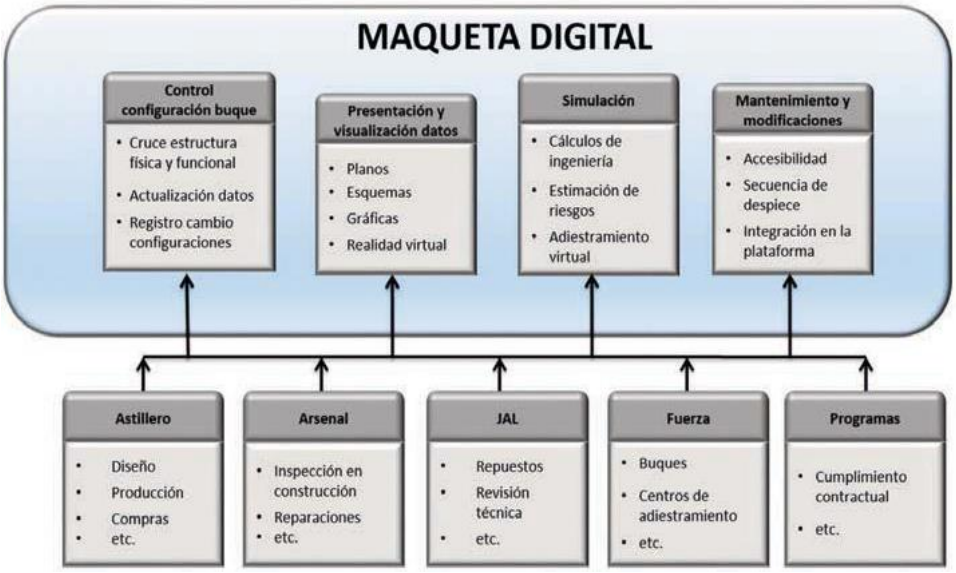
Continuando con el artículo “La Maqueta Digital”, el autor plantea que la maqueta digital debe ser la base sobre la que se fundamente el apoyo al ciclo de vida de los buques del futuro. Así

que el modelo de maqueta desarrollado para la Armada deberá estar orientado principalmente al sostenimiento de las unidades a través de tres funciones logísticas fundamentales:
— Mantenimiento (preventivo, correctivo, predictivo y prognosis): exigirá de la maqueta disponer del desarme y la monitorización del estado de los sistemas y equipos.
de mantenimiento informatizados.
— Aprovisionamiento: requerirá de la maqueta una gestión eficaz junto con la actualización en tiempo útil de existencias, pedidos, cargos, y la predicción de necesidades futuras.
— Ingeniería del ciclo de vida: gestión de obsolescencias rigurosa y un robusto y eficiente control de la configuración.

APLICACIÓN DE LA MAQUETA DIGITAL EN LA ARMADA DEL SIGLO XXI [88]

Debido al intercambio de información entre el buque inteligente y la maqueta se obtendrán tanto datos de interés logístico como aquellos derivados del uso masivo de la sensorización (Internet de las Cosas), que serán procesados y analizados en la nube (cloud computing), la cual deberá disponer de un apropiado grado de protección (ciberseguridad) para evitar posibles intrusiones o ciberataques. Además, la maqueta se irá enriqueciendo con la información que proporcionen los buques a lo largo de su ciclo de vida y dispondrá de capacidad de autoaprendizaje (inteligencia artificial), al incluir modelos de predicción de prestaciones y análisis de comportamientos de los equipos y sistemas del buque para el apoyo a la toma de decisiones.

Para llevar a cabo las diferentes funciones logísticas, la maqueta digital deberá de disponer una estructura de datos como la que se proporciona a continuación.



ESTRUCTURA DE DATOS DATOS ÚNICA. USO DIFERENTE [88]

Y se tendrán distintas categorías de datos:

Tipo de dato		Asociación
CAD		Interfaces físicas más básicas (geométrica, dimensiones, localización).
Tipo logístico		Fiabilidad de componentes, tiempo entre fallos, disponibilidad operativa, periodicidad de mantenimiento, repuestos necesarios, etc.
Modelado físico		Comportamiento físico (potencia de un motor, caudal de una bomba).
Modelado lógico		Describir las funciones de los sistemas (contraincendios, alimentación, alumbrado).
Modelado estocástico		Describir las incertidumbres asociadas a los anteriores (probabilidad de rotura de una tubería).
Complementarios		Identificación, estándares, descripciones, etcétera.
Asociados a agrupaciones (elementos configurados en la maqueta)	Analíticos	Suma directa de los elementos que forman la agrupación (el peso de un motor diésel).
	Holísticos	Introducidos de forma directa sin conexión con los de los elementos del grupo (la curva de revoluciones de una turbina).

TABLA 2: TIPOS DE DATOS DE LA MAQUETA DIGITAL EN LA ARMADA [76]

En el artículo, también hace mención al programa de obtención de la fragata F-110, en el cual la maqueta digital que se desarrolle dentro de este programa, si bien estará inicialmente limitada en su alcance, deberá ser flexible, adaptable y escalable a los cambios que se vayan produciendo a medida que el proceso de obtención avance. Debido a eso, se está articulando una estrategia de inserción tecnológica incremental de la maqueta de la F-110, incluyendo su progresión a la categoría de gemelo digital y su posterior desarrollo. El proceso inicial rodará en torno al pilar de la configuración, para su posterior evolución al grado de gemelo digital y la correspondiente explotación de los servicios de apoyo al ciclo de vida.

En una apuesta por reforzar la ciberdefensa en el ámbito naval, se ha comenzado a trabajar en el desarrollo de un sistema de ciberseguridad reforzado para los submarinos de la clase S-80 además de las fragatas F-110 [90]. Dicho trabajo es una colaboración del Ministerio de Defensa, Navantia y Telefónica Tech en su división de Ciberseguridad. La ciberdefensa del submarino S-80 otorgará a los sistemas principales del submarino de protección ante intentos de intrusión o ciber ataques. Asimismo, mediante la monitorización en tiempo real del funcionamiento del sistema de combate o del sistema avanzado de comunicaciones, se podrá alertar la detección de cualquier amenaza potencial. De dicha amenaza se podrá identificar su procedencia, el grado de esta y el mecanismo usado para la intrusión para adoptar las acciones correctivas pertinentes gracias a su avanzado sistema de registro que permitirá la realización de análisis forense.

Por otra parte, en el ejemplar diciembre 2018- marzo 2019 de la revista *Expertica Militar* se encuentra el artículo "La Transformación de las Fuerzas Armadas en un Mundo Complejo", donde se indica que el ataque sobre el objetivo no es como en las Guerra de Vietnam de 1970 o la Guerra del Golfo de 1991. En la actualidad, el ataque sobre el objetivo considerado podría alcanzarse utilizando una única Munición de Ataque Directo Conjunto (JDAM, por su sigla en inglés) lanzada desde una plataforma tripulada remotamente, consiguiendo reducir drásticamente el coste humano y de material para llevar a cabo el ataque. En cambio, el coste económico y la complejidad de la tecnología empleada ha incrementado exponencialmente debido a la Cuarta Revolución Industrial. Dicha revolución, según el autor, está caracterizada por el intercambio de información debido a la capacidad de conectar todos los sistemas, incluyendo máquinas y herramientas, y no solo los informáticos; y cuyos tres buques insignia son la inteligencia artificial, la robotización y el Big Data. También, que el empleo del Big Data y data science junto con cloud computing, la realidad aumentada, el internet de las cosas o la impresión 3D representan en el campo de la defensa un conjunto de tecnologías de naturaleza disruptiva para los procesos, productos y modelos de negocio de la industria tradicional cuyas consecuencias no pueden ser valoradas con precisión pero que con pero que con seguridad traerán consigo un cambio sistémico entre ello en las fuerzas armadas.

En la revista de aeronáutica y astronáutica de enero-febrero 2020 se publicó el dossier "El Ejército del Aire conect@do" [91] que tiene como objetivo llamar la atención a todos los miembros del Ejército del Aire para que contribuyan a crear una corriente de cambio dentro de la organización mediante la transformación digital. En el dossier se presentan cuatro artículos en los cuales se mencionan la incorporación de la tecnología del Big Data además de otras tecnologías dentro de la transformación digital:

- Un Ejército del Aire ágil y conectado: describe desde un punto de vista estratégico, la necesidad de la trasformación digital en el Ejército del Aire.
- Un destacamento del Ejército del Aire en la era digital: plantea un ejercicio de imaginación donde se atreve a describir cómo podría ser un destacamento aéreo en un futuro a medio/largo plazo.
- Base aérea conectada inteligente (BAC-i): expone la iniciativa «Base Aérea Conectada Inteligente», como uno de los ejes principales de transformación en el Ejército del Aire.
- El Ejército del Aire 4.0 La perspectiva del sostenimiento: describe el estado de determinadas tecnologías aplicadas al sostenimiento aeroespacial y a las bases aéreas, así como proyectos tecnológicos en curso como por ejemplo, Big Data y la base aérea conectada-inteligente.

En un artículo de la Revista Ejercito nº955 de noviembre 2020, bajo el título "Data Science E Inteligencia Artificial, Manual De Campo: Ejército Futuro" [92], el autor plantean que en la actualidad las misiones militares no pueden ser concebidas sin sistemas que permitan la

obtención y elaboración de información procedente de diversas fuentes y sensores. Para ello, en el artículo elaboran las posibilidades de las nuevas tecnologías de inteligencia artificial y Big Data junto con sensores e infraestructuras para ayudar a la comunidad de Defensa a superar los actuales desafíos de los sistemas C4ISR, simulación, logística, planeamiento, apoyo a la decisión y ciberdefensa. En el texto, el autor explica que en el ámbito militar se ha comenzado a desarrollar proyectos de inteligencia artificial que requieren una alta cuantía de recursos humanos y financieros como son:

- Conocimiento situacional, Identificación y gestión de sistemas y sensores, Sistemas C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance).
- Inteligencia a través de capacidades de minería de datos para la superioridad de la información.
- Operaciones en el ciberespacio.
- Apoyo a la toma de decisiones y planificación operativa para decisión rápida, de alta precisión y estimación de los posibles efectos.
- Vehículos autónomos y robótica a través de la navegación, la orientación y el control para aliviar a las fuerzas militares de tareas repetitivas o peligrosas.
- Mantenimiento predictivo para la seguridad de las fuerzas y la disponibilidad de rutas y municiones.

Asimismo, mencionan algunas aplicaciones de deep learning en el ámbito de la defensa como:

- Detección, predicción y prevención de amenazas sofisticadas en tiempo real en el campo de la ciberseguridad.
- Detección, clasificación y reconocimiento de objetivos.
- Seguimiento automático de objetivos.
- Mejoras de las imágenes: eliminación de ruido, super resolución y filtrado.
- Integración de información de sensores multiespectrales (teledetección) para mejorar la percepción humana y la detección de objetos.
- Estudios de camuflaje para plataformas militares.
- Reconocimiento de actividades y comportamientos

El impacto potencial de la inteligencia artificial en la defensa del futuro que no se puede negar, pero no será uniforme en todas las áreas ya que habrá zonas dónde será más apreciable: conocimiento de la situación, inteligencia, apoyo a la toma de decisión, vehículos autónomos, robots y funciones logísticas, lo que alterará las capacidades ofensivas y defensivas, del mismo modo que sucedió con la tecnología aeroespacial o la nuclear. En el presente bastantes de las guerras modernas no son libradas en el campo de batalla, sino en el plano digital, pues cualquier ciudadano de a pie puede ser atacado a través de sus dispositivos personales en forma de noticias falsas, desinformación y otras técnicas de manipulación, persuasión y ocultación que consiguiendo desestabilizar procesos electorales y amenazar al modelo occidental de vida y gobierno

Según el autor, en España hay en marcha proyectos en el ámbito de la defensa que están basados en inteligencia artificial como los llevados a cabo por investigadores del grupo Sistemas Inteligentes y Minería de Datos, de la Universidad de Jaén, en unión con investigadores del grupo Soft Computing y Sistemas de Información Inteligentes, de la Universidad de Granada, que se encuentran desarrollando para el Ministerio de Defensa un software que permita disponer de sistemas de inteligencia artificial como soporte a la toma de decisiones para entornos de

amenaza y conflicto. O, el de la Universidad de Córdoba (UCO) que desarrolla el proyecto de investigación de mantenimiento predictivo para plataformas terrestres (MANPREDIC) para el mando de apoyo logístico del Ejército de Tierra, aumentando la disponibilidad de los vehículos y mejorando en eficiencia económica, al evadir averías antes no predecibles.

Adicionalmente, se plantea que para que los ejércitos puedan beneficiarse de las posibilidades de la IA y el Big Data se requiere de una infraestructura de datos de gran capacidad, gestionada por estas tecnologías, que incorpore el concepto de centralización de datos y escalabilidad del sistema, y disponibilidad de recursos humanos especialistas en estas tecnologías (científicos de datos) [93].

Se puede considerar que la aplicación del Big Data en defensa y seguridad pasa por la obtención de herramientas que complementen y ayuden a los usuarios, tanto al analista como al combatiente, a la identificación de amenazas actuales y futuras. Para ello, se puede hacer uso de clasificación robusta y precisa para detección, geo-referenciación, clasificación e identificación de objetos y elementos en la superficie terrestre con independencia de su entorno, configuración y disposición. También hacer uso de herramientas de automatización para la identificar patrones de actividad de objetos y elementos en la superficie terrestre, y herramientas para la captura, almacenamiento y análisis de información de HUMINT (Inteligencia de Fuentes Humanas) [94].

Obviamente, lo recogido en estos párrafos es un resumen de una frenética actividad hasta la primavera del año 2022. El lector entenderá que no puede ser completo y, sobre todo, que estará desactualizado en la medida que pase el tiempo a consecuencia del vertiginoso desarrollo de estas actividades.

3. Aplicaciones de Big Data en Defensa y seguridad

En el documento "Military Implications of Big Data" [95], los autores plantean que el Big Data se puede utilizar en muchas áreas con fines militares, además en el futuro, uno de los factores más importantes que afectan el destino de la guerra serán los grandes datos. Para ello, los autores esbozan la siguiente tabla de algunos de los campos en los que el Big Data puede ser empleado por las fuerzas armadas y fuerzas y cuerpos de seguridad del estado.

FIELDS OF BIG DATA USAGE IN MILITARY

Direct	Indirect
Intelligence Development	Conventional Warfare
Knowledge Management	Irregular Warfare
Common Operational Picture	Hybrid Warfare
Military Decision Making Process	Asymmetric Warfare
Cyber Defense	Anti-Terrorism Operations
Information System Management	Military Logistics
Military Forensics	Operations Centers
Geographical Data Systems	Military Technology Development

TABLA 3: CAMPOS MILITARES DEL USO DEL BIG DATA [95]

Por otra parte, en el artículo publicado en el año 2015, "Redefining Military Intelligence Using Big Data Analytics" [96], se plantea la pregunta ¿Cómo puede Big Data Analytics mejorar la productividad de la inteligencia militar? Para contestar a la pregunta se plantea que en un futuro próximo estaremos nadando en sensores y ahogándonos en datos, pero las inmensas cantidades de datos recopilados pueden ser analizados automáticamente mediante la analítica de Big Data. Además, la participación en las redes sociales puede darnos respuestas a preguntas como por qué, cuándo, qué, dónde, quién, cómo, a muchos incidentes de seguridad que de otro modo podrían pasar desapercibidos.

En los escenarios de combate modernos, afirman, un científico de datos que ayude a interpretar y analizar datos podría salvar muchas más vidas que cien soldados en tierra. Big Data, con análisis computacional, pueden brindar información que permita a los comandantes identificar de manera proactiva los puntos calientes para la planificación operativa. El análisis sofisticado de los conjuntos de datos masivos será posible a largo plazo con herramientas analíticas desarrolladas específicamente para este propósito. Los sistemas de monitoreo de recursos dedicados proporcionarán una mejor visibilidad de los activos, una necesidad para la guerra centrada en la red. La capacidad de análisis de Big Data que utiliza el aprendizaje automático como herramienta garantizará que ninguna información oculta escape a los ojos del comandante, por muy grande que sea el conjunto de datos, como ejemplos de aplicaciones que probablemente se implementarán, se citan: el terrorismo, la guerra por poderes, los extremismos, la realización de entrenamientos por parte de los oponentes, el despliegue de fuerzas o el patrocinio de actores no estatales.

El análisis de Big Data tiene un papel importante en la capacidad predictiva para anticipar incidentes específicos, asimismo, puede proporcionar las siguientes plataformas como valor añadido:

- Sistema de alerta de amenazas: los algoritmos pueden ser diseñados de forma que puedan alertar a los comandantes sobre la mención de conceptos como terrorismo, bombas, disturbios, etc. en diversas fuentes de información, mediante la obtención de tendencias en videos / contenido ofensivo específico para una persona, organizaciones, geografía, etc., por ejemplo, un aumento en las discusiones en Twitter relacionadas con un tema específico.
- Monitorización de social media: los temas / conceptos principales debatidos en los medios de comunicación pueden ser monitoreados y estudiados de manera específica a la geografía, la persona y la organización, etc. El análisis de las fuentes de información, por ejemplo, la afinidad de las fuentes de información con un grupo de usuarios específico, geografía, etc., tendrá gran valor de inteligencia. Los sentimientos de las personas con respecto a una política o conceptos se pueden conocer y se pueden tomar acciones proactivas, según sea necesario.
- Minería de información: Información en las noticias / documentos relacionados con un persona, conceptos, etc., se puede buscar para encontrar los conceptos relacionados con un concepto dado. También, se pueden encontrar documentos relacionados que proporcionan diferentes representaciones de la misma información, por ejemplo, las diferentes formas en que se mencionan los explosivos en los artículos. La nueva información sobre un tema específico, por ejemplo, nuevos artículos, publicaciones, libros blancos, patentes relacionadas con la defensa antimisiles, comprenden entradas que serán de gran ayuda en la planificación de la estrategia de inteligencia en el nivel superior.
- Monitoreo de redes sociales: un estudio de personas relacionadas basado en redes sociales se puede realizar. Los temas discutidos por personas relacionadas que representan información sobre el comportamiento de una persona tendrán un valor de inteligencia muy alto. Diferentes perfiles sociales de una persona en Twitter, Facebook, LinkedIn, etc. pueden ser estudiados y sitios web relacionados con una persona específica en función de su perfil social, contenido creado, círculo de amigos, etc., puede ser analizado mediante el análisis macro de gráficos de redes sociales para identificar los grupos de usuarios activos en un sitio web.
- Analítica de documentos: conceptos, temas discutidos en una colección de documentos pueden ser estudiados y los documentos agrupados en segmentos separados: documentos sobre política, deportes, juegos, asuntos exteriores, etc. Encontrar tendencias relacionadas con temas específicos puede ser una forma importante de descubrir los conocimientos ocultos en un documento.
- Seguridad cibernética: los administradores de red se enfrentarán a millones de ataques todos los días, y el análisis de Big Data se puede aplicar para detectar amenazas persistentes avanzadas, como ataques de ingeniería social diseñados para robar información del gobierno. La mayoría de los piratas informáticos tienen un modus operandi, que una vez identificado se puede utilizar para predecir la forma de futuros ataques y poner en práctica las medidas defensivas adecuadas. La aplicación también se puede utilizar para aspectos ofensivos de seguridad cibernética.

Por otro lado, es relevante resaltar, que en las operaciones de contrainteligencia/contraterrorismo (CI/CT), los grandes datos recopilados por drones, satélites, UAV, etc. se pueden analizar automáticamente en función del escenario general proporcionado por los datos que se pueden crear como parte de la iniciativa de Big Data, permitiendo que las

operaciones de CI/CT se realicen en tiempo real. Las aplicaciones basadas en el sistema de información terrestre (SIG) intensivo en datos se pueden utilizar con plataformas de Big Data en el interior para ayudar a las fuerzas desplegadas para luchar contra los extremismos. Al final, los sistemas de inteligencia deben poder recopilar, cotejar, filtrar y procesar todo tipo de información, desde estructurada a no estructurada, incluida la transmisión en vivo, y mostrarla a los comandantes en el nivel jerárquico.

Considerando los distintos campos del uso del Big Data que se plantean en la tabla 3 junto los planteados en el artículo Redefining Military Intelligence Using Big Data Analytics" [81], los campos del Big Data en el ámbito de defensa y seguridad los vamos a agrupar en los siguientes campos de aplicación:

- Sistemas de información
    - Gestión del conocimiento
    - Inteligencia
    - Análisis de Redes sociales y Fake news
    - Logística
- Ciberdefensa y ciberseguridad
- Common Operational Picture, Consciencia Situacional y Toma de decisiones
- Análisis Forense Digital
- Sistemas de datos geográficos

Siguiendo esta clasificación, en cada una de las secciones se planteará una revisión de lo que consisten cada una de ellas, además de incorporar artículos relacionados. Los artículos serán tanto del ámbito militar como civil.

3.1. Sistemas de Información

Un sistema de información es un conjunto de datos, dispositivos informáticos y métodos de gestión que respaldan las operaciones rutinarias de la empresa. Un sistema de información de gestión es un subconjunto específico del sistema de información, y se refiere a una gran infraestructura utilizada por una empresa o corporación, que ayuda a una empresa a tomar decisiones y coordinar y analizar información [97].

En la gestión de la información, la tendencia es a implantar sistemas que permitan que la información que tiene la organización y los individuos que la componen puedan ser compartida por todos, mediante la elaboración de "mapas documentales" y de "conocimientos" en los que se representa y da acceso de manera gráfica a toda la tipología documental que se produce o maneja en una organización [98].

El sistema de información con el apoyo de la tecnología de Big Data puede usar el mapa de situación general y otros formatos de información de inteligencia necesarios para acceder a la información masiva del campo de batalla de acuerdo con el privilegio y los requisitos. Esto permite la adquisición de información de inteligencia de todas las fuentes y el procesamiento de información jerárquica de varios niveles. Además, en el caso de los sistemas de armas, el intercambio de información en tiempo real entre los comandantes en todos los niveles y el extremo del arma garantiza que la información esté altamente integrada con la potencia de fuego, alcanzando el objetivo directamente en los puntos clave del enemigo y logrando un posicionamiento de reconocimiento preciso y un comando preciso [99].

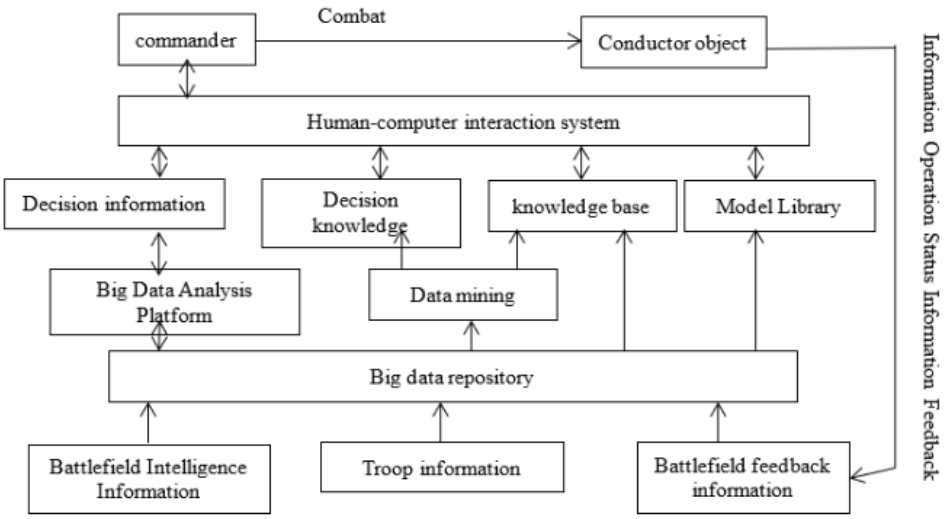


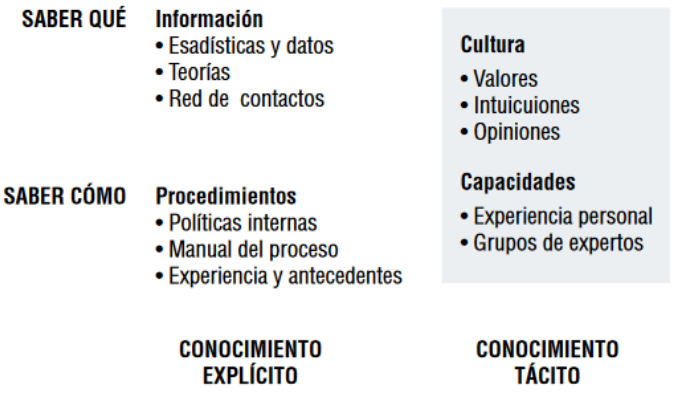
DIAGRAMA DE FLUJO DE TRABAJO DEL SISTEMA AUXILIAR DE MANDO Y DECISIÓN SOPORTADO EN BIG DATA [99]

Los sistemas de información se van a dividir a su vez en gestión del conocimiento, inteligencia, análisis de redes sociales y fake news y, para acabar esta sección, logística.

3.1.1. Gestión del conocimiento

La gestión del conocimiento es todo el conjunto de actividades realizadas con el fin de utilizar, compartir y desarrollar los conocimientos de una organización y de los individuos que en ella trabajan, encaminándolos a la mejor consecución de sus objetivos. El conocimiento en una organización se produce cuando un individuo de esta hace uso de lo que sabe y de la información que tiene disponible para la resolución de un problema o el desarrollo de un proyecto [98]. Se pueden distinguir entre dos tipos de conocimientos:

- Conocimiento explícito: es el dentro de la organización tiene establecidas las fórmulas por las cuales se puede trasmitir a otras personas
- Conocimiento tácito: es aquel que toda organización tiene, pero que no queda plasmado ni registrado en lugar alguno, estando totalmente ligado al grupo de personas que componen la organización en cada momento.

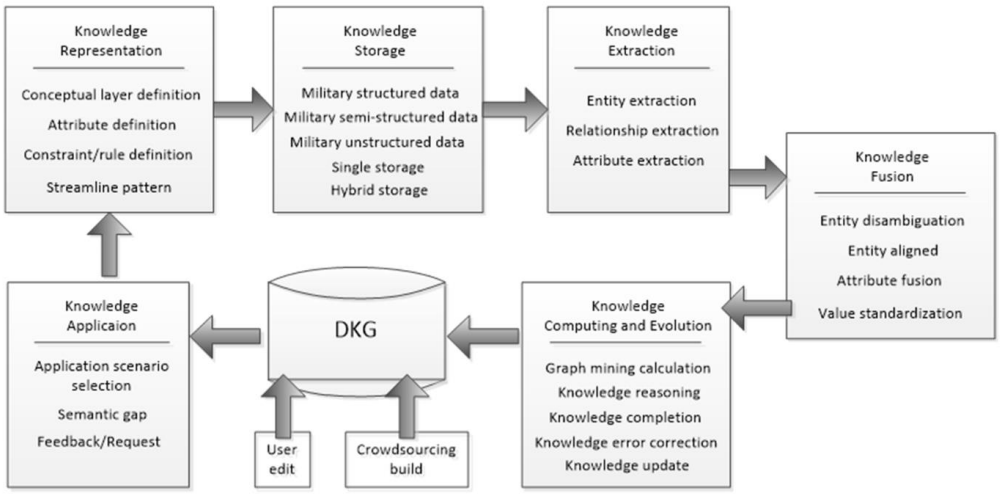


CONOCIMIENTO EXPLÍCITO VS. TÁCITO [98]

Debido a la evolución del desarrollo tecnológico en los últimos años, la gestión del conocimiento se puede ver como la teoría de gestión que responde a la adaptación de las últimas innovaciones tecnológicas en el tratamiento de la información y las telecomunicaciones.

La diferencia entre gestión de la información y gestión del conocimiento es destaca en el artículo, "La Gestión del Conocimiento en La Armada" [100]. La primera está orientada a la utilización de técnicas de gestión que permitan un uso eficiente de la información para alcanzar los objetivos de la organización, mientras que la gestión del conocimiento, como escalón más desarrollado de la gestión de la información, asume como elementos esenciales el conocimiento y las habilidades de las personas. Por tanto, la diferencia radica en que la gestión del conocimiento reconoce el papel que las personas juegan en la organización.

En el campo militar, *Domain- specific Knowledge Graph* (DKG) es un puente para conectar todo tipo de factores de batalla, como fuerzas de combate, sistema de comando, plataformas de armas, además de ser un medio importante para superar la brecha de información entre diferentes áreas de diferentes servicios, según el paper "Construction and Application Technology Architecture of Domain- specific Knowledge Graph in Military Field" [101]. La mayor parte de los gráficos de conocimiento existentes son gráficos de conocimiento general para campos generales, pero no existe un método maduro de construcción y expresión de gráficos de conocimiento para los datos de la industria de campos militares específicos. Entonces, en base a las necesidades especiales de adquisición, almacenamiento, representación, consulta y otras tecnologías de conocimiento militar en la información futura y las operaciones inteligentes, y los escenarios de aplicación se puede construir el gráfico de conocimiento en el dominio militar. La capa de datos es la base de toda la construcción de DKG, a diferencia de los datos tradicionales de Internet, las fuentes de datos de campo militar y otros tipos, incluida la base de datos militar, texto de combate, imágenes, documentos, información, militar de datos heterogéneos de múltiples fuentes, como la transmisión multimedia, provienen principalmente de la base de datos estándar militar, y el modelo de investigación de sistemas de información existente para obtener la información.



ARQUITECTURA TECNOLÓGICA DE CONSTRUCCIÓN Y APLICACIÓN DE DKG EN ÁMBITO MILITAR [101]

A modo de ejemplo, un caso de aplicación de la gestión del conocimiento es el empleo del Big Data en la gestión de las prisiones, a través de la recopilación y el almacenamiento de información, el análisis y la minería de datos inteligentes. La aplicación de Big Data de la prisión mejora en gran medida el nivel de control del refinamiento de la prisión, mejora efectivamente

la calidad de la corrección de los delincuentes y reduce la tasa de reincidencia de los liberados, debido a que la Prisión Inteligente en sí misma es un gran sistema de datos.[102]. En el artículo "Big Data Technology and Prison Management Analysis" [103] analiza las necesidades de la tecnología del Big Data en la gestión de prisiones planteando diversos módulos:

- Módulo de desarrollo del sistema: se emplea para clasificar la información existente, pudiendo ordenar los datos incompletos, los datos erróneos y los datos duplicados en la gestión penitenciaria, y luego usar la información de los datos ordenados para complementar el contenido relevante en el módulo de desarrollo del sistema.
- Módulo de registro de visitas: la función de registro de visitantes atiende principalmente a las familias de los reclusos. El uso de la tecnología de Big Data puede apoyarse en Internet para completar consultas de datos, determinando así el grado de coincidencia de información entre visitantes y reclusos. Solo el personal que cumpla con los requisitos de la exploración puede visitar al prisionero y, al mismo tiempo, usar tecnología de Big Data para registrar el tiempo y la duración de cada visita. Organizando los datos de acceso periódicamente se puede observar si hay alguna anomalía.
- Módulo de consulta de ubicación de prisioneros: la función de consulta de ubicación del prisionero es principalmente para determinar la ubicación específica del prisionero. Si se hace un buen manejo de los datos se puede ubicar la ubicación del recluso a tiempo y entender la dinámica específica del recluso.
- Módulo de función de libro: el módulo de función del libro tiene como objetivo principal proporcionar a los presos lugares de aprendizaje, para que puedan integrarse mejor en la sociedad después de cumplir sus condenas. Realizando un buen trabajo en el manejo de este módulo se puede lograr un conocimiento oportuno de la situación de endeudamiento y plazo de devolución de la información del libro, además de facilitar la suplementación oportuna de libros y satisfacer las necesidades de aprendizaje de conocimientos de los reclusos.
- Módulo de Acceso a Citas: atiende principalmente al manejo psicológico de los reclusos. Algunos reclusos son propensos a problemas como la depresión psicológica durante su estancia en prisión debido a su escasa capacidad para soportar la presión psicológica. En este momento, estos presos necesitan que intervenga un psicólogo, y el proceso de intervención debe completarse con cita previa. En actividades de gestión específicas, el uso de la tecnología de Big Data puede depender de la red para completar la consulta de datos. La prisión puede usar esto para determinar la información del visitante, la información del prisionero y otro contenido para la determinación. Una vez que se determina que no hay problema con el contenido, la prisión puede hacer arreglos para que el recluso lleve a cabo una intervención psicológica. Al mismo tiempo, la prisión puede usar tecnología de Big Data para registrar el tiempo de la consulta psicológica y la duración de la visita. El personal penitenciario puede organizar periódicamente los datos de acceso para ver si hay alguna anomalía. De esta forma, se puede mantener mejor la salud mental del personal y se puede reducir la probabilidad de problemas psicológicos de los reclusos.
- Módulo de Cultura Penitenciaria: tiene como objetivo crear un buen ambiente para la reforma y reducir la sensación de depresión en el entorno penitenciario, para que los presos puedan integrarse mejor en la sociedad después de cumplir sus condenas. Haciendo un buen trabajo en la gestión de este módulo se puede recolectar información relevante en el proceso actual de gestión penitenciaria en tiempo y forma, además de facilitar la formulación oportuna de la cultura penitenciaria y satisfacer las necesidades relevantes de los reclusos durante el período de gestión. El uso de la tecnología de Big

Data puede depender de la red para establecer un sistema de gestión de la cultura penitenciaria para comprender el entorno cultural externo, y elaborar actividades penitenciarias en torno a contenidos culturales para mejorar el ambiente depresivo en la prisión. Mediante la recopilación de información de retroalimentación se puede refinar continuamente el contenido de la gestión de la cultura penitenciaria, creando así una buena atmósfera de gestión y satisfacer las necesidades de gestión correspondientes.

Pero para optimizar la gestión penitenciaria se ha de profundizar en la integración de Big Data, fortalecer la construcción del sistema de gestión, mejorar el intercambio de datos, aumentar el capital de inversión, crear un sistema de oficina inteligente y establecer un mecanismo de entrenamiento normalizado.

También se puede optimizar la gestión de operaciones y mantenimiento de comunicaciones de buques de guerra mediante el empleo de Big Data de acuerdo a lo investigado en el artículo "Research on Warship Communication Operation and Maintenance Management Based on Big Data" [104]. La capacidad de procesamiento de Big Data se está convirtiendo en un elemento fundamental de la guerra moderna debido a sus ventajas:

- El procesamiento de Big Data puede brindar información precisa y procesable que los comandantes y analistas cuestan 100 veces más rápido que la comprensión actual de la inteligencia, la vigilancia y una gran cantidad de datos recopilados por los sensores que detectan. La fusión de gran cantidad de datos de video, imagen, voz y otros documentos de varios sensores, consiguen la formación de un espectro completo de la vista del campo de batalla, y extraer inteligencia de alto valor, entregar información precisa y procesable, para cambiar el modo de la decisión de comando fundamentalmente y mejorar la capacidad de respuesta rápida.
- La tecnología de procesamiento de Big Data puede mejorar las capacidades de conocimiento de la situación y seguridad de la red, y puede detectar anomalías en la red, identificación automática de amenazas y comportamiento de guerra no convencional.

En España el Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC) [105] que depende del Ministerio de Defensa, entre sus funciones se encarga de coordinar la gestión de la información y del conocimiento en el Departamento, en el marco de su transformación digital y el de la Administración General del Estado. También de definir, planificar y coordinar las políticas de los sistemas de información, telecomunicaciones, transformación digital y seguridad de la información del Departamento.

Realizando un análisis de los artículos que se presentan a continuación se extrae que las aplicaciones más significativas del Big Data aplicado a la gestión del conocimiento son:

- Análisis de datos y evaluación de la eficacia de la formación
- Identificación de los factores críticos de gestión que afectan al éxito de proyectos de defensa
- Plataforma para analizar y utilizar de manera eficiente grandes volúmenes de datos policiales
- Análisis de la gestión de gastos de equipamiento militar
- Gestión de operaciones de ayuda humanitaria
- Empleo de técnicas de grafos para analizar la organización
- Sistema de alerta temprana para alertar ante riesgos de escasez en el futuro.

Artículos relacionados

Año	Artículo	Enlace
2006	Critical managerial factors affecting defense projects success	https://doi.org/10.1016/j.engappai.2005.12.002
2014	Big Data in the air force – Process, use and understand for safety	https://doi.org/10.1109/DASC.2014.6979539
2014	Research on Warship Communication Operation and Maintenance Management based on Big Data	https://doi.org/10.1109/CBD.2014.24
2015	The U.S. Army Person-Event Data Environment: A Military–Civilian Big Data Enterprise	https://doi.org/10.1089/big.2014.0055
2016	A Police Big Data Analytics Platform: Framework and Implications	https://doi.org/10.1109/DSC.2016.84
2016	Application Prospect of Big Data in Military Physical Education and Sports	https://doi.org/10.1007/978-981-10-2323-1_70
2016	Military Knowledge Management: Sense-making, Decision making and Knowledge creation	https://d1wqtxts1xzle7.cloudfront.net/48765509/Military_knowledge_management_ECKM16_Fin-with-cover-page-v2.pdf?Expires=1650383355&Signature=Vx7Gzsw6qB6msl3q4JokduxBu9xF4myB1SpTIitr8wDmame8W7r-OcOukTJFVG67N1tE7FQKsG~SOSj81Qsk~FhKXEVNdSbnzpb895-lfZWaNd0~gADrwW8VMzj~G9MZkXCfpslrV8euCaTe5FAPY0WqxZGBz3AGY3m7bX0mjFc8I9PIN1zhy8-pn2DYOsrO~7a-a2L1Job0p0qJ0RfF4ZKrgVGzrsmMEmJC4W-MuAvcT1HhIDTKMdTn7gyFQwqm0y~eQLkLBdhYQspPe9flAx9ha5VCdinXbPptF1pX4EbHmStzy1qFx2gh319urvwmCFzNe7SqlLGnuhIFUbELFg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA
2017	Big Data Management for Cloud-Enabled Geological Information Services	https://doi.org/10.1155/2018/1327214
2017	Some Key Problems of Data Management in Army Data Engineering Based on Big Data	https://doi.org/10.1109/ICBDA.2017.8078796
2018	Analysis of Military Academy Smart Campus Based on Big Data	https://doi.org/10.1109/IHMSC.2018.00031
2018	Data Analytics and Training Effectiveness Evaluation	https://doi.org/10.1201/9780429445491
2018	A Virtual Reality Soldier Simulator with Body Area Networks for Team Training	https://doi.org/10.3390/s19030451
2019	Analysis on the Application of Big Data in Military Equipment Expense Management	https://doi.org/10.1145/3341069.3341079
2019	Application of Big Data Technology in Scientific Research Data Management of Military Enterprises	https://doi.org/10.1016/j.procs.2019.01.221
2019	Design and Development of Data Map Visualization Tool for Property Search of Police Information	https://doi.org/10.23919/ELINFOCOM.2019.8706358
2019	Leveraging Big Data Analytics to Improve Military Recruiting	https://www.rand.org/pubs/research_reports/RR2621.html

2019	Preliminary Psychometrics and Potential Big Data Uses of the U.S. Army Family Global Assessment Tool	https://doi.org/10.1080/21635781.2019.1676334
2020	A New Method for information security risk management in Big Data environment	https://doi.org/10.1109/ITCA52113.2020.00100
2020	A Survey on Trajectory Data Management, Analytics, and Learning	https://doi.org/10.48550/arXiv.2003.11547
2020	Application Research on Big Data of Military Training in Military Academy Teaching	https://doi.org/10.1109/ICMEIM51375.2020.00088
2020	Distributed Data Strategies to Support Large-Scale Data Analysis Across Geo-Distributed Data Centers	https://doi.org/10.1109/ACCESS.2020.3027675
2020	Exploring Knowledge Management Practices in Military RnD Agency: An Indonesian Case Study	https://doi.org/10.1109/IC2IE50715.2020.9274601
2020	Management of humanitarian relief operations using satellite Big Data analytics: the case of Kerala floods	https://doi.org/10.1007/s10479-020-03593-w
2020	Mooc Method of Military Theory Course Based on Network Technology	https://doi.org/10.1088/1742-6596/1648/4/042122
2020	Research on Big Data Reference Architecture Model	https://doi.org/10.1109/ICAIBD49809.2020.9137451
2020	Research on Evaluation of Operation Effect of Military-Civil Integration in Military Industry Enterprises---Take Aviation Industry Corporation L as an Example	https://doi.org/10.1109/BDEIM52318.2020.00045
2020	Multi-source Heterogeneous Data Association Technology to Build Public Safety Big Data Integration Research	https://doi.ieeecomputersociety.org/10.1109/BDEIM52318.2020.00012
2021	BBS: A Blockchain Big-Data Sharing System	https://doi.org/10.48550/arXiv.2111.08822
2021	Developing an Air Force Retention Early Warning System	https://www.rand.org/pubs/research_reports/RRA545-1.html
2021	Data analytics in military human performance: Getting in the game: Summary of a keynote address	https://doi.org/10.1016/j.jsams.2021.04.003
2021	Big Data Technology and Prison Management Analysis	https://doi.org/10.1109/BDACS53596.2021.00016
2021	Construction and Application Technology Architecture of Domain-specific Knowledge Graphin Military Field	https://doi.org/10.1088/1742-6596/1792/1/012044
2021	Review of Government Performance Management in the Big Data Era: Practice, Issues and Prospects	https://www.atlantis-press.com/article/125956660.pdf
2021	The Concept of Information Graphs as a Tool to Identify Vulnerabilities in the Information Map of an Organisation	https://doi.org/10.1007/978-3-030-79463-7_18
2021	Non-Modifiable Risk Factors for Stress Fractures in Military Personnel Undergoing Training: A Systematic Review	https://doi.org/10.3390/ijerph19010422
2022	Quantification of Recruit Training Demands and Subjective Wellbeing during Basic Military Training	https://doi.org/10.3390/ijerph19127360

2022	Factors Predicting Training Delays and Attrition of Recruits during Basic Military Training	https://doi.org/10.3390/ijerph19127271
2022	Development of a Methodology for Assessing Workload within the Air Traffic Control Environment in the Czech Republic	https://doi.org/10.3390/su14137858
2022	Three-Faceted Approach to Perceived Stress A Longitudinal Study of Stress Hormones, Personality, and Group Cohesion in the Real-Life Setting of Compulsory Basic Military Training	https://doi.org/10.3390/su14031046
2022	Study of the Competence of Cadets of Military Universities in the Organization of Rational Water Use and Water Management	https://doi.org/10.1088/1755-1315/987/1/012016
2022	Risk Factors Associated with Cartilage Defects after Anterior Cruciate Ligament Rupture in Military Draftees	https://doi.org/10.3390/jpm12071076
2022	Body Composition of Female Air Force Personnel: A Comparative Study of Aircrew, Airplane, and Helicopter Pilots	https://doi.org/10.3390/ijerph19148640
2022	"It Depends on Where You Are and What Job You Do": Differences in Tobacco Use across Career Fields in the United States Air Force	https://doi.org/10.3390/ijerph19148598

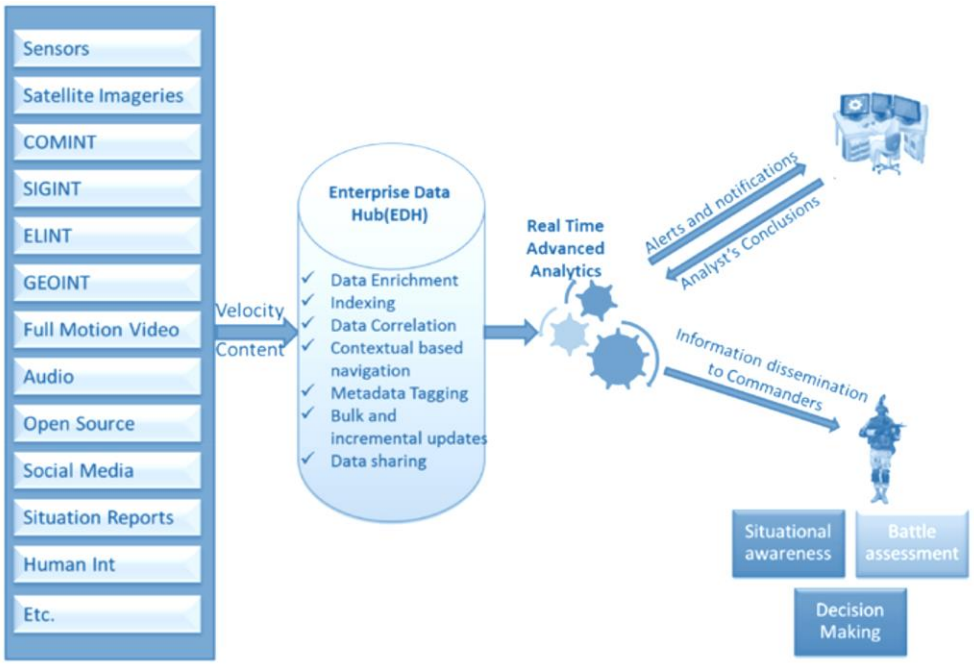
TABLA 4: ARTÍCULOS GESTIÓN DEL CONOCIMIENTO

3.1.2. Inteligencia

La inteligencia tiene por objetivo proporcionar información útil, mediante la recolección, evaluación e interpretación de la información disponible, ofreciendo un valor inmediato o potencial para el planeamiento y conducción de operaciones militares-. De ahí la importancia de la información y la inteligencia para las fuerzas armadas debido a que es fundamental tener los datos correctos para la planificación de cualquier operación militar en paz o en guerra.

Los militares han llevado a cabo tareas de reconocimiento y vigilancia desde tiempos inmemoriales antes de montar cualquier ataque contra el enemigo. El éxito de la misión depende del correcto análisis de la información disponible durante la etapa de planificación. La recopilación de información, su análisis y posterior difusión es de suma importancia para cualquier ejército. Hoy en día, los métodos de recopilación de información han cambiado debido a la rápida disponibilidad de información de combate de alta calidad y confiabilidad de una variedad de sensores y fuentes. [106]

Los sistemas de inteligencia basado en aplicaciones de Big Data deben poder recopilar, cotejar, filtrar y procesar todo tipo de información, desde estructurada hasta no estructurada, incluida la transmisión en vivo, y mostrarla a los comandantes en el nivel jerárquico, a través de los sistemas a los comandantes de campo y a través de sistema de Comando, Control, Comunicación, Computación, Inteligencia, Información (C4I2) a los líderes a nivel estratégico. Además, la inteligencia basada en análisis de Big Data, permitirá a los comandantes evaluar la situación del campo de batalla en tiempo real y de una mejor manera para tomar decisiones apropiadas y oportunas.



DISEÑO CONCEPTUAL DEL SISTEMA DE RECOPILACIÓN DE INTELIGENCIA BASADO EN APLICACIONES DE BIG DATA [96]

Del esquema del diseño conceptual del sistema de recopilación de inteligencia se aprecian distintos tipos de datos de inteligencia, los cuales el ejército continúa reuniendo junto con la Comunidad de Inteligencia en varias disciplinas, como son [107]:

- HUMINT (Human Intelligence): la inteligencia humana recopila información a través del contacto personal con las personas. La información toma la forma de documentos, fotos, archivos digitales y otros materiales, adquiridos de manera encubierta a través de canales no oficiales o abiertamente a través de personal diplomático o consular, así como comunicaciones autorizadas con funcionarios extranjeros. Los militares también pueden obtener inteligencia a través del interrogatorio del enemigo o del informe de los viajeros. Los datos recopilados a través de HUMINT suelen estar en diferentes formatos, tanto analógicos como digitales, pueden ser audio, video, texto o imágenes, y tendrá que pasar por un análisis para integrarlo con los datos recopilados a través de otras disciplinas.
- GEOINT (Geospatial Intelligence): la inteligencia geoespacial se refiere al uso y estudio de imágenes y datos geoespaciales para explicar, revisar y representar visualmente las características y actividades terrestre, es decir, GEOINT incluye toda la inteligencia recopilada a partir de imágenes, videos y otras representaciones visuales tomadas desde el aire, en tierra o bajo el agua. En la mayoría de los casos, los datos GEOINT son una integración de datos geoespaciales de diferentes fuentes para crear una representación tridimensional de la situación. Los datos visuales generalmente provienen de satélites, vehículos aéreos no tripulados (UAV), vehículos submarinos autónomos (AUV) y otras tecnologías topográficas. El valor de GEOINT en un sentido militar es proporcionar la ubicación precisa de objetos y actividades, interpretar su significado y brindar el marco para ayudar a tomar decisiones militares.
- SIGINT (Signals Intelligence): la inteligencia de señales es información sobre las acciones, objetivos y capacidades de un objetivo extranjero adquirida a través de la interceptación

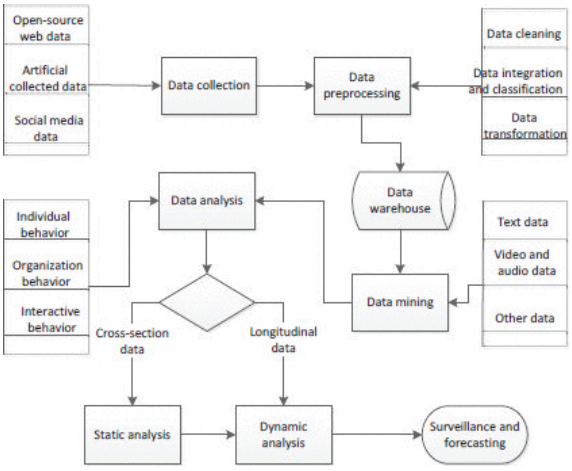
de señales y transmisiones como sería la recopilación sobre terroristas, organizaciones y personas con asociaciones internacionales o extranjeras. Las fuentes de datos son múltiples desde como son las conversaciones telefónicas, los correos electrónicos, las ondas de radio, las transmisiones por satélite, las conexiones inalámbricas e incluso las vibraciones del teclado están sucediendo todo el tiempo. El desafío es extraer los migas de información valiosa de las señales aleatorias. El proceso de recopilación implica primero extraer ciertos tipos de señales de capas de señales o conversaciones de la verbosidad de conversaciones. Después de la extracción, el analista de SIGINT filtra los elementos candidatos para seleccionar los que se conservarán en función de un conjunto de parámetros, para posteriormente ser seleccionados y enviados para un análisis más detallado. Existen tres subconjuntos de SIGINT según el tipo de transmisión; COMINT proviene de los sistemas de comunicación, ELINT (Inteligencia Electrónica) de los sistemas de armas y radar, y FISINT (Inteligencia de Señales de Instrumentación Extranjera) de los sistemas de armas en desarrollo o prueba. Además, el rápido aumento de las actividades cibernéticas y electromagnéticas (CEMA) sofisticadas y la guerra electrónica de los adversarios está obligando al Ejército a converger los sistemas SIGINT, cibernético y electromagnético en una sola plataforma: Sistema de inteligencia de capa terrestre.

- OSINT (Open Source Intelligence): La inteligencia de código abierto es la recopilación de datos de fuentes abiertas o disponibles públicamente para su explotación con un propósito específico. Las fuentes de OSINT han evolucionado a lo largo de los años, en un principio, las fuentes OSINT más prolíficas fueron la televisión, la radio y los medios impresos, pero, los operadores humanos tenían que revisar estas fuentes de datos manualmente, aunque posteriormente, las agencias de inteligencia utilizaron software comercial estándar para recopilar, limpiar y analizar datos OSINT. Los medios tradicionales siguen siendo fuentes de OSINT, pero la verdadera fuente de energía para la recopilación de datos es Internet, debido al acceso instantáneo a datos fácilmente disponibles y en constante actualización beneficia las operaciones de recopilación de inteligencia. Estos incluyen blogs, periódicos en línea, redes sociales, servicios de transmisión de video, foros y otro contenido aportado por los usuarios, así como gemas ocultas en el backend de los sitios web. El dilema es el gran volumen y la complejidad de los datos disponibles dado que los flujos de datos de Internet tienen capas y capas de matices, y los analistas tienen que realizar todo, desde la verificación de hechos hasta el análisis de sentimientos, siempre teniendo en cuenta el contexto de los datos.

La controversia a menudo rodea la recopilación de grandes datos en el ejército de acuerdo con el articulo web “Big Data in the Military – Preparing for AI” [107]. Un debate reciente está relacionado con la recopilación de datos visuales utilizando una plataforma de aprendizaje automático de código abierto. Los drones fueron el método utilizado en este caso para la recopilación de datos, pero el dilema no se encontraba en los datos per se, sino del uso potencial de machine learning para actividades de ataque.

Diferentes actividades siempre dejaran trazas en internet y aunque los datos en Internet son de gran escala, variados y no estructurados, mediante el uso de técnicas y herramientas de Big Data se puede extraer información útil para intentar luchar contra el terrorismo. En el artículo “Research on counter-terrorism based on Big Data” [108], realizan una investigación sistemática sobre las aplicaciones de Big Data en el campo de la lucha contra el terrorismo mediante el uso de un método de análisis cuantitativo.

- Recopilación y preprocesamiento de datos: La recopilación de datos se puede hacer de datos web de código abierto, redes sociales y métodos tradicionales de recolección de datos. En el preprocesamiento de los grandes datos relacionados con el terrorismo hay tres aspectos: limpieza de datos, integración de datos, transformación y clasificación de datos.
- Minería y análisis de datos: analizar y descubrir las características temporales y espaciales de los ataques terroristas, los patrones de comportamiento de las organizaciones terroristas y sus miembros, etc., y luego proporcionar una base teórica para la alerta temprana y el seguimiento de la lucha contra el terrorismo.
- Vigilancia y Pronóstico: la aplicación de Big Data en la investigación antiterrorista tiene como objetivo extraer y analizar los factores relacionados con los ataques terroristas y descubrir las características temporales y espaciales para prevenir los ataques terroristas.



EL MARCO DE APLICACIÓN DE BIG DATA EN EL TRABAJO ANTITERRORISTA [108]

Dentro de las aplicaciones más significativas de Inteligencia se encuentran:

- Identificación y detección de objetos en imágenes radar y ópticas
- Aprendizaje profundo para realizar subtitulado de imágenes militares
- Análisis de informaciones para luchar contra el terrorismo
- Algoritmos para la selección y evaluación de armas
- Análisis de datos de movilidad
- Identificación y detección de objetos
- Simulaciones militares
- Comando de combate inteligente
- Minería de texto; pronóstico de tendencias
- Reconocimiento de matrículas
- Análisis de fuentes abiertas (OSINT)

Artículos relacionados

Año	Artículo	Referencia
2009	Detecting influenza epidemics using search engine	https://doi.org/10.1038/nature07634

2011	An intelligent weapon selection method for aircraft weapon control system	https://doi.org/10.1109/ICEICE.2011.5778179
2013	Research on the platform system of military chess computer game	https://doi.org/10.1109/CCDC.2013.6561216
2014	An open source framework to add spatial extent and geospatial visibility to Big Data	https://doi.ieeecomputersociety.org/10.1109/BigData.2014.7004495
2014	Optimization ELM Based on Rough Set for Predicting the Label of Military Simulation Data	https://doi.org/10.1155/2014/706178
2015	Big Data and industrial Internet of Things for the maritime industry in Northwestern Norway	https://doi.org/10.1109/TENCON.2015.7372918
2015	Construction of FuzzyFind Dictionary using Golay Coding Transformation for Searching Applications	https://doi.org/10.48550/arXiv.1503.06483
2015	Integrated Information Supporting Systems in Big Data Applications	https://doi.org/10.1109/ICICSE.2015.12
2015	Military Simulation Big Data Background, State of the Art, and Challenges	https://doi.org/10.1155/2015/298356
2015	pvsR: An Open Source Interface to Big Data on the American Political Sphere	https://doi.org/10.1371/journal.pone.0130501
2015	Statistical Modeling and Visualizing Open Big Data Using a Terrorism Case Study	https://doi.org/10.1109/FiCloud.2015.15
2016	Adaptive immune genetic algorithm for weapon system portfolio optimization in military Big Data environment	https://doi.org/10.1007/s10586-016-0596-3
2016	A New Learning Method Study of Military Simulation Data	https://doi.org/10.1007/978-981-10-2666-9_38
2016	Outdoor Air Quality Level Inference via Surveillance Cameras	https://doi.org/10.1155/2016/9825820
2016	A New Data Representation Based on Training Data Characteristics to Extract Drug Named-Entity in Medical Text	https://doi.org/10.1155/2016/3483528
2016	A Review on Application of Data Mining Techniques to Combat Natural Disasters	https://doi.org/10.1016/j.asej.2016.01.012
2016	Big Data and the Military: First World War Personnel Records in Australia, Britain, Canada, New Zealand and British Africa	https://doi.org/10.1080/1031461X.2016.1205639
2016	Cloud Computing Intelligent Data-Driven Model: Connecting the Dots to Combat Global Terrorism	https://doi.org/10.1109/BigDataCongress.2016.69
2016	Genetic Fuzzy based Artificial Intelligence for Unmanned Combat Aerial	http://dx.doi.org/10.4172/2167-0374.1000144
2016	Open Big Data infrastructures to everyone	https://doi.org/10.1109/BigData.2016.7840841
2016	Research on counter-terrorism based on Big Data	https://doi.org/10.1109/ICBDA.2016.7509788
2016	Research on Big Data Real-Time Public Opinion Monitoring under the Double Cloud Architecture	https://doi.org/10.1109/BigMM.2016.35

2017	Big Data analyses reveal patterns and drivers of the movements of southern elephant seals	https://doi.org/10.1038/s41598-017-00165-0
2017	Identification of Objects Based on Generalized Amplitude-Phase Images Statistical Models	https://doi.org/10.1007/978-3-319-67229-8_6
2017	Leveraging Big Data to combat terrorism in developing countries	https://doi.org/10.1109/ICTAS.2017.7920662
2017	Toward Approaches to Big Data Analysis for Terroristic Behavior Identification: Child Soldiers in Illegal Armed Groups During the Conflict in the Donbas Region (East Ukraine)	http://dx.doi.org/10.4018/IJCWT.2017010101
2017	The Thinking of Digitization Management of Weapon Equipment Development in Big Data Era	https://doi.org/10.1109/ICCCBDA.2017.7951904
2017	Towards development of spark based agricultural information system including geo-spatial data	https://doi.org/10.1109/BigData.2017.8258336
2017	Research on weapon system portfolio selection based on combat network modeling	https://doi.org/10.1109/SYSCON.2017.7934733
2017	Using Deep Networks for Drone Detection	https://doi.org/10.48550/arXiv.1706.05726
2018	A Novel Approach to Spam Filtering Using Semantic Based Naive Bayesian Classifier in Text Analytics	https://doi.org/10.1007/978-981-13-1498-8_27
2018	Analytics for Military Training in Virtual Reality Environments	https://doi.org/10.1201/9780429445491
2018	Autoregressive Bayesian Networks for Information Validation and Amendment in Military Applications	https://doi.org/10.1201/9780429445491
2018	Applying Big Data Technologies to Detect Cases of Money Laundering and Counter Financing of Terrorism	https://doi.org/10.1109/W-FiCloud.2018.00017
2018	A Virtual Reality Soldier Simulator with Body Area Networks for Team Training	https://doi.org/10.3390/s19030451
2018	Big Data Tools in Processing Information from Open Sources	https://doi.org/10.1109/SAIC.2018.8516800
2018	Bayesian Networks for Descriptive Analytics in Military Equipment Applications	https://doi.org/10.1201/9780429445491
2018	Big Data Approach for Epidemiology and Prevention of HIV/AIDS	https://doi.org/10.1007/978-981-13-1498-8_21
2018	Classification of Military Aircraft in Real-time Radar Systems based on Supervised Machine Learning with Labelled ADS-B Data	https://doi.org/10.1109/SDF.2018.8547077
2018	Context Level Entity Extraction Using Text Analytics with Big Data Tools	https://doi.org/10.1007/978-981-13-1498-8_32
2018	Data Analytics for Electric Power and Energy Applications	https://doi.org/10.1201/9780429445491
2018	Deep Learning for Military Image Captioning	https://doi.org/10.23919/ICIF.2018.8455321
2018	Detecting Port Scan Attempts with Comparative Analysis of Deep Learning and Support Vector Machine Algorithms	https://doi.org/10.1109/IBIGDELFT.2018.8625370

2018	Exploring Student Migration in Rural Region of Bangladesh	https://doi.org/10.1007/978-981-13-1498-8_3
2018	Mining Patterns with Durations from E-Commerce Dataset	https://doi.org/10.1007/978-3-030-05411-3_49
2018	Military Object Real-Time Detection Technology Combined with Visual Salience and Psychology	https://doi.org/10.3390/electronics7100216
2018	Harnessing Single Board Computers for Military Data Analytics	https://doi.org/10.1201/9780429445491
2018	The Evolution of Environmental Data Analytics in Military Operations	https://doi.org/10.1201/9780429445491
2018	The Role of Big Data in Intelligent Combat Command	https://dx.doi.org/10.2991/cecs-18.2018.27
2018	The Big Data Imperative-Air Force Intelligence for the Information Age	https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-32_Issue-1/F-Hamilton_Kreuzer.pdf
2018	Text-based Sentiment Analysis and Music Emotion Recognition	https://doi.org/10.48550/arXiv.1810.03031
2018	Research on Terrorism, 2007–2016: A Review of Data, Methods, and Authorship	https://doi.org/10.1080/09546553.2018.1439023
2018	Simple Implementation of Criminal Investigation using Call Data Records (CDRs) through Big Data Technology	https://doi.org/10.1109/ICSCET.2018.8537389
2018	Spam Detection in SMS Based on Feature Selection Techniques	https://doi.org/10.1007/978-981-13-1498-8_49
2018	Using Deep Convolutional Neural Network Architectures for Object Classification and Detection Within X-Ray Baggage Security Imagery	https://doi.org/10.1109/TIFS.2018.2812196
2019	A Case Study of Intra-library Privacy Issues on Android GPS Navigation Apps	https://doi.org/10.1007/978-3-030-37545-4_3
2019	An analysis of Crime data under Apache Pig on Big Data	https://doi.org/10.1109/I-SMAC47947.2019.9032565
2019	An Automated Text Mining Approach for Classifying Mental-Ill Health Incidents from Police Incident Logs for Data-Driven Intelligence	https://doi.org/10.1109/SMC.2019.8914240
2019	A Novel Linear Spectrum Frequency Feature Extraction Technique for Warship Radio Noise Based on Complete Ensemble Empirical Mode Decomposition with Adaptive Noise, Duffing Chaotic Oscillator, and Weighted-Permutation Entropy	https://doi.org/10.3390/e21050507
2019	A Heterogeneous Battlefield Situation Information Sharing Method Based on Content	https://doi.org/10.3390/app10010184
2019	Battlefield Target Aggregation Behavior Recognition Model Based on Multi-Scale Feature Fusion	https://doi.org/10.3390/sym11060761

2019	Big Data Analytics: From Threatening Privacy to Challenging Democracy	https://doi.org/10.1007/978-3-030-37545-4_1
2019	Big Data Analytics and Mining for Effective Visualization and Trends Forecasting of Crime Data	https://doi.org/10.1109/ACCESS.2019.2930410
2019	Detecting Pickpocketing Offenders by Analyzing Beijing Metro Subway Data	https://doi.org/10.1109/ICBDA.2019.8712833
2019	LPI Radar Waveform Recognition Based on CNN and TPOT	https://doi.org/10.3390/sym11050725
2019	Optimal Target Assignment with Seamless Handovers for Networked Radars	https://doi.org/10.3390/s19204555
2019	The Design and Realization of Dynamic Evaluation Strategy of Pieces in Military Chess Game System	https://doi.org/10.1109/CCDC.2019.8832609
2020	Defensa 4.0: Internet de las Cosas en Sistemas de Batalla (IoBT) en Defensa Naval	https://www.researchgate.net/publication/341256197_Defensa_40_Internet_de_las_Cosas_en_Sistemas_de_Batalla_IoBT_en_Defensa_Naval
2020	A Framework of Abnormal Behavior Detection and Classification Based on Big Trajectory Data for Mobile Networks	https://doi.org/10.1155/2020/8858444
2020	Analysis Model of Terrorist Attacks Based on Big Data	https://doi.org/10.1109/CCDC49329.2020.9164626
2020	Application of Data Science to Discover Violence-Related Issues in Iraq	https://doi.org/10.48550/arXiv.2006.07980
2020	Application of Artificial Intelligence in Military From Projects View	https://doi.org/10.1109/BigDIA51454.2020.00026
2020	Application of Artificial Intelligence in Airborne Weapon Combat Identification Simulation Test	https://doi.org/10.1109/ICBAIE49996.2020.00049
2020	Artificial Intelligence in the Defence Sector	https://doi.org/10.1007/978-3-030-70740-8_17
2020	Brain Drain and Brain Gain in Russia: Analyzing International Migration of Researchers by Discipline using Scopus Bibliometric Data 1996-2020	https://doi.org/10.1007/s11192-021-04091-x
2020	Data Analysis of Various Terrorism Activities Using Big Data Approaches on Global Terrorism Database	https://doi.org/10.1109/PDGC50313.2020.9315784
2020	Emotional Analysis of Netizens Based on Big Data of Network Petition	https://doi.org/10.1109/AIEA51086.2020.00053
2020	Hybrid Malware Classification Method Using Segmentation-Based Fractal Texture Analysis and Deep Convolution Neural Network Features	https://doi.org/10.3390/app10144966
2020	Firearm Detection via Convolutional Neural Networks: Comparing a Semantic Segmentation Model Against End-to-End Solutions	https://doi.org/10.48550/arXiv.2012.09662

2020	Internet of Underwater Things and Big Marine Data Analytics – A Comprehensive Survey	https://doi.org/10.1109/COMST.2021.3053118
2020	Intelligent Design for Simulation Models of Weapon Systems Using a Mathematical Structure and Case-Based Reasoning	https://doi.org/10.3390/app10217642
2020	Higher Order Temporal Analysis of Global Terrorism Data	https://doi.org/10.48550/arXiv.2005.14002
2020	Human migration: the Big Data perspective	https://doi.org/10.1007/s41060-020-00213-5
2020	License Plate Character Segmentation Algorithm Based on Improved Regression Model	https://doi.org/10.1088/1742-6596/1453/1/012030
2020	"When they say weed causes depression, but it's your fav antidepressant": Knowledge-aware Attention Framework for Relationship Extraction	https://doi.org/10.1371/journal.pone.0248299
2020	A Comparative Analysis of dot NET-Based and Open Source Platforms for Ontologies Development	https://doi.org/10.1109/icABCD49160.2020.9183887
2020	Development and Application of Big Data in the Field of Satellite Navigation	https://doi.org/10.1155/2021/8850350
2020	La inteligencia artificial en el campo de batalla (Usos militares de la inteligencia artificial, la automatización y la robótica (IAA&R))	https://publicaciones.defensa.gob.es/usos-militares-de-la-inteligencia-artificial-la-automatizacion-y-la-robotica-iaa-r-libros-ebook.html
2020	Models and algorithms for solving problems associated with large amounts of data in the military sphere	https://doi.org/10.1109/ICISCT50599.2020.9351506
2020	Public Transport GPS Probe and Rail Gate Data for Assessing the Pattern of Human Mobility in the Bangkok Metropolitan Region, Thailand	https://doi.org/10.3390/su13042178
2020	Real-time License plate number detection based on image contour	https://doi.org/10.1088/1742-6596/1650/3/032073
2020	Research Progress on Ship Anomaly Detection Based on Big Data	https://doi.org/10.1109/ICSESS49938.2020.9237642
2020	Research on the Development of Maritime and Air Intelligence Big Data	https://doi.org/10.1109/BigDIA51454.2020.00065
2020	Research on the Colors of Military Symbols in Digital Situation Maps Based on Event-Related Potential Technology	https://doi.org/10.3390/ijgi9070420
2020	Service-oriented weapon systems of system portfolio selection method	https://doi.org/10.23919/JSEE.2020.000034

2020	Study on the Evaluation Module of Ship Operation Management under Big Data View	https://doi.org/10.1109/ECIT50008.2020.00027
2020	Weapon Equipment System Value Analysis Method Based on Massive Text Data	https://doi.org/10.1109/BigDIA51454.2020.00059
2020	Weapon system portfolio selection based on structural robustness	https://doi.org/10.23919/JSEE.2020.000094
2020	Use of open data in Ukraine: some important aspects	https://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/article/view/1564
2021	A Big Data intelligence marketplace and secure analytics experimentation platform for the aviation industry	https://doi.org/10.48550/arXiv.2111.09872
2021	An Approach to Spatiotemporal Trajectory Clustering Based on Community Detection	https://doi.org/10.1155/2021/5582341
2021	A Cloud-Based Robot Framework for Indoor Object Identification Using Unsupervised Segmentation Technique and Convolution Neural Network (CNN)	https://doi.org/10.1007/978-3-030-79463-7_17
2021	Air Combat Simulation System for Airborne Weapon Equipment Verification	https://doi.org/10.1109/ICMAE52228.2021.9522497
2021	Air Quality and Active Transportation Modes: A Spatiotemporal Concurrence Analysis in Guadalajara, Mexico	https://doi.org/10.3390/su132413904
2021	An Analysis of Global News Coverage of Refugees Using a Big Data Approach	https://doi.org/10.1007/978-3-030-80387-2_11
2021	An Efficient Approach for Multiple Moving Objects Tracking with Occlusion	https://doi.org/10.1007/978-981-16-1781-2_62
2021	Augmented Audio Data in Improving Speech Emotion Classification Tasks	https://doi.org/10.1007/978-3-030-79463-7_30
2021	Automatic Term Recognition Method for Military Domain	https://doi.org/10.1088/1742-6596/2078/1/012031
2021	Data Analysis Method of Intelligent Analysis Platform for Big Data of Film and Television	https://doi.org/10.1155/2021/9947832
2021	Detecting Fake Points of Interest from Location Data	https://doi.org/10.48550/arXiv.2111.06003
2021	Deep Reinforcement Learning for Intelligent Dual-UAV Reconnaissance Mission Planning	https://doi.org/10.3390/electronics11132031
2021	Facial Emotion Recognition from an Unmanned Flying Social Robot for Home Care of Dependent People	https://doi.org/10.3390/electronics10070868
2021	Improving Human Emotion Recognition from Emotive Videos Using Geometric Data Augmentation	https://doi.org/10.1007/978-3-030-79463-7_13
2021	Fusing BERT and BiLSTM Model to Extract the Weaponry Entity	https://doi.org/10.1007/978-3-030-77428-8_8
2021	Graph-Based Horizon Line Detection for UAV Navigation	https://doi.org/10.1109/JSTARS.2021.3126586

2021	Green Wave Zone Evaluation Method Based on Electronic Police Data	https://doi.org/10.1109/ICBDIE52740.2021.00043
2021	IMAGE-2-AQI: Aware of the Surrounding Air Qualification by a Few Images	https://doi.org/10.1007/978-3-030-79463-7_28
2021	Machine Learning for the Dynamic Positioning of UAVs for Extended Connectivity	https://doi.org/10.3390/s21134618
2021	Quantitative Analysis and Prediction of Global Terrorist Attacks Based on Machine Learning	https://doi.org/10.1155/2021/7890923
2021	Query by Humming for Song Identification Using Voice Isolation	https://doi.org/10.1007/978-3-030-79463-7_27
2021	Heterogeneous Noisy Short Signal Camouflage in Multi-Domain Environment Decision-Making	https://doi.org/10.48550/arXiv.2106.02044
2021	Robust Approach to Supervised Deep Neural Network Training for Real-Time Object Classification in Cluttered Indoor Environment	https://doi.org/10.3390/app11157148
2021	Research on Classification of Travel Time for Electronic Police Based on the DBSCAN Algorithm	https://doi.org/10.1109/ICBDIE52740.2021.00064
2021	Research On Evaluation Method Used To Quality Performance Of Missile Weapon Based On Rough Set Rule Extraction	https://doi.org/10.1109/CIS.2012.83
2021	Research on Intelligent Identification Method for Access Equipment of Grid Information System	https://doi.org/10.1088/1742-6596/1792/1/012015
2021	Research on Encrypted Text Classification Based on Natural Language Processing	https://doi.org/10.1088/1742-6596/1792/1/012001
2021	Research on the Algorithm of Locating and Cutting in License Plate Character Extraction	https://doi.org/10.1088/1742-6596/1792/1/012073
2021	Ship Classification Based on Improved Convolutional Neural Network Architecture for Intelligent Transport Systems	https://doi.org/10.3390/info12080302
2021	Deep Learning Models for Passive Sonar Signal Classification of Military Data	https://doi.org/10.3390/rs14112648
2021	Towards an Open Format for Scalable System Telemetry	https://doi.org/10.48550/arXiv.2101.10474
2021	MRE: A Military Relation Extraction Model Based on BiGRU and Multi-Head Attention	https://doi.org/10.3390/sym13091742
2021	Open Source Control Device for Industry 4.0 Based on RAMI 4.0	https://doi.org/10.3390/electronics10070869
2021	Edge Artificial Intelligence for 6G Vision, Enabling Technologies, and Applications	https://doi.org/10.48550/arXiv.2111.12444
2021	The Text Classification Based on Big Data Analysis for Keyword Definition Using Stemming	https://doi.org/10.1109/CSIT52700.2021.9648764

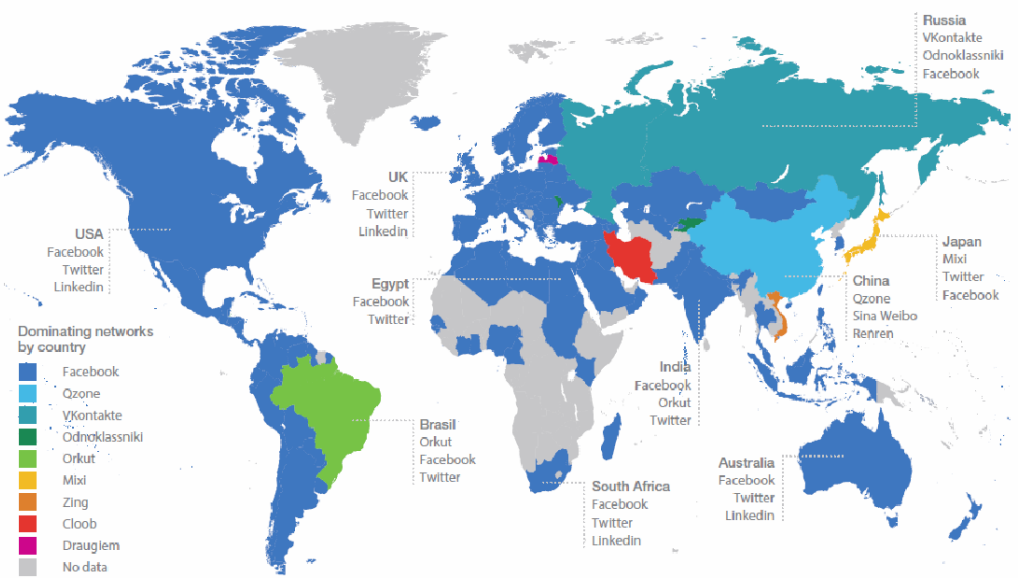
2021	Simulated Data Generation Through Algorithmic Force Coefficient Estimation for AI-Based Robotic Projectile Launch Modeling	https://doi.org/10.48550/arXiv.2105.12833
2021	The Investigation of Different Loss Functions with Capsule Networks for Speech Emotion Recognition	https://doi.org/10.1155/2021/9916915
2021	Unmanned Aerial Vehicles for the Future Classification Challenges and Opportunities	https://doi.org/10.1109/icABCD51485.2021.9519367
2022	A Novel Method of Generating Geospatial Intelligence from Social Media Posts of Political Leaders	https://doi.org/10.3390/info13030120
2022	Position-Aware Guided Hiding Data Scheme with Reversibility and Adaptivity for Dual Images	https://doi.org/10.3390/sym14030509
2022	State of the Art Solutions for Privacy Preserving Machine Learning in the Medical Context	https://doi.org/10.48550/arXiv.2201.11406
2022	Data-driven behavioural modelling for military applications	http://dx.doi.org/10.46713/jdst.004.02
2022	Instance segmentation convolutional neural network based on multi-scale attention mechanism	https://doi.org/10.1371/journal.pone.0263134
2022	Travel similarity estimation and clustering - Big Data and Mobility as a Service (Book)	https://www.sciencedirect.com/book/9780323901697/big-data-and-mobility-as-a-service
2022	Data fusion technologies for MaaS - Big Data and Mobility as a Service (Book)	https://www.sciencedirect.com/book/9780323901697/big-data-and-mobility-as-a-service
2022	Data-driven optimization technologies for MaaS - Big Data and Mobility as a Service (Book)	https://www.sciencedirect.com/book/9780323901697/big-data-and-mobility-as-a-service
2022	Data-driven estimation for urban travel shareability - Big Data and Mobility as a Service (Book)	https://www.sciencedirect.com/book/9780323901697/big-data-and-mobility-as-a-service
2022	Data mining technologies for Mobility-as-a-Service (MaaS) - Big Data and Mobility as a Service (Book)	https://www.sciencedirect.com/book/9780323901697/big-data-and-mobility-as-a-service
2022	MaaS system visualization - Big Data and Mobility as a Service (Book)	https://www.sciencedirect.com/book/9780323901697/big-data-and-mobility-as-a-service
2022	Object recognition datasets and challenges: A review	https://doi.org/10.1016/j.neucom.2022.01.022

TABLA 5: ARTÍCULOS INTELIGENCIA

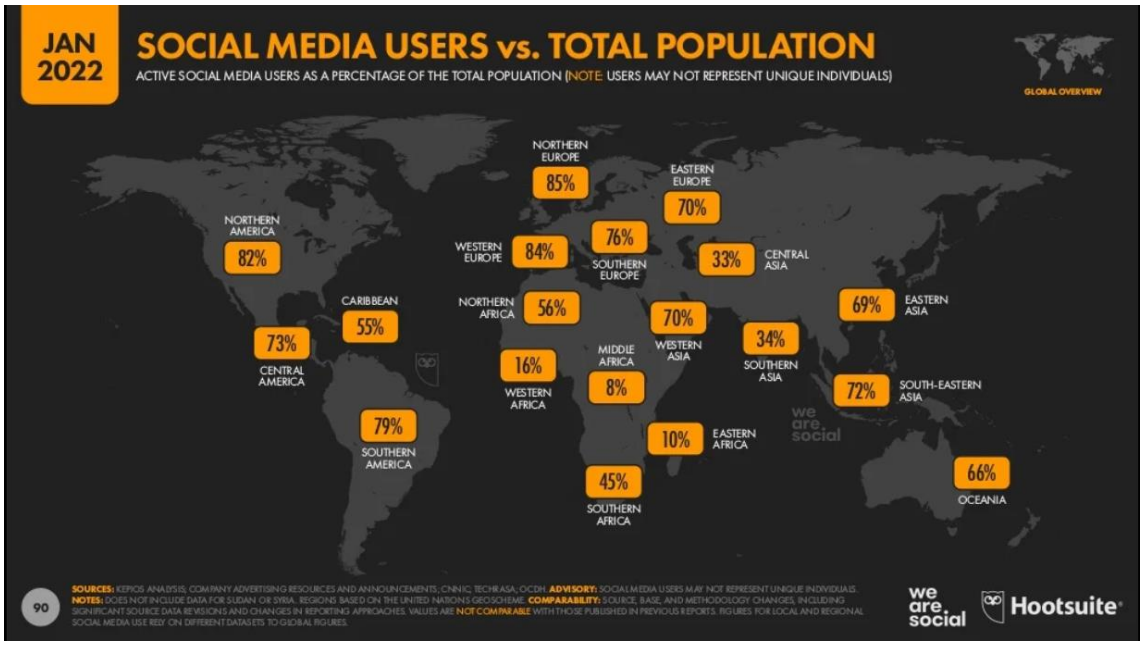
3.1.3. Análisis de Redes sociales y Fake news

Como se ha comentado anteriormente, las redes sociales y el contenido multimedia social, pueden ser de gran utilidad a la hora de descubrir temas en auge además de las opiniones de las personas respecto a distintos aspectos que pueden provocar confrontaciones además de movilizar a grandes multitudes y provocar cambios culturales como ha sucedido en el mundo árabe [109].

El impacto de las redes sociales es a nivel mundial como se puede observar en los siguientes mapas, con mayor implicación de usuarios o de ciertas redes o aplicaciones dependiendo de la región.

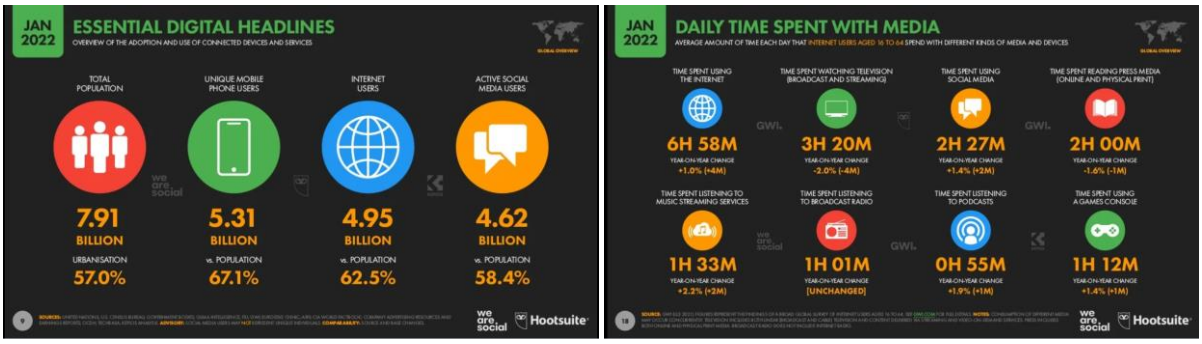


LAS REDES SOCIALES EN EL MUNDO EN 2012 [110]



USUARIOS DE SOCIAL MEDIA VS. POBLACIÓN TOTAL [111]

Así mismo, a enero del 2022 hay más de 4.95 billones de usuarios de internet y 4.62 de usuarios de redes sociales los cuales en media emplean bastantes horas en contenido multimedia.



TITULAR DIGITAL ESENCIAL Y TIEMPO EMPLEADO EN MULTIMEDIA [111]

Las fake news o noticias falsas difunden deliberadamente información falsa en forma de artículo, imagen o vídeo que se presenta real y cuyo objetivo es conseguir manipular y escandalizar a la opinión pública. Las fake news pueden ser creadas tanto por individuos, como por grupos, que actúan en su propio interés o en nombre de otros, teniendo objetivos personales**,** políticos o económicos. [112]

Las fake news suelen aparecer con bastante frecuencia mediante titulares falsos, desinformación liberada, publicaciones virales y sátira y suelen ser los usuarios de las redes sociales o los *social bots* los encargados de difundir *fake news*, comentando, compartiendo o retuiteando el contenido.

El uso de las redes sociales en combinación con las fake news se puede considerar como una amenaza hibrida dado que combina de forma coherente y coordinada fuerzas irregulares, actos criminales y elementos de guerra de quinta generación debido a los desarrollos tecnológicos y la masificación de estos. [113]

Las estrategias que promueven el uso de amenazas híbridas pretenden, en última instancia, dificultar, retrasar e impedir la oportuna toma de decisiones y socavar la capacidad de una nación o de una alianza para responder a dicha amenaza de forma rápida, firme y eficaz, de acuerdo con el artículo “La inteligencia artificial en el campo de la información: su utilización en apoyo a la desinformación” que se encuentra en una publicación realizada por el Centro Conjunto de Desarrollo de Conceptos bajo el título “Usos militares de la inteligencia artificial, la automatización y la robótica (IAA&R)” [114]. Actualmente, existen diversos tipos de acciones llevados a cabo en el campo de la información relacionadas con las redes sociales y la desinformación como son:

- Obtención de datos personales de posibles objetivos (Reconocimiento): mediante la utilización abusiva o improcedente de los algoritmos de redes sociales y motores de búsqueda para a partir de los datos generados por los usuarios de las plataformas digitales obtener una imagen muy precisa de su comportamiento, patrones de consumo, o para promover cierto tipo de información y eliminar otra, pudiendo ser utilizados para amplificar el impacto de las campañas de desinformación de una manera más precisa y eficaz.
- Generación de contenidos (Preparación del ataque): generación de imágenes, audios y videos creíbles pero falsos.
- Difusión de contenidos (Ejecución del ataque): el empleo de perfiles digitales falsificados mediante la simulación maliciosa de cuentas y perfiles reales, creación de perfiles digitales falsos o parodias y el hackeo de perfiles digitales. También empleando bots sociales ilegitimos que son es un tipo particular de programa manejado en las redes

sociales que simula ser un usuario humano, siendo capaz de suministrar respuestas automáticas creíbles. Existen diversos tipos de bots: bots de propaganda, bots de seguidores, bots obstaculizadores (roadblocks) y bots de inteligencia artificial.

La detección de noticias falsas en las redes sociales es un proceso en capas que implica análisis de los contenidos de las noticias para determinar la veracidad de las noticias. El contenido de las noticias puede contener información en diversos formatos como texto, imagen, video, audio, etc. Se ha de tener en cuenta que la combinación de diferentes tipos de datos dificulta el proceso al no poder tratarlos de la misma manera. Adicionalmente, se espera que los datos sin procesar recopilados no estén estructurados y falten valores en los datos, por tanto, el pre procesamiento de datos sin procesar es extremadamente importante para limpiar y estructurar los datos antes de introducirlos en los modelos de detección, debido a que las noticias falsas producen grandes, incompletos, no estructurados y ruidosos datos.

Aunque el empleo de las redes sociales puede verse como una amenaza hibrida también se pueden emplear para la detección y prevención del bullying o las reacciones adversas a medicamentos y la prevención de desastres naturales o mediante el uso de tecnologías del Big Data.

El análisis del uso que hacen las autoridades canarias de las redes sociales, en concreto Twitter, en materia de prevención de riesgos naturales, y en segundo lugar, analizar la gestión de información surgida de las redes sociales en las cuentas de Twitter de las autoridades canarias durante los incendios de agosto de 2019 tiene como objetivos el artículo de investigación “Social-Media Analysis for Disaster Prevention: Forest Fire in Artenara and Valleseco, Canary Islands” [115]. Los autores del artículo tras realizar el análisis empleando Big Data, concluyen que las autoridades canarias no usaron mensajes para prevenir futuros desastres naturales, sino que utilizaron una estrategia de comunicación digital únicamente sobre la base de información y actualizaciones en vivo sobre el desarrollo de los incendios forestales. Por ello, destacan la necesidad de investigar a fondo cómo se pueden emplear las redes sociales, y en especial Twitter, como herramientas para sensibilizar a los ciudadanos a ser proactivos en la prevención de desastres naturales, es decir, cómo las autoridades pueden superar la gestión reactiva de las redes sociales en para fortalecer su capacidad de uso proactivo de las redes sociales. Conjuntamente, el uso de las redes sociales por parte de una administración pública y su eficacia para comunicarse con los ciudadanos de forma proactiva requieren un cambio en la cultura organizativa de esta administración considerando que las redes sociales permiten que diferentes actores establezcan sinergias de conocimiento para fortalecer la inteligencia colectiva. Asimismo, plantean unas recomendaciones sobre el manejo de las redes sociales por parte de las autoridades durante la ocurrencia de desastres naturales como son:

- La gestión de las redes sociales durante una emergencia debe priorizar los mensajes informativos utilizando los datos disponibles de las autoridades para anticipar el desarrollo de un desastre y alertar a la ciudadanía.
- Las autoridades deben convertir la enorme cantidad de datos disponibles en un lenguaje claro y directo acompañado principalmente de elementos audiovisuales que hagan comprensible la información para todos los públicos. Es decir, transformar el lenguaje del Big Data en información que los ciudadanos entiendan.
- El análisis de las bases de datos de Twitter es una oportunidad única para que los centros de atención temprana de desastres mapeen las crisis en tiempo real, desde sus orígenes hasta el posterior análisis del impacto de los eventos catastróficos.

En la actualidad, la Policía Nacional tiene perfiles en distintas redes sociales dirigido por el Grupo de Redes Sociales del Cuerpo Nacional de Policía y las emplean para la que los ciudadanos puedan contactar con ellos, además de proveer información verídica y así conseguir combatir los bulos y las fake news cortando su difusión. [116] [117]

Twitter	Facebook	Instagram
• Policía Nacional ESP, 3,17 millones.	• Policía Federal BR, 2,74 millones.	• Policía Federal BR, 653.000.
• FBI USA, 2,42 millones.	• FBI USA, 2,37 millones.	• Policía Nacional ESP, 390.000.
• Guardia Civil ESP, 1,27 millones.	• Policía Federal MEX, 918.000.	• NYDP USA, 331.000.
• Policía Federal BR, 1,24 millones.	• NYPD USA, 820.000.	• Guardia Civil ESP, 184.000.
• Scotland Yard RU, 1,21 millones.	• Gendarmerie FR, 750.000.	• FBI USA, 182.000.
• NYPD USA, 602.000.	• Policía Nacional ESP, 700.000.	• Polizia di Stato IT, 125.000.
• Mossos ESP, 513.000.	• Police Nationale FR, 689.000.	• Mossos ESP, 115.000.
• Police Nationale FR, 450.000.	• Polizia di Stato IT, 464.000.	• Gendarmerie FR, 85.900.
• Gendarmerie FR, 423.000.	• Australian Federal Police, 416.000.	• Bundespolizei ALE, 70.500.
• Policía Municipal Madrid ESP, 370.000.	• Mossos ESP, 335.000.	• Gendarmería ARG, 42.500.
• Policía Federal MEX, 351.000.	• Policía Federal ARG, 305.000.	• Scotland Yard RU, 39.800.
• Policía Montada CAN, 223.000.	• Guardia Civil ESP, 270.000.	• Police Nationale FR, 39.200.
• National Police Agency JAP, 220.000.	• Gendarmería ARG, 143.000.	• Policía Federal MEX, 26.500.
• Bundespolizei ALE, 190.000.	• Policía Montada CAN, 219.000.	• Australian Federal Police, 24.300.
• Interpol, 149.000.	• Scotland Yard RU, 211.000.	• Policía Federal ARG, 22.200.
• Policía Federal ARG, 112.000.	• Interpol, 124.000.	• Policía Montada CAN, 19.700.
• Gendarmería ARG, 85.900.	• Bundespolizei ALE, 77.000.	• Interpol, 18.700.
• Polizia di Stato IT, 81.800.	• Europol, 61.500.	• Guardia Urbana Barcelona ESP, 14.000.
• Europol, 81.500.	• Guardia Urbana Barcelona ESP, 16.000.	• Policía Municipal Madrid ESP, 11.000.
• Guardia Urbana Barcelona ESP, 53.000.	• Policía Municipal Madrid ESP, 12.000.	• Europol, 10.500.
• Australian Federal Police, 26.100.	• National Police Agency JAP, 2.000.	• Policía Foral ESP, 1.700.
• Ertzaintza ESP, 25.400.	• Policía Foral ESP, 1.800.	
• Policía Foral ESP, 23.900.		
• Policía Canaria ESP, 8.328.		

RANKING DE POLICÍAS POR NÚMERO DE SEGUIDORES EN REDES SOCIALES [117]

Como aplicaciones más significativas del empleo del Big Data en redes sociales y “fake news” se encuentran:

- Detección de artículos falsos
- Análisis de redes sociales para la prevención de desastres
- Detección de comunidades extremistas
- Análisis de sentimientos
- Detección de suicidios
- Análisis de cómo los rumores se extienden
- Predicción de la difusión de la información
- Predicción del tráfico mediante redes sociales
- Detección de reacciones adversas a drogas en las redes sociales
- Medición del impacto de los spammers

A continuación, se presentan una selección de artículos relacionados con las redes sociales y las fake news.

Artículos relacionados

Año	Artículo	Referencia

2012	Secure Military Social Networking and Rapid Sensemaking in Domain Specific Concept Systems: Research Issues and Future Solutions	https://doi.org/10.3390/fi4010253
2014	A New Approach for Finding Cloned Profiles in Online Social Networks	https://doi.org/10.48550/arXiv.1406.7377
2014	Discovering spread mode of public opinions in incidents and mapping it with GIS: A case on big geospatial data analytics	https://doi.org/10.1109/Agro-Geoinformatics.2014.6910597
2015	A "Big Data" approach to HIV epidemiology and prevention	https://doi.org/10.1016/j.ypmed.2014.11.002
2016	Examining ISIS Support and Opposition Networks on Twitter	https://doi.org/10.7249/RR1328
2016	Fine-grained Mining of Illicit Drug Use Patterns Using Social Multimedia Data from Instagram	https://doi.org/10.1109/BigData.2016.7840812
2017	Identifying Unsafe Videos on Online Public Media using Real-time Crowdsourcing	https://doi.org/10.48550/arXiv.1708.09654
2017	Social Bots Human-Like by Means of Human Control?	https://doi.org/10.48550/arXiv.1706.07624
2017	Fake News Detection on Social Media: A Data Mining Perspective	https://doi.org/10.48550/arXiv.1708.01967
2017	Fighting fake news spread in online social networks: Actual trends and future research directions	https://doi.org/10.1109/BigData.2017.8258484
2017	Considering the ethics of Big Data research: A case of Twitter and ISIS/ISIL	https://doi.org/10.1371/journal.pone.0187155
2017	Online extremism and the communities that sustain it Detecting the ISIS supporting community on Twitter	https://doi.org/10.1371/journal.pone.0181405
2017	On the relevance of social media platforms in predicting the volume and patterns of web defacement attacks	https://doi.org/10.1109/BigData.2017.8258513
2018	Entity Resolution in Online Multiple Social Networks (@Facebook and LinkedIn)	https://doi.org/10.1007/978-981-13-1498-8_20
2018	Fake News Detection Enhancement with Data Imputation	https://doi.org/10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00042
2018	Fake News: A Method to Measure Distance from Fact	https://doi.org/10.1109/BigData.2018.8621951
2018	Cyberbullying and Self-harm in Adolescence, an Assessment of Detection, Prevention, and Recovery from Forum	https://doi.org/10.1007/978-981-13-1498-8_44
2018	Community Detection Based Tweet Summarization	https://doi.org/10.1007/978-981-13-1498-8_70
2018	Detecting Fake News in Social Media Networks	https://doi.org/10.1016/j.procs.2018.10.171
2018	Summarizing Microblogs During Emergency Events: A Comparison of Extractive Summarization Algorithms	https://doi.org/10.1007/978-981-13-1498-8_76
2018	A Comparative Study on Cluster Analysis of Microblogging Data	https://doi.org/10.1007/978-981-13-1498-8_77

2018	Predicting Information Diffusion in Online Social Platforms: A Twitter Case Study	https://doi.org/10.1007/978-3-030-05411-3_33
2018	Social Media Analysis of User's Responses to Terrorism Using Sentiment Analysis and Text Mining	https://doi.org/10.1016/j.procs.2018.10.297
2018	Behavior-Interior-Aware User Preference Analysis Based on Social Networks	https://doi.org/10.1155/2018/7371209
2018	Supervised Learning for Suicidal Ideation Detection in Online User Content	https://doi.org/10.1155/2018/6157249
2018	Weibo Attention and Stock Market Performance: Some Empirical Evidence	https://doi.org/10.1155/2018/9571848
2018	Segregation of Similar and Dissimilar Live RSS News Feeds Based on Similarity Measures	https://doi.org/10.1007/978-981-13-1274-8_26
2019	A Survey on Automatic Fake News Identification Techniques for Online and Socially Produced Data	https://doi.org/10.1109/ICCCEEE46830.2019.9070857
2019	Can EU Data Protection Legislation Help to Counter "Fake News" and Other Threats to Democracy?	https://doi.org/10.1007/978-3-030-37545-4_15
2019	Detecting Fake News Articles	https://doi.org/10.1109/BigData47090.2019.9005980
2019	Investigating the Impact of Podcast Learning in Health via Social Network Analysis	https://doi.org/10.1007/978-3-030-16187-3_48
2019	How Does Fake News Spread: Raising Awareness & Educating the Public with a Simulation Tool	https://doi.org/10.1109/BigData47090.2019.9005953
2019	Mining Social Media Content to Predict Peer Trust Level in Social Networks	https://www.researchgate.net/publication/342999932_A_Survey_on_Trust_Prediction_in_Online_Social_Networks
2019	Misinformation Harms During Crises: When The Human And Machine Loops Interact	https://doi.org/10.1109/BigData47090.2019.9005561
2019	Rumor Detection on Time-Series of Tweets via Deep Learning	https://doi.org/10.1109/MILCOM47813.2019.9020895
2019	The Spread of Disinformation on the Web: An Examination of Memes on Social Networking	https://doi.org/10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00256
2019	The Role of Social Media in Crisis Situation Management: A Survey	https://doi.org/10.1007/978-981-13-1498-8_39
2019	Towards Designing a Knowledge Graph-Based Framework for Investigating and Preventing Crime on Online Social Networks	https://doi.org/10.1007/978-3-030-37545-4_12
2020	#Coronavirus or #Chinesevirus?!: Understanding the negative sentiment reflected in Tweets with racist hashtags across the development of COVID-19	https://doi.org/10.48550/arXiv.2005.08224

2020	Adverse Drug Reaction Detection Using Data Mining Techniques: A Review Article	https://doi.org/10.1109/ICCKE50421.2020.9303709
2020	FakeSafe Human Level Data Protection by Disinformation Mapping using Cycle-consistent Adversarial Network	https://doi.org/10.48550/arXiv.2011.11278
2020	From Twitter to traffic predictor: Next-day morning traffic prediction using social media data	https://doi.org/10.1016/j.trc.2020.102938
2020	KryptoOracle: A Real-Time Cryptocurrency Price Prediction Platform Using Twitter Sentiments	https://doi.org/10.48550/arXiv.2003.04967
2020	Multimedia Network Public Opinion Supervision Prediction Algorithm Based on Big Data	https://doi.org/10.1155/2020/6623108
2020	Social-Media Analysis for Disaster Prevention: Forest Fire in Artenara and Valleseco, Canary Islands	https://doi.org/10.3390/joitmc6040169
2020	TopicBERT: A Transformer transfer learning based memory–graph approach for multimodal streaming social media topic detection	https://doi.org/10.48550/arXiv.2008.06877
2020	La inteligencia artificial en el campo de la información: su utilización en apoyo a la desinformación (Usos militares de la inteligencia artificial, la automatización y la robótica (IAA&R))	https://publicaciones.defensa.gob.es/usos-militares-de-la-inteligencia-artificial-la-automatizacion-y-la-robotica-iaa-r-libros-ebook.html
2020	The containment of fake news propagation in online social networks	https://doi.org/10.1109/ICIBA50161.2020.9276936
2020	Detecting Fake News on Social Media: A Multi-Source Scoring Framework	https://doi.org/10.1109/ICCCBDA49378.2020.9095586
2020	Rejection and Hate Speech in Twitter: Content Analysis of Tweets about Migrants and Refugees in Spanish	https://reis.cis.es/REIS/PDF/REIS_172_02_ENG1598426449235.pdf
2020	Rumor Detection on Twitter Using Features Extraction Method	https://doi.org/10.1109/IT-ELA50150.2020.9253027
2020	TRUSTD: Combat Fake Content using Blockchain and Collective Signature Technologies	https://doi.org/10.1109/COMPSAC48688.2020.00-87
2020	Use of social media in crisis management: A survey	https://doi.org/10.1016/j.ijdrr.2020.101584
2021	Applying an Epidemiological Model to Evaluate the Propagation of Misinformation and Legitimate COVID-19-Related Information on Twitter	https://doi.org/10.1007/978-3-030-80387-2_3
2021	Automatic Monitoring Social Dynamics During Big Incidences: A Case Study of COVID-19 in Bangladesh	https://doi.org/10.48550/arXiv.2101.09667
2021	Assessing Bias in YouTube's Video Recommendation Algorithm in a Cross-lingual and Cross-topical Context	https://doi.org/10.1007/978-3-030-80387-2_7
2021	Bot-Based Emotion Behavior Differences in Images During Kashmir Black Day Event	https://doi.org/10.1007/978-3-030-80387-2_18

2021	Crawling political communities in Twitter and extracting political affiliations	https://doi.org/10.48550/arXiv.2102.00849
2021	Deciphering Social Opinion Polarization Towards Political Event Using Topic Modelling And Dynamic Network Analysis	https://doi.org/10.48550/arXiv.2102.08249
2021	Decision Making For Celebrity Branding: An Opinion Mining Approach Based On Polarity And Sentiment Analysis Using Twitter Consumer-Generated Content (CGC)	https://doi.org/10.48550/arXiv.2109.12630
2021	Detecting Adverse Drug Reactions from Social Media Based on Multichannel Convolutional Neural Networks Modified by Support Vector Machine	https://doi.org/10.1109/ICWR51868.2021.9443128
2021	Fine-Grained Analysis of the Use of Neutral and Controversial Terms for COVID-19 on Social Media	https://doi.org/10.1007/978-3-030-80387-2_6
2021	Intelligent Agent for Hurricane Emergency Identification and Text Information Extraction from Streaming Social Media Big Data	https://doi.org/10.48550/arXiv.2106.07114
2021	Malicious and Low Credibility URLs on Twitter During the AstraZeneca COVID-19 Vaccine Development	https://doi.org/10.1007/978-3-030-80387-2_1
2021	Measuring the Impact of Spammers on E-Mail and Twitter Networks	https://doi.org/10.1016/j.ijinfomgt.2018.09.009
2021	Mining Online Social Media to Drive Psychologically Valid Agent Models of Regional Covid-19 Mask Wearing	https://doi.org/10.1007/978-3-030-80387-2_5
2021	PANDORA Talks: Personality and Demographics on Reddit	https://doi.org/10.48550/arXiv.2004.04460
2021	Real-time Spatio-temporal Event Detection on Geotagged Social Media	https://doi.org/10.1186/s40537-021-00482-2
2021	Seeing and Believing Evaluating the Trustworthiness of Twitter Users	https://doi.org/10.48550/arXiv.2107.08027
2021	Suicide Classification for News Media Using Convolutional Neural Network	https://doi.org/10.48550/arXiv.2103.03727
2021	A Memory Network Information Retrieval Model for Identification of News Misinformation	https://doi.org/10.1109/TBDATA.2020.3048961
2021	Detection of Fake News Text Classification on COVID-19 Using DL approaches	https://dx.doi.org/10.1155%2F2021%2F5514220
2021	Pursuit for Authentic News using Machine Learning Models	https://doi.org/10.1109/ICRITO51393.2021.9596286
2021	Simulating Social-Cyber Maneuvers to Deter Disinformation Campaigns	https://doi.org/10.1007/978-3-030-80387-2_15
2021	Studying the Role of Social Bots During Cyber Flash Mobs	https://doi.org/10.1007/978-3-030-80387-2_16
2021	The fake news propagate with more self-loop in online social networks	https://doi.org/10.1109/ICIBA52610.2021.9688320
2021	Using Social Network Analysis to Analyze Development Priorities of Moroccan Institutions	https://doi.org/10.1007/978-3-030-80387-2_19

2022	Development of Fake News Model Using Machine Learning through Natural Language Processing	https://doi.org/10.48550/arXiv.2201.07489
2022	A Novel Method of Generating Geospatial Intelligence from Social Media Posts of Political Leaders	https://doi.org/10.3390/info13030120
2022	Detecting COVID-19-Related Fake News Using Feature Extraction	https://doi.org/10.3389/fpubh.2021.788074

TABLA 6: ARTÍCULOS REDES SOCIALES Y FAKE NEWS

3.1.4. Logística

De acuerdo con la definición propuesta por la entidad norteamericana Council of Supply Chain Management Professionals (CSCMP), la logística contempla la planificación, implementación y control de un flujo de servicios, información y bienes entre el punto de origen y el de consumo, a fin de garantizar su calidad final. [118]

En el ámbito militar, se realizan ciertas actividades inherentes al transporte, abastecimiento y alojamiento de unidades. La logística militar es, el apoyo a estas actividades, para conseguir asegurar una increíble garantía. Se puede considerar que, tras la finalización de la Segunda Guerra Mundial, el sector empresarial se fue adaptando y la logística empezó a funcionar como una actividad de producción, distribución y abastecimiento de bienes y servicios, a partir de las experiencias en el sector militar [119].

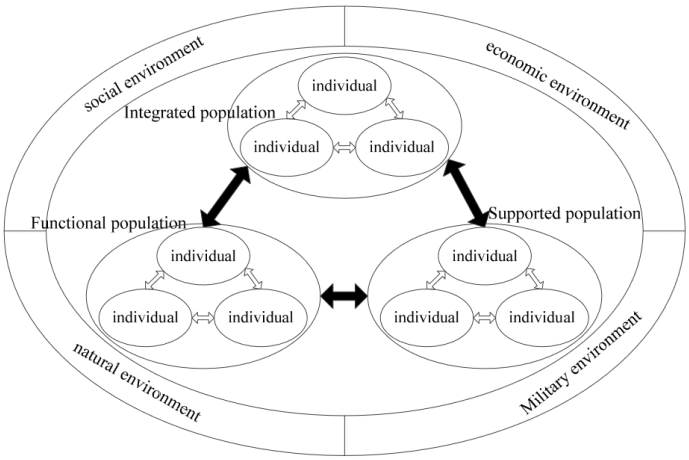
La logística militar considera tres tipos de abastecimiento:

- Autoabastecimiento: el abastecimiento de recursos depende de dónde se encuentran las unidades de combate, debido a esto puede haber escasez de recursos al depender completamente del entorno.
- Local: el gasto en logística militar es bajo porque los recursos se obtienen generalmente por acuerdos con los habitantes locales.
- A larga distancia: los recursos de apoyo provienen de ciudades aliadas y, por lo tanto, el gasto en logística militar es alto, debido a la administración y el transporte a larga distancia conllevan el uso de muchos más recursos

Para garantizar la efectividad de la logística militar se plantean los siguientes grupos funcionales:

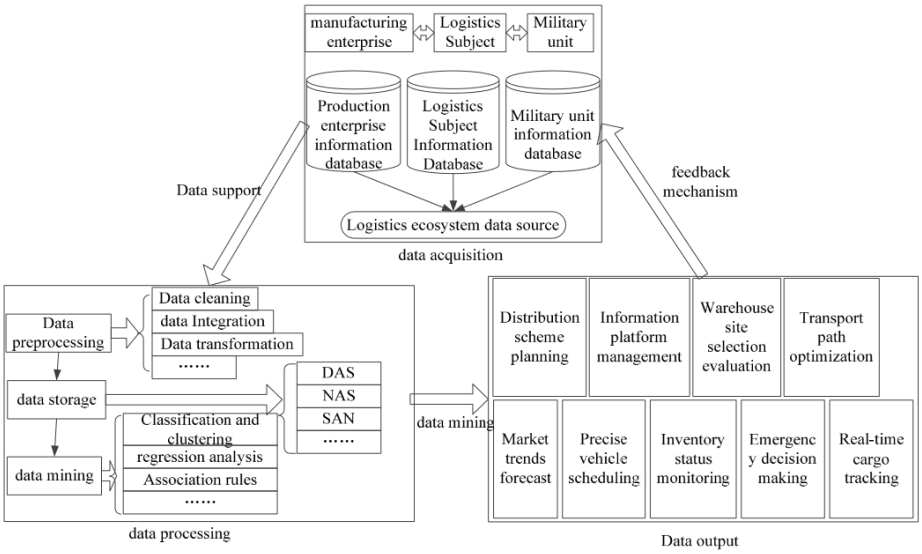
- Cadena de suministro: provee los recursos que precisan las unidades para sus operaciones militares, desde el diseño-desarrollo de productos, compra de productos, distribución de los productos y la administración de los productos sobre el terreno. Los principales recursos que provee la cadena de suministro militar son los básicos (como el agua, comida y medicinas), de transporte (vehículos y combustible) y de combate (como componentes electrónicos).
- Transporte: desplazamiento de un punto a otro punto, empleando vehículos especializados para distribuir y administrar la cadena de suministro. El transporte viene caracterizado por la capacidad de carga, la velocidad y el medio de desplazamiento.
- Instalaciones: infraestructuras que permiten hacer diferentes actividades sobre el terreno.
- Servicios: actividades que permiten hacer un uso efectivo de todo lo anteriormente mencionado.

De acuerdo con el artículo de investigación “Research on Military Logistics based on Big Data” [120], el ecosistema logístico es un sistema de red complejo que se compone del organismo vivo y el entorno relacionado. Las empresas logísticas, como cuerpo principal del ecosistema logístico, se pueden dividir en tipo de soporte, tipo funcional y tipo integrado según el tipo de población. Estos grupos de logística confían en la tecnología de la información y la tecnología de Internet en un ecosistema logístico simbiótico interdependiente y armonioso, y cuando la vitalidad del "Big Data" se inyecta en la construcción del ecosistema logístico, se puede mejorar la capacidad de procesamiento de información y la utilización de las empresas de logística, lo que promoverá el beneficio mutuo del ecosistema logístico.



MARCO DEL ECOSISTEMA DE LOGÍSTICA MILITAR [120]

Asimismo, debe de haber una coordinación poblacional del ecosistema logístico militar: coordinación entre poblaciones logísticas, coordinación entre empresas de logística y coordinación entre unidades de logística, para adquirir, extraer, analizar, compartir y comunicar datos de logística militar.



COORDINACIÓN ENTRE ESPECIES EN LOGÍSTICA MILITAR (ESPECIES FUNCIONALES) [120]

Se plantea que los sectores de la logística y el transporte son de los más ideales para beneficiarse de los avances metodológicos y las capacidades analíticas de las tecnologías Big Data, según los autores del artículo “Big Data for Transport and Logistics: A review” [121]. Esto es debido a la

creciente digitalización de dichos sectores que generan grandes flujos de datos de bienes y personas. Aprovechando el valor que pueden proporcionar los datos y la información, el uso de tecnologías Big Data se está convirtiendo en un nuevo objetivo estratégico para la mayoría de las organizaciones y empresas. Desde el punto de vista del valor, la adopción de Big Data en cualquier sector industrial o de servicios generalmente puede caer en una de las tres dimensiones: eficiencia operativa, experiencia del cliente y nuevos modelos de negocios.

La industria China ha sido una de las industrias dónde el transporte y la logística ha tenido mayor impacto y eso se ve reflejado en el documento "The Application and Development of Big Data in Transport Logistics Industry in China" [122], donde los autores plantean que la recopilación de información logística, el intercambio de información logística entre dominios, la fusión heterogénea de información logística y el análisis de Big Data logístico se han convertido en el foco del país, la industria y el mercado, consiguiendo que la plataforma de información logística empresarial se centre principalmente en la coordinación de la cadena de suministro y la optimización de la organización del transporte. La recopilación de información logística es el proceso de obtener el estado en tiempo real (principalmente datos de ubicación) de conductores, vehículos, unidades de transporte y mercancías. En la actualidad, existen tres formas principales de recopilar información logística:

- Uso de tecnología de posicionamiento satelital
- Uso de la tecnología de Internet móvil
- Utilizando tecnología RFID y código de barras

Mediante la recopilación y el tratamiento de los datos de transporte logístico, en China las autoridades de la industria del transporte han aplicado gradualmente la tecnología de análisis de decisiones de grandes datos logísticos en la planificación, gestión y servicios. Sin embargo, la perfección del sistema de análisis de decisiones de Big Data de datos de logística de transporte también involucra los mecanismos de gestión, la seguridad de la información y muchos otros aspectos.

La tecnología del Big Data también se puede emplear para encontrar las mejores localizaciones para los centros logísticos [123] [124] e incluso la ubicación de las estaciones de rescate [125]. Asimismo, se puede emplear para la optimización de la cadena de suministro [126], [127] o la detección de fallos [128], [129].

Un aspecto importante de la logística en el presente es que requiere de profesionales especializados en Big Data, robotización y realidad virtual, entre otras materias, según un artículo del Diario de Cordoba [130], donde se narra que el ejército de Tierra busca talento digital para la futura base logística militar de Córdoba. De acuerdo con el Jefe del Estado Mayor de Defensa en Córdoba, Amador Enseñat, será necesario contar con profesionales formados en tecnologías emergentes y disruptivas como son Big Data y los sistemas de inteligencia artificial para aplicarlos en el análisis y toma de decisiones, sistemas autónomos de transportes, automatización en almacenes y geolocalización. El objetivo es modernizar todos los sistemas, además de concentrar las once sedes del Ejército que actualmente están dispersas en una sola mejorando su eficacia y eficiencia en términos de sostenibilidad, tecnología e innovación.

Antes de presentar la selección de artículos relacionados con la logística, se van mencionar las aplicaciones más significativas de esta área.

- Mantenimiento predictivo

- Gestión del inventario
- Análisis de riesgos
- Rutas de arrastre
- Mejora de la eficiencia operacional
- Análisis de datos de trayectoria de objetos en movimiento
- Elaboración de los mapas de transitabilidad para vehículos terrestres no tripulados
- Estrategia de aplicación de construcción logística de Fuerzas Armadas Policiales basada en ingeniería de sistemas de datos

Artículos relacionados

Año	Artículo	Referencia
-	Data Analytics and Machine Learning based on Trajectories	https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-SET-262/MP-SET-262-13.pdf
2004	Lead the fleet a structured approach to predicting helicopter failures	https://doi.org/10.1109/AERO.2004.1368174
2014	Research on Warship Communication Operation and Maintenance Management based on Big Data	https://doi.org/10.1109/CBD.2014.24
2015	Big Data analytics for logistics and transportation	https://doi.org/10.1109/ICAdLT.2015.7136630
2016	Unmanned Aerial Vehicle Flight Point Classification	https://doi.org/10.3390/sym9010001
2017	Big Data for Transport and Logistics: A Review	https://doi.org/10.1109/ICAdLT.2017.8547029
2017	Big Data analytics in supply chain management: A state-of-the-art literature review	https://doi.org/10.1016/j.cor.2017.07.004
2018	Diverse Visualization Techniques and Methods of Moving-Object-Trajectory Data: A Review	https://doi.org/10.3390/ijgi8020063
2018	Design a Smart and Intelligent Routing Network Using Optimization Techniques	https://doi.org/10.1007/978-981-13-1274-8_23
2018	Method of developing the maps of passability for unmanned ground vehicles	https://doi.org/10.1088/1755-1315/169/1/012027
2018	Research on path guidance of logistics transport vehicle based on image recognition and image processing in port area	https://doi.org/10.1186/s13640-018-0384-5
2018	Unstructured Big Data analytics for air cargo logistics management	https://doi.org/10.1109/SOLI.2018.8476741
2018	Moving Objects Analytics: Survey on Future Location & Trajectory Prediction Methods	https://doi.org/10.48550/arXiv.1807.04639
2018	Research on the Optimization of Military Supplies under Big Data Background	https://doi.org/10.1109/BDAI.2018.8546629
2019	Analysis of the Application of Military Big Data in Equipment Quality Information Management	https://doi.org/10.1109/ICCCBDA.2019.8725744

2019	Aircraft Location Prediction using Deep Learning	https://doi.org/10.1109/MILCOM47813.2019.9020888
2019	Big Data Management in Maritime Transport	https://docplayer.net/7780300-Military-implications-of-big-data.html
2019	Big Data fusion and parametrization for strategic transport demand models	https://doi.org/10.1109/MTITS.2019.8883333
2019	Big Data Logistics Inventory Control Model Based on Error Correction Model	https://doi.org/10.1109/ICMTMA.2019.00080
2019	Data Driven Vessel Trajectory Forecasting Using Stochastic Generative Models	https://doi.org/10.1109/ICASSP.2019.8683444
2019	Maritime Situation Awareness through Data Analytics, Machine Learning and Risk Assessment Based on Ship Trajectories	https://www.cmre.nato.int/msaw-2019-home/msaw2019-papers/1375-msaw2019-opitz-maritimesituationawarenessthroughdataanalyticsmachinelearningandriskassessmentbasedonshiptrajectories/file
2019	Research on Military Logistics based on Big Data	https://dx.doi.org/10.2991/icmeit-19.2019.40
2019	Research on Location Selection of Railway Logistics Center	https://dx.doi.org/10.2991/icmeit-19.2019.6
2019	Seaport Data Space for Improving Logistic Maritime Operations	https://doi.org/10.1109/ACCESS.2019.2963283
2019	The Application and Development of Big Data in Transport Logistics Industry in China	https://doi.org/10.1109/ITNEC.2019.8729484
2020	Analysis on the Influence and Countermeasures of Big Data in Military Logistics Support	https://doi.org/10.1109/ICITBS49701.2020.00142
2020	Application Strategy of Armed Police Force Logistics Construction Based on Data System Engineering	https://doi.org/10.1109/ICRIS52159.2020.00104
2020	Big Data e Internet de las Cosas para los sistemas inteligentes del transporte. Características y áreas de oportunidad.	https://trid.trb.org/view/1846486
2020	Big Data Analytics for Time-Critical Mobility Forecasting: From Raw Data to Trajectory-Oriented Mobility Analytics in the Aviation and Maritime Domains	https://link.springer.com/book/10.1007/978-3-030-45164-6
2020	Big Trajectory Data Mining: A Survey of Methods, Applications, and Services	https://dx.doi.org/10.3390%2Fs20164571
2020	Construction of Port Logistics Service Platform Based on Big Data	https://doi.org/10.1088/1742-6596/1648/4/042048
2020	Combining Epidemiological and Constructive Simulations for Robotics and Autonomous Systems	https://doi.org/10.1007/978-3-030-70740-8_6

	Supporting Logistic Supply in Infectious Diseases Affected Areas	
2020	Estimation of ship operational efficiency from AIS data using Big Data technology	https://doi.org/10.1016/j.ijnaoe.2020.03.007
2020	Intelligent Logistics System Based on Big Data	https://doi.org/10.1109/ICRIS52159.2020.00081
2020	Intelligent Technology Related to Warehousing and Distribution in Intelligent Logistics	https://doi.org/10.1109/ICWCSG50807.2020.00046
2020	Investigation of the Model of Testing for Weapons and Military Equipment	https://doi.org/10.1007/978-3-030-58124-4_30
2020	Localization of Transport and Logistics Centers in the Region	https://doi.org/10.1088/1757-899X/753/7/072021
2020	Method for Optimising Mission-Specific Inventory of Aviation Materials	https://doi.org/10.1109/ICIBA50161.2020.9276911
2020	Knowledge Discovery in Simulation Data	https://doi.org/10.1145/3391299
2020	Machine Learning Aided Air Traffic Flow Analysis Based on Aviation Big Data	https://doi.org/10.1109/TVT.2020.2981959
2020	Prediction of Vessel Trajectories From AIS Data Via Sequence-To-Sequence Recurrent Neural Networks	https://doi.org/10.1109/ICASSP40776.2020.9054421
2020	Origin-Destination-Based Travel Time Reliability under Different Rainfall Intensities An Investigation Using Open-Source Data	https://doi.org/10.1155/2020/8816020
2020	Research on Key Technologies of Logistic and Equipment Supports of Unmanned Combat System	https://doi.org/10.1109/ICUS50048.2020.9274960
2020	Research on Delivered Logistics Management Information System Based on Big Data	https://doi.org/10.1109/ICICTA51737.2020.00113
2020	Thinking on the Application of Big Data in Fault Diagnosis of Military Equipment	https://doi.org/10.1109/ITAIC49862.2020.9339172
2020	Thinking of Equipment Support Capacity Building based on Big Data	https://doi.org/10.1109/MLBDBI51377.2020.00076
2021	A Case-Based Reasoning Approach for a Decision Support System in Manufacturing	https://doi.org/10.1007/978-3-030-79463-7_22
2021	Application of Flight Test Data Mining in Safety Monitoring of Civil Aviation Products	https://doi.org/10.1007/978-981-16-7423-5_70
2021	Big Data Accident Prediction System in Green Networks and Intelligent Transportation Systems	https://doi.org/10.1007/978-3-030-53440-0_14
2021	Construction of intelligent logistics information platform based on Big Data technology	https://doi.org/10.1109/ECIE52353.2021.00050
2021	Future and Innovative Design Requirements Applying Industry 4.0 Technologies on Underground Ammunition Storage	https://doi.org/10.3390/asi4010022
2021	Intelligent System of Mooring Planning, Based on Deep Q-Learning	https://doi.org/10.1007/978-3-030-79463-7_31

2021	Map-Matching Based on HMM for Urban Traffic	https://doi.org/10.1007/978-3-030-79463-7_39
2021	Near-Real-Time IDS for the U.S. FAA's NextGen ADS-B	https://doi.org/10.3390/bdcc5020027
2021	Research on Logistics Management Information System Based on Big Data	https://doi.org/10.1109/ICMTMA52658.2021.00141
2021	Research on Classification of Travel Time for Electronic Police Based on the DBSCAN Algorithm	https://doi.org/10.1371/journal.pone.0259472
2021	Spare Parts Inventory Management: A Literature Review	https://ideas.repec.org/a/gam/jsusta/v13y2021i5p2460-d505374.html
2021	Research on Integrated Data Engineering of Equipment Maintenance Support in the Big Data Era	https://doi.org/10.1109/IMCEC51613.2021.9482005
2021	Research on Military Logistics Ecosystem Based on Big Data	https://doi.org/10.1088/1742-6596/1813/1/012027
2021	Research on Real-Time Anomaly Detection of Fishing Vessels in a Marine Edge Computing Environment	https://doi.org/10.1155/2021/5598988
2021	Vessel Navigation Behavior Analysis and Multiple-Trajectory Prediction Model Based on AIS Data	https://doi.org/10.1155/2022/6622862
2021	Ship Classification Based on Improved Convolutional Neural Network Architecture for Intelligent Transport Systems	https://doi.org/10.3390/info12080302
2021	Research on Site Selection and Algorithm of Military Logistics Center	https://doi.org/10.1088/1742-6596/1792/1/012034
2021	Search and rescue station location selection and conceptual design: a case study of western region of Indonesia	https://doi.org/10.1088/1755-1315/649/1/012069
2021	Cybersecurity Challenges in the Maritime Sector	https://doi.org/10.3390/network2010009
2022	Aircraft Rotation Detection in Remote Sensing Image Based on Multi-Feature Fusion and Rotation-Aware Anchor	https://doi.org/10.3390/app12031291
2022	Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends	https://doi.org/10.3390/info13030146
2022	Basic Ship-Planning Support System Using Big Data in Maritime Logistics for Simulating Demand Generation	https://doi.org/10.3390/jmse10020186
2022	Digitalizing Maritime Containers Shipping Companies: Impacts on Their Processes	https://doi.org/10.3390/app12052532

TABLA 7: ARTÍCULOS LOGÍSTICA

3.2. Common Operational Picture, Conciencia Situacional y Toma de decisiones

Common Operational Picture (COP) que en español sería Imagen Operativa Común se define como la combinación de todos los datos del área operativa recopilados y luego correlacionando estos datos para dar sentido al conocimiento, y finalmente mostrándolos en un mapa común.

En situaciones críticas, tomar las decisiones correctas se basa en una comprensión tridimensional del entorno estratégico. Para los comandantes militares, los socorristas, los administradores civiles, los directores de operaciones y los administradores de la cadena de suministro por igual, es esencial tener un sólido conocimiento de la situación sobre los eventos en tiempo real. El desarrollo de esta conciencia situacional requiere un conjunto de tecnología que aproveche los activos en el campo para proporcionar a los responsables de la toma de decisiones la información precisa y actualizada que necesitan para gestionar las amenazas en evolución y otros escenarios, desde la gestión de amenazas de seguridad en los campus universitarios hasta el cambio de ruta de las flotas de envío durante las interrupciones de la cadena de suministro, una imagen operativa común sólida puede marcar la diferencia entre una mala decisión y una buena [131].

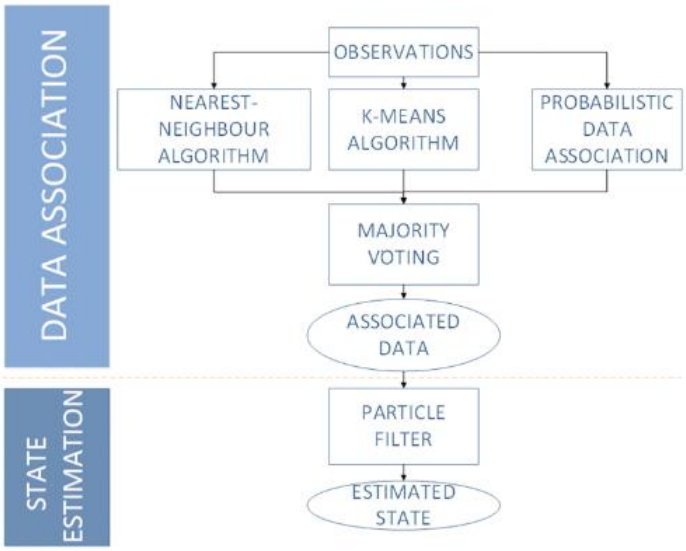
La conciencia situacional implica saber lo que sucede a tu alrededor en un momento dado, no solo por tema de seguridad personal. También juega un papel crucial en la eficacia y la eficiencia de las empresas en una variedad de industrias, desde el ejército y el gobierno hasta la seguridad pública y el transporte.

Comprender cómo las acciones y los eventos afectarán el estado actual y futuro de las cosas, ya sea que incluya personas, lugares, tiempo, objetivos o todo lo anterior, es esencial para la toma de decisiones sobre el terreno, sea en una zona de combate o en una calle de la ciudad, la acción inmediata e informada puede afectar de manera crítica el resultado de cualquier situación. Lograr la conciencia situacional depende de la capacidad para ver, comprender y analizar el mundo que lo rodea en el contexto de lo que está tratando de hacer.

A fines de la década de 1980, la psicóloga Mica Endsley desarrolló un modelo de conciencia situacional con tres componentes principales: la percepción de los elementos en un entorno dentro de un volumen de tiempo y espacio, la comprensión de su significado y la proyección de su estado en el cercano. futuro después de que alguna variable ha cambiado. En pocas palabras, la conciencia situacional implica captar señales del entorno, juntar esas señales para comprender lo que está sucediendo y usar esa comprensión para predecir lo que puede suceder a continuación. [132]

El uso de los grandes datos ayuda a aumentar la conciencia situacional actual, asimismo nos permite comprender lo que realmente sucedió en el pasado para comprender la situación actual. Para adquirir los resultados correctos de conciencia situacional, hay que analizar los datos correctos provenientes de la fuente correcta, mediante el uso de herramientas de Big Data, los sensores instalados en satélites, vehículos terrestres, tanques y otras plataformas incrementan la conciencia situacional. La combinación de tecnología de Big Data junto con un aumento espectacular en la tecnología de sensores producirá un efecto sinérgico. Esa adquisición de la capacidad de fusionar los datos del sensor hace una contribución importante al desarrollo de la base de datos para que se recopile más información de lo que se pensaba anteriormente.

Fusionando datos de sensores se puede generar un método de desarrollo de conciencia de la situación y una herramienta elaborada para el apoyo de soldados individuales y comandantes de bajo nivel, como la propuesta en el artículo de investigación "Military and Crisis Management Decision Support Tools for Situation Awareness Development Using Sensor Data Fusion" [133]. El sistema que proponen, mCOP, en sí es una prueba de concepto innovadora y un software de banco de pruebas, que utiliza sensores, tecnologías inalámbricas y realidad aumentada para apoyar a las tropas terrestres durante varias operaciones de combate en entornos de capacidades habilitadas para redes, mediante el empleo de terminales móviles disponibles en el mercado. El empleo de terminales móviles es intencional ya que el sistema debe ofrecer funciones de seguridad al mismo tiempo que mantener una alta disponibilidad y accesibilidad para todos los soldados. El sistema está respaldado por servicios de integración de datos SOA que albergan NFFI (NATO Friendly Forces Information), TSO (Tactical Situation Object) y JC3IEDM (Joint Consultation Command & Control Information Exchange Data Model) servicios militares y de gestión de crisis.



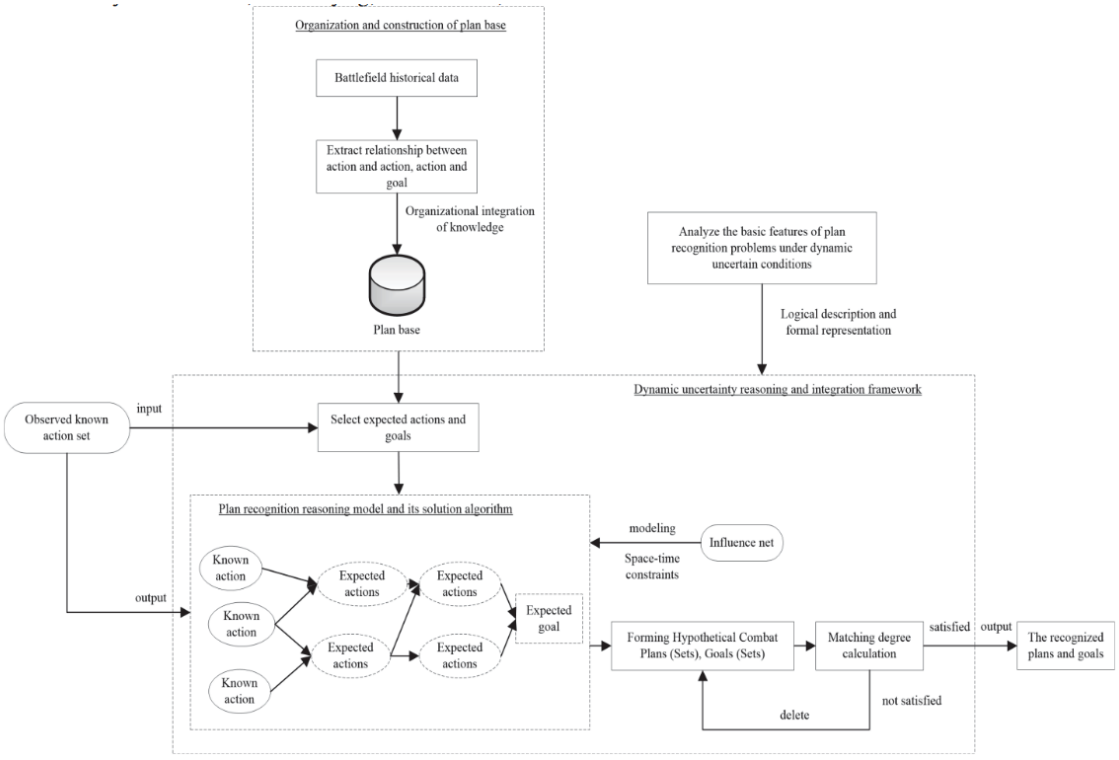
IMPLEMENTACIÓN DEL ALGORITMO DE FUSIÓN DE DATOS EN LA SOLUCIÓN DSS QUE FUSIONA PRODUCTOS DE IMÁGENES OPERATIVAS EN EL SOFTWARE MCOP [133]

Otra aplicación de la fusión de diversos datos de sensores es el seguimiento automático de objetos detectados en el área de vigilancia como el proyecto FOLDOUT estudiado en "Tracking of objects in a multi-sensor fusion system for border surveillance" [134]. FOLDOUT se centra en la detección de follaje en las regiones interiores y exteriores de la UE. La fusión de varias señales de sensores aumenta la eficacia de la detección, especialmente en áreas boscosas y ocultas por el follaje, donde los sistemas basados en cámaras particularmente tradicionales se enfrentan al problema de la oclusión severa provocada por el área foliada y deben lidiar potencialmente con detecciones fragmentadas.

También relacionado con la vigilancia se puede considerar la gestión del tráfico mediante las cámaras pertenecientes a un circuito cerrado de televisión (CCTV). En la gestión del tráfico, se instalan CCTV para monitorear la ubicación específica en la carretera, y las CCTV genera datos no estructurados en formato de imagen y video, los cuales son difíciles de procesar debido a la complejidad de los datos al constar de atributos inestables. Aunque mediante el empleo de tecnologías de Big Data mediante los algoritmos de aprendizaje profundo y las bases de datos NoSQL se pueden procesar datos no estructurados en tiempo real y así ayudar a comprender las

condiciones del tráfico además de ayudar al oficial a monitorear la carretera. En el artítuclo "Big Data Analytics for Processing Real-time Unstructured Data from CCTV in Traffic Management" [135] proponen un prototipo que es capaz de detectar objetos como automóviles, camiones, autobuses, etc. y agregar el tipo de vehículos mediante imágenes de CCTV, además de analizar situaciones normales y anormales en los datos no estructurados en tiempo real.

La conciencia situacional y la toma de decisiones se puede considerar que van unidas de la mano tener una predicción del futuro mediante datos del pasado es importante para dar el soporte necesario. Además, la decisión de mando es la base de acción militar debido a que la decisión correcta depende de la comprensión de la consistencia del espacio de batalla y la correcta evaluación y juicio del campo de batalla, por lo que es muy necesario y urgente reconocer el plan táctico del enemigo en el proceso de mando y control (C2) como plantean en la investigación "Research on the Method of Operational Plan Recognition Driven by Big Data in Battlefield Awareness" [136]. La investigación indaga sobre los problemas científicos clave del reconocimiento del plan operativo impulsado por Big Data en la conciencia del campo de batalla. El problema del reconocimiento del plan involucra unidades de combate que están distribuidas, con una dinámica de la situación muy dinámica y los planes del enemigo claramente jerárquicos. Además, la fuente y el proceso de entrega de la incertidumbre del campo de batalla deben ser considerados en su totalidad. Por lo tanto, plantean construir dinámicamente redes influenciadas por el tiempo en función de las características de distribución, dinámica, incertidumbre y jerarquía del reconocimiento del plan, los nodos de la red se generan dinámicamente en función de los conjuntos de acciones conocidas adquiridas en tiempo real.



ESQUEMA DE INVESTIGACIÓN DEL RECONOCIMIENTO DEL PLAN OPERATIVO [136]

A la hora de predecir eventos futuros que requieran la toma de decisiones se pueden considerar también la predicción de ataques terroristas [137] o los movimientos de refugiados y los desplazados internos [138]. En el caso de la detección de ataques terrorista se requiere un amplio espectro de datos que, en muchos casos, se recopilan de diversas fuentes. El proceso de unificación, fusión e interpretación de los datos recopilados es crucial debido a la redundancia

de datos y especialmente para permitir predicciones precisas debido a que puede haber datos poco fiables. De una forma similar para la predicción de movimientos migratorios se necesita datos de múltiples fuentes aunque no existe una fuente completa de datos sobre los movimientos de refugiados y el desplazamiento interno, aunque se tiende a recurrir a diversos tipos de datos como son los de conflicto, violencia y represión política, datos de dispositivos telefónico, teledetección y datos geográficos, económicos y medio ambiéntales y datos de redes sociales.

A continuación se presentan las aplicaciones más significativas y la selección de artículos relacionados con la imagen operativa común, la consciencia situacional y la toma de decisiones.

- Pronosticar y analizar relaciones entre delitos
- Seguimiento de objetos en un sistema de fusión multisensor para vigilancia de fronteras
- Soporte de decisiones semánticas
- Apoyo de diagnóstico para la concienciación sobre la amenaza del terrorismo
- Vigilancia de enfermedades
- Soporte de triaje de combate
- Apoyo a los soldados y comandantes de bajo nivel en operaciones terrestres.

Artículos relacionados

Año	Artículo	Referencia
2003	A probabilistic multidimensional data model and algebra for OLAP in decision support systems	https://doi.org/10.1109/SECON.2003.1268426
2004	A concept of simulation based diagnostic support tool for terrorism threat awareness	https://www.researchgate.net/publication/233863015_A_concept_of_simulation_based_diagnostic_support_tool_for_terrorism_threat_awarness
2008	Data Fusion Based On Ontology Model For Common Operational Picture Using Openmap And Jena Semantic Framework	https://www.researchgate.net/publication/233859425_DATA_FUSION_BASED_ON_ONTOLOGY_MODEL_FOR_COMMON_OPERATIONAL_PICTURE_USING_OPENMAP_AND_JENA_SEMANTIC_FRAMEWORK
2008	The prediction of terrorist threat on the basis of semantic association acquisition and complex network evolution	https://www.itl.waw.pl/czasopisma/JTIT/2008/2/14.pdf
2009	Ontology Applications for Achieving Situation Awareness in Military Decision Support Systems	https://doi.org/10.1007/978-3-642-04441-0_46
2010	Semantic Battlespace Data Mapping Using Tactical Symbology	https://doi.org/10.1007/978-3-642-12090-9_14
2011	Multi Sensor Anti Sniper System	www.eda.europa.eu/docs%2Fdocuments/MUSAS_Executive_Summary.pdf

2014	Big Data Survaillance	https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/download/bds_ed/bds_editorial
2014	Pandemics of the future: Disease surveillance in real time	https://doi.org/10.24908/ss.v12i2.4735
2014	From self-tracking to smart urban infrastructures: towards an interdisciplinary research agenda on Big Data	https://doi.org/10.24908/ss.v12i2.4605
2014	Data Flood - Helping the Navy Address the Rising Tide of Sensor Information	https://doi.org/10.7249/RR31
2015	A Big-Data-Based Urban Flood Defense Decision Support System	http://dx.doi.org/10.14257/ijsh.2015.9.12.09
2016	Forecasting the Underlying Psychological Forces to Political Violence through Big Data Symbol Mining	https://doi.org/10.1109/EISIC.2016.050
2016	Identifying Trolls and Determining Terror Awareness Level in Social Networks Using a Scalable Framework	https://doi.org/10.1109/BigData.2016.7840796
2017	A Computer System for CBRN Contamination Threats Analysis Support, Prediction Their Effects and Alarming the Population: Polish Case Study	https://doi.org/10.1051/matecconf/201712502012
2017	A Common Operational Picture in Support of Situational Awareness for Efficient Emergency Response Operations	https://doi.org/10.18488/journal.102.2017.21.10.35
2017	A Review on Applications of Big Data for Disaster Management	https://doi.org/10.1109/SITIS.2017.67
2017	Big Data Surveillance: The Case of Policing	https://www.asanet.org/sites/default/files/attach/journals/oct17asrfeature.pdf
2017	Combat triage support using the Internet of Military Things	https://doi.org/10.15439/2017F186
2017	Measuring patterns of human behaviour through large-scale mobile phone data	https://www.duo.uio.no/bitstream/handle/10852/55139/Sundsoy-PhD-2017.pdf?isAllowed=y&sequence=4
2017	Military and Crisis Management Decision Support Tools for Situation Awareness Development Using Sensor Data Fusion	https://doi.org/10.1007/978-3-319-67229-8_17
2017	Situation Awareness tools supporting soldiers and low level commanders in land operations. Application of GIS and augmented reality mechanisms	https://www.researchgate.net/publication/319911548_SITUATION_AWARENESS_TOOLS_SUPPORTING_SOLDIERS_AND_LOW_LEVEL_COMMANDERS_IN_LAND_OPERATIONS_APPLICATION_OF_GIS_AND_AUGMENTED_REALITY_MECHANISMS

2017	Terrorist event prediction based on revealing data	https://doi.org/10.1109/ICBDA.2017.8078815
2017	Weather Data Analysis and Sensor Fault Detection Using An Extended IoT Framework with Semantics, Big Data, and Machine Learning	https://doi.org/10.1109/BigData.2017.8258150
2018	Big Data and Deep Learning Models for Automatic Dependent Surveillance	http://rbr.cs.umass.edu/lta/papers/FSS-18_paper_56.pdf
2018	Big Data in Natural Disaster Management: A Review	https://doi.org/10.3390/geosciences8050165
2018	Context for Maritime Situation Awareness	https://doi.org/10.1201/9780429445491
2018	Renewable Energy Integration in Distribution System -- Synchrophasor Sensor based Big Data Analysis, Visualization, and System Operation	https://doi.org/10.48550/arXiv.1803.06076
2018	Research on the Method of Operational Plan Recognition Driven by Big Data in Battlefield Awareness	https://doi.org/10.1109/IICSPI.2018.8690485
2018	Using Big Data Analytics to Create a Predictive Model for Joint Strike Fighter	https://doi.org/10.1109/BigData.2018.8622388
2018	The Role of Big Data in Intelligent Combat Command	https://dx.doi.org/10.2991/cecs-18.2018.27
2019	Aircraft Location Prediction using Deep Learning	https://doi.org/10.1109/MILCOM47813.2019.9020888
2019	Application of Augmented Reality, Mobile Devices, and Sensors for a Combat Entity Quantitative Assessment Supporting Decisions and Situational Awareness Development	https://doi.org/10.3390/app9214577
2019	Battlefield Target Aggregation Behavior Recognition Model Based on Multi-Scale Feature Fusion	https://doi.org/10.3390/sym11060761
2019	CRISIS: Integrating AIS and Ocean Data Streams Using Semantic Web Standards for Event Detection	https://doi.org/10.1109/ICMCIS.2019.8842749
2019	Command and Control System Construction in Big Data Era	https://doi.org/10.1088/1742-6596/1168/3/032022
2019	Handheld combat support tools utilising IoT technologies and data fusion algorithms as reconnaissance and surveillance platforms	https://doi.org/10.1109/WF-IoT.2019.8767263
2019	Prediction of Marine Pycnocline Based on Kernel Support Vector Machine and Convex Optimization Technology	https://doi.org/10.3390/s19071562
2019	Prediction of Passenger Flow in Urban Rail Transit Based on Big Data Analysis and Deep Learning	https://doi.org/10.1109/ACCESS.2019.2944744
2019	Research and Application of Smart Grid Early Warning Decision Platform Based on Big Data Analysis	https://doi.org/10.1109/IGBSG.2019.8886291
2019	Research on Intelligent Task Management and Control Mode of Space Information Networks Based on Big-Data Driven	https://doi.org/10.1007/978-981-15-3442-3_10

2019	Systematic Analysis of a Military Wearable Device Based on a Multi-Level Fusion Framework: Research Directions	https://doi.org/10.3390/s19122651
2020	A Hierarchical Decision-Making Method with a Fuzzy Ant Colony Algorithm for Mission Planning of Multiple UAVs	https://doi.org/10.3390/info11040226
2020	A Research on Battlefield Situation Analysis and Decision-making Modeling based on a Hadoop Framework	https://doi.org/10.1109/MLBDBI51377.2020.00083
2020	A Survey on Integrated and Comprehensive Disaster Reduction Technology in the Era of Big Data	http://dx.doi.org/10.13203/j.whugis20200108
2020	An IoT Inspired Distributed Data Fusion Architecture for Coastal Surveillance Applications	https://doi.org/10.23919/FUSION45008.2020.9190591
2020	Big Data Analytics for Processing Real-time Unstructured Data from CCTV in Traffic Management	https://doi.org/10.1109/ICoDSA50139.2020.9212858
2020	Construction Status and Prospect of the China Fire Rescue Command Big Data Platform	https://doi.org/10.1109/ICUEMS50872.2020.00162
2020	De las células a los bits (Usos militares de la inteligencia artificial, la automatización y la robótica (IAA&R))	https://publicaciones.defensa.gob.es/usos-militares-de-la-inteligencia-artificial-la-automatizacion-y-la-robotica-iaa-r-libros-ebook.html
2020	Improving Incident Response in Big Data Ecosystems by Using Blockchain Technologies	https://doi.org/10.3390/app10020724
2020	Intelligent Data Fusion and Multi-Agent Coordination for Target Allocation	https://doi.org/10.3390/electronics9101563
2020	Integración de datos para obtener la Common Operational Picture a nivel operacional y estratégico (Usos militares de la inteligencia artificial, la automatización y la robótica (IAA&R))	https://publicaciones.defensa.gob.es/usos-militares-de-la-inteligencia-artificial-la-automatizacion-y-la-robotica-iaa-r-libros-ebook.html
2020	Modeling the Impact of Border-Enforcement Measures	https://doi.org/10.7249/RR4348
2020	Multi-source Heterogeneous Data Association Technology to Build Public Safety Big Data Integration Research	https://doi.org/10.1109/BDEIM52318.2020.00012
2020	Methods and analytical tools for assessing tactical situation in military operations using potential approach and sensor data fusion	https://doi.org/10.1016/j.promfg.2020.02.255
2020	Operation Framework of the Command Information System Based on Big Data Analysis	https://doi.org/10.1109/ICCCBDA49378.2020.9095568
2020	Prediction of Future Terrorist Activities Using Deep Neural Networks	https://doi.org/10.1155/2020/1373087

2020	Research on the Model of Command and Decision System for Big Data	https://doi.org/10.1109/ICISCAE51034.2020.9236929
2020	Research on Public Safety Management under the Application of Big Data and Internet of Things	https://doi.ieeecomputersociety.org/10.1109/BDEIM52318.2020.00010
2021	A Case-Based Reasoning Approach for a Decision Support System in Manufacturing	https://doi.org/10.1007/978-3-030-79463-7_22
2021	Artificial Intelligence Applications in Military Systems and Their Influence on Sense of Security of Citizens	https://doi.org/10.3390/electronics10070871
2021	Big Data Driven Marine Environment Information Forecasting: A Time Series Prediction Network	https://doi.org/10.1109/TFUZZ.2020.3012393
2021	Building a Maritime Picture in the Era of Big Data: The Development of the Geospatial Communication Interface+	https://doi.org/10.1109/ICMCIS52405.2021.9486392
2021	Construction of a Social Security Monitoring and Early Warning Platform Driven by Big Data	https://doi.org/10.1109/IMCEC51613.2021.9482215
2021	Data Science and Big Data Analytics in Smart Environments	https://doi.org/10.1201/9780367814397
2021	Electromagnetic Environment Portrait Based on Big Data Mining	https://doi.org/10.1155/2021/5563271
2021	From common operational picture to common situational understanding: An analysis based on practitioner perspectives	https://doi.org/10.1016/j.ssci.2021.105381
2021	Having a Bad Day? Detecting the Impact of Atypical Events Using Wearable Sensors	https://doi.org/10.1007/978-3-030-80387-2_25
2021	Learning future terrorist targets through temporal meta-graphs	https://doi.org/10.1038/S41598-021-87709-7
2021	Measuring Intelligence, Surveillance, and Reconnaissance Effectiveness at the United States Central Command	https://www.rand.org/pubs/research_reports/RR4360.html
2021	Mining Online Social Media to Drive Psychologically Valid Agent Models of Regional Covid-19 Mask Wearing	https://doi.org/10.1007/978-3-030-80387-2_5
2021	Multiple Feature Fusion-based Video Face Tracking for IoT Big Data	https://doi.org/10.48550/arXiv.2104.08096
2021	Network Structures and Humanitarian Need	https://doi.org/10.1007/978-3-030-80387-2_21
2021	Public Security Big Data Application and Public Safety Governance	https://doi.ieeecomputersociety.org/10.1109/PMIS52742.2021.00013
2021	Research on Information System Risk Analysis and Security Situation Assessment Method	https://doi.org/10.1088/1742-6596/1792/1/012047
2021	Optimization of Mitigation Strategies During Epidemics Using Offline Reinforcement Learning	https://doi.org/10.1007/978-3-030-80387-2_4
2021	Time Series Data Mining Algorithms Towards Scalable and Real-Time Behavior Monitoring	https://doi.org/10.48550/arXiv.2112.14630

2021	The latest progress of data fusion for integrated disaster reduction intelligence service	https://doi.org/10.1080/19479832.2021.1970931
2021	The Technique of Operational Processing of Heterogeneous Surveillance Data in Assessing Situation in Geographic Information Systems	https://doi.org/10.1109/ATIT54053.2021.9678766
2021	Using Big Data, An Extensible System for Forecasting and Analyzing Relations Among Crimes	https://www.researchgate.net/publication/358490175_Using_Big_Data_An_Extensible_System_for_Forecasting_and_Analyzing_Relations_Among_Crimes
2022	Big Data in Criteria Selection and Identification in Managing Flood Disaster Events Based on Macro Domain PESTEL Analysis: Case Study of Malaysia Adaptation Index	https://doi.org/10.3390/bdcc6010025
2022	Electrical Load Forecasting Using Edge Computing and Federated Learning	https://doi.org/10.1109/ICC40277.2020.9148937
2022	Predictive modeling of movements of refugees and internally displaced people Towards a computational framework	https://doi.org/10.48550/arXiv.2201.08006
2022	Using Machine Learning to Predict Visitors to Totally Protected Areas in Sarawak, Malaysia	https://doi.org/10.3390/su14052735
2022	Military Dataset Processing Approaches or Trauma Risk Mitigation in Machine Learning Practitioners	http://dx.doi.org/10.46713/jdst.004.01
2022	Tracking of objects in a multi-sensor fusion system for border surveillance	http://dx.doi.org/10.46713/jdst.005.02
2022	Towards On-Device Dehydration Monitoring Using Machine Learning from Wearable Device's Data	https://doi.org/10.3390/s22051887
2022	Introducing the CYSAS-S3 Dataset for Operationalizing a Mission-Oriented Cyber Situational Awareness	https://doi.org/10.3390/s22145104

TABLA 8: ARTÍCULOS COP, CONCIENCIA SITUACIONAL, TOMA DE DECISIONES

3.3. Ciberdefensa y ciberseguridad

De acuerdo a [95], una de las mayores contribuciones de Big Data para los ejércitos nacionales modernos será la ciberdefensa debido a que las agencias militares y de inteligencia podrán hacer frente de manera más efectiva a las amenazas cibernéticas al implementar el Big Data como una solución técnica estratégica. Debido a eso, la tecnología Big Data será una herramienta indispensable en el análisis de ciberamenazas y sistemas de seguridad.

La ciberdefensa es el conjunto de acciones de tipo activo, pasivo, proactivo, preventivo y reactivo que se aplican para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición. Mientras que la ciberseguridad es el conjunto de acciones de carácter preventivo que tienen por objeto asegurar el uso propio de las redes y negarlo a terceros. Ambas, la ciberseguridad y la ciberdefensa son dos herramientas fundamentales para luchar contra los ciber riesgos actuales. [139]

Cuando se habla del análisis de Big Data en ciberseguridad, este refleja la capacidad de recopilar enormes cantidades de información digital, extrayendo, visualizando y analizando información futurista para que las amenazas y ataques cibernéticos adversos se puedan predecir con anticipación. Se ha de considerar que cada vez que se desarrolla una nueva tecnología o sistema, también lo hacen nuevas amenazas y vulnerabilidades, por lo que la seguridad se ha convertido en un objetivo en movimiento a medida que se generan cantidades sin precedentes de datos en diversas formas a velocidades impredecibles. Los grandes datos recopilados de redes, ordenadores, sensores y sistemas en la nube permiten a los administradores y analistas de sistemas conocer con precisión los detalles de las vulnerabilidades y las ciberamenazas, para poder planificar una mejor estrategia de soluciones de seguridad para hacer frente a las amenazas. Para que cualquier solución de seguridad cibernética sea efectiva, el análisis de Big Data se está convirtiendo gradualmente en un requisito previo. [140]

En el artículo de investigación "Big Data Analytics for Cyber Security" [141], se plantea que se están desarrollando nuevos enfoques en el campo de la ciberseguridad o la ciberdefensa teniendo en cuenta numerosos aspectos como son:

- representación unificada de datos
- detección de ataques de día cero
- intercambio de datos entre sistemas de detección de amenazas,
- análisis en tiempo real
- muestreo y reducción de dimensionalidad
- procesamiento de datos con recursos limitados
- análisis de series temporales para la detección de anomalías.

Con la evolución de Big Data, los métodos tradicionales de protección de redes rápidamente se volverán insuficientes para mantenerse al día con los diferentes métodos de ataque según los autores de "Big Data Cybersecurity Monitoring System using Machine Learning" [142]. La detección y mitigación de intrusiones y fallas es el eje alrededor del cual debe construirse cualquier sistema de seguridad seguro y confiable. Los datos, ya sean entrantes o salientes, deben cifrarse adecuadamente y, una vez entregados o recibidos, deben ser de fácil acceso como los datos de DNS, datos de flujo de IP y datos de tráfico HTTP para detectar cualquier vulnerabilidad en una plataforma de Big Data. Los datos en sí mismos son extensos y se pueden clasificar por fuente como activos y pasivos. Independientemente de si son activas o pasivas, generan inmensas cantidades de datos y requieren una gran potencia de procesamiento.

Fuentes de datos pasivos

- Basado en móvil: ubicación GPS, datos WAP
- Basado en computadora: ubicación IP, datos WAP
- Datos SIEM: registros de red, aplicación y base de datos de amenazas

Fuentes de datos activos

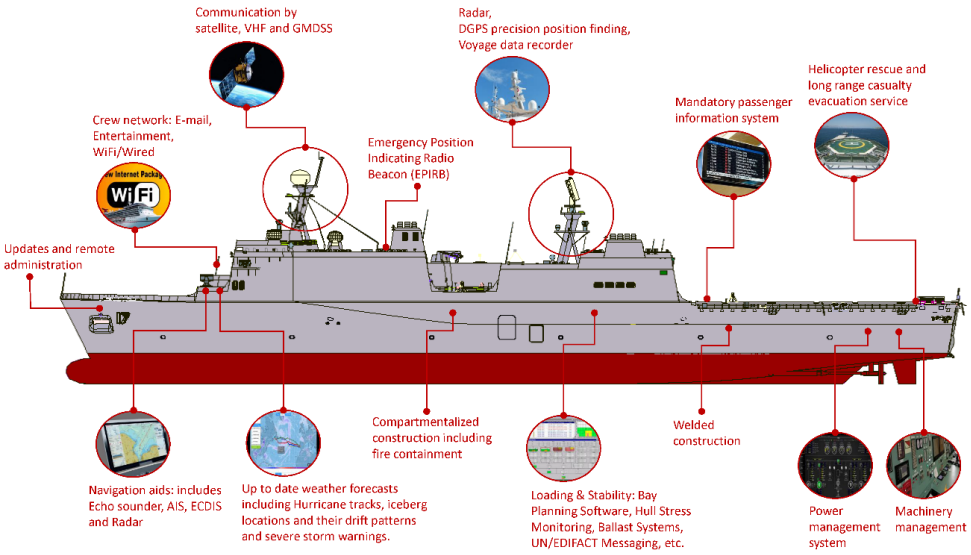
- Contraseñas 2FA
- Contraseñas de un solo uso
- Certificados digitales

El documento "Big Data in cybersecurity: a survey of applications and future trends" [143], examina la investigación de vanguardia en diferentes áreas de aplicaciones de Big Data en

ciberseguridad, mediante la clasificación de las aplicaciones en áreas de intrusión y detección de anomalías, detección de spam y suplantación de identidad, detección de malware y ransomware, seguridad de código, seguridad en la nube, junto con otra categoría que examina otras direcciones de investigación en Big Data y ciberseguridad. Además, se plantea que el futuro de la ciberseguridad está altamente conectado con los grandes datos, debido a los beneficios de estos para crear sistemas de ciberseguridad robustos, adaptables y rápidos los cuales se está convirtiendo más en una necesidad que en una opción, debido a que los métodos de detección clásicos se quedan atrás en términos de precisión y capacidad para detectar amenazas. Como la mayoría de los sistemas de ciberseguridad actuales dependen en gran medida de los registros generados por dispositivos de red, hosts, IDS e IPS, etc., que pueden ser fácilmente de varios GB, por lo que, si no se aprovecha el Big Data, el aprendizaje automático y la computación en la nube, los sistemas de detección de amenazas pueden quedarse atrás fácil y rápidamente. Asimismo, la utilización del Big Data en ciberseguridad se rige, en gran medida, por la capacidad para mantener la integridad de los Big Data utilizados en la toma de decisiones por lo que plantan como una dirección futura el centrarse en la protección de las técnicas de aprendizaje automático utilizadas en las aplicaciones de ciberseguridad para que no sean manipuladas por actores maliciosos.

Debe tenerse en cuenta, que el empleo del Big Data tiene sus escollos como se plantea en el artículo del 2020, “Seven Pitfalls of Using Data Science in Cybersecurity” [144]. En dicho artículo, los autores identifican siete escollos del empleo de la ciencia de datos en la ciberseguridad, que son la fuente de datos, la ingeniería de características, las métricas de evaluación, la selección de algoritmos, la convergencia de algoritmos, el envenenamiento de algoritmos y el aprendizaje automático adversario. Esta investigación llama a la cautela y la atención al utilizar el aprendizaje automático y el Big Data en aplicaciones de ciberseguridad. También, el documento considera la importancia de la fuente de datos y señala la tensión entre el uso de datos sintéticos y del mundo real, junto con el impacto de la selección del algoritmo en el resultado general.

El sector marítimo que hasta ahora se consideraba seguro debido a la falta de conectividad a Internet y la naturaleza aislada de los barcos en el mar, está mostrando un aumento del 900 % en las brechas de ciberseguridad en la tecnología operativa a medida que ingresa a la era digital. Aunque se están realizando algunas investigaciones en esta área, la ciberseguridad marítima no se ha investigado en profundidad, como plantean los autores del documento de investigación “Cybersecurity Challenges in the Maritime Sector” [145]. Las embarcaciones generan infinidad de datos debido a los diversos sistemas de automatización que incorporan, los cuales pueden ser corrompidos por hackers, además un ciber ataque podría cerrar un barco, divulgar información valiosa, deshabilitar el AIS (Automatic Identification System) del barco y/o crear informes AIS falsos o engañosos que faciliten la piratería cibernética y actores criminales, terroristas o incluso estatales.



SISTEMAS DE AUTOMATIZACIÓN PARA BARCOS MODERNOS Y AUTÓNOMOS [145]

Efectuando un análisis de las publicaciones recopiladas se obtienen las siguientes aplicaciones más significativas:

- Detección de anomalías en redes mediante registros de tráfico
- Detección de ataques basados en la Web
- Análisis del comportamiento de los atacantes enemigos
- Métodos de defensa de seguridad de red estadística y eficiencia técnica
- Análisis y pronóstico del peligro potencial oculto y ley del ataque del enemigo
- Clasificación de malware y de los ataque de seguridad

Artículos relacionados

Año	Artículo	Referencia
2013	Big Data Analytics for Security	https://doi.org/10.1109/MSP.2013.138
2015	Big Data in Distributed Analytics, Cybersecurity, Cyber Warfare and Digital Forensics	http://pubs.sciepub.com/dt/1/1/5
2016	Application of Big Data in cyberspace warfare	https://doi.org/10.1109/CCDC.2016.7531833
2016	Big Data analytics for security and privacy challenges	https://doi.org/10.1109/CCAA.2016.7813688
2016	Security issues and challenges of Big Data analytics and visualization	https://doi.org/10.1109/IC3I.2016.7917961
2017	Data Placement for Privacy-Aware Applications over Big Data in Hybrid Clouds	https://doi.org/10.1155/2017/2376484
2017	Cybersecurity and Network Forensics: Analysis of Malicious Traffic towards a Honeynet with Deep Packet Inspection	https://doi.org/10.3390/app7101082
2017	Big Data Analytics with Applications in Insider Threat Detection	https://doi.org/10.1201/9781315119458

2017	Big Data Analytics in Cyber Security	https://www.ijert.org/big-data-analytics-in-cyber-security
2018	Big Data Analytics for Information Security	https://doi.org/10.1155/2018/7657891
2018	Big-Data Analysis of Multi-Source Logs for Network Anomaly Detection	https://doi.org/10.1109/ICCSS.2018.8572364
2018	Big Data Meet Cyber-Physical Systems	https://doi.org/10.1109/ACCESS.2018.2878681
2018	Big Data Security and Privacy Protection	https://dx.doi.org/10.2991/icmcs-18.2018.56
2018	Collective Data-Sanitization for Preventing Sensitive Information Inference Attacks in Social Networks	https://doi.org/10.1109/TDSC.2016.2613521
2018	Developing Cyber-Personas from Syslog Files for Insider Threat Detection: A Feasibility Study	https://doi.org/10.1201/9780429445491
2018	Hardware/Software Adaptive Cryptographic Acceleration for Big Data Processing	https://doi.org/10.1155/2018/7631342
2018	Fighting Cyber Terrorism Comparison of Turkey and Russia	https://doi.org/10.1109/IBIGDELFT.2018.8625270
2018	Quasi-cliques Analysis for IRC Channel Thread Detection	https://doi.org/10.1007/978-3-030-05411-3_47
2018	New Techniques in Profiling Big Datasets for Machine Learning with A Concise Review of Android Mobile Malware Datasets	https://doi.org/10.1109/IBIGDELFT.2018.8625275
2018	Network Modelling and Analysis of Data and Relationships: Developing Cyber and Complexity Science	https://doi.org/10.1201/9780429445491
2018	The Next Generation Cognitive Security Operations Center Adaptive Analytic Lambda Architecture for Efficient Defense against Adversarial Attacks	https://doi.org/10.3390/bdcc3010006
2019	Big Data Analytics for Cyber Security	https://doi.org/10.1155/2019/4109836
2019	Artificial Intelligence and Big Data Analytics in Support of Cyber Defense	http://dx.doi.org/10.4018/978-1-5225-8304-2.ch002
2019	Cybercrime Investigations in the Era of Smart Applications: Way Forward Through Big Data	https://doi.org/10.1109/BigData47090.2019.9006596
2019	Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey	https://doi.org/10.3390/app9204396
2019	Bitcoin and Cybersecurity: Temporal Dissection of Blockchain Data to Unveil Changes in Entity Behavioral Patterns	https://doi.org/10.3390/app9235003
2020	A Systematic Review of Defensive and Offensive Cybersecurity with Machine Learning	https://doi.org/10.3390/app10175811
2020	A Stacking Ensemble for Network Intrusion Detection Using Heterogeneous Datasets	https://doi.org/10.1155/2020/4586875

2020	Detecting Cyber Threat Event from Twitter Using IDCNN and BiLSTM	https://doi.org/10.3390/app10175922
2020	Improving Incident Response in Big Data Ecosystems by Using Blockchain Technologies	https://doi.org/10.3390/app10020724
2020	Endogenous Security Defense against Deductive Attack: When Artificial Intelligence Meets Active Defense for Online Service	https://doi.org/10.1109/MCOM.001.1900367
2020	Inteligencia artificial para la seguridad y defensa del ciberespacio (Usos militares de la inteligencia artificial, la automatización y la robótica (IAA&R))	https://publicaciones.defensa.gob.es/usos-militares-de-la-inteligencia-artificial-la-automatizacion-y-la-robotica-iaa-r-libros-ebook.html
2020	Cybersecurity data science: an overview from machine learning perspective	https://doi.org/10.1186/s40537-020-00318-5
2020	Cyber-Attack Consequence Prediction	https://doi.org/10.48550/arXiv.2012.00648
2020	Challenge and Countermeasure of Big Data to Army Information Security	https://doi.org/10.1016/j.dsm.2021.06.001
2020	Data Science in Cybersecurity and Cyberthreat Intelligence	https://link.springer.com/book/10.1007/978-3-030-38788-4
2020	Seven Pitfalls of Using Data Science in Cybersecurity	https://doi.org/10.1007/978-3-030-38788-4_6
2020	Intrusion detection in computer systems by using artificial neural networks with Deep Learning approaches	https://doi.org/10.48550/arXiv.2012.08559
2020	Hybrid Malware Classification Method Using Segmentation-Based Fractal Texture Analysis and Deep Convolution Neural Network Features	https://doi.org/10.3390/app10144966
2020	Providing Email Privacy by Preventing Webmail from Loading Malicious XSS Payloads	https://doi.org/10.3390/app10134425
2021	Enabling Efficient Cyber Threat Hunting With Cyber Threat Intelligence	https://doi.org/10.48550/arXiv.2010.13637
2021	A Machine Learning Approach for DDoS Detection on IoT Devices	https://doi.org/10.48550/arXiv.2110.14911
2021	An Efficient implementation of Network Malicious Traffic Screening based on Big Data Analytics	https://doi.org/10.1109/ICOSEC51865.2021.9591700
2021	Big Data in cybersecurity: a survey of applications and future trends	https://doi.org/10.1007/s40860-020-00120-3
2021	Classifying Security Attacks in IoT Using CTM Method	https://doi.org/10.1007/978-3-030-53440-0_32
2021	Data security governance in the era of Big Data: status, challenges, and prospects	https://doi.org/10.1016/j.dsm.2021.06.001
2021	Darknet Traffic Big-Data Analysis and Network Management for Real-Time Automating of the Malicious	https://doi.org/10.3390/electronics10070781

	Intent Detection Process by a Weight Agnostic Neural Networks Framework	
2021	Designing Trojan Detectors in Neural Networks Using Interactive Simulations	https://doi.org/10.3390/app11041865
2021	Data Poisoning Attacks and Defenses to Crowdsourcing Systems	https://doi.org/10.48550/arXiv.2102.09171
2021	Intelligent Cyber Attack Detection and Classification for Network-Based Intrusion Detection Systems	https://doi.org/10.3390/app11041674
2021	Differential Privacy in Privacy-Preserving Big Data and Learning: Challenge and Opportunity	https://doi.org/10.1007/978-3-030-96057-5_3
2021	C4I System Security Architecture A Perspective on Big Data Lifecycle in a Military Environment	https://doi.org/10.3390/su132413827
2021	Journalistic Voting System's Effects on Election Security Threats and Gerrymandering	https://doi.org/10.48550/arXiv.2110.04642
2021	Big Data Cybersecurity Monitoring System using Machine Learning	https://doi.org/10.1109/FABS52071.2021.9702637
2021	On the Scalability of Big Data Cyber Security Analytics Systems	https://doi.org/10.1016/j.jnca.2021.103294
201	Bayesian games for the cybersecurity of nuclear power plants	https://doi.org/10.1016/j.ijcip.2021.100493
2021	Encryption and Real Time Decryption for protecting Machine Learning models in Android Applications	https://doi.org/10.48550/arXiv.2109.02270
2021	TEDL A Text Encryption Method Based on Deep Learning	https://doi.org/10.3390/app11041781
2021	Trust but Verify: Cryptographic Data Privacy for Mobility Management	https://doi.org/10.48550/arXiv.2104.07768
2021	Two-stage Deep Stacked Autoencoder with Shallow Learning for Network Intrusion Detection System	https://doi.org/10.48550/arXiv.2112.03704
2021	Machine Learning-Based Malicious X.509 Certificates' Detection	https://doi.org/10.3390/app11052164
2021	Studying the Role of Social Bots During Cyber Flash Mobs	https://doi.org/10.1007/978-3-030-80387-2_16
2021	Use of Security Logs for Data Leak Detection: A Systematic Literature Review	https://doi.org/10.1155/2021/6615899
2021	Detecting Web-Based Attacks with SHAP and Tree Ensemble Machine Learning Methods	https://doi.org/10.3390/app12010060
2021	Security Threats and Defensive Approaches in Machine Learning System Under Big Data Environment	https://doi.org/10.1007/s11277-021-08284-8
2021	VMFCVD: An Optimized Framework to Combat Volumetric DDoS Attacks using Machine Learning	https://doi.org/10.1007/s13369-021-06484-9
2021	Research on Intelligent Analysis Technology of Network Security Risk Based on Big Data	https://doi.org/10.1088/1742-6596/1792/1/012036
2021	Cybersecurity Challenges in the Maritime Sector	https://doi.org/10.3390/network2010009
2022	Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends	https://doi.org/10.3390/info13030146

2022	Investigating the Influence of Feature Sources for Malicious Website Detection	https://doi.org/10.3390/app12062806
2022	Security for Machine Learning-based Software Systems: a survey of threats, practices and challenges	https://doi.org/10.48550/arXiv.2201.04736
2022	Achieving Differential Privacy with Matrix Masking in Big Data	https://doi.org/10.48550/arXiv.2201.04211
2022	Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review	https://doi.org/10.3390/electronics11020198
2022	Interactive Stereoscopically Perceivable Multidimensional Data Visualizations for Cybersecurity	http://dx.doi.org/10.46713/jdst.004.03
2022	Introducing the CYSAS-S3 Dataset for Operationalizing a Mission-Oriented Cyber Situational Awareness	https://doi.org/10.3390/s22145104

TABLA 9: ARTÍCULOS CIBERDEFENSA Y CIBERSEGURIDAD

3.4. Análisis Forense Digital

El análisis forense digital es una rama de la ciencia forense centrada en la detección, adquisición, tratamiento, análisis y comunicación de datos almacenados por medios electrónicos. En la actualidad, las pruebas electrónicas están presentes en casi todas las actividades delictivas, por lo que el apoyo que proporciona el análisis forense digital es fundamental para las investigaciones que llevan a cabo las fuerzas del orden. Dicha evidencia puede extraerse de una amplia gama de fuentes, como, por ejemplo, ordenadores, teléfonos inteligentes, soportes de almacenamiento a distancia, sistemas aéreos no tripulados o aparatos náuticos. El objetivo principal del análisis forense digital es extraer datos contenidos en pruebas electrónicas, transformarlos en información de utilidad operativa y presentar las conclusiones con miras a la persecución penal. En todas las fases del proceso se utilizan avanzadas técnicas forenses, a fin de que las conclusiones resulten admisibles ante un tribunal. [146]

Se propone la existencia de los siguientes tipos de análisis forense digital de acuerdo con en el documento “Big Data Forensic Analytics” [147]:

- Análisis forense de redes
- Informática Forense
- Análisis forense móvil
- Forense en vivo
- Análisis forense de grandes datos
- Base de datos forense

Cuando se emplean grandes flujos de datos, los investigadores forenses se enfrentan a grandes dificultades mientras identifican las pruebas necesarias de un gran conjunto de datos y recopilan y analizan esas pruebas. En efecto, cuantos más datos estén disponibles, más difícil será detectar actividades fraudulentas y usuarios maliciosos detrás de esas actividades. [148].

Un flujo de trabajo para el análisis forense es planteado en “Digital Forensics as a Big Data Challenge” [149], además de considerar cómo cada fase puede tener que adaptarse a escenarios de Big Data, pero siguiendo la normativa internacional ISO/IEC 27037 que cubre la identificación, recopilación, adquisición y conservación de evidencia digital o evidencia "potencial".

- Identificación y colección: seleccionar evidencia de manera oportuna, justo en la escena.
- Adquisición: cuando la imagenología bit a bit clásica no es factible debido al tamaño de la evidencia, se pueden realizar procedimientos de priorización o “triaje”, debidamente justificados y documentados porque la integridad ya no es absoluta y la fuente original se ha modificado, aunque solo sea seleccionando qué adquirir. La visualización puede ser una herramienta muy útil, tanto para el análisis de sistemas de archivos de bajo nivel como para el análisis de contenido de nivel superior.
- Preservación: la conservación de todas las pruebas de forma segura y el cumplimiento de los requisitos legales exige una inversión considerable para los laboratorios forenses que trabajan en un número significativo de casos.
- Análisis: la integración de métodos y herramientas de la ciencia de datos implica superar el análisis forense de la "fábrica de salchichas" todavía muy extendido en la actualidad, donde los operadores poco calificados dependen en gran medida de las herramientas todo en uno de apuntar y hacer clic para realizar el análisis. Los analistas deberán incluir una pluralidad de herramientas en su panoplia y no solo eso, sino comprender y evaluar los algoritmos y las implementaciones en las que se basan.
- Informes el informe final de un análisis realizado utilizando conceptos de ciencia de datos debe contener evaluaciones precisas de las herramientas, los métodos utilizados, incluidos los datos del proceso de validación, y la documentación precisa es aún más fundamental ya que la repetibilidad estricta se vuelve muy difícil de mantener.

Como técnicas de Big Data para poder emplear plantea el mapa reducido, los arboles de decisión y el random forest. Para audio forense recomienda técnicas de aprendizaje no supervisado y técnicas de clasificación para imágenes. También el uso de redes neuronales para el reconocimiento de patrones complejos en el análisis forense de redes, y para la verificación de autoría o la clasificación de grandes cuerpos de textos no estructurados el empleo de técnicas de Procesamiento del lenguaje natural (NLP).

Los retos del análisis forense digital son planteados en el artículo “Big Data and Digital Forensics” [150]. Entre los retos mayoritariamente conocidos se encuentran el uso de cifrado, la necesidad de manejar diferentes tipos de dispositivos, formatos de archivos y contenidos, la necesidad de analizar a veces datos incompletos e inconsistentes, la disponibilidad de herramientas anti-forense y la necesidad para formas especializadas de extraer información de algunos dispositivos. En cambio, entre los retos emergentes incluyen el número y el tamaño cada vez mayores de la capacidad de almacenamiento en muchos dispositivos, el volumen cada vez mayor de datos que se pueden recopilar en relación con una investigación y la necesidad de proporcionar resultados rápidos durante dicho análisis. Dichos desafíos emergentes se pueden atribuir a los avances tecnológicos, la capacidad de interconexión entre dispositivos capaces de generar volúmenes de datos, la necesidad de recopilar e investigar los datos que se encuentran en las bases de datos, así como la necesidad de realizar análisis forenses. sobre la información almacenada en las nubes.

Los autores del artículo “Even Big Data is not enough: need for a novel reference modelling for forensic document authentication” [151], plantean que en el ámbito de la ciencia forense muchos expertos a menudo se ocupan de la autenticación o verificación de una entidad determinada, como puede ser la autenticación o verificación de firma, escritura a mano, papel legal, moneda bancaria, arte, audio, video, etc. Basado en este problema, ha surgido una disciplina separada de la ciencia forense que se conoce como examen de documentos cuestionados (QDE), que tiene el objetivo de brindar una opinión sobre un documento sospechoso o cuestionable basado en una variedad de procesos y métodos científicos. El

problema de autenticación de documentos forenses es que los datos de ciertas clases pueden no estar disponibles incluso en el escenario de Big Data, aunque se espera que la investigación futura se concentre en desarrollar enfoques más nuevos para el modelado de referencia para explotar la característica del problema de autenticación.

Hay que considerar, que dentro de la ciencia forense, en concreto para la identificación humana forense, se encuentra el análisis biométrico que sirve para identificar y autenticar personas de una manera rápida, mediante el uso de características biológicas / morfológicas o de comportamiento únicas de la persona, como son las huellas dactilares, el iris del ojo, la voz o el reconocimiento facial, que a menudo son utilizados por oficiales de policía y testigos en su descripción de sospechosos no identificados. Un ejemplo de aplicación de la identificación mediante el uso del iris es el caso de la "chica afgana", dónde durante 17 años el fotógrafo Steve McCurry intentó localizar a la niña que fotografío en 1984. Finalmente fue localizada y reconocida por el patrón de sus iris en 2002 en Afghanistán. [152]

El reconocimiento facial se ha vuelto significativo para videos de Internet debido a que la auditoría de contenido para videos de Internet se está volviendo cada vez más importante, para el reconocimiento de personas políticamente sensibles, el reconocimiento de personas prohibidas en Internet, el reconocimiento de personas criminales, etc. Aunque los sistemas de reconocimiento facial actuales funcionan bien en escenas relativamente restringidas, enfrentan serios desafíos cuando se usan en videos de Internet del mundo real, como la creación secundaria de internautas, imágenes borrosas graves, cambios de postura abundantes o oclusión [153].

Durante las últimas décadas, el panorama de la biometría ha estado dominado en gran medida por sistemas que adquieren y procesan datos de huellas dactilares, cara, iris, voz o combinaciones de estos. Debido a la creciente tasa de éxito de la falsificación o elusión de tales enfoques, los investigadores se han visto obligados a considerar información sensorial alternativa y mejores soluciones para la toma de decisiones, manteniendo una configuración de operación y adquisición cómoda y fácil de usar, de acuerdo a lo planteado en el paper "Off-Person ECG Biometrics Using Spatial Representations and Convolutional Neural Networks" [154]. Una sólida línea de investigación ha considerado los rastros fisiológicos como el electrocardiograma (ECG), el fotopletismograma (PPG) o incluso el electroencefalograma (EEG) como promesas viables para aumentar la resistencia contra el fraude.

A la hora de emplear datos biométricos se pueden utilizar para dos funciones distintas, autentificación e identificación. La identificación responde la pregunta "¿Quién es usted?" y requiere una base de datos centralizada, mientras que la autenticación responde a la pregunta: "¿Es usted realmente quien dice ser?" y los datos pueden ser almacenados en un dispositivo descentralizado. Los riesgos de emplear datos biométricos surgen cuando dichos datos son usados para fines distintos a los acordados por el ciudadano, ya sea por los proveedores de servicios o por estafadores. [155]

Como aplicaciones más significativas en el ámbito forense digital se pueden distinguir las siguientes:

- Detección de video manipulado y localización de fotogramas manipulados
- Identificación humana a través de datos biométricos (ojos, oreja, EEG)
- Detección de fraudes
- Clasificación basada en la huella digital
- Detección de huellas de zapatos

- Análisis de evidencia digital extraída de dispositivos electrónicos
- Reconocimiento de voz
- Detección de Deep Fakes
- Detección de falsificaciones

Artículos relacionados

Año	Artículo	Referencia
2013	Digital Forensics as a Big Data Challenge	https://doi.org/10.1007/978-3-658-03371-2_17 https://www.forensicfocus.com/articles/digital-forensics-as-a-big-data-challenge/
2015	Big Data Computing for Digital Forensics on Industrial Control Systems	https://doi.org/10.1109/IRI.2015.94
2015	Digital Forensics in the Age of Big Data: Challenges, Approaches, and Opportunities	https://doi.org/10.1109/HPCC-CSS-ICESS.2015.305
2016	Big Data and digital forensics	https://doi.org/10.1109/ICCCF.2016.7740422
2016	Big forensic data reduction: digital forensic images and electronic evidence	https://doi.org/10.1007/s10586-016-0553-1
2016	A forensic cloud environment to address the Big Data challenge in digital forensics	https://doi.org/10.1109/SAI.2016.7556039
2017	Big Data as a challenge and opportunity in digital forensic investigation	https://doi.org/10.1109/TEL-NET.2017.8343573
2017	Entities of Interest, Discovery in Digital Traces	https://doi.org/10.48550/arXiv.2102.10962
2017	Cybersecurity and Network Forensics: Analysis of Malicious Traffic towards a Honeynet with Deep Packet Inspection	https://doi.org/10.3390/app7101082
2018	Accurate and Scalable Image Clustering Based On Sparse Representation of Camera Fingerprint	https://doi.org/10.48550/arXiv.1810.07945
2018	Election Forensics quantitative methods for electoral fraud detection	https://doi.org/10.1016/j.forsciint.2018.11.010
2018	Queue Classification for Fraud Types: Banking Domain	https://doi.org/10.1007/978-981-13-1274-8_20
2018	A Uniformed Evidence Process Model for Big Data Forensic Analysis	https://doi.org/10.1007/978-981-13-1328-8_82
2018	Big Data Forensic Analytics	https://doi.org/10.1007/978-981-13-1274-8_9
2018	Big Data Forensics: Challenges And Approaches	https://www.ijrar.org/papers/IJRAR1944282.pdf
2018	Evidence Collection Agent Model Design for Big Data Forensic Analysis	https://doi.org/10.1007/978-981-13-1328-8_83
2018	Greening Cloud-Enabled Big Data Storage Forensics: Syncany as a Case Study	https://doi.org/10.1109/TSUSC.2017.2687103
2018	CloudMe Forensics: A Case of Big-Data Investigation	https://doi.org/10.1002/cpe.4277

2018	A Review of Evidence Extraction Techniques in Big Data Environment	https://doi.org/10.1109/ICSCEE.2018.8538437
2018	Evaluating Automated Facial Age Estimation Techniques for Digital Forensics	https://doi.org/10.1109/SPW.2018.00028
2019	Human identification using a new matching Pursuit-based feature set of ECG	https://doi.org/10.1016/j.cmpb.2019.02.009
2019	Face Recognition in Real-world Internet Videos Based on Deep Learning	https://doi.org/10.1109/ISNE.2019.8896630
2019	Shoe-Print Image Retrieval With Multi-Part Weighted CNN	https://doi.org/10.1109/ACCESS.2019.2914455
2019	Autonomous Vehicles' Forensics in Smart Cities	https://doi.org/10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00301
2019	Even Big Data is not enough: need for a novel reference modelling for forensic document authentication	https://doi.org/10.1007/s10032-019-00345-w
2019	Learning Wear Patterns on Footwear Outsoles Using Convolutional Neural Networks	https://doi.org/10.1109/TrustCom/BigDataSE.2019.00067
2019	Research on Forensic Model of Online Social Network	https://doi.org/10.1109/ICCCBDA.2019.87257464
2019	Research on Digital Forensics Framework for Malicious Behavior in Cloud	https://doi.org/10.1109/IAEAC47372.2019.8997702
2020	Comparative analysis on integrated digital forensic tools for digital forensic investigation	https://doi.org/10.1088/1757-899X/834/1/012034
2020	A Framework for Digital Forensic Investigation of Big Data	https://doi.org/10.1109/ICAIBD49809.2020.9137498
2020	Deep learning for EEG-based biometric recognition	https://doi.org/10.1016/j.neucom.2020.06.009
2020	FATE:Fingerprints Automatically Targeting and Extracting for image source identification	https://doi.org/10.1109/BigCom51056.2020.00024
2020	Forensic Analysis of digital evidence extracted from Amazon Echo	https://doi.org/10.1109/ICATMRI51801.2020.9398391
2020	Forensic Analysis of Instagram on Android	https://doi.org/10.1088/1757-899X/1007/1/012116
2020	Multiple Microphone Speaker Recognition System for Second Language Based on Biomimetic Pattern Recognition with Big Data Fusion	https://doi.org/10.1088/1757-899X/790/1/012144
2020	SoK: Exploring the State of the Art and the Future Potential of Artificial Intelligence in Digital Forensic Investigation	https://doi.org/10.1145/3407023.3407068
2020	Methodology for Forensics Data Reconstruction on Mobile Devices with Android Operating System Applying In-System Programming and Combination Firmware	https://doi.org/10.3390/app10124231
2020	On the using Datamessage as evidence of Cybercrime	https://doi.org/10.1088/1757-899X/1069/1/012037
2020	Off-Person ECG Biometrics Using Spatial Representations and Convolutional Neural Networks	https://doi.org/10.1109/ACCESS.2020.3042547
2020	Research on Forensics of Social Network Relationship Based on Big Data	https://doi.org/10.1088/1742-6596/1584/1/012022

2020	Research on Computer Forensics Technology Based on Data Recovery	https://doi.org/10.1088/1742-6596/1648/3/032025
2021	DECADE - Deep Learning Based Content-hiding Application Detection System for Android	https://doi.org/10.1109/BigData52589.2021.9671842
2021	Email Classification and Forensics Analysis using Machine Learning	https://doi.org/10.1109/SWC50871.2021.00093
2021	Extracting features from wrist vein images using fractional fourier transform for person verification	https://doi.org/10.1088/2057-1976/abf7d2
2021	Digital Forensics Process of an Attack Vector in ICS environment	https://doi.org/10.1109/BigData52589.2021.9671986
2021	Evidence Collection and Qualitative Analysis of Electronic Data in the Background of Artificial Intelligence	https://doi.org/10.1088/1742-6596/2037/1/012096
2021	A Study of Voice Print Recognition Technology	https://doi.org/10.1109/IWCMC51323.2021.9498681
2021	Answering to 5W Using Digital Forensics Data	https://doi.org/10.1109/ISCSIC54682.2021.00043
2021	Mobile APP fingerprint feature extraction pattern recognition based on Random Game	https://doi.org/10.1088/1742-6596/1792/1/012003
2021	Next Generation Digital Forensic Investigation Model (NGDFIM) - Enhanced, Time Reducing and Comprehensive Framework	https://doi.org/10.1088/1742-6596/1767/1/012054
2021	Speaker Identification Based On Ivector And Xvector	https://doi.org/10.1088/1742-6596/1827/1/012133
2021	Hybrid deep convolutional neural models for iris image recognition	https://doi.org/10.1007/s11042-021-11482-y
2021	3D corrective nose reconstruction from a single image	https://doi.org/10.1007/s41095-021-0237-5
2021	A Comprehensive Survey of Detection of Tampered Video and Localization of Tampered Frame	https://doi.org/10.1007/s11277-021-09227-z
2022	An improved detection of blind image forgery using hybrid deep belief network and adaptive fuzzy clustering	https://doi.org/10.1007/s11042-022-12923-y
2022	AEPI: insights into the potential of deep representations for human identification through outer ear images	https://doi.org/10.1007/s11042-022-12025-9
2022	Dental biometric systems: a comparative study of conventional descriptors and deep learning-based features	https://doi.org/10.1007/s11042-022-12019-7
2022	An enhanced copy-move forgery detection using machine learning based hybrid optimization model	https://doi.org/10.1007/s11042-022-11977-2
2022	Mobile Contactless Fingerprint Recognition: Implementation, Performance and Usability Aspects	https://doi.org/10.3390/s22030792

TABLA 10: ARTÍCULOS ANÁLISIS FORENSE

3.5. Sistemas de datos Geográficos

Los geocientíficos militares, principalmente geógrafos y geólogos, aplican las ciencias de la tierra para apoyar el combate militar y las actividades en tiempo de paz, proporcionando un análisis del terreno que permite a los líderes militares comprender las limitaciones de un entorno operativo, maximizar su potencial para acciones ofensivas o defensivas y explotar sus recursos naturales. Tradicionalmente, los geógrafos han generado mapas topográficos y temáticos, además de información sobre el tiempo, el clima, la vegetación y otras características de la superficie, importantes para la planificación estratégica o táctica y las decisiones sobre el movimiento y/o concentración de tropas. Mientras que los geólogos han guiado la ubicación y construcción de fortificaciones, el desarrollo de suministros seguros de agua, la excavación de túneles mineros y otras instalaciones subterráneas, la ubicación y construcción de caminos, puentes y aeródromos temporales, la evaluación de la movilidad a campo traviesa y la determinación de las fuentes de piedra y agregados para carreteras, balasto ferroviario o trabajos de construcción militar [156]. En las últimas décadas estas disciplinas se han fusionado con otras geociencias para proporcionar una mejor comprensión de los panoramas operativos actuales mediante el empleo de sistemas de datos geográficos.

Un Sistema de Información Geográfica (SIG), entre sus múltiples definiciones se encuentran [157]:

- Tecnología informática para gestionar y analizar información espacial.
- Conjunto de herramientas para reunir, introducir en el ordenador, almacenar, recuperar, transformar y cartografiar datos espaciales sobre el mundo real para un conjunto particular de objetivos.
- Tipo especializado de base de datos con capacidad de manejar datos geográficos (espacialmente referenciados) y que se pueden representar como imágenes.

Dentro de las funciones de un SIG se encuentran: incorporación de la información, gestión de la información, análisis de la información e interrelación con el usuario. Adicionalmente, un SIG puede usarse como sistema de apoyo a la decisión, en donde el propio sistema es estructurado como un elemento de ayuda a la toma de decisiones mediante distintas hipótesis de simulación que convergen en diferentes resultados en función de los datos y procedimientos elegidos.

La teledetección o *remote sensing* es un modo de obtener información acerca de objetos tomando y analizando datos sin que los instrumentos empleados para adquirir los datos estén en contacto directo con el objeto [158]. En la teledetección hay varios elementos fundamentales:

1 - plataforma para sostener el instrumento

2 - objeto que se va a observar

3 - instrumento o sensor para observar el objetivo

4 - información que se obtiene con los datos de la imagen y cómo se emplea y almacena esta información

Habitualmente, la teledetección consiste en la adquisición de datos de la superficie terrestre desde sensores instalados en plataformas espaciales, como son los satélites, debido al a interacción electromagnética entre el terreno y el sensor genera una serie de datos que son procesados posteriormente para obtener información interpretable de la Tierra. [159]

En España, se adquieren y procesan datos de distintos satélites comerciales con distintos tamaños de píxel y cada año más organismos públicos hacen uso sistemático de ellas. Se puede considerar que el uso masivo de imágenes de teledetección comenzó en el año 2008, con la puesta a disposición de imágenes Landsat bajo licencia libre y abierta, pero la verdadera democratización de la teledetección llegó en el año 2014, con el lanzamiento del satélite radar Sentinel 1A en 2014 y el satélite óptico Sentinel 2A en 2015, pertenecientes ambos al programa Copérnicus de la Comisión Europea (anteriormente conocido como GMES). [159] Los satélites Sentinel proporcionan una diversidad de datos:

- Sentinel-1, que proporcionan imágenes radar terrestres y oceánicas.
- Sentinel-2, que proporcionan imágenes ópticas terrestres.
- Sentinel-3, proporciona servicios globales de vigilancia terrestre y oceánica.
- Sentinel-4, proporciona datos para la vigilancia de la composición atmosférica.
- Sentinel-5, también proporciona datos para la vigilancia de la composición atmosférica.
- Sentinel-6, proporciona datos altimétricos de alta precisión.

Últimamente en lugar de emplear imágenes obtenidas de satélites en algunas aplicaciones se tiende a emplear imágenes aéreas recopiladas por UAV al presentar varias ventajas, incluido un gran campo de visión, alta resolución espacial, flexibilidad y alta movilidad. En comparación con las imágenes satelitales las imágenes aéreas basadas en UAV tienen un costo mucho menor y brindan vistas más actualizadas debido a que muchos mapas satelitales tienen varios meses de antigüedad y no presentan cambios recientes.

Aunque el uso masivo de datos de teledetección ha sido impulsado en la últimas décadas debido a las innovaciones en sistemas y tecnologías, en un documento de RAND de 1993, “U.S. Spaced-Bases Remote Sensing Challenges and prospects” [160], se concluía que a medida que la utilidad de los datos de teledetección se comprenda y aprecie más ampliamente, aumentarán los esfuerzos para explotar esos datos de maneras únicas, borrando así las distinciones entre los usuarios en las agencias federales, los gobiernos estatales y locales y las entidades privadas. También en él, se mostraba en forma de tabla las aplicaciones de la teledetección en función de los sectores y usuarios, como se muestra a continuación.

Table S.1

Illustrative Remote Sensing Applications by Sectors and Users

Remote Sensing Applications	Civil Sector	National Security/ Military Sector	Scientific Sector	Commercial Sector
Agriculture, forestry, range resources	Assessment of flood damage (FEMA) Grove surveys (Forestry Service)	Determination of soil, vegetation conditions (USA) Assessment of foreign agricultural output (DOS, AID)	Crop diseases analysis (USDA, academia) Global change research (NASA, international research organizations)	Identification of vegetation, crops, timber, range vegetation (USDA, farmers, GIS industry)
Land use and planning	Urban planning (DOT, state and local governments)	Terrain analysis (USA, USMC) Base siting (DoD)	Wetlands monitoring (EPA)	Solid waste management (state and local governments, private industry)
Mapping	Siting/surveying for public/ private facilities (HUD, state and local governments) Emergency planning (FEMA, state and local governments)	Position locating (all services) Monitoring of support equipment movement (all services) Threat analysis (DIA)	Environmental impact assessments (EPA, scientific research organizations) Forest, grove monitoring (DOI)	Transportation networks planning (state and local governments, private industry) Regional planning (state and local governments, private industry)
Geology	Radioactive waste storage (DOE, NRC)	Soil compaction (USA, USMC)	Mapping linears (fractures) (USGS)	Search for surface guides to mineralization (private industry)
Water resources	Floods and flood plains mapping and assessment (DOT, state and local governments, Water Resources Council)	Ice, water surface analysis (USN) Disaster relief (FEMA, many federal agencies, state and local governments)	Pollution monitoring (EPA, academia) Soil salinity (local governments, scientific researchers)	Ground water location (state and local governments, private developers)
Coastal resources	Mapping of shoals and shallow areas (USCG) Drug law enforcement (DEA)	Base and port siting, closing (DoD, USN)	Wildlife habitat monitoring (NSF, EPA, Fish and Wildlife Service)	Ice floe mapping for shipping (USCG, private shipping companies)
Environmental monitoring	Civil weather forecasting (NOAA) Hurricane prediction (National Hurricane Center, FEMA, state and local governments)	Monitoring of air turbulence (USAF) Weather monitoring for air, ground operations (all services)	Atmospheric research (NASA) Global climate change (NASA, international research organizations)	Drought impact assessment (agricultural industry)

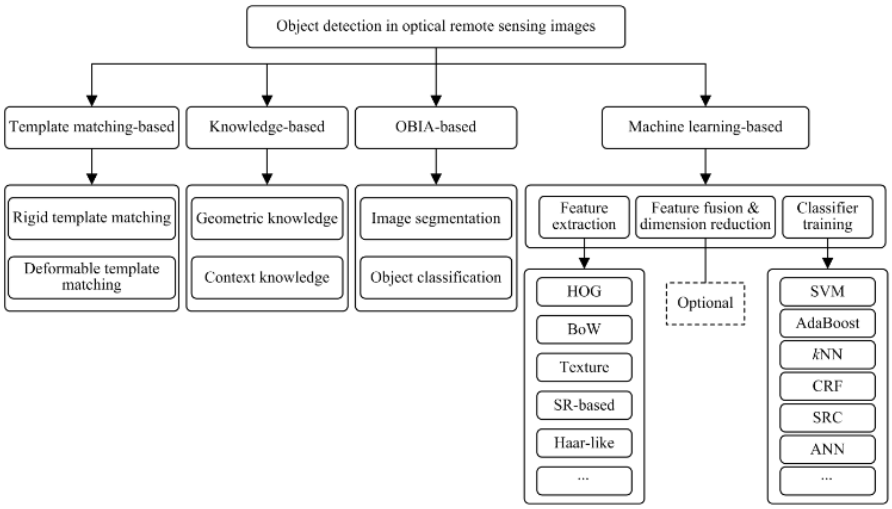
SOURCES: Office of Space Commerce, *Space Business Indicators, June 1992*, Department of Commerce, Washington, D.C., June 1992, pp. 26–27, citing Earth Observation Satellite Company (EOSAT); Office of Technology Assessment, *Remotely Sensed Data From Space: Distribution, Pricing, and Applications; An OTA Background Paper*, Congress of the United States, Washington, D.C., July 1992, p. 3; and RAND.

N.B.: See the list of acronyms on page xv of this Note for organizational titles.

APLICACIONES ILUSTRATIVAS DE LA TELEDETECCIÓN POR SECTORES Y USUARIOS [160]

El reciente desarrollo de nuevos sensores ha permitido la medición remota de una gran área de la superficie terrestre, en conjunto con los avances en visión artificial, aprendizaje automático e inteligencia artificial, combinados con un aumento sin precedentes en el poder de procesamiento computación, han dado lugar a técnicas innovadoras de procesamiento de datos de detección remota que simplifican el manejo de grandes cantidades de datos complejos. Los datos de teledetección se integran en algoritmos de modelado que describen procesos de superficie y subsuelo a diferentes escalas. Aunque en ciertos casos antes de que puedan utilizarse, los datos de teledetección deben corregirse por los efectos que se originan en los sensores, las plataformas en las que se implementan, las características atmosféricas y las restricciones geométricas. Cuando los datos están calibrados y geo localizados, pueden usarse como cantidades físicas, como reflectancia y temperaturas, o como imágenes. La teledetección geológica actualmente abarca enfoques multitemporales, de múltiples fuentes y de múltiples escalas, consiguiendo caracterizar con precisión la configuración geológica de grandes áreas e incluso sus cambios a lo largo del tiempo. Logrando garantizar encuestas y monitoreo rentables, seguros y rápidos que no solo beneficien a la comunidad investigadora sino a la sociedad en general. [161]

El empleo de las imágenes de teledetección para la detección de objetos es un problema fundamental pero desafiante en el campo del análisis de imágenes aéreas y satelitales, al jugar un papel importante para una amplia gama de aplicaciones y estar recibiendo una atención significativa en los últimos años. En el documento “A survey on object detection in optical remote sensing images” [162] revisan la literatura sobre la detección de objetos pero no limitándose a la detección de categorías como carreteras, edificios, árboles, vehículos, barcos, aeropuertos y áreas urbanas. Para la detección de objetos se plantean métodos de detección de objetos basados en coincidencia de plantillas, métodos de detección de objetos basados en conocimiento, métodos de detección de objetos basados en análisis de imágenes basados en objetos (OBIA), métodos de detección de objetos basados en aprendizaje automático.



TAXONOMÍA DE MÉTODOS PARA LA DETECCIÓN DE OBJETOS EN TELEDETECCIÓN [162]

Una de las categorías de detección de objetos es la detección de vehículos, en concreto la detección de coche, aunque las ideas y principios se pueden explotar a la detección de convoyes, tanques u otros vehículos militares. En el artículo de investigación "Vehicle Detection from Aerial Images Using Deep Learning: A Comparative Study" [163], se aborda el problema de la detección de coches a partir de imágenes aéreas empleando redes neuronales convolucionales Este problema presenta desafíos adicionales en comparación con la detección de automóviles (o cualquier objeto) a partir de imágenes terrestres porque las características de los vehículos a partir de imágenes aéreas son más difíciles de discernir. Para afrontar el problema los autores emplean dos conjuntos de datos con diferentes características para verificar el impacto de varios factores, como la altitud del UAV, la resolución de la cámara y el tamaño del objeto, mediante la realización de diversos experimentos de entrenamiento para tener en cuenta el efecto de diferentes valores de hiperparámetros y empleo de una variedad de métricas. Aunque el problema que encontraron con varios de los métodos analizados es que exhiben un menor recuerdo cuando los tamaños y las escalas de los objetos en el conjunto de datos de prueba difieren en gran medida de los del conjunto de datos de entrenamiento.

Para fines militares es importante disponer de información real y precisa del terreno para un área específica de interés en cualquier parte del mundo debido a que el éxito de las operaciones militares depende cada vez más de la disponibilidad de buena información y de una buena infraestructura de información. En el artículo "Use of Remote Sensing Imagery for Fast Generation of Military Maps and Simulator databases" [164] plantean la información geográfica que en los conflictos forma un segmento de la historia dado que es importante como base para elcomando y control. Por otro lado, es importante para el funcionamiento de los sistemas de armas individuales, todos los cuales utilizan su propia base de datos de información. La información geográfica real y precisa es importante para:

- Simulación de Misión: para simular una misión se requieren trabajar con información real del terreno, para lo cual se puede utilizar información de teledetección. Los datos de teledetección se pueden utilizar para mejorar la precisión de los cálculos del modelo, y también se pueden manejar datos de teledetección para mejorar el reconocimiento del terreno.
- Planificación de Misión: la simulación de la planificación la misión permite a los pilotos de aeronaves familiarizarse con el terreno de batalla y componer rutas de vuelo Además

de considerar las restricciones de vuelo actuales, condiciones climáticas y amenazas tanto en las áreas amigas como enemigas.

- Planificación de Defensa Aérea: requiere el análisis de un área de operación por medio de mapas digitales del terreno y secciones transversales del terreno, mediante una base de datos de terreno digitalizada para calcular los diagramas de cobertura. Los datos del terreno se derivan del Digital Land Mass System (DLMS), un estándar disponible para todos los miembros de la OTAN.

Una selección de artículos junto con las aplicaciones más significativas que emplean datos geográficos se presenta a continuación.

- Detección y clasificación de objetos en imágenes aéreas/satelitales
- Detección de patrones y cambios
- Detección de yacimientos
- Cartografía de la población
- Detección de daños en infraestructuras
- Detección de radares terrestres activos.

Artículos relacionados

Año	Artículo	Referencia
1975	The military applications of remote sensing by infrared	https://doi.org/10.1109/PROC.1975.9711
1987	Image Processing and its Military Applications	https://doi.org/10.14429/dsj.37.5932
2000	Use Of Remote Sensing Imagery For Fast Generation Of Military Maps And Simulator Databases	https://www.isprs.org/proceedings/XXXIII/congress/part2/573_XXXIII-part2.pdf
2001	Real-time classification of multiple non-separated battlefield ordnance events using ELMO	https://doi.org/10.1109/AERO.2001.931518
2008	Data Fusion and Prediction for CBRN Transport and Dispersion for Security	https://doi.org/10.1109/AERO.2008.4526584
2011	Observación de la Tierra desde el Espacio	https://publicaciones.defensa.gob.es/tecnologias-del-espacio-aplicadas-a-la-industria-y-servicios-de-la-defensa.html
2014	Big Geo Data: Standards and Best Practices	https://doi.org/10.1109/COM.Geo.2014.2
2014	Military Use of Satellite Communications, Remote Sensing, and Global Positioning Systems in the War on Terror	https://scholar.smu.edu/jalc/vol79/iss1/2/
2014	Discovering spread mode of public opinions in incidents and mapping it with GIS: A case on big geospatial data analytics	https://doi.org/10.1109/Agro-Geoinformatics.2014.6910597

2015	Survey Paper on Big Data Analytics in Real Time Satellite Data	https://www.ijsr.net/archive/v6i1/ART20164303.pdf
2016	A Survey on Object Detection in Optical Remote Sensing Images	https://doi.org/10.1016/j.isprsjprs.2016.03.014
2016	Big Data for Remote Sensing: Challenges and Opportunities	https://doi.org/10.1109/JPROC.2016.2598228
2016	Big Data processing using hpc for remote sensing disaster data	https://doi.org/10.1109/IGARSS.2016.7730540
2016	Combining Human Computing and Machine Learning to Make Sense of Big (Aerial) Data for Disaster Response	https://doi.org/10.1089/big.2014.0064
2016	Deep Learning Earth Observation Classification Using ImageNet Pretrained Networks	https://doi.org/10.1109/LGRS.2015.2499239
2016	Improving Fishing Pattern Detection from Satellite AIS Using Data Mining and Machine Learning	https://doi.org/10.1371/journal.pone.0163760
2017	A Novel Method of Aircraft Detection Based on High-Resolution Panchromatic Optical Remote Sensing Images	https://doi.org/10.3390/s17051047
2017	High Detail Terrain Models and Multiresolution Path Finding Algorithms for Border Guard Constructive Simulator. A Study of Effective Movement Algorithms in High Resolution Simulation Environment	https://doi.org/10.1109/MCSI.2017.51
2017	Towards development of spark based agricultural information system including geo-spatial data	https://doi.org/10.1109/BigData.2017.8258336
2018	An Automated Method for Power Line Points Detection from Terrestrial LiDAR Data	https://doi.org/10.1007/978-981-13-1498-8_41
2018	Automatic Geospatial Objects Classification from Satellite Images	https://doi.org/10.1007/978-981-13-1498-8_10
2018	Thunderstorm Characteristics Over the Northeastern Region (NER) of India During the Pre-monsoon Season, 2011 Using Geosynchronous Satellite Data	https://doi.org/10.1007/978-981-13-1498-8_26
2018	Worldpop - Fusion of Earth and Big Data for Intraurban Population Mapping	https://doi.org/10.1109/IGARSS.2018.8518181
2019	Advanced Processing of Remotely Sensed Big Data for Cultural Heritage Conservation	https://doi.org/10.1109/IGARSS.2019.8899318
2019	Automated global delineation of human settlements from 40 years of Landsat satellite data archives	http://orcid.org/0000-0003-0620-439X
2019	Identifying Subsurface Drainage using Satellite Big Data and Machine Learning via Google Earth Engine	https://doi.org/10.1029/2019WR024892
2019	Mining discriminative spatial cues for aerial image quality assessment towards Big Data	https://doi.org/10.1016/J.IMAGE.2019.115646
2019	Remote sensing and GIS techniques for reconstructing the military fort system on the Roman boundary (Tunisian section) and identifying archaeological sites	https://doi.org/10.1016/j.rse.2019.111418
2019	SBIRS: Missions, Challenages and Oppotunities	https://doi.org/10.1109/ICCCBDA.2019.8725616
2019	Visualising Air Pollution Datasets with Real-Time Game Engines	https://doi.org/10.1007/978-3-030-16187-3_30

2020	Aerial Scene Classification through Fine-Tuning with Adaptive Learning Rates and Label Smoothing	https://doi.org/10.3390/app10175792
2020	Big Data Geospatial Processing for Massive Aerial LiDAR Datasets	https://doi.org/10.3390/rs12040719
2020	Big Data for Remote Sensing: Challenges and Opportunities	https://www.myecole.it/biblio/wp-content/uploads/2020/11/3DK2DS_Big_Data_Remote_Sensing.pdf
2020	A Robust Airport Runway Detection Network Based on R-CNN Using Remote Sensing Images	https://doi.org/10.1109/MAES.2021.3088477
2020	Application of remote sensing Big Data technology in refined urban management	https://doi.ieeecomputersociety.org/10.1109/ICBAIE49996.2020.00089
2020	Google Earth Engine Cloud Computing Platform for Remote Sensing Big Data Applications: A Comprehensive Review	https://doi.org/10.1109/JSTARS.2020.3021052
2020	Hot Region Selection Based on Selective Search and Modified Fuzzy C-Means in Remote Sensing Images	https://doi.org/10.1109/JSTARS.2020.3025582
2020	Feature-Free Explainable Data Mining in SAR Images Using Latent Dirichlet Allocation	https://doi.org/10.1109/JSTARS.2020.3039012
2020	Management of humanitarian relief operations using satellite Big Data analytics: the case of Kerala floods	https://doi.org/10.1007/s10479-020-03593-w
2020	Overview of Big Data Applications in Remote Sensing	https://doi.org/10.1109/ISMSIT50672.2020.9255244
2020	Object-Scale Adaptive Convolutional Neural Networks for High-Spatial Resolution Remote Sensing Image Classification	https://doi.org/10.1109/JSTARS.2020.3041859
2020	Sea surface wind speed retrieval and validation with future SWOT data	https://doi.org/10.1088/1742-6596/1792/1/012013
2020	Understanding satellite images: a data mining module for Sentinel images	https://doi.org/10.1080/20964471.2020.1820168
2020	Using KOCOA Military Terrain Analysis for the Assessment of Twentieth Century Battlefield Landscapes	https://doi.org/10.3390/heritage3030042
2021	A deep learning based approach for trajectory estimation using geographically clustered data	https://doi.org/10.1007/s42452-021-04556-x
2021	A Novel Method of Aircraft Detection under Complex Background Based on Circular Intensity Filter and Rotation Invariant Feature	https://doi.org/10.3390/s22010319
2021	Application of improved CNN in SAR image noise reduction	https://doi.org/10.1088/1742-6596/1792/1/012053
2021	An Analysis on Spatio-temporal Evolution of Human-land Interaction in China Based on Big Data	https://doi.org/10.1109/IEEECONF54055.2021.9687508
2021	Automation of the Terrain Classification Process due to Passability Taking the Microrelief Shapes into Consideration	https://doi.org/10.1109/ICMT52455.2021.9502821

2021	Automatic Deforestation Detection based on the Deep Learning in Ukraine	https://doi.org/10.1109/IDAACS53288.2021.9661008
2021	Big Earth Data and Advanced Processing Techniques for Monitoring Water Quality	https://doi.org/10.1109/IGARSS47720.2021.9554420
2021	Detection and Classification of Objects in Satellite Images using Custom CNN	https://www.ijert.org/detection-and-classification-of-objects-in-satellite-images-using-custom-cnn
2021	Detecting Post Hurricane House Damage Using Geographic Information Related Multi-Resource Classification Model	https://doi.org/10.1109/ICBASE53849.2021.00098
2021	Evaluation of multimodal transport for emergency rescue based on online GIS and scheduled timetables	https://doi.org/10.1088/1742-6596/1792/1/012040
2021	GPU-Based Parallel Implementation of VLBI Correlator for Deep Space Exploration System	https://doi.org/10.3390/rs13061226
2021	Interband Retrieval and Classification Using the Multilabeled Sentinel-2 BigEarthNet Archive	https://doi.org/10.1109/JSTARS.2021.3112209
2021	Land Use/Land Cover Change Analysis Due to Tourism in the Chittagong Hill Tracts of Bangladesh	https://doi.org/10.1007/978-3-030-79463-7_15
2021	Light-Weight Semantic Segmentation Network for UAV Remote Sensing Images	https://doi.org/10.1109/JSTARS.2021.3104382
2021	Study on Mountain Space in Mount Tai Region Based on GIS Spatial Data Analysis	https://doi.org/10.1109/TOCS53301.2021.9689009
2021	Yield forecasting with machine learning and small data: what gains for grains?	https://doi.org/10.1016/j.agrformet.2021.108555
2021	Marine Ship Detection Method for SAR Image Based on Improved Faster RCNN	https://doi.org/10.1109/BIGSARDATA53212.2021.9574162
2021	Research on Crop Disaster Stress Risk Mapping System Based on Agriculture Big Data	https://doi.org/10.1109/ICEITSA54226.2021.00105
2021	Simultaneous Estimation of Land Surface and Atmospheric Parameters From Thermal Hyperspectral Data Using a LSTM–CNN Combined Deep Neural Network	https://doi.org/10.1109/LGRS.2021.3104501
2021	Determining the critical geographical directions of sand and dust storms in urban areas by remote sensing	https://doi.org/10.1016/j.rsase.2021.100561
2021	Vehicle Detection from Aerial Images Using Deep Learning A Comparative Study	https://doi.org/10.3390/electronics10070820
2021	GIS cloud computing based government Big Data analysis platform	https://doi.org/10.1109/ICBAIE52039.2021.9390052
2021	Satellite Big Data Ingestion for Environmentally Sustainable Development	https://doi.org/10.1007/978-3-030-53440-0_29
2021	Small object detection in remote sensing images based on super-resolution	https://doi.org/10.1016/j.patrec.2021.11.027

2021	The Technique of Operational Processing of Heterogeneous Surveillance Data in Assessing Situation in Geographic Information Systems	https://doi.org/10.1109/ATIT54053.2021.9678766
2021	Enhancement of the sustainability of wolfram mining using drone remote sensing technology	https://doi.org/10.1016/j.rsase.2021.100542
2021	Multi-Aspect SAR Target Recognition Based on Prototypical Network with a Small Number of Training Samples	https://doi.org/10.3390/s21134333
2021	A Novel Method of Aircraft Detection under Complex Background Based on Circular Intensity Filter and Rotation Invariant Feature	https://doi.org/10.3390/s22010319
2021	Res2-Unet+, a Practical Oil Tank Detection Network for Large-Scale High Spatial Resolution Images	https://doi.org/10.3390/rs13234740
2021	S2Looking: A Satellite Side-Looking Dataset for Building Change Detection	https://doi.org/10.3390/rs13245094
2021	Remote Sensing Image Target Detection: Improvement of the YOLOv3 Model with Auxiliary Networks	https://doi.org/10.3390/rs13193908
2022	Aircraft Rotation Detection in Remote Sensing Image Based on Multi-Feature Fusion and Rotation-Aware Anchor	https://doi.org/10.3390/app12031291
2022	Analysis of Drought and Flood Variations on a 200-Year Scale Based on Historical Environmental Information in Western China	https://doi.org/10.3390/ijerph19052771
2022	Automatic Generation of Urban Road 3D Models for Pedestrian Studies from LiDAR Data	https://doi.org/10.3390/rs14051102
2022	Relay Placement Algorithms for IoT Connectivity and Coverage in an Outdoor Heterogeneous Propagation Environment	https://doi.org/10.1109/ACCESS.2022.3147488
2022	Assessing the role of slope, lithology and land use in the formation and conservation of war-related geomorphic features (Case study of WW1 railway artillery in Montagne de Reims, Marne, France)	https://doi.org/10.1016/j.apgeog.2022.102691
2022	Meta captioning: A meta learning based remote sensing image captioning framework	https://doi.org/10.1016/j.isprsjprs.2022.02.001
2022	Water body classification from high-resolution optical remote sensing imagery: Achievements and perspectives	https://doi.org/10.1016/j.isprsjprs.2022.03.013
2022	Detection of remote sensing targets with angles via modified CenterNet	https://doi.org/10.1016/j.compeleceng.2022.107979
2022	Extraction of Water Body Information from Remote Sensing Imagery While Considering Greenness and Wetness Based on Tasseled Cap Transformation	https://doi.org/10.3390/rs14133001
2022	Land-use/land-cover changes and implications in Southern Ethiopia: evidence from remote sensing and informants	https://doi.org/10.1016/j.heliyon.2022.e09071
2022	Research on image recognition of Wushu action based on remote sensing image and embedded system	https://doi.org/10.1016/j.micpro.2021.103841

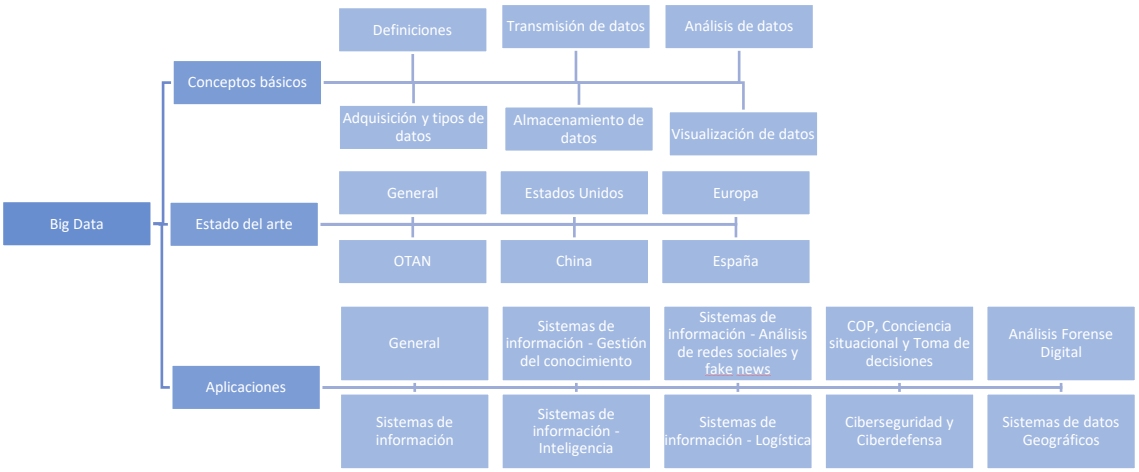
2022	Ship Detection in Visible Remote Sensing Image Based on Saliency Extraction and Modified Channel Features	https://doi.org/10.3390/rs14143347

TABLA 11: ARTÍCULOS SISTEMAS DE DATOS GEOGRÁFICOS

4. Mapa de conocimientos

En el fichero Excel “Referencias_BasesDatos_2022”, se ha incorporado las referencias a artículos utilizados en este documento. Para ello, en el Excel se ha mantenido la estructura anterior aunque añadiendo una columna adicional llamada “año” y se ha desglosado la información de la siguiente forma:

LÍNEA DE INVESTIGACIÓN	TECNOLOGÍA	DESGLOSE DE TECNOLOGÍA

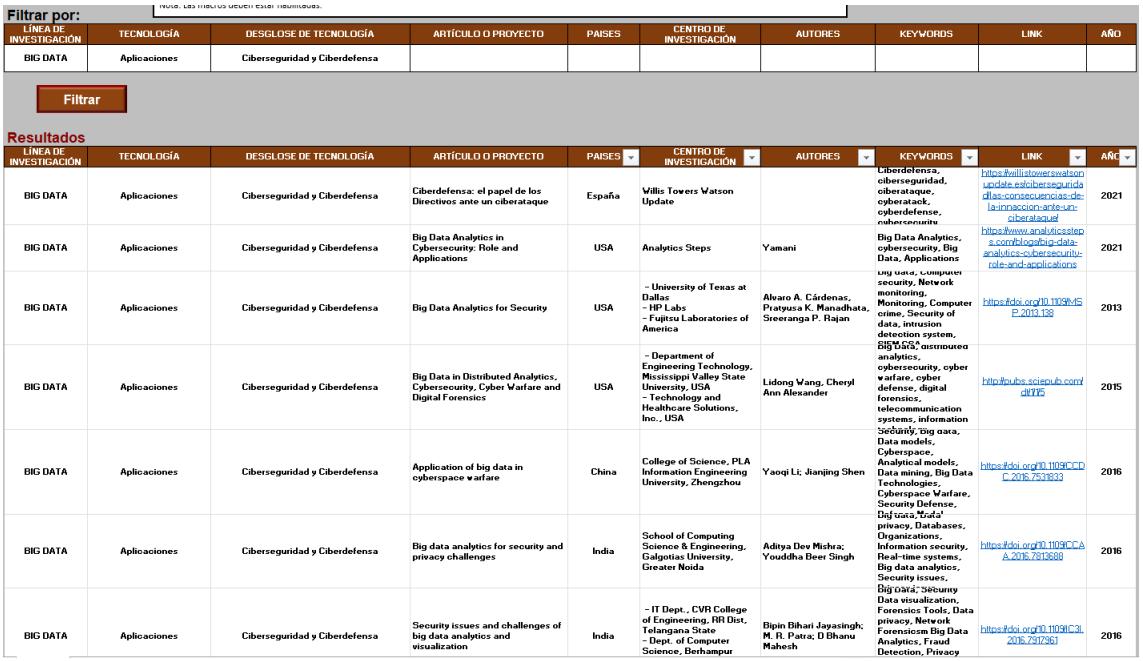


DESGLOSE DEL MAPA DE CONOCIMIENTO

A continuación, se presenta un ejemplo de aplicación del mapa de conocimiento.

1) El primer campo por el que se puede filtrar es la línea de investigación. Si solo se filtra por la línea de investigación de “Big Data” se mostrarán todas las entradas bajo dicha línea de investigación.
   Se puede hacer un filtrado más específico, especificando la tecnología y el desglose de tecnología dentro de las opciones disponibles en el desplegable.

   En el ejemplo se hace un primer filtrado por:
   - Línea de investigación: Big Data
   - Tecnología: Aplicaciones
   - Desglose de tecnología: Ciberseguridad y Ciberdefensa



Filtrar por:

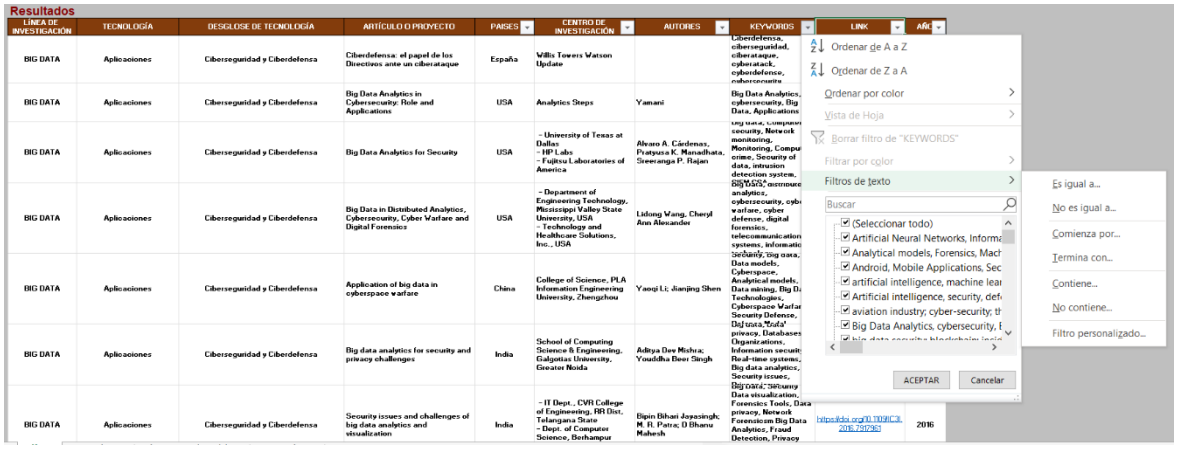
LÍNEA DE INVESTIGACIÓN	TECNOLOGÍA	DESGLOSE DE TECNOLOGÍA	ARTÍCULO O PROYECTO	PAISES	CENTRO DE INVESTIGACIÓN	AUTORES	KEYWORDS	LINK	AÑO
BIG DATA	Aplicaciones	Ciberseguridad y Ciberdefensa							

Filtrar

Resultados

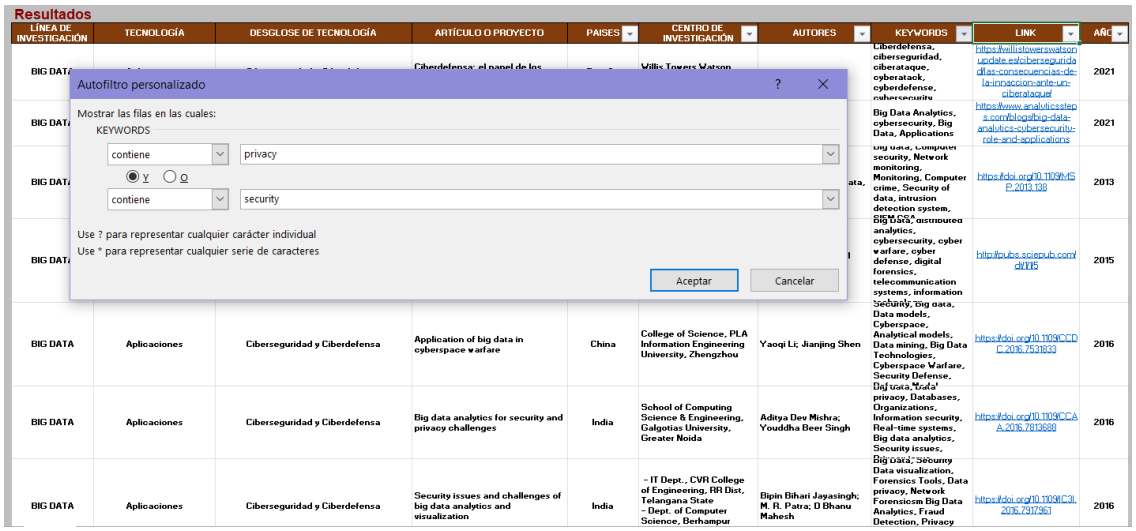
LÍNEA DE INVESTIGACIÓN	TECNOLOGÍA	DESGLOSE DE TECNOLOGÍA	ARTÍCULO O PROYECTO	PAISES	CENTRO DE INVESTIGACIÓN	AUTORES	KEYWORDS	LINK	AÑO
BIG DATA	Aplicaciones	Ciberseguridad y Ciberdefensa	Ciberdefensa: el papel de los Directivos ante un ciberataque	España	Willis Towers Watson Update		Ciberdefensa, ciberseguridad, ciberataque, cyberatack, cyberdefense,	https://willistowerswatson update.es/ciberseguridad dllas-consecuencias-de-la-innaccion-ante-un-ciberataque/	2021
BIG DATA	Aplicaciones	Ciberseguridad y Ciberdefensa	Big Data Analytics in Cybersecurity: Role and Applications	USA	Analytics Steps	Yamani	Big Data Analytics, cybersecurity, Big Data, Applications	https://www.analyticssteps.com/blogs/big-data-analytics-cybersecurity-role-and-applications	2021
BIG DATA	Aplicaciones	Ciberseguridad y Ciberdefensa	Big Data Analytics for Security	USA	- University of Texas at Dallas - HP Labs - Fujitsu Laboratories of America	Alvaro A. Cárdenas, Pratyusa K. Manadhata, Sreeranga P. Rajan	security, Network monitoring, Monitoring, Computer crime, Security of data, intrusion detection system,	https://doi.org/10.1109/MSP.2013.138	2013
BIG DATA	Aplicaciones	Ciberseguridad y Ciberdefensa	Big Data in Distributed Analytics, Cybersecurity, Cyber Warfare and Digital Forensics	USA	- Department of Engineering Technology, Mississippi Valley State University, USA - Technology and Healthcare Solutions, Inc., USA	Lidong Wang, Cheryl Ann Alexander	analytics, cybersecurity, cyber warfare, cyber defense, digital forensics, telecommunication systems, information	http://pubs.sciepub.com/dit/1/5	2015
BIG DATA	Aplicaciones	Ciberseguridad y Ciberdefensa	Application of big data in cyberspace warfare	China	College of Science, PLA Information Engineering University, Zhengzhou	Yaoqi Li; Jianjing Shen	Data models, Cyberspace, Analytical models, Data mining, Big Data Technologies, Cyberspace Warfare, Security Defense,	https://doi.org/10.1109/ICCDC.2016.7531033	2016
BIG DATA	Aplicaciones	Ciberseguridad y Ciberdefensa	Big data analytics for security and privacy challenges	India	School of Computing Science & Engineering, Galgotias University, Greater Noida	Aditya Dev Mishra; Youddha Beer Singh	privacy, Databases, Organizations, Information security, Real-time systems, Big data analytics, Security issues,	https://doi.org/10.1109/CCAA.2016.7813688	2016
BIG DATA	Aplicaciones	Ciberseguridad y Ciberdefensa	Security issues and challenges of big data analytics and visualization	India	- IT Dept., CVR College of Engineering, RR Dist, Telangana State - Dept. of Computer Science, Berhampur	Bipin Bihari Jayasingh; M. R. Patra; D Bhanu Mahesh	Data visualization, Forensics Tools, Data privacy, Network Forensicsm Big Data Analytics, Fraud Detection, Privacy	https://doi.org/10.1109/IC3I.2016.7917961	2016

2) Para posibilitar un filtrado más concreto, se ha habilitado el filtrado mediante los campos de “Países”, “Centro de Investigación”, “Autores”, “Keywords”, y “Año”. Para ello hay que utilizar la lista desplegable de cada campo.



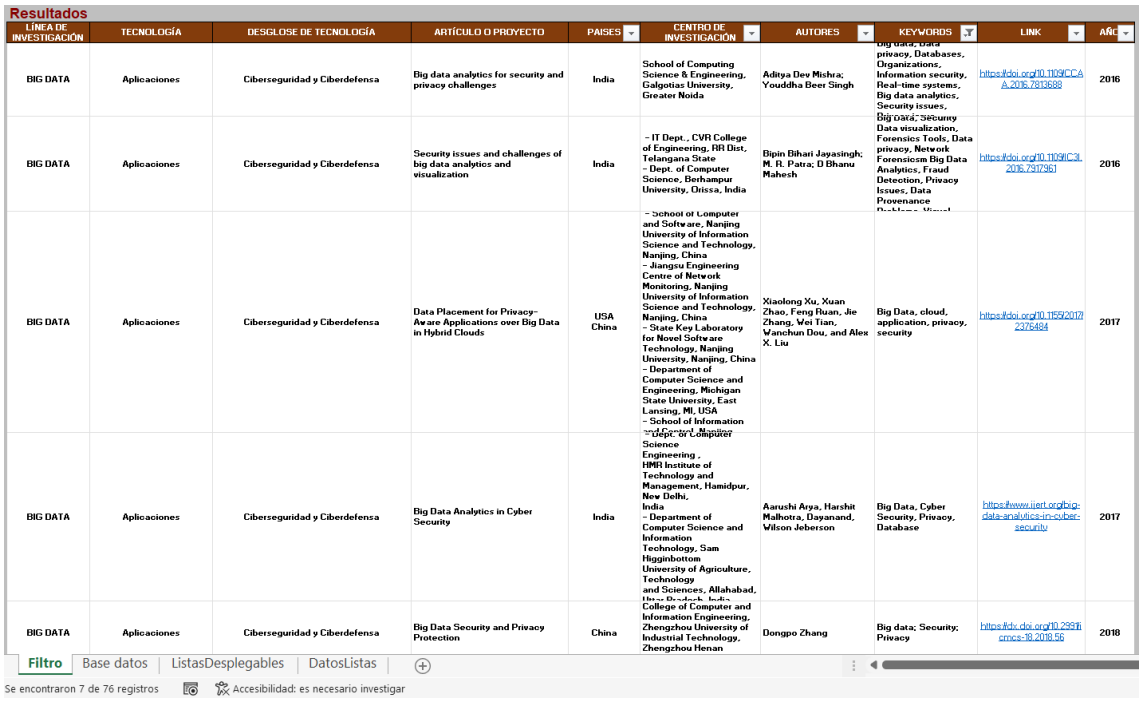
En la zona de *buscar* del desplegable se recomienda escribir la palabra especifica en lugar de seleccionar un campo, en concreto para los campos de “Paises”, “Centro de Investigación”, “Autores”, “Keywords”. También se pueden emplear filtros de texto para realizar filtros personalizados.

A continuación, se muestra un filtrado por “keywords” *privacy* y *security.*



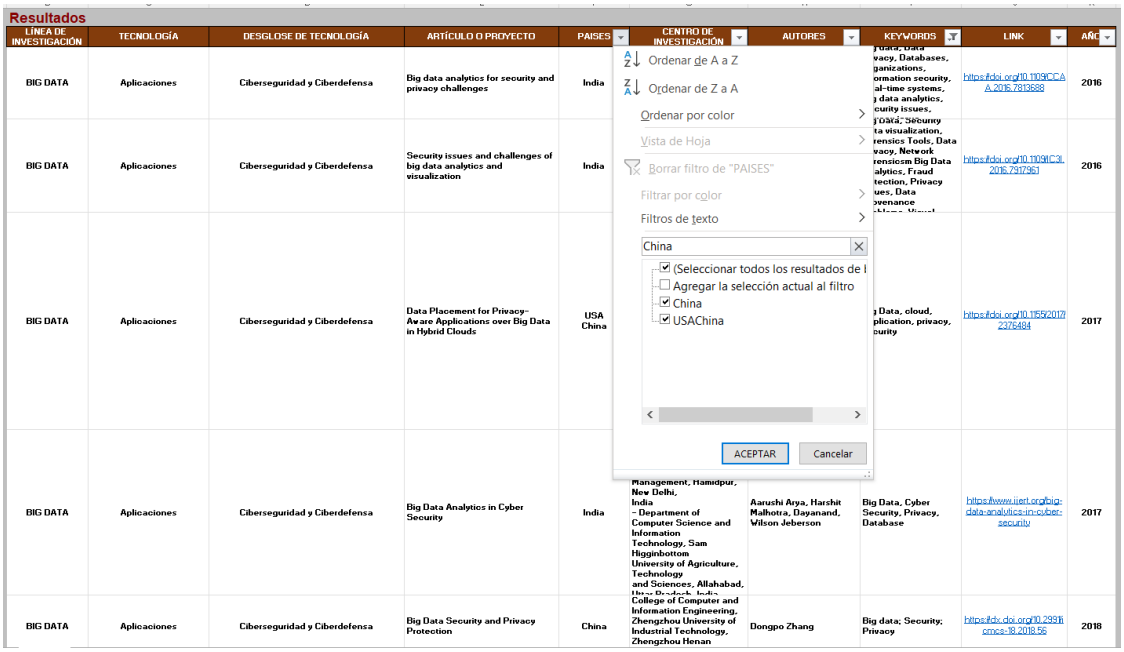
LÍNEA DE INVESTIGACIÓN	TECNOLOGÍA	DESGLOSE DE TECNOLOGÍA	ARTÍCULO O PROYECTO	PAISES	CENTRO DE INVESTIGACIÓN	AUTORES	KEYWORDS	LINK	AÑO
BIG DATA			Ciberdefensa: el papel de las		Willis Towers Watson		Ciberdefensa, ciberseguridad, ciberataque, cyberattack, cyberdefense, cybersecurity	https://willistowerswatson.com/update-es/ciberseguridad/dias-consecuencias-de-la-injnaccion-ante-un-ciberataque/	2021
BIG DATA							Big Data Analytics, cybersecurity, Big Data, Applications	https://www.analyticssteps.com/blogs/big-data-analytics-cybersecurity-role-and-applications	2021
BIG DATA							Big data, Computer security, Network monitoring, Monitoring, Computer crime, Security of data, intrusion detection system, Big data, automated	https://doi.org/10.1109/MSP.2013.138	2013
BIG DATA							analytics, cybersecurity, cyber warfare, cyber defense, digital forensics, telecommunication systems, information	http://pubs.sciepub.com/jdi/1/15	2015
BIG DATA	Aplicaciones	Ciberseguridad y Ciberdefensa	Application of big data in cyberspace warfare	China	College of Science, PLA Information Engineering University, Zhengzhou	Yaoqi Li; Jianjing Shen	Security, Big data, Data models, Cyberspace, Analytical models, Data mining, Big Data Technologies, Cyberspace Warfare, Security Defense,	https://doi.org/10.1109/CCDC.2016.7531833	2016
BIG DATA	Aplicaciones	Ciberseguridad y Ciberdefensa	Big data analytics for security and privacy challenges	India	School of Computing Science & Engineering, Galgotias University, Greater Noida	Aditya Dev Mishra; Youddha Beer Singh	Big data, Data privacy, Databases, Organizations, Information security, Real-time systems, Big data analytics, Security issues,	https://doi.org/10.1109/CCAA.2016.7813688	2016
BIG DATA	Aplicaciones	Ciberseguridad y Ciberdefensa	Security issues and challenges of big data analytics and visualization	India	- IT Dept., CVR College of Engineering, RR Dist, Telangana State - Dept. of Computer Science, Berhampur	Bipin Bihari Jayasingh; M. R. Patra; D Bhanu Mahesh	Big data, Security Data visualization, Forensics Tools, Data privacy, Network Forensicsm Big Data Analytics, Fraud Detection, Privacy	https://doi.org/10.1109/IC3I.2016.7917961	2016

Resultado del filtrado.

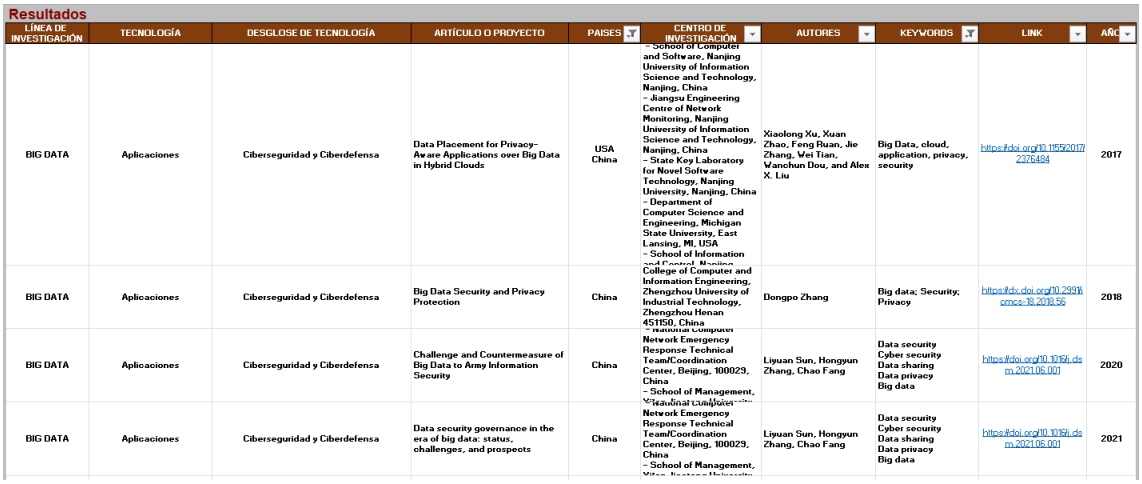


LÍNEA DE INVESTIGACIÓN	TECNOLOGÍA	DESGLOSE DE TECNOLOGÍA	ARTÍCULO O PROYECTO	PAISES	CENTRO DE INVESTIGACIÓN	AUTORES	KEYWORDS	LINK	AÑO
BIG DATA	Aplicaciones	Ciberseguridad y Ciberdefensa	Big data analytics for security and privacy challenges	India	School of Computing Science & Engineering, Galgotias University, Greater Noida	Aditya Dev Mishra; Youddha Beer Singh	Big data, Data privacy, Databases, Organizations, Information security, Real-time systems, Big data analytics, Security issues,	https://doi.org/10.1109/CCAA.2016.7813688	2016
BIG DATA	Aplicaciones	Ciberseguridad y Ciberdefensa	Security issues and challenges of big data analytics and visualization	India	- IT Dept., CVR College of Engineering, RR Dist, Telangana State - Dept. of Computer Science, Berhampur University, Orissa, India	Bipin Bihari Jayasingh; M. R. Patra; D Bhanu Mahesh	Big data, Security Data visualization, Forensics Tools, Data privacy, Network Forensicsm Big Data Analytics, Fraud Detection, Privacy Issues, Data Provenance	https://doi.org/10.1109/IC3I.2016.7917961	2016
BIG DATA	Aplicaciones	Ciberseguridad y Ciberdefensa	Data Placement for Privacy-Aware Applications over Big Data in Hybrid Clouds	USA China	- School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, China - Jiangsu Engineering Centre of Network Monitoring, Nanjing University of Information Science and Technology, Nanjing, China - State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing, China - Department of Computer Science and Engineering, Michigan State University, East Lansing, MI, USA - School of Information	Xiaolong Xu, Xuan Zhao, Feng Ruan, Jie Zhang, Wei Tian, Wanchun Dou, and Alex X. Liu	Big Data, cloud, application, privacy, security	https://doi.org/10.1155/2017/2376484	2017
BIG DATA	Aplicaciones	Ciberseguridad y Ciberdefensa	Big Data Analytics in Cyber Security	India	- Dept. of Computer Science Engineering , HMR Institute of Technology and Management, Hamidpur, New Delhi, India - Department of Computer Science and Information Technology, Sam Higginbottom University of Agriculture, Technology and Sciences, Allahabad,	Aarushi Arya, Harshit Malhotra, Dayanand, Wilson Jeberson	Big Data, Cyber Security, Privacy, Database	https://www.ijert.org/big-data-analytics-in-cyber-security	2017
BIG DATA	Aplicaciones	Ciberseguridad y Ciberdefensa	Big Data Security and Privacy Protection	China	College of Computer and Information Engineering, Zhengzhou University of Industrial Technology, Zhengzhou Henan	Dongpo Zhang	Big data; Security; Privacy	https://dx.doi.org/10.2991/icmcs-18.2018.56	2018

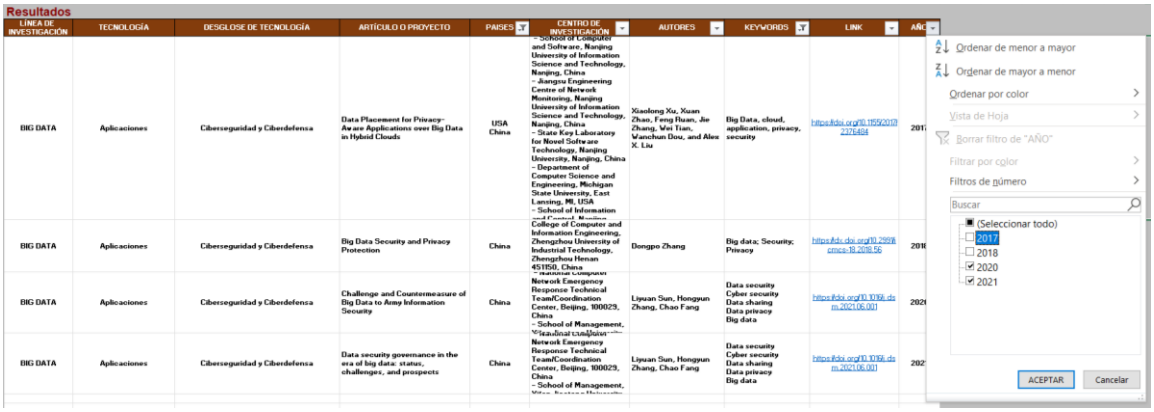
De los resultados ahora se desea filtrar por “Paises”, en este caso se va a filtrar por *China*.



El resultado obtenido es el siguiente



Un siguiente filtrado es filtrar por “Año” para tener los trabajos de los últimos años.

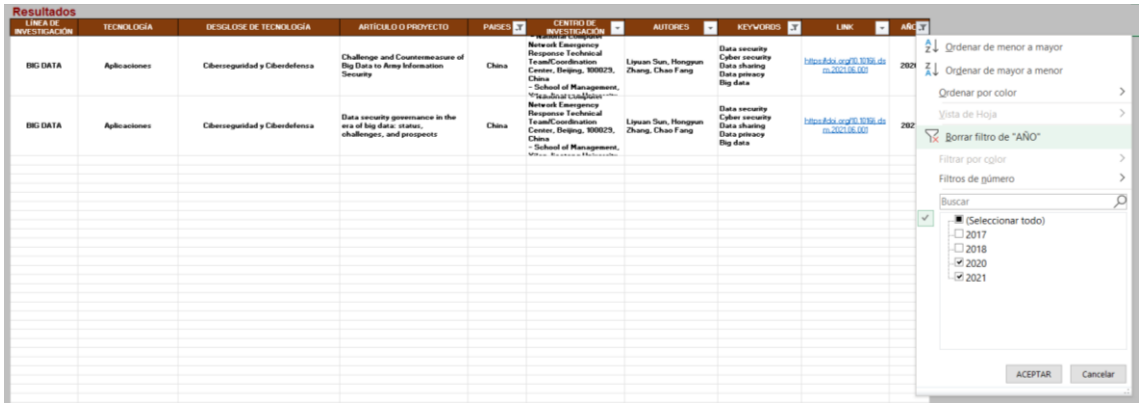


Obteniendo como resultado final los siguientes resultados.

Resultados

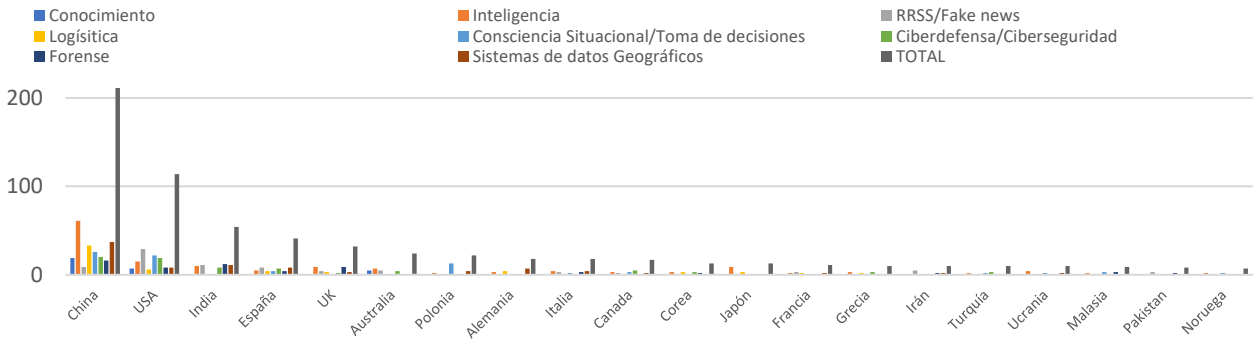
LÍNEA DE INVESTIGACIÓN	TECNOLOGÍA	DESGLOSE DE TECNOLOGÍA	ARTÍCULO O PROYECTO	PAISES	CENTRO DE INVESTIGACIÓN	AUTORES	KEYWORDS	LINK	AÑO
BIG DATA	Aplicaciones	Ciberseguridad y Ciberdefensa	Challenge and Countermeasure of Big Data to Army Information Security	China	National Computer Network Emergency Response Technical Team/Coordination Center, Beijing, 100029, China - School of Management,	Liyuan Sun, Hongyun Zhang, Chao Fang	Data security Cyber security Data sharing Data privacy Big data	https://doi.org/10.1016/j.dsm.2021.06.001	2020
BIG DATA	Aplicaciones	Ciberseguridad y Ciberdefensa	Data security governance in the era of big data: status, challenges, and prospects	China	National Computer Network Emergency Response Technical Team/Coordination Center, Beijing, 100029, China - School of Management,	Liyuan Sun, Hongyun Zhang, Chao Fang	Data security Cyber security Data sharing Data privacy Big data	https://doi.org/10.1016/j.dsm.2021.06.001	2021

Si se desea realizar una búsqueda nueva se recomienda borrar todos los filtros que se hayan empleado.

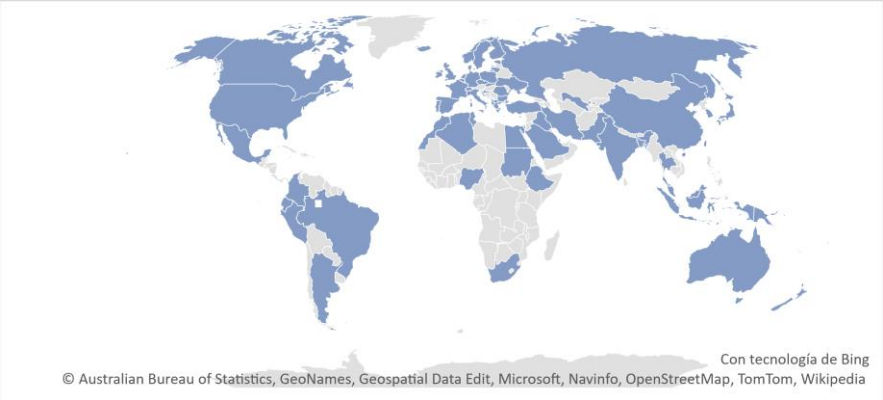


Adicionalmente, se ha realizado un análisis de las publicaciones para ver el país de origen de los artículos en los distintos campos de aplicación. De dicho análisis se han elaborado las gráficas mostradas a continuación.

El país con mayor número de publicaciones totales es China, seguido de Estados Unidos, India, España y Reino Unido. Pero que se hayan tenido estos resultados no implica que sea proporcional a la actividad relacionada con el Big Data en defensa y seguridad en los distintos países.



NÚMERO DE PUBLICACIONES EN LAS DISTINTAS ÁREAS DE LOS 20 PAÍSES QUE TIENEN MAYOR NÚMERO DE PUBLICACIONES TOTALES.



MAPA CON LOS PAÍSES IDENTIFICADOS CON PUBLICACIONES EN LAS DISTINTAS ÁREAS

En el gráfico mundial se puede observar que en la mayoría de los países desarrolladas, se realiza investigación sobre el empleo de las técnicas del Big Data en el campo de la defensa y seguridad.

5. Conclusiones

El Big Data está teniendo un impacto importante en los distintos ámbitos de la sociedad, debido a la habilidad de analizar grandes cantidades de datos y obtener resultados de utilidad, entre ellos en el ámbito de la defensa y seguridad.

La utilización masiva de técnicas de análisis de datos suele ir de la mano de la IA pues se están fusionando en una relación sinérgica, donde la IA es inútil sin datos y el dominio de los datos pasa por el uso masivo de IA. Sin embargo, apenas se referencia el uso de auténticas técnicas de Big Data (estructuras especiales de proceso, uso de supercomputadores…), lo que no significa que no se estén usando en contextos confidenciales. La razón no es otra que la escasez de datos que cumplan con las mencionadas "cinco uves".

La importancia creciente en el ámbito de la defensa y seguridad es debido a que la obtención y el análisis de datos se está convirtiendo en el centro de las operaciones del campo de batalla. Para ello, distintos países están tomando medidas diferentes como invertir grandes cantidades de dinero en proyectos de investigación para posteriormente implementarlos en el campo de batalla, como Estados Unidos y China. En el caso concreto de España, se puede considerar que ciertos proyectos se realizan bajo el marco de la Unión Europea y otros individualmente.

En el ámbito de la defensa y seguridad se han diferenciado seis áreas de aplicación del Big Data: ciberdefensa y ciberseguridad, COP, conciencia situacional y toma de decisiones, análisis forense digital, sistemas de datos geográficos y sistemas de información dividido a su vez en gestión del conocimiento, inteligencia, análisis de redes sociales y fake news, y logísitica. Para cada uno de los campos de aplicación se han distinguido múltiples aplicaciones, por lo que se ha de manejar datos procedentes de diversas fuentes y se requiere de estructuras capaces de analizar grandes ingestas de datos y en ciertos casos en tiempo real.

Con toda la información recopilada se ha realizado un mapa de conocimiento mediante la generación de una base de datos y la puesta a punto de una herramienta que optimiza su utilización. Esta base de datos se ha realizado con el fin de indagar los distintos grupos o centros de investigación además de los países involucrados en los distintos campos. Para ello, para cada uno de los artículos se ha compilado la siguiente información: "países", "centro de investigación", "autores", "keywords", "link" y "año. Se puede observar que el país con mayor número de publicaciones es China seguido de Estados Unidos y, ya a considerable distancia, India.

6. Agradecimientos

Este trabajo es fruto de las actividades realizadas en el Observatorio de Defensa y Seguridad de la Red Horizontes, articuladas a través de la Cátedra Isdefe-ETSIT-UPM.

ANEXO: Algunos ejemplos del uso del análisis de datos y el Big Data en la invasión de Ucrania

La invasión rusa de Ucrania se puede considerar como un episodio bélico a gran escala que tuvo fecha de comienzo el 24 de febrero de 2022. Durante dicho conflicto han ido apareciendo distintos artículos de la aplicación del Big Data, tanto de investigación como periodísticos, donde se pone de manifiesto el uso de técnicas de análisis de datos y de Big Data. En la Tabla 12 se recogen las aplicaciones detectadas en un análisis sencillo de algunas de las informaciones publicadas sobre el conflicto.

Sistemas de información	
Gestión del conocimiento	Análisis de los países que proporcionan ayuda a Ucrania; análisis del impacto humanitario en las ciudades bajo bombardeo.
Inteligencia	Empleo de fuentes abiertas como Oryx Blog, Ukraine Weapons Tracker, Bellingcat, La Brigada Osint, etc., en conjunto con las imágenes satelitales proporcionadas por compañías como EOS Data Analytics, Maxar, Planet, Satellogic o Capella Space para contrastar y analizar imágenes e información sobre el terreno con el fin de producir conocimiento aplicado; investigar el comportamiento de las cuentas y sus transacciones en la criptomoneda Ethereum durante el conflicto de Rusia-Ucrania; Analizar la crisis de refugiados mediante el análisis de las mediciones de Internets; uso de los índices de Google Trends para predecir la migración forzada de Ucrania a la UE; análisis de datos de Speedtest para medir el impacto del conflicto en el rendimiento de Internet en Ucrania y en Rusia; análisis sobre la sincronización de emergencia de las redes de Ucrania y Moldavia con la red eléctrica de Europa continental ha afectado la dinámica de frecuencia y los flujos transfronterizos de energía eléctrica; seguimiento del uso de municiones en racimo en áreas civiles; análisis de grabaciones de soldados rusos; análisis de distintas fuentes de datos como metadata, posiciones de aviones, estaciones meteorológicas; identificación de objetivos; empleo de minas inteligentes; empleo de la plataforma inteligente GNOM; análisis del impacto de la guerra en la latencia y routing.
Redes Sociales y fake news	Creación de bases de datos de distintas redes sociales (Twitter, Weibo, Reddit, VKontakte) con el fin de estudiar el discurso político, la minería de opiniones y la propagación de (des)información; uso del aprendizaje profundo para la detección de noticias falsas y detección de noticias generadas artificialmente; análisis del uso de la teoría de conjuntos de elementos frecuentes y reglas de asociación, la teoría de grafos para el análisis de tendencias de noticias; análisis de sentimientos; análisis de la influencia de las imágenes digitales en la propagación de “fake news”; explorar la naturaleza anti- o pro-genocida de las reacciones de los usuarios rusos en Telegram a los eventos en Bucha; obtención de conocimientos demográficos sobre edad y género de los refugiados, los flujos migratorios y las tendencias de integración de datos de Facebook; #DataforUkraine tiene por objetivo analizar tweets e informar sobre incidentes en Ucrania; comprender cómo la actividad de los bots influye en el discurso en línea; análisis de los consejos de seguridad y privacidad en redes sociales.
Logística	Aplicación de la teoría de grafos en la logística de la guerra de Ucrania; desarrollo de un modelo para analizar y extraer la información más relevante de informes para la identificación de infraestructuras dañadas; análisis de la cadena logística de la guerra ruso-ucraniana; cálculo de la ruta óptima de un dron; seguimiento del control de tropas y vehículos; análisis de datos de tráfico para modelar patrones de viaje
Ciberdefensa y Ciberseguridad	
Uso de la inteligencia de ciberamenazas como apoyo a la comprensión del adversario; análisis de malware, ciberataques y ciberactividad; ciberataques a redes eléctricas; robo de datos ucranianos para	

proporcionar a Rusia información sobre dicha población; detección e interrupción de actividad de comportamiento sospechoso; análisis de la ciberdelincuencia clandestina en el conflicto.
Consciencia Situacional y Toma de decisiones
Creación de una 'alerta temprana' de Big Data para abusos en Ucrania; análisis de la afluencia de ucranianos a Polonia y los posibles escenarios para el futuro; empleo de IA y aprendizaje automático para analizar grandes cantidades de datos, generar inteligencia útil en el campo de batalla y aprender sobre tácticas y estrategia rusas; uso de HALO Trust para analizar la destrucción en Ucrania evaluando el riesgo de las municiones sin detonar; obtener información útil sobre dónde es probable que se desplacen las personas que huyen de Ucrania tras la invasión rusa; anticipar el traslado de refugiados para que las autoridades locales y nacionales puedan gestionar mejor los desafíos relacionados con su acogida e integración; anticipar y evitar la escasez de alimentos y las hambrunas.
Análisis forense
Empleo de un 'deep fake' de Zelensky donde pide la rendición de sus tropas; diseño de un modelo que puede distinguir el presidente real del falso mediante el modelado de comportamiento facial y gestual que captura las características distintivas del estilo de hablar de Zelensky; uso de Clearview AI para identificar a los soldados rusos, vivos o muertos, y para verificar que los viajeros en Ucrania son quienes afirman; ayudar en las investigaciones de Ucrania sobre los crímenes de guerra rusos mediante reconocimiento facial, análisis de video, geoespacial y otras técnicas de IA; encontrar y resumir el contenido de imágenes remezcladas en grandes colecciones de datos sin etiquetar y sin clasificar para identificar contenido que se alinea más estrechamente con las preferencias y expectativas de los observadores humanos: empleo de granjas de trolls rusos para generar rostros humanos para personas falsas y propagandísticas en redes sociales.
Sistemas de datos geográficos
Detección de señales de la invasión de Rusia mediante el análisis del tráfico; empleo del análisis de imágenes satelitales para la identificación de crímenes de guerra; análisis de datos satelitales SAR para comprender los movimientos de tropas y vehículos rusos durante la noche; uso de imágenes SAR para clasificación, segmentación semántica y detección de cambios; análisis de la perturbación de la guerra; detección de fuegos activos.

TABLA 12: APLICACIONES DEL BIG DATA EN EL CONFLICTO DE UCRANIA

A continuación, se analizan algunas de las primeras publicaciones que aparecieron sobre el uso del Big Data en el conflicto.

En el artículo web “Here’s the technology being used to watch Russian troops as Ukraine invasion fears linger” [165], publicado el 16 de febrero, unos días antes de que se produjera la invasión se menciona que las imágenes de satélite, las redes sociales y una rápida explosión de datos transforman los planes para la guerra, debido al haber eliminado gran parte del elemento sorpresa y los preparativos de la misma. La acumulación de alrededor de 150.000 soldados rusos en las fronteras de Ucrania fue muy visible a través de imágenes de satélite, además, los videos y las fotos fueron difundidas ampliamente, proporcionando mucha información de inteligencia en fuentes abiertas tanto para expertos como para aficionados. Los signos de una acumulación de recursos para el combate comenzaron la primavera pasada, lo que generó preocupación, pero las campanas de alarma comenzaron a sonar alrededor de diciembre "cuando comenzamos a ver cosas que eran un poco inusuales" en relación con la actividad anterior, dijo Lukas Andriukaitis, director asociado de Digital Forensic con sede en Bruselas. Laboratorio de investigación operado por el Atlantic Council, un grupo de expertos en política exterior con sede en EE. UU. Además, Andriukaitis dice que estaba claro que se estaban colocando más equipos y personal, y la acumulación de tropas y equipos en la vecina Bielorrusia, pero que vale la pena saber dónde buscar otros tipos de información disponible públicamente. Aunque se cerraron cuando la acumulación cobró fuerza, por ejemplo, antes era posible acceder a las bases de datos de los ferrocarriles públicos en Rusia. Las imágenes de vagones de tren con números de

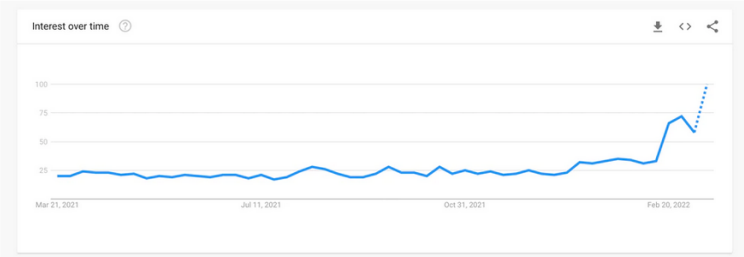
identificación podrían cotejarse con la base de datos para determinar de dónde procedían y qué unidades o equipos transportaban.

En otro artículo web “Google disables Maps traffic data in Ukraine to protect citizens” [166] y en su resumen en español “¿Por qué Google desactivó los datos de tráfico de Maps en Ucrania?” [167], dicen que los datos de Google Maps pueden ser peligrosos durante la invasión, y por tanto Google desactivó de manera temporal las funciones de tráfico en directo que proporciona Google Maps en Ucrania, para así proteger a la población. La herramienta recoleta de forma anónima datos de localización de terminales Android para identificar dónde hay más trafico más tráfico en las carreteras y qué locales comerciales se encuentran abiertos. De acuerdo con los artículos, un experto en inteligencia de fuente abierta (OSINT) dijo que vio señales de la invasión rusa después de detectar “atascos de tráfico” inusuales en la frontera con Ucrania en Google Maps. Los datos de ubicación recopilados por los servicios de mapas a menudo ofrecen este tipo de información inesperada. Por ejemplo, cuando la aplicación de seguimiento del estado físico Strava lanzó un mapa en 2017 de la actividad de los usuarios, reveló accidentalmente la ubicación de varias bases militares de EE. UU. y mostró dónde los soldados habían estado dando vueltas alrededor de los aeródromos. Del mismo modo, las funciones de geolocalización de Snapchat se han utilizado para recopilar imágenes y videos de la primera línea en la Guerra de Irak. Y con o sin datos de ubicación, la información compartida en zonas de guerra a través de las redes sociales se ha convertido en una herramienta vital para investigadores de código abierto, periodistas y otros, aunque estos datos deben combinarse con otras fuentes para proporcionar información confiable.

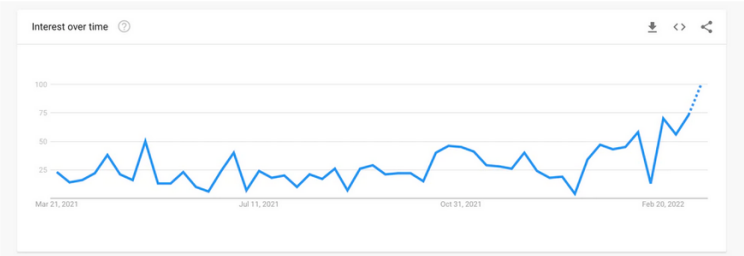
Google Maps muestra información sobre el tráfico en Europa (izquierda), pero no del territorio ucraniano (derecha). [166]

En un artículo de El País, bajo el título de “Analistas aficionados ofrecen en internet una fuente básica de información sobre Ucrania” [168], cuenta que la agresión rusa ha elevado el papel de la investigación de fuentes abiertas (OSINT) a un rol indispensable para contrastar imágenes e información sobre el terreno. Entre las fuentes abiertas destacan Oryx Blog [169], en la cual un par de holandeses llevan años recopilando fotos de material militar perdido, como por ejemplo vehículos y armamento pesado que van enlazado con la imagen de donde lo han sacado, lo cual se puede considerar un trabajo de orfebrería digital. También una cuenta de reciente creación

de Twitter bajo el sobrenombre de Ukraine Weapons Tracker [170], tiene como objetivo identificar armamento sobre el terreno y ponerlo en su contexto. En el artículo afirman que las cuentas de aficionados de geolocalización, armas, historia militar, seguimiento de vuelos, fotos vía satélite han ido perfeccionando su labor en los últimos años consiguiendo que que todo queda documentado, no hay dato sin un vídeo o foto detrás donde se analiza con detalle lo que se ve, consiguiendo que el público puede valorar por sí mismo cuánto creerse. Asimismo, en el artículo mencionan un grupo español que prefiere el uso de foros como Discord o Telegram por su cercanía, en lugar de Twitter, llamado La Brigada Osint, cofundado en mayo de 2020 por Aimery Parekh. Parekh comparte el incremento de búsquedas de ”osint” en Google en el último año tanto en todo el mundo como en España, además cree el gran potencial que supone el análisis de fuentes abiertas en Ucrania en parte por la exigencia de los ciudadanos de encontrar información contrastada. También considera que de cara al futuro ve prometedor la profesión de analista OSINT y da como ejemplo “El Centro de Inteligencia de las Fuerzas Armadas acaba de sacar un contrato en el que entre los perfiles que busca está el de analista OSINT”, pero que los Ejércitos están recurriendo a expertos civiles, aunque hay muchos miembros de los cuerpos de seguridad se están formando en el análisis OSINT.



Tendencia global de búsquedas de "osint" en Google en los últimos 12 meses.



Tendencia en España de búsquedas de "osint" en Google en los últimos 12 meses.

Tendencia de búsquedas de “osint” en Google en los últimos 12 meses a nivel global y en España. [63]

También, durante el conflicto de Ucrania, los hackers rusos han hecho uso del Deep fake para crear un video falso del presidente Zelenski pidiendo la rendición de sus tropas [171]. Un Deep fake es un vídeo en el que se muestran imágenes falsas, habitualmente del rostro de una persona, que parecen ser reales. Los Deep fakes se producen utilizando inteligencia artificial; en concreto, empleando técnicas de Deep learning, que utilizan algoritmos de redes neuronales. Para el objetivo de Deep fake, los algoritmos aprenden a crear imágenes de personas reales o ficticias tras procesar una base de datos de imágenes de ejemplo, y al ser entrenados con imágenes de una persona concreta, pueden generar vídeos muy realistas de esta. También se puede recrear la voz de un modo similar. [172]

En [173], la Dra. Michelle Lazcano Álvarez plantea que la invasión de Ucrania por parte de Rusia se viene fraguando desde hace bastantes años mediante el análisis de ciertos detalles aislados:

- Los análisis de contenido a textos, discursos, caricaturas, mensajes, redes sociales, etc. aplicados en lo particular, describen la naturaleza de los individuos que escriben dichos textos, el estilo e intención del escrito puede perfilar educación, entorno social y profesional, incluso estado psicológico del autor. Haciendo que, de manera masiva, marquen las tendencias de comunicación, los cambios en símbolos tanto territoriales como universales e inclinaciones sociales.
- Una investigación de mercado reveló que los símbolos de la revolución rusa, el martillo que simboliza la revolución industrial, y la hoz mostrando la fuerza rural, ya no representaban prácticamente nada para las generaciones más actuales debido a que no conectaban con esa historia de la que hablaba, haciendo que la consigna de la entonces unión soviética pierda el encanto.
- Cierta página de internet para la venta de juguetes infantiles en conjunto con una comunidad de consejos para jóvenes madres rusas fracaso debido a que era una amenaza a futuro para el régimen al permitir a las nuevas generaciones imaginar y crear.
- La Ley "Yarova" da al estado el derecho de obligar a operadores de comunicaciones a almacenar intercambio de información de todos sus usuarios durante 6 meses aunque existieron protestas y firmas con contra de ella. En el año 2018 el Comité de vigilancia de Rusia recibió una sanción de Distrito Tagansky (Moscú) por bloquear masivamente direcciones IP y exigir claves de descodificación, lo que trajo errores en servicios como Google, Telegram y Amazon.

Al final, lo que Rusia está intentado conseguir es volver a su añorada ´grandeza´ de los años 80´s que incluía territorios ucranianos, Bielorrusia, Kazajistán, Armenia, entre otros.

Finalmente, en un artículo web de BigDatamagazine, "Cómo se usa el Big Data en guerras como la de Rusia y Ucrania" [174], esbozan que el uso de algoritmos y de datos es cada vez más habitual en los conflictos militares como el de Rusia y Ucrania para realizar una 'guerra inteligente'. Debido a que el Big Data y los algoritmos forjan a los datos y a la información del campo de batalla ser ordenados y eficaces. La ley especial de la información determina el valor absoluto de los datos, y un buen algoritmo puede activar los datos para hacerlos valiosos en el combate. También, los sistemas informáticos militares pueden optimizarse y crear nuevos datos e información, debido a que el ritmo de recopilación de datos no frena el ritmo de desarrollo del algoritmo y viceversa, consiguiendo un gran avance en el complejo tecnológico militar.

Bibliografía

[1] J. Wang, Y. Yang, T. Wang, R. S. Sherratt, and J. Zhang, "Big Data Service Architecture: A Survey," *J. Internet Technol.*, vol. 21, no. 2, Art. no. 2, Mar. 2020.

[2] "Big data: The next frontier for innovation, competition, and productivity | McKinsey." https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation

[3] "Definition of Big Data - Gartner Information Technology Glossary," *Gartner*. https://www.gartner.com/en/information-technology/glossary/big-data

[4] "Macrodatos," *Wikipedia, la enciclopedia libre*. Oct. 15, 2021. [Online]. Available: https://es.wikipedia.org/w/index.php?title=Macrodatos&oldid=139064438

[5] "¿Qué es el big data? | Oracle España." https://www.oracle.com/es/big-data/what-is-big-data/

[6] E. Wilder-James, "What is big data?," *O'Reilly Media*, Jan. 11, 2012. https://www.oreilly.com/radar/what-is-big-data/

[7] RAE, "Definición de big data - Diccionario panhispánico del español jurídico - RAE," *Diccionario panhispánico del español jurídico - Real Academia Española*. https://dpej.rae.es/lema/big-data

[8] "Publicación de Instagram de Real Academia Española (RAE): '#Extranjerismo | «big data» Como alternativa a «big data», se puede usar «macrodatos» para el conjunto ingente de datos e «inteligencia de…,'" *Instagram*. https://www.instagram.com/p/B_6oJalglTr/

[9] "The Importance of 'Big Data': A Definition," *Gartner*. https://www.gartner.com/en/documents/2057415/the-importance-of-big-data-a-definition

[10] "The 5 V's of big data," *Watson Health Perspectives*, Sep. 17, 2016. https://www.ibm.com/blogs/watson-health/the-5-vs-of-big-data/

[11] Arockia Panimalar.S, Varnekha Shree.S, Veneshia Kathrine.A, "The 17 V's Of Big Data," *Int. Res. J. Eng. Technol. IRJET*, [Online]. Available: https://www.irjet.net/archives/V4/i9/IRJET-V4I957.pdf

[12] P. Layton, *Algorithmic Warfare Applying Artificial Intelligence to Warfighting*. 2018.

[13] B. Vuleta, "How Much Data Is Created Every Day? +27 Staggering Stats," *SeedScientific*, Oct. 28, 2021. https://seedscientific.com/how-much-data-is-created-every-day/

[14] H. Patel, "What Happen in an Internet Minute," *Bond High Plus*, Apr. 14, 2021. https://www.bondhighplus.com/2021/04/14/what-happen-in-an-internet-minute/

[15] "¿Qué son los datasets y los dataframes en el Big Data? | Deusto Formación." https://www.deustoformacion.com/blog/programacion-tic/que-son-datasets-dataframes-big-data

[16] "Ships in Satellite Imagery." https://kaggle.com/rhammell/ships-in-satellite-imagery

[17] N. Mohamed and J. Al-Jaroodi, "Real-time big data analytics: Applications and challenges," in *2014 International Conference on High Performance Computing Simulation (HPCS)*, Jul. 2014, pp. 305–310. doi: 10.1109/HPCSim.2014.6903700.

[18] *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Connectivity for a Competitive Digital Single Market - Towards a European Gigabit Society*. 2016.

[Online]. Available: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52016DC0587
[19] Sitha Sok, "5G a Technology Vision," 08:59:56 UTC. [Online]. Available: https://es.slideshare.net/soksitha/5g-a-technology-vision
[20] "Tracking Change Over Time—Understanding Remote Sensing." https://pubs.usgs.gov/gip/133/pdf/RemSens-Student_web.pdf
[21] "What is Data Latency? | Earthdata." https://earthdata.nasa.gov/learn/backgrounders/data-latency/
[22] "Conoce las ubicaciones de nuestros centros de datos," *Centros de datos de Google*. https://www.google.com/intl/es/about/datacenters/locations/
[23] "Homepage - Facebook Data Centers," *Facebook Data Centers*. https://datacenters.fb.com/
[24] "¿Qué es Hadoop?" https://www.sas.com/es_es/insights/big-data/hadoop.html
[25] M. G.-M. García, "Data Science (Ciencia de Datos): aclaración de conceptos básicos," *Fundación iS+D*, Sep. 01, 2021. https://isdfundacion.org/2021/09/01/data-science-ciencia-de-datos-aclaracion-de-conceptos-basicos/
[26] D. Grossman, C. Curriden, L. Ma, L. Polley, J. D. Williams, and C. A. I. Cooper, "Chinese Views of Big Data Analytics," RAND Corporation, Sep. 2020. [Online]. Available: https://www.rand.org/pubs/research_reports/RRA176-1.html
[27] "What is Machine Learning? | IBM." https://www.ibm.com/cloud/learn/machine-learning#toc-machine-le-SzgJbkmk
[28] "Diferencias entre Data Science, Inteligencia Artificial, Machine Learning y Deep Learning," *PROGRAMMATIC SPAIN*. https://www.programaticaly.com/education/las-diferencias-que-hay-entre-data-science-artificial-intelligence-machine-learning-y-deep-learning
[29] "The Difference Between AI, Machine Learning, and Deep Learning? | NVIDIA Blog." https://blogs.nvidia.com/blog/2016/07/29/whats-difference-artificial-intelligence-machine-learning-deep-learning-ai/
[30] R. Schmelzer, "The Human-Powered Companies That Make AI Work," *Forbes*. https://www.forbes.com/sites/cognitiveworld/2020/02/02/the-human-powered-companies-that-make-ai-work/
[31] W. Wang, T. Nie, T. Fu, J. Ren, and L. Jin, "A Novel Method of Aircraft Detection Based on High-Resolution Panchromatic Optical Remote Sensing Images," *Sensors*, vol. 17, no. 5, Art. no. 5, May 2017, doi: 10.3390/s17051047.
[32] T. Redondo and A. M. Sandoval, "Text Analytics: the convergence of Big Data and Artificial Intelligence," *Int. J. Interact. Multimed. Artif. Intell.*, vol. 3, no. Special Issue on Big Data and AI, 2016, [Online]. Available: https://www.ijimai.org/journal/bibcite/reference/2540
[33] "Data Analysis of the 'Spotify' dataset using the Pandas library," *The #1 Data Science Channel*, Apr. 26, 2021. https://datascience.fm/fun-analysis-of-spotify-dataset-to-gain-insights-on-music-industry/
[34] "Big Data and Mobility as a Service - 1st Edition." https://www.elsevier.com/books/big-data-and-mobility-as-a-service/zhang/978-0-323-90169-7
[35] "A Tour Through the Visualization Zoo." https://homes.cs.washington.edu/~jheer/files/zoo/
[36] "Intelligence in a Data-Driven Age." https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-90/jfq-90_4-9_Weinbaum-Shanahan.pdf

[37] "BIG DATA EN LOS ENTORNOS DE DEFENSA Y SEGURIDAD." https://www.ieee.es/Galerias/fichero/docs_investig/DIEEEINV03-2013_Big_Data_Entornos_DefensaSeguridad_CarrilloRuiz.pdf
[38] "Multimedia Visualization of Massive Military Datasets (Atelier OTAN sur la visualisation multimedia d'ensembles massifs de donnees militaires)," NATO RESEARCH AND TECHNOLOGY ORGANIZATION NEUILLY-SUR-SEINE (FRANCE), Aug. 2002. [Online]. Available: https://apps.dtic.mil/sti/citations/ADA408812
[39] "Big Data and Artificial Intelligence for Decision Making: Dutch Position Paper." https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-IST-160/MP-IST-160-PP-1.pdf
[40] "STONewsArchive - NATO Guide to Data Collection and Management..." https://www.sto.nato.int/Lists/STONewsArchive/displaynewsitem.aspx?ID=563
[41] G. C. Edward Hunter Christie, "NATO Decision-Making in the Age of Big Data and Artificial Intelligence," *IAI Istituto Affari Internazionali*, Feb. 26, 2021. https://www.iai.it/en/pubblicazioni/nato-decision-making-age-big-data-and-artificial-intelligence
[42] "Military use of artificial intelligence has potential for 'destruction and disruption': Ng Eng Hen," *CNA*. https://www.channelnewsasia.com/singapore/ai-artificial-intelligence-military-space-ng-eng-hen-2238761
[43] NATO, "Summary of the NATO Artificial Intelligence Strategy," *NATO*. http://www.nato.int/cps/en/natohq/official_texts_187617.htm
[44] "DoD Data Strategy," 2020. https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF
[24] "DISA Strategic Plan 2013 2018.pdf." [Online]. Available: https://www.dau.edu/cop/pm/DAU%20Sponsored%20Documents/DISA%20Strategic%20Plan%202013%202018.pdf
[46] "DISA Strategic Plan 2019-2022 v1." https://disa.mil/-/media/Files/DISA/About/Strategic-Plan-version1.ashx
[47] "DISA Strategic Plan 2019-2022 v2." https://www.disa.mil/-/media/Files/DISA/About/Strategic-Plan.ashx
[48] M. Cooney, "DARPA does Big Data in a big way," *Network World*, Mar. 29, 2012. https://www.networkworld.com/article/2222020/darpa-does-big-data-in-a-big-way.html
[49] B. J. Lutton and 2015 Apr 15, "DARPA is spending big on big data," *FCW*. https://fcw.com/articles/2015/04/15/snapshot-data-programs.aspx
[50] "DARPA - AI Next Campaign." https://www.darpa.mil/work-with-us/ai-next-campaign
[51] "Big Data in DOD's FY 2021 Procurement and RDT&E Budget Programs | GovWin IQ." https://iq.govwin.com/neo/marketAnalysis/view/Big-Data-in-DODs-FY-2021-Procurement-and-RDTE-Budget-Programs/4504?researchTypeId=1&researchMarket=
[52] "The Pentagon is hunting ISIS using big data and machine learning," *Engadget*. https://www.engadget.com/2017-05-15-the-pentagon-is-hunting-isis-using-big-data-and-machine-learning.html
[53] "AI Experts Needed to Lead 'Project Maven' Move Within DOD," *Bloomberg Government*. https://about.bgov.com/news/ai-experts-needed-to-lead-project-maven-move-within-dod/
[54] T. Brewster, "Project Maven: Startups Backed By Google, Peter Thiel, Eric Schmidt And James Murdoch Are Building AI And Facial Recognition Surveillance Tools For The Pentagon," *Forbes*.

https://www.forbes.com/sites/thomasbrewster/2021/09/08/project-maven-startups-backed-by-google-peter-thiel-eric-schmidt-and-james-murdoch-build-ai-and-facial-recognition-surveillance-for-the-defense-department/
[55] "China crea agencia de tecnología militar avanzada, similar a la estadounidense DARPA." https://nmas1.org/news/2017/07/28/DARPA-chino
[56] S. Rodríguez, "Investigadores chinos desarrollan un submarino con Inteligencia Artificial," *Big Data Magazine*, Jul. 26, 2018. https://bigdatamagazine.es/investigadores-chinos-desarrollan-un-submarino-con-inteligencia-artificial
[57] Center for Security and Emerging Technology and D. Peterson, "Designing Alternatives to China's Repressive Surveillance State," Center for Security and Emerging Technology, Oct. 2020. doi: 10.51593/20200016.
[58] C. Chen, "China's Sharp Eyes CCTV surveillance program redefines the Neighborhood Watch," *PIA VPN Blog*, Mar. 04, 2021. https://www.privateinternetaccess.com/blog/chinas-sharp-eyes-cctv-surveillance-program-redefines-the-neighborhood-watch/
[59] I. M. y Ladera, "Las armas de China para derrotar el coronavirus: Big Data e Inteligencia Artificial," *El Radar*, Mar. 20, 2020. https://www.elradar.es/las-armas-de-china-para-derrotar-el-coronavirus-big-data-e-inteligencia-artificial/
[60] T. Pesonen and D. Defis, "Joint quest for future defence applications - Train together, deploy together," p. 44.
[61] "On a mission. EDA's support to CSDP operations." https://eda.europa.eu/docs/default-source/eda-magazine/edm21-single-1-48-web.pdf
[62] "Big Data analytics for defence," *Default*. https://eda.europa.eu/webzine/issue14/cover-story/big-data-analytics-for-defence
[63] "EDA studies points towards Big Data potential for defence." https://eda.europa.eu/news-and-events/news/2017/12/18/eda-studies-points-towards-big-data-potential-for-defence#
[64] "EDA's CySAP project launched - Shephard Media." https://www.shephardmedia.com/news/digital-battlespace/edas-cysap-project-launched-member-states/
[65] "ABIDE: Artificial Intelligence and Big Data for Decision Making in C4ISR | IPTC." https://iptc.upm.es/abide-artificial-intelligence-and-big-data-decision-making-c4isr
[66] R. D. Infodefensa.com, "GMV aplicará la inteligencia artificial a las comunicaciones militares," *Infodefensa*. https://www.infodefensa.com/texto-diario/mostrar/3130541/gmv-aplicara-inteligencia-artificial-comunicaciones-militares
[67] "Horizon 2020." https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-2020_en
[68] "Search | CORDIS | European Commission." https://cordis.europa.eu/search?q=contenttype%3D%27project%27%20AND%20programme%2Fcode%3D%27ICT-51-2020%27&p=1&num=10&srt=/project/contentUpdateDate:decreasing
[69] "Presentaciones del seminario: 'Aplicaciones de Big Data en los entornos de Defensa y Seguridad.'" https://www.tecnologiaeinnovacion.defensa.gob.es/en-us/Contenido/Pages/detallepublicacion.aspx?publicacionID=174
[70] "Thales y Atos crean el campeón europeo en big data e inteligencia artificial para defensa y seguridad," *Thales Group*.

https://www.thalesgroup.com/es/group/journalist/press-release/thales-atos-crean-el-campeon-europeo-big-data-e-inteligencia

[71] "Cómo la transformación digital está potenciando la superioridad naval," *Thales Group*. https://www.thalesgroup.com/es/el-mundo/defence/magazine/como-transformacion-digital-esta-potenciando-superioridad-naval

[72] "Big Data Analytics In Aerospace And Defense Market Trends, Size | Industry Growth, 2027." https://www.marketresearchfuture.com/reports/aerospace-big-data-analytics-market-7667

[73] "IV Congreso de Inteligencia Artificial: ¿dónde queda Europa?," *El Independiente*, Oct. 24, 2021. https://www.elindependiente.com/economia/2021/10/25/iv-congreso-de-inteligencia-artificial-donde-queda-europa/

[74] "David Carmona (Microsoft): 'EEUU abre más a capital privado la Inteligencia Artificial que otras regiones,'" *El Independiente*, Nov. 26, 2021. https://www.elindependiente.com/futuro/inteligencia-artificial/2021/11/26/david-carmona-microsoft-eeuu-abre-mas-a-capital-privado-la-inteligencia-artificial-que-otras-regiones/

[75] "Aplicaciones de Big Data en Defensa y Seguridad." https://www.tecnologiaeinnovacion.defensa.gob.es/Lists/Publicaciones/Attachments/174/AplicacionesBigDataDefensaSeguridad.pdf

[76] A. Torres, "Aplicaciones BIG DATA en las Administraciones Publicas." https://www.tecnologiaeinnovacion.defensa.gob.es/Lists/Publicaciones/Attachments/174/BIG%20DATA%20en%20la%20ADMINISTRACION%20final.pdf

[77] "Igape - Oportunidades industria 4.0 en Galicia." https://www.atiga.es/web/wp-content/uploads/2017/03/Estado-del-Arte-Big-Data-CC-DA.pdf

[78] "La ministra Cospedal inaugura el Congreso Big Data en Valencia: «Debemos igualar el paso de la seguridad a los cambios tecnológicos»," *Las Provincias*, Nov. 23, 2017. https://www.lasprovincias.es/sociedad/congreso-big-data-valencia-cospedal-20171123104745-nt.html

[79] Ministerio Defensa, "La facilidad con la que la información privada, o que creemos privada, se multiplica y almacena, ha de venir acompañada de una protección global y de una seguridad integral, asegura @mdcospedal #BigDataLP @lasprovincias https://t.co/3dybwsYTPQ," *@defensagob*, Nov. 23, 2017. https://twitter.com/defensagob/status/933650312312827904

[80] E. Press, "AI & Big Data Congress vincula la competitividad con la predicción de la inteligencia artificial," Oct. 15, 2020. https://www.europapress.es/economia/noticia-ai-big-data-congress-vincula-competitividad-prediccion-inteligencia-artificial-20201015181948.html

[81] INAP, "Congreso (webinar): Regulación y explotación de big data para los servicios públicos." http://laadministracionaldia.inap.es/noticia.asp?id=1208411

[82] "Congreso: Regulación y explotación de big data para los servicios públicos - YouTube." https://www.youtube.com/playlist?list=PLMqWVbmUv8ThOnXhLZSsfB9U_nsqnu3G2

[83] "El 'Big Data' se estanca en España: Solo el 6 % de las empresas lo emplearon de forma recurrente en 2020," *Confilegal*, Oct. 23, 2021. https://confilegal.com/20211023-el-big-data-retrocede-solo-el-6-de-las-empresas-lo-emplearon-el-pasado-ano-de-forma-recurrente/

[84] R. D. Infodefensa.com, "CNI modernizará sus procedimientos con el big data y la inteligencia artificial," *Infodefensa*. https://www.infodefensa.com/texto-diario/mostrar/3233452/cni-modernizara-procedimientos-big-data-inteligencia-artificial

[85] "PLAN DE ACCIÓN DEL MINISTERIO DE DEFENSA PARA LA TRANSFORMACIÓN DIGITAL." https://publicaciones.defensa.gob.es/media/downloadable/files/links/t/r/transformaci_n_digial_minisdef.pdf
[86] "IEEE - Despega la transformación digital del Ministerio de Defensa (DIEEEM28-2015)." https://www.ieee.es/publicaciones-new/documentos-marco/2015/DIEEEM28-2015.html
[87] D. G.-A. Lacalle and F. L. López, "Evolución del Centro de Supervisión y Análisis de Datos de la Armada (CESADAR)," *Rev. Gen. Mar.*, vol. 275, no. 2, pp. 333–346, 2018.
[88] V. C. Gamboa, "La maqueta digital," *Rev. Gen. Mar.*, vol. 275, no. 2, pp. 321–331, 2018.
[89] A. Herranz, "Digital twins: qué son, para qué sirven y cuáles son los beneficios y problemas de los gemelos digitales," *Xataka*, May 26, 2021. https://www.xataka.com/pro/digital-twins-que-sirven-cuales-beneficios-problemas-gemelos-digitales
[90] Defensa.com, "Navantia y Telefónica Tech instalarán un sistema de ciberseguridad reforzado en los submarinos S-80-noticia defensa.com - Noticias Defensa Defensa Naval," *Defensa.com*, Dec. 01, 2021. https://www.defensa.com/defensa-naval/navantia-telefonica-tech-instalaran-sistema-ciberseguridad-s-80
[91] "Dossier El EA conectado RAA.pdf." Accessed: Dec. 15, 2021. [Online]. Available: https://ejercitodelaire.defensa.gob.es/EA/bacsi/files/Dossier%20El%20EA%20conectado%20RAA.pdf
[92] Pablo Julián García-Patos Herreros, "DATA SCIENCE E INTELIGENCIA ARTIFICIAL, MANUAL DE CAMPO: EJÉRCITO FUTURO - Revista Ejercito," Nov. 2020. https://ejercito.defensa.gob.es/Galerias/multimedia/revista-ejercito/2020/955/accesible/revista-ejercito-noviembre-955.pdf
[93] "La Inteligencia Artificial aplicada a la defensa," CESDEN 2018. https://www.ieee.es/Galerias/fichero/docs_trabajo/2019/DIEEET0-2018La_inteligencia_artificial.pdf
[94] "Concepto de BIG DATA y su aplicación a defensa y seguridad." https://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Contenido/Paginas/detallereferencia.aspx?referenciaID=33
[95] "Military Implications of Big Data - PDF Free Download." https://docplayer.net/7780300-Military-implications-of-big-data.html
[96] "1511401708_RedefiningMilitaryIntelligenceUsingBigDataAnalytics.pdf." Accessed: Dec. 30, 2021. [Online]. Available: https://archive.claws.in/images/journals_doc/1511401708_RedefiningMilitaryIntelligenceUsingBigDataAnalytics.pdf
[97] "Difference In Management Information Systems vs. Information Technology," *Investopedia*. https://www.investopedia.com/ask/answers/040315/what-difference-between-mis-management-information-system-and-information-technology.asp
[98] "Gestión del conocimiento y gestión de la información | revista PH", [Online]. Available: https://www.iaph.es/revistaph/index.php/revistaph/article/view/1153
[99] Y. Qin, X. Zhang, G. Gao, and K. Wang, "The Role of Big Data in Intelligent Combat Command," presented at the 2018 International Symposium on Communication Engineering & Computer Science (CECS 2018), Hohhot, China, 2018. doi: 10.2991/cecs-18.2018.27.
[100] "LA GESTIÓN DEL CONOCIMIENTO EN LA ARMADA." https://dialnet.unirioja.es/descarga/articulo/4581820.pdf

[101] X. Meng, J. Li-ya, Y. Chao-hong, and B. Jian-quan, "Construction and Application Technology Architecture of Domain-specific Knowledge Graphin Military Field," *J. Phys. Conf. Ser.*, vol. 1792, no. 1, p. 012044, Feb. 2021, doi: 10.1088/1742-6596/1792/1/012044.

[102] P. Sun, "Prison Big Data," in *Smart Prisons*, P. Sun, Ed. Singapore: Springer, 2022, pp. 89–105. doi: 10.1007/978-981-16-9657-2_5.

[103] J. Yang, "Big Data Technology and Prison Management Analysis," in *2021 International Conference on Big Data Analysis and Computer Science (BDACS)*, Jun. 2021, pp. 35–38. doi: 10.1109/BDACS53596.2021.00016.

[104] D. Ning, P. Chen, G. Yuan, J. Xu, and L. Xu, "Research on Warship Communication Operation and Maintenance Management Based on Big Data," in *2014 International Conference on Cloud Computing and Big Data*, Nov. 2014, pp. 126–129. doi: 10.1109/CCBD.2014.24.

[105] "Centro de Sistemas y Tecnologías de la Información y las Comunicaciones - Ministerio de Defensa de España." https://www.defensa.gob.es/ministerio/organigrama/sedef/cestic/

[106] S. Kulshrestha, "Big Data in Military Information & Intelligence," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 2765008, Jan. 2016. [Online]. Available: https://papers.ssrn.com/abstract=2765008

[107] M. Abadicio, "Big Data in the Military - Intelligence Gathering and AI," *Emerj*. https://emerj.com/ai-sector-overviews/big-data-military/

[108] S. Nie and D. Sun, "Research on counter-terrorism based on big data," in *2016 IEEE International Conference on Big Data Analysis (ICBDA)*, Mar. 2016, pp. 1–5. doi: 10.1109/ICBDA.2016.7509788.

[109] R. Mourtada and F. Salem, *Social Media in the Arab World: Influencing Societal and Cultural Change?* 2012. [Online]. Available: https://www.researchgate.net/publication/230709418_Social_Media_in_the_Arab_World_Influencing_Societal_and_Cultural_Change

[110] de M. de, "Nuevo horizonte tecnológico surgido del BigData Ejemplo de capacidades y aplicaciones en Defensa: aplicaciones OSINT - Future Space," p. 18.

[111] DataReportal, "Digital 2022 Global Overview Report (January 2022) v05," 07:37:19 UTC. [Online]. Available: https://www.slideshare.net/DataReportal/digital-2022-global-overview-report-january-2022-v05

[112] "¿Qué son las fake news? Definición, tipos y métodos para identificarlas," *IONOS Digitalguide*. https://www.ionos.es/digitalguide/online-marketing/redes-sociales/que-son-las-fake-news/

[113] A. F. O. Palacio and E. S. de G. "General R. R. Prieto", "La Inteligencia Artificial en el Contexto Militar Internacional y sus Posibles Aplicaciones en el Ejército Nacional de Colombia | Diálogo Americas." https://dialogo-americas.com/es/articles/la-inteligencia-artificial-en-el-contexto-militar-internacional-y-sus-posibles-aplicaciones-en-el-ejercito-nacional-de-colombia/

[114] Centro Conjunto de Desarrollo de Conceptos, "Usos militares de la inteligencia artificial, la automatización y la robótica (IAA&R)." https://emad.defensa.gob.es/Galerias/CCDC/files/USOS_MILITARES_DE_LA_INTELIGENCIA_ARTIFICIALx_LA_AUTOMATIZACION_Y_LA_ROBOTICA_xIAAxRx.-_VV.AA.pdf

[115] G. Zamarreño-Aramendia, F. J. Cristòfol, J. de-San-Eugenio-Vela, and X. Ginesta, "Social-Media Analysis for Disaster Prevention: Forest Fire in Artenara and Valleseco, Canary Islands," *J. Open Innov. Technol. Mark. Complex.*, vol. 6, no. 4, Art. no. 4, Dec. 2020, doi: 10.3390/joitmc6040169.

[116] "Policía Nacional: 'En la vida virtual lo que hacemos también tiene sus consecuencias,'" *El blog de Orange*, May 07, 2019. https://blog.orange.es/responsabilidad-social-corporativa/policia-nacional-vida-virtual-consecuencias/

[117] R. R. Andrés and J. M. López-García, "Aproximación al uso de las redes sociales por las fuerzas y cuerpos de seguridad en España en perspectiva internacional," *index.comunicación*, vol. 9, no. 1, Art. no. 1, Sep. 2019, doi: 10.33732/ixc/09/01Aproxi.

[118] Mecalux, "¿Qué es la logística de una empresa?" https://www.mecalux.es/manual-almacen/logistica

[119] "Logística militar: qué es y cómo se aplica en empresas hoy," Jan. 07, 2021. https://novocargo.com/logistica-militar-que-es-como-se-aplica-empresas-hoy/

[120] H. Shi, F. Wan, and X. Lei, "Research on Military Logistics based on Big Data," Apr. 2019, pp. 231–237. doi: 10.2991/icmeit-19.2019.40.

[121] T. Borgi, N. Zoghlami, and M. Abed, "Big data for transport and logistics: A review," in *2017 International Conference on Advanced Systems and Electric Technologies (IC_ASET)*, Jan. 2017, pp. 44–49. doi: 10.1109/ASET.2017.7983742.

[122] P. Ren and R. Ding, "The Application and Development of Big Data in Transport Logistics Industry in China," in *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, Mar. 2019, pp. 149–154. doi: 10.1109/ITNEC.2019.8729484.

[123] J. Du, H. Zhan, and L. Du, "Research on Site Selection and Algorithm of Military Logistics Center," *J. Phys. Conf. Ser.*, vol. 1792, no. 1, p. 012034, Feb. 2021, doi: 10.1088/1742-6596/1792/1/012034.

[124] A. Bardal and M. Sigitova, "Localization of Transport and Logistics Centers in the Region," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 753, no. 7, p. 072021, Feb. 2020, doi: 10.1088/1757-899X/753/7/072021.

[125] F. Hadi, H. I. Nur, N. K. P. Maharani, C. B. S. Permana, I. G. N. S. Buana, and E. W. Ardhi, "Search and rescue station location selection and conceptual design: a case study of western region of Indonesia," *IOP Conf. Ser. Earth Environ. Sci.*, vol. 649, no. 1, p. 012069, Feb. 2021, doi: 10.1088/1755-1315/649/1/012069.

[126] M. Hao, X. Yong, X. Xi, T. Zhang, and Y. Zhang, "Method for Optimising Mission-Specific Inventory of Aviation Materials," in *2020 IEEE International Conference on Information Technology,Big Data and Artificial Intelligence (ICIBA)*, Nov. 2020, vol. 1, pp. 506–511. doi: 10.1109/ICIBA50161.2020.9276911.

[127] C. Zhai, X. Jiang, Y. Zhang, and N. Liu, "Research on the Optimization of Military Supplies under Big Data Background," in *2018 International Conference on Big Data and Artificial Intelligence (BDAI)*, Jun. 2018, pp. 18–23. doi: 10.1109/BDAI.2018.8546629.

[128] F. Li, "Application of Flight Test Data Mining in Safety Monitoring of Civil Aviation Products," in *Proceedings of the 5th China Aeronautical Science and Technology Conference*, Singapore, 2022, pp. 719–727. doi: 10.1007/978-981-16-7423-5_70.

[129] T. Wang, X. Wang, H. Qu, and J. Zhang, "Thinking on the Application of Big Data in Fault Diagnosis of Military Equipment," in *2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*, Dec. 2020, vol. 9, pp. 1451–1457. doi: 10.1109/ITAIC49862.2020.9339172.

[130] A. R. Arjona, "El Ejército de Tierra busca talento digital para la base logística de Córdoba," *Diario Córdoba*, Jan. 17, 2022.

https://www.diariocordoba.com/cordoba-ciudad/2022/01/17/ejercito-tierra-busca-talento-digital-61659811.html (accessed Apr. 06, 2022).

[131] "Common Operational Picture Defined," *Coolfire*. https://www.coolfiresolutions.com/blog/common-operational-picture-defined/

[132] "What is Situational Awareness? | Coolfire Solutions Blog," *Coolfire*. https://www.coolfiresolutions.com/blog/what-is-situational-awareness/

[133] M. Chmielewski, M. Kukiełka, D. Frąszczak, and D. Bugajewski, "Military and Crisis Management Decision Support Tools for Situation Awareness Development Using Sensor Data Fusion," in *Information Systems Architecture and Technology: Proceedings of 38th International Conference on Information Systems Architecture and Technology – ISAT 2017*, Cham, 2018, pp. 189–199. doi: 10.1007/978-3-319-67229-8_17.

[134] "Tracking of objects in a multi-sensor fusion system for border surveillance_jdst_article.pdf." Accessed: Apr. 18, 2022. [Online]. Available: https://www.jdst.eu/sites/jdst.eu/files/publications/jdst_tracking_article_ait-uor_submission-final_za_saita_-2.pdf

[135] F. Hamami, I. A. Dahlan, S. W. Prakosa, and K. F. Somantri, "Big Data Analytics for Processing Real-time Unstructured Data from CCTV in Traffic Management," in *2020 International Conference on Data Science and Its Applications (ICoDSA)*, Aug. 2020, pp. 1–5. doi: 10.1109/ICoDSA50139.2020.9212858.

[136] C. Yao, K. Cheng, X. Zhang, and Z. Wang, "Research on the Method of Operational Plan Recognition Driven by Big Data in Battlefield Awareness," in *2018 IEEE International Conference of Safety Produce Informatization (IICSPI)*, Dec. 2018, pp. 800–803. doi: 10.1109/IICSPI.2018.8690485.

[137] "The prediction of terrorist threat on the basis of semantic association acquisition and complex network evolution.pdf." Accessed: Apr. 18, 2022. [Online]. Available: https://www.itl.waw.pl/czasopisma/JTIT/2008/2/14.pdf

[138] K. H. Pham and M. Luengo-Oroz, "Predictive modeling of movements of refugees and internally displaced people: Towards a computational framework," *ArXiv220108006 Cs*, Jan. 2022, [Online]. Available: http://arxiv.org/abs/2201.08006

[139] "Ciberdefensa: el papel de los Directivos ante un ciberataque - WTW," *Willis Towers Watson Update*, Jul. 10, 2021. https://willistowerswatsonupdate.es/ciberseguridad/las-consecuencias-de-la-innaccion-ante-un-ciberataque/

[140] Yamini, "Applications of Big Data Analytics in Cybersecurity | Analytics Steps." https://www.analyticssteps.com/blogs/big-data-analytics-cybersecurity-role-and-applications

[141] P. Angin, B. Bhargava, and R. Ranchal, "Big Data Analytics for Cyber Security," *Secur. Commun. Netw.*, vol. 2019, p. e4109836, Sep. 2019, doi: 10.1155/2019/4109836.

[142] R. P. Krupani, M. G. Aditya, C. S. Prithvi Raghavan, and H. S. Gururaja, "Big Data Cybersecurity Monitoring System using Machine Learning," in *2021 International Conference on Forensics, Analytics, Big Data, Security (FABS)*, Dec. 2021, vol. 1, pp. 1–7. doi: 10.1109/FABS52071.2021.9702637.

[143] M. M. Alani, "Big data in cybersecurity: a survey of applications and future trends," *J. Reliab. Intell. Environ.*, vol. 7, no. 2, pp. 85–114, Jun. 2021, doi: 10.1007/s40860-020-00120-3.

[144] M. Johnstone and M. Peacock, "Seven Pitfalls of Using Data Science in Cybersecurity," in *Data Science in Cybersecurity and Cyberthreat Intelligence*, L.

F. Sikos and K.-K. R. Choo, Eds. Cham: Springer International Publishing, 2020, pp. 115–129. doi: 10.1007/978-3-030-38788-4_6.

[145] F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, and M. Michaloliakos, "Cybersecurity Challenges in the Maritime Sector," *Network*, vol. 2, no. 1, Art. no. 1, Mar. 2022, doi: 10.3390/network2010009.

[146] "Análisis forense digital." https://www.interpol.int/es/Como-trabajamos/Innovacion/Analisis-forense-digital

[147] D. Mane and K. Shibe, "Big Data Forensic Analytics," in *Data Management, Analytics and Innovation*, Singapore, 2019, pp. 113–129. doi: 10.1007/978-981-13-1274-8_9.

[148] S. Zawoad and R. Hasan, "Digital Forensics in the Age of Big Data: Challenges, Approaches, and Opportunities," in *2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems*, Aug. 2015, pp. 1320–1325. doi: 10.1109/HPCC-CSS-ICESS.2015.305.

[149] F. Focus, "Digital Forensics as a Big Data Challenge," *Forensic Focus*, Aug. 07, 2017. https://www.forensicfocus.com/articles/digital-forensics-as-a-big-data-challenge/

[150] O. M. Adedayo, "Big data and digital forensics," in *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, Jun. 2016, pp. 1–7. doi: 10.1109/ICCCF.2016.7740422.

[151] U. Garain and B. Halder, "Even big data is not enough: need for a novel reference modelling for forensic document authentication," *Int. J. Doc. Anal. Recognit. IJDAR*, vol. 23, no. 1, pp. 1–11, Mar. 2020, doi: 10.1007/s10032-019-00345-w.

[152] "La Biometría en Apoyo a la Procuración de Justicia," *Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública - México*. https://fgjem.edomex.gob.mx/sites/fgjem.edomex.gob.mx/files/files/SeguridadDelincuencia/JornadaCriminalistica/biometria%20en%20apoyo.pdf

[153] Z. Li, Y. Tie, and L. Qi, "Face Recognition in Real-world Internet Videos Based on Deep Learning," in *2019 8th International Symposium on Next Generation Electronics (ISNE)*, Oct. 2019, pp. 1–3. doi: 10.1109/ISNE.2019.8896630.

[154] I. B. Ciocoiu and N. Cleju, "Off-Person ECG Biometrics Using Spatial Representations and Convolutional Neural Networks," *IEEE Access*, vol. 8, pp. 218966–218981, 2020, doi: 10.1109/ACCESS.2020.3042547.

[155] "Biometría para identificación y autenticación," *Thales Group*. https://www.thalesgroup.com/es/countries/americas/latin-america/dis/gobierno/inspiracion/biometria

[156] F. A. Galgano and E. P. F. Rose, "Military Geoscience," in *Encyclopedia of Geology (Second Edition)*, D. Alderton and S. A. Elias, Eds. Oxford: Academic Press, 2021, pp. 648–659. doi: 10.1016/B978-0-12-409548-9.09141-7.

[157] "SISTEMAS DE INFORMACIÓN GEOGRÁFICA." https://administracionelectronica.gob.es/pae_Home/dam/jcr:3440992b-44ee-4240-8000-ac0a502ffb56/Ponencia_130.pdf

[158] "ESA - Eduspace ES - Inicio - ¿Qué es la teledetección?," Dec. 09, 2009. https://www.esa.int/SPECIALS/Eduspace_ES/SEMO1U3FEXF_0.html

[159] "Teledetección." http://www.ign.es/web/ign/portal/obs-teoria-teledeteccion

[160] D. J. Johnson, M. Nelson, and R. J. Lempert, "U.S. Spaced-Based Remote Sensing: Challenges and Prospects," RAND Corporation, Jan. 1993. [Online]. Available: https://www.rand.org/pubs/notes/N3589.html

[161] R. Booysen, R. Gloaguen, S. Lorenz, R. Zimmermann, and P. A. M. Nex, "Geological Remote Sensing," in *Encyclopedia of Geology (Second Edition)*, D. Alderton and S. A. Elias, Eds. Oxford: Academic Press, 2021, pp. 301–314. doi: 10.1016/B978-0-12-409548-9.12127-X.

[162] G. Cheng and J. Han, "A survey on object detection in optical remote sensing images," *ISPRS J. Photogramm. Remote Sens.*, vol. 117, pp. 11–28, Jul. 2016, doi: 10.1016/j.isprsjprs.2016.03.014.

[163] A. Ammar, A. Koubaa, M. Ahmed, A. Saad, and B. Benjdira, "Vehicle Detection from Aerial Images Using Deep Learning: A Comparative Study," *Electronics*, vol. 10, no. 7, Art. no. 7, Jan. 2021, doi: 10.3390/electronics10070820.

[164] "Use of Remote Sensing Imagery for Fast Generation af Military Maps and Simulator databases.pdf." Accessed: Apr. 19, 2022. [Online]. Available: https://www.isprs.org/proceedings/XXXIII/congress/part2/573_XXXIII-part2.pdf

[165] W. Watts, "Here's the technology being used to watch Russian troops as Ukraine invasion fears linger," *MarketWatch*. https://www.marketwatch.com/story/how-fears-of-russian-invasion-of-ukraine-put-open-source-intelligence-in-spotlight-11645033603

[166] J. Vincent, "Google disables Maps traffic data in Ukraine to protect citizens," *The Verge*, Feb. 28, 2022. https://www.theverge.com/2022/2/28/22954426/google-disables-maps-traffic-data-in-ukraine-to-protect-citizens

[167] "¿Por qué Google desactivó los datos de tráfico de Maps en Ucrania?," *Digital Trends Español*, Feb. 28, 2022. https://es.digitaltrends.com/tendencias/google-desactivo-datos-trafico-maps-ucrania/

[168] J. P. Colomé, "Un puñado de investigadores de internet se convierte en una fuente básica de información sobre Ucrania (también desde España)," *El País*, Mar. 18, 2022. https://elpais.com/tecnologia/2022-03-18/un-punado-de-investigadores-de-internet-se-convierte-en-una-fuente-basica-de-informacion-sobre-ucrania-tambien-desde-espana.html

[169] Oryx, "Attack On Europe: Documenting Equipment Losses During The 2022 Russian Invasion Of Ukraine," *Oryx*. https://www.oryxspioenkop.com/2022/02/attack-on-europe-documenting-equipment.html

[170] "UA Ukraine Weapons Tracker (@UAWeapons) / Twitter," *Twitter*. https://twitter.com/UAWeapons

[171] O. Kardoudi, "El primer 'deep fake' usado en un conflicto armado muestra a Zelenski rindiéndose," *elconfidencial.com*, Mar. 17, 2022. https://www.elconfidencial.com/tecnologia/novaceno/2022-03-17/hackers-rusos-difunden-un-video-falso-de-zelensky-ordenando-la-rendicion_3393225/

[172] "Deep fakes: qué es, cómo se crean y cuáles fueron los primeros | ESIC." https://www.esic.edu/rethink/tecnologia/deep-fakes-que-es-como-se-crean-primeros-y-futuros

[173] "Análisis de contenido: Pudimos visualizar esta guerra mucho antes," *CETYS*, Mar. 07, 2022. https://www.cetys.mx/noticias/analisis-de-contenido-pudimos-visualizar-esta-guerra-mucho-antes/

[174] "Cómo se usa el Big Data en guerras como la de Rusia y Ucrania," *Big Data Magazine*, Feb. 28, 2022. https://bigdatamagazine.es/como-se-usa-el-big-data-en-guerras-como-la-de-rusia-y-ucrania