

INTELIGENCIA DE CÓDIGO ABIERTO (OSINT). EL CAMINO POR DELANTE

Gabriel-Traian UNGUREANU

Academia Nacional de Inteligencia "Mihai Viteazul", Bucarest, Rumania

Resumen: Los avances tecnológicos han llevado a un crecimiento exponencial en la cantidad y complejidad de la información de fuentes abiertas. El peso de este tipo de información en la base de recolección ha aumentado significativamente y ahora contamos con servicios de inteligencia que recolectan más del 80% de su inteligencia de fuentes abiertas. Por ello, en este artículo, haciendo referencia a las tecnologías de punta de manera exhaustiva, analizamos cómo las nuevas tecnologías sustentan a los servicios de inteligencia en sus acciones de recolección de inteligencia de fuente abierta y aumentan la eficiencia de los procesos relacionados. Además, analizamos cómo estas tecnologías pueden complementarse y potenciarse entre sí a lo largo de las fases del ciclo de inteligencia para hacer más eficiente la actividad de los servicios de inteligencia. Finalmente, analizando los avances históricos, pronosticaremos qué tecnologías se espera que soporten OSINT en los próximos diez años y cómo se integrarán en las fases del ciclo de inteligencia, pronosticando cómo OSINT avanzará a través del cambio tecnológico.

Palabras clave: inteligencia de código abierto, OSINT, cambio tecnológico, intelli
ciclo de gencia, impacto de las nuevas tecnologías.

1. INTRODUCCIÓN

El proceso de recopilación de información de fuente abierta se considera y aborda de manera diferente, según el campo de actividad. De un área a otra (inteligencia académica, empresarial, periodística o de seguridad nacional), la visión estratégica, las operaciones relacionadas o los pasos tácticos son distintos cuando se trata de fuentes abiertas. La principal diferencia

de OSINT -inteligencia de código abierto sobre seguridad nacional- es la gran cantidad de datos e información recopilada. Otra característica distintiva de OSINT es la gran cantidad de fuentes, fuentes extremadamente variadas que también requieren varios métodos de recopilación. Los mecanismos utilizados por los servicios de inteligencia del gobierno para procesar datos de fuente abierta en información validada (de OSD - Datos de fuente abierta a OSIF - Open

Información de origen en OSINT - Inteligencia de código abierto en OSINT-V - Inteligencia validada de código abierto) también son muy complejos (OTAN: 2011).

A pesar de las dificultades mencionadas anteriormente, los servicios de inteligencia actualmente pueden proporcionar inteligencia procesable recopilada solo de fuentes abiertas. Además, OSINT puede proporcionar soporte o inteligencia contextual. Así, junto con la Inteligencia Humana (HUMINT), la Inteligencia de Señales (SIGINT), la Inteligencia de Imágenes (IMINT) y la Inteligencia de Medida y Firma (MASINT), los servicios de inteligencia pueden asegurar, source, la información requerida por los beneficiarios. (OTAN: 2011). Junto con los otros tipos de fuentes, OSINT contribuye significativamente a la base de recopilación.

Para hacer frente a los retos que plantea OSINT y no sólo por el volumen de datos e información, el número y diversidad de fuentes y la complejidad de procesos específicos del ciclo de inteligencia, los servicios de inteligencia siempre han innovado y utilizado tecnologías de última generación. -tecnologías del arte (CRS: 2020).

Como el propósito de este artículo es estimar qué tecnologías mejorarán OSINT en los próximos diez años y cómo estas tecnologías se integrarán en los procesos específicos de recopilación, procesamiento, análisis, difusión de información,

y almacenamiento, en el apartado II "OSINT" analizaremos la evolución de OSINT desde la Edad Moderna hasta la actualidad, estableciendo las tendencias actuales y futuras. En la sección III, considerando las tendencias de OSINT y los posibles avances tecnológicos, analizaremos las tecnologías que se utilizan actualmente y pronosticaremos qué tecnologías se utilizarán en un futuro cercano a mediano.

2. INTELIGENCIA DE CÓDIGO ABIERTO (OSINT)

2.1. Evolución de OSINT

Aunque las primeras referencias históricas sobre la recopilación de código abierto datan de la antigüedad, sus procesos específicos se definieron una vez que aparecieron los medios impresos.

El primer hito relevante retenido al discutir la evolución de OSINT es el comienzo de la recopilación sistémica y sistemática de fuentes abiertas. En su lucha por el control del Mar Mediterráneo, la República de Venecia y la República de Dubrovnik (o Ragusa) contribuyeron significativamente al desarrollo de la inteligencia.

Así, en el siglo XV, tanto Venecia como Ragusa tenían redes de inteligencia estructuradas (sistémicas) que transmitían información de forma constante y sistemática. En el contexto de esta feroz lucha por la recopilación de información, a mediados del siglo XVI, tanto Venetia como Ragusa

señaló “el valor de las gacetas que comenzaron a circular” (Huges Wilson: 2018, 29). Es por esto que apareció la primera recopilación sistemática de fuentes abiertas. “Una vez que aparecieron los medios impresos, el espionaje se volvió más abierto y sistemático”. Además, “los agentes venecianos comenzaron a recopilar información de mercado cuando se organizaron las grandes ferias europeas” (Huges-Wilson: 2018, 30). Como tal, alrededor del año 1540, para aprovechar las circunstancias que promueven la recopilación de información de fuente abierta y semiabierta, Venetia tenía una red emergente (sistémica) de inteligencia sobre el dinero, los mercados, el comercio y los flujos relacionados. la cual estaba siendo utilizada en interés del Estado (Huges-Wilson: 2018).

El segundo hito en el desarrollo de OSINT es el momento en que una red de inteligencia estructurada influyó y controló los medios impresos. En 1865 se instaló un centro de poder secreto al servicio de Otto von Bismarck: una red de más de 45.000 espías coordinada por Wilhelm Stieber. La red proporcionó información nacional y extranjera y, a menudo, llevó a cabo misiones contra objetivos diplomáticos.

Por ejemplo, para el ataque de 1870 contra Francia, Stieber organizó el sistema de inteligencia más grande que involucró a más de 35,000 personas y proporcionó más de 1650 informes para cada problema posible y probable

(Huges-Wilson: 2018). Además, primero inició una verdadera guerra psicológica con el objetivo de mejorar la moral de su propio ejército y debilitar la moral del enemigo publicando los errores, las malas noticias y las pérdidas del enemigo y enfatizando su propio éxito.

Además de los aspectos políticos, diplomáticos o militares, también es relevante mencionar que Stieber “fue el primer jefe de un servicio de inteligencia nacional que utilizó agentes para monitorear y controlar la prensa” (Huges-Wilson: 2018, 46). A partir de ese momento, los servicios de inteligencia debían validar la información recogida de la prensa en base a criterios como publicación, autor, contexto, etc.

El tercer hito es el momento en que los servicios de inteligencia se convirtieron en instituciones gubernamentales y se ampliaron. Debido a las tensiones sociales surgidas a raíz de las actuaciones de los servicios secretos, los servicios de inteligencia se convirtieron en una obsesión pública y los gobiernos, alimentados por estos temores, empezaron a constituir las primeras organizaciones nacionales. Así, la Oficina del Servicio Secreto se formó en 1909, cambiando posteriormente su nombre en MI5. En 1912 se formó el

“Servicio Secreto de Inteligencia” y estuvo a cargo de las operaciones en el extranjero. Posteriormente se convirtió en MI6 (Williams, Blum: 2018) (Herman: 1999). El desarrollo de los

servicios de inteligencia nacionales y extranjeros ha lle

El enfoque ahora era bivalente, la información de código abierto se recopilaba de fuentes nacionales y de territorios objetivo en el extranjero (Herman: 1999).

El cuarto hito sería el auge de la radio y la televisión. Durante las dos guerras mundiales, la inteligencia adquirió una importancia sustancialmente mayor. En Estados Unidos se fundó la Oficina de Servicios Estratégicos (OSS), predecesora de la CIA. Stalin también desarrolló los servicios secretos.

En este contexto de servicios de inteligencia en continua expansión, se hizo evidente la necesidad de desarrollar OSINT (Herman: 1999).

Al ser la Guerra Fría una guerra de inteligencia, había que acceder a todo tipo de fuentes y se utilizaban todos los métodos de recopilación conocidos, jugando OSINT un papel cada vez más importante, teniendo en cuenta además que este período coincidió con el desarrollo de las redes públicas y privadas de radio y televisión. . (Williams, Blum: 2018)

Si bien los servicios de inteligencia se centraron anteriormente en indexar, almacenar y acceder fácilmente a la información escrita, ahora comenzaron a preocuparse por convertir la voz en texto para procesar la información difundida a través de la radio. Este es también el momento en que surge la necesidad de capturar, indexar, guardar y acceder a la información del video.

Es el período en el que se hizo evidente que, además de SIGINT, IMINT o MASINT, la eficiencia

de OSINT dependía en gran medida de la eficiencia de la informática y otras tecnologías utilizadas (Williams, Blum: 2018).

El quinto hito es el uso masivo de Internet. El hecho de que el inicio de www coincidiera con el final de la Guerra Fría, la eliminación de ciertas tensiones internacionales y la erradicación de algunos sistemas de censura provocaron la exposición y el tránsito de un volumen de datos mucho mayor, también debido a la aceleración de la globalización. . El año 2000 y el estallido de la burbuja de las puntocom provocaron un crecimiento exponencial del volumen de datos disponibles en Internet (CRS: 2020).

Además, las redes sociales abrieron nuevas perspectivas, proporcionando nuevas categorías de datos y metadatos que permitieron el microperfilado y el perfilado de una entidad o grupo en cualquier nivel (Miller: 2015)

(Huges-Wilson: 2018). Esta tendencia se vio reforzada por la aparición de dispositivos móviles de acceso a datos que llevaron a un aumento significativo en el uso de las redes sociales (Williams, Blum: 2018). Las nuevas tecnologías cubrieron las necesidades de los servicios de inteligencia de gestionar grandes volúmenes de datos, facilitando las actividades específicas del ciclo de inteligencia, especialmente en lo que se refiere a la recogida, tratamiento, gestión y difusión de la información. Por ejemplo, en 2008, DNI Open- Source Center (OSC) estaba utilizando tecnología para recopilar información económica de

más de 2000 publicaciones periódicas, 300 estaciones de radio, 235 estaciones de televisión, 95 organizaciones extranjeras (por ejemplo, The Economist, Thomson Reuters, Lexis-Nexis, Stratfor, etc.) y otras fuentes de más de 160 países, con información en más de 80 idiomas, de sitios web, prensa, programas, televisión, radio, mapas, bases de datos, literatura gris, fotografías e imágenes satelitales comerciales (Hamilton: 2011).

Además, desde principios de la década de 2000, las nuevas tecnologías han permitido implementar flujos y procedimientos de comunicación eficientes, en tiempo real, entre diversos grupos de entidades dentro de las estructuras de inteligencia, cumpliendo también con las restricciones impuestas por los criterios de clasificación de la información (ieee.es: 2013). El paso de lo analógico a lo digital permitió afinar los métodos de recolección. Los flujos de radio se convirtieron automáticamente en texto y los flujos de televisión en texto y secuencias de cuadros. Esto permitió su indexación y procesamiento automáticos, por ejemplo, las correlaciones quién-dónde-cuándo.

La búsqueda e indexación por imagen se hizo posible para todas las categorías de datos. También se habilitaron las correlaciones OSINT – IMINT – SIGINT – MASINT, etc. En este punto, los desafíos planteados por OSINT consistían en la capacidad de convertir en inteligencia accionable los grandes volúmenes de datos, que en la mayoría

los casos no estaban organizados, procedían de múltiples fuentes, estaban disponibles en diferentes formas y se recopilaban a través de varias categorías de canales para convertirlos posteriormente en inteligencia validada (Hamilton: 2011). Los métodos e instrumentos específicos podrían ayudar en la creación, validación y mejora de una base de recopilación ajustada a las necesidades de inteligencia. Es un paso fundamental considerando el elevado número de fuentes, de diferente tipo (bases de datos -gubernamentales y privadas-, bases de datos estructuradas, no estructuradas, estudios, prospectos, publicaciones, etc.), provenientes de diversas áreas clave (economía, política, diplomacia, estado aparato administrativo, etc.) con temas anisotrópicos (procesos, productos, regulaciones, competidores, fusiones, sociedades, información sectorial, tendencias sociales, etc.)

(Marrón: 2019). La calibración de la base de recopilación es un proceso en el que las fuentes se revisan continuamente, teniendo en cuenta, sin embargo, que las fuentes deben cubrir todas las áreas clave requeridas para la base de inteligencia.

Resumiendo los cinco hitos, presentamos brevemente a continuación la evolución de OSINT en los últimos 200 años: • el advenimiento de los medios impresos conduce al establecimiento de sistemas de inteligencia que permiten la recopilación sistémica y sistemática de fuentes abiertas;

- las redes estructuradas de inteligencia comienzan a influir y controlar los medios impresos y los servicios de inteligencia necesitan categorizar la información recolectada de la prensa en base a criterios relacionados con la publicación, el autor y el contexto; • los servicios de inteligencia se convierten en instituciones gubernamentales y se produce la segregación entre nacionales y extranjeros, la información de fuente abierta se recopila ahora de fuentes nacionales y de territorios objetivo en el extranjero por diferentes estructuras; •

Se desarrollan las redes públicas de radio y televisión y, si hasta ese momento los servicios de inteligencia se enfocaban en indexar, almacenar y acceder fácilmente a la información escrita, ahora comienzan a preocuparse por convertir la voz en texto para procesar la información difundida a través de la radio. . La necesidad de capturar, indexar, almacenar y acceder a información de video también se hace evidente; • además de SIGINT, IMINT o MASINT, la eficiencia de OSINT pasa a depender en gran medida de la eficiencia de los equipos informáticos y de las tecnologías utilizadas; • el uso masivo de Internet provoca un crecimiento exponencial en el volumen de datos disponibles en Internet; • el paso de lo analógico a lo digital permite la segmentación de datos y series de datos, facilitando la recolección, procesamiento y análisis;

- las redes sociales y la aparición de dispositivos de acceso a datos móviles (www) proporcionan nuevas categorías de datos y metadatos que permiten la creación de microperfiles y perfiles de una entidad o un grupo en cualquier nivel. • utilizando las nuevas tecnologías, las estructuras OSINT transforman en inteligencia procesable grandes volúmenes de datos, que en la mayoría de los casos no están organizados, se derivan de múltiples fuentes, están disponibles en diferentes formas y se recopilan a través de varias categorías de canales; • dado que los volúmenes de datos disponibles son enormes, el propósito ya no es recopilar toda la información que podría ser de interés, y la base de recopilación debe adaptarse continuamente a las necesidades de inteligencia.

Teniendo en cuenta los hitos mencionados anteriormente, identificamos las siguientes tendencias: 1. el volumen de información de código abierto está creciendo continuamente a un ritmo exponencial; 2. el número de fuentes aumenta continuamente y sus tipos son cada vez más diversos;

3. el progreso tecnológico y las nuevas tecnologías permiten la recogida y el tratamiento automatizado de grandes volúmenes de datos y su integración a partir de diversos tipos de fuentes; 4. Los procesos para establecer los límites del sistema fuente y calibrar la base de recolección en relación con las necesidades de inteligencia son dinámicos.

2.2. Estados, estrategias y centros

OSINT A la luz de las

tendencias mencionadas anteriormente, podemos inferir que OSINT ocupa un lugar destacado en la agenda de la mayoría de los servicios de inteligencia. Esto se refleja además en la estrategia de la comunidad de inteligencia y es parte de las estrategias de seguridad nacional.

Así, la Estrategia de Seguridad Nacional de los Estados Unidos de América - 2017, en una primera mención a OSINT, enfatiza que los rivales estadounidenses (con referencia directa a China y Rusia) utilizan información y técnicas de marketing para atacar a personas e instituciones.

Se enfatiza que los riesgos para la seguridad nacional de EE. UU. crecieron a medida que los atacantes integran de múltiples fuentes y utilizan métodos de análisis basados en herramientas de inteligencia artificial. Las contramedidas identificadas por el gobierno estadounidense se refieren a la recopilación y mejora de información de todas las fuentes disponibles y la creación de plataformas tecnológicas de vanguardia. Además, dentro de una de las acciones estratégicas prioritarias en términos de inteligencia, EE. UU. "utilizará, en concierto con aliados y socios, el entorno de código abierto rico en información para negar la capacidad de los actores estatales y no estatales de atacar a nuestros ciudadanos, realizar actividades de inteligencia ofensivas y degradar las instituciones democráticas de Estados Unidos"

(White House: 2017, 32), y esta línea estratégica se basa en las nuevas tecnologías. La idea se detalla en

el capítulo "Information Statecraft" que menciona claramente las herramientas utilizadas: grandes bases de datos que integran información derivada de fuentes personales y comerciales con información de código abierto y capacidades de análisis y procesamiento de datos basadas en Inteligencia Artificial (White House: 2017).

La Revisión Estratégica de Defensa y Seguridad Nacional de Francia - 2017 se centra en la Parte C en el fortalecimiento de su Base Industrial y Tecnológica de Defensa (DITB). Esta infraestructura tecnológica sostiene la economía nacional y ayuda a Francia a expandir su influencia en el mundo. La autonomía estratégica y la superioridad tecnológica de Francia solo son posibles si sostiene y mantiene la excelencia de las entidades dentro del DITB. Además, uno de los enfoques apoyados por el Ministerio de Defensa exige que la administración, en colaboración con la comunidad investigadora, haga un uso sistemático de las fuentes abiertas (Presidente de la República Francesa: 2017).

En la Estrategia de Seguridad Nacional de Rusia - 2009, la innovación y las inversiones en nuevas tecnologías se denominan prioridades estratégicas nacionales. Además, se detallan líneas estratégicas claras, como el desarrollo de las ciencias aplicadas, de las nuevas tecnologías o la cooperación interdisciplinaria (Presidente de la Federación de Rusia: 2015). Incluso si no hay referencias directas al código abierto

colección, las referencias contextuales son frecuentes (Presidente de la Federación Rusa: 2015) (CRS: 2020). También se encuentran referencias similares en "Doctrina de Seguridad de la Información de la Federación Rusa" – 2016, que hace mención a la inteligencia técnica (Ministerio de Relaciones Exteriores de la Federación Rusa: 2016).

En la "Estrategia de Seguridad Nacional - 2013", Japón subraya su necesidad de fortalecer las capacidades de la comunidad de inteligencia. El Capítulo 7, "Mejora de las capacidades de inteligencia", establece claramente que el desarrollo de OSINT es crucial, porque además de HUMINT, SIGINT, IMINT y otros tipos de fuentes, garantizará un sistema consistente de fuentes (Ministerio de Relaciones Exteriores de Japón: 2013). Como muestra de consistencia estratégica, en "2020 Defense of Japan", OSINT se menciona como uno de los seis pilares que contribuyen al desarrollo de las capacidades de los servicios de inteligencia (Ministerio de Defensa de Japón: 2020).

Enfoques similares se encuentran en las estrategias de seguridad de otros estados, como Canadá, Inglaterra, Alemania, Holanda o China, este último también muestra un enfoque especial en OSINT (Bereziuk: 2016).

Por lo tanto, podemos concluir que la recopilación de código abierto se encuentra entre las principales preocupaciones de los servicios de inteligencia en todo el mundo.

Como la importancia de la recopilación de código abierto ha aumentado con el tiempo en términos de volumen, reflejándose en consecuencia en la composición de la base de recopilación, los servicios de inteligencia se vieron obligados a utilizar en mayor medida la tecnología en el proceso, con el fin de recopilar y automatizar procesar la avalancha de grandes volúmenes de datos (Tabatabaei, Wells: 2016). Como tal, se han formado y fortalecido estructuras dedicadas, como el "Centro de código abierto" dentro de la CIA (EE. UU.), el "Centro de fuentes abiertas" dentro del DNI (Francia) o el "Centro de Internet" dentro del NPA (Japón). Rusia actúa a través de la Dirección General 12 dentro de la GRU, "guerra de información", FAPSI "La Agencia Federal para las Comunicaciones e Información Gubernamentales" y la IRA "Agencia de Investigación de Internet". China estableció el "Tercer Departamento" o "Departamento Técnico de la Comisión Militar Central".

3. TECNOLOGÍAS

Mientras antes del final de Cold Si bien las tecnologías utilizadas se originaron principalmente en los centros de investigación dentro de las estructuras de defensa y seguridad, en los últimos 20 años los entornos académico y empresarial también han contribuido significativamente al cambio tecnológico, ya que se implementaron cada vez más proyectos y programas conjuntos (Williams, Blum :

2018). Un ejemplo de ello es Hacking for Defense, que actualmente involucra a DOD, IC, 31 universidades y 66 empresas. Estos programas dieron lugar a una nueva tendencia, a saber: si hasta la década de 1990 la mayoría de las tecnologías de punta se desplazaban del entorno de defensa al entorno empresarial, a partir del año 2000 esta tendencia se revirtió. Además, comenzaron a notarse empresas privadas que actuaban en el campo de la inteligencia competitiva (Katz: 2020). Como tal, ahora podemos hacer una evaluación relativamente exhaustiva de las tecnologías utilizadas en OSINT con referencia a la información no clasificada y la información que proviene predominantemente de fuentes abiertas. Así, considerando las fases del ciclo de inteligencia, enumeramos a continuación, en la tabla I, las nuevas tecnologías que podrían asegurar una explotación más eficiente de la inteligencia en los centros OSINT (Williams, Blum: 2018).

Tabla 1. Ciclo OSINT y Tecnologías

OSINT Cycle	Operational Steps	Intell Category	Technologies							
			CSS	BD	AI			RPA	BC	Δ
					SA	ML	NLP			
Collection	Scanning Sources	OSD	CSS		SA		NLP			Δ
	Monitoring Sources		CSS		SA	ML	NLP			Δ
	Collection		CSS							Δ
	OSD Storage			BD	SA			RPA		Δ
Processing	Normalize	OSIF OSINT			SA	ML	NLP			Δ *1
	Aggregate				SA	ML		RPA		Δ
	Processed Data Indexation				SA		NLP			Δ
	Correlations				SA	ML	NLP			Δ
	Clearance Permissions				SA	ML		RPA		Δ
	OSIF Storage			BD	SA			RPA		Δ
Analysis	Source Validation	OSINT OSINT-V			SA					Δ *2
	Intell Validation				SA	ML	NLP			Δ
	Integration			BD	SA	ML	NLP	RPA		Δ
	Analyze				SA	ML	NLP			Δ
Dissemination	Production	OSINT-V			SA	ML	NLP	RPA		Δ
	Intell Indexation				SA	ML	NLP	RPA		Δ
	Distribution				SA				BC	*3
	OSINT Storage			BD	SA			RPA		Δ
	Feed-back						NLP		BC	Δ

OSD: Open Source Data
OSIF: Open Source Information
OSINT: Open Source Intelligence
OSINT-V: Validated OSINT
Δ- other applications
*1- converters
*2- social network analysis; geointell
*3- electronic post applications

CSS: Crawlers - Spiders - Scrapers
BD: Big Data
AI: Artificial Intelligence
ML: Machine Learning
NLP: Natural Language Processing
SA: Statistic Algorithms and Analytics
RPA: Robot Process Automation
BC: Blockchain Technologies

Fuente: autor, 2021

Analizando más el marco contextual anterior, podemos notar que en un futuro próximo, el impacto más significativo en los sistemas de inteligencia económica será el de las nuevas tecnologías (Johnson: 2010) (ODNI, DNS: 2018). Como indica la “Tabla I”, existen cuatro grandes tipos de tecnologías que tienen y tendrán un aporte cada vez más importante: Big Data, Inteligencia Artificial, Robot Process Automation y Blockchain.

3.1. Big Data

Big Data es el campo tecnológico que se ocupa de las formas sistemáticas de almacenamiento, extracción y análisis de datos e información. Big Data apareció como una solución al problema que planteaban los conjuntos de datos que eran demasiado grandes o complejos para ser manejados por las aplicaciones tradicionales. Big Data está asociado con tres conceptos clave: volumen, variedad y velocidad (Miller: 2015).

Big Data facilita la captura, el almacenamiento, la actualización, la consulta, la búsqueda, el intercambio, la transferencia, el análisis y la visualización de datos, al tiempo que garantiza la confidencialidad de la información y las fuentes. Big Data permite identificar correlaciones entre conjuntos de datos específicos, determinar patrones específicos y promueve el uso de análisis predictivo y otros métodos de análisis que permiten

extracción de inteligencia procesable (Katz: 2020).

Las altas capacidades de almacenamiento, indexación y análisis de la información permiten acceder fácilmente a grandes cantidades de datos e información (Johnson: 2010) (ODNI, DNS: 2018). Las bases de datos se pueden conectar a sistemas automáticos para la recopilación de información de código abierto, junto con sistemas para la indexación automática de datos e información recopilados, lo que permite la estructuración de datos e información, incluida también la implementación de políticas relacionadas con los permisos (los derechos de acceso) (Miller: 2015).

Además, las tecnologías 5G aumentarán significativamente las capacidades técnicas y tácticas en el campo de la recopilación de datos, el monitoreo, las telecomunicaciones (transferencias de datos extensivas en tiempo real desde el área táctica: automatización basada en la transmisión a través de redes celulares, Internet de las cosas o computación perimetral) . Al mismo tiempo, surgirán vulnerabilidades específicas de estas capacidades que requerirán importantes esfuerzos de contraespionaje en el campo de la ciberseguridad (The Economist – Intelligence Unit: 2020).

3.2. Inteligencia artificial

Inteligencia artificial demostrada es

inteligencia por

dispositivos tecnológicos que recogen señales y perciben el entorno en el que operan, iniciando y gestionando acciones que maximizan las posibilidades de lograr con éxito sus objetivos, replicando las funciones cognitivas asociadas a la mente humana, como el aprendizaje, el análisis y la resolución de problemas (Miller: 2015) .

La inteligencia artificial incluye tres amplios tipos de algoritmos:

- Algoritmos Estadísticos y Analítica – generación de estructuras estadísticas y cálculo de probabilidad, análisis predictivo,
- Aprendizaje automático: redes neuronales y razonamiento, aprendizaje profundo, y - Procesamiento del lenguaje natural: aprendizaje y representación, acceso al conocimiento (Williams, Blum: 2018) (Nacci: 2017).

En la mayoría de las soluciones de software, estas tecnologías se complementan y potencian entre sí, procesando y analizando grandes bases de datos (Big Data Analytics), siendo su resultado utilizado e interpretado en estructuras clásicas de software y programación (Williams, Blum: 2018) (Nacci: 2017).

Las tecnologías de Inteligencia Artificial pueden permitir la automatización de plataformas de recolección, optimizando también la selección de fuentes en función de la recolección requisitos Los algoritmos pueden

generar modelos que sean capaces de anticipar ciertas tareas de recolección de acuerdo con la información actualmente procesada, pueden desencadenar la selección de las mejores fuentes o determinar frecuencias de recolección óptimas.

Además, los algoritmos de aprendizaje profundo facilitan la toma de decisiones automática permitiendo una adaptación dinámica de las tareas de recolección.

Así, la colección se vuelve adaptable, lo que también implica una contribución humana reducida.

(Katz: 2020) (Nacci: 2017).

Además, las aplicaciones de inteligencia artificial permitirán el uso de soluciones automatizadas eficientes durante las fases de procesamiento de la información y posteriormente en la fase de análisis. El análisis de escenarios, el análisis predictivo, el establecimiento de patrones recurrentes y futuros son posibles utilizando tecnologías de inteligencia artificial (The Economist – Intelligence Unit: 2019). Además, el desarrollo de capacidades de hardware (por ejemplo, computadoras cuánticas) mejorará las capacidades del software basado en inteligencia artificial, lo que tendrá un impacto futuro significativo. Según un estudio emitido por Emerging Technology and National Security Team, el 32% de las tecnologías críticas utilizadas por los sistemas de inteligencia se basarán en el futuro en Inteligencia Artificial y el 16% en computadoras cuánticas (Miller: 2015) (ODNI, DNS: 2018) .

3.3. Automatización de procesos robóticos

Robot Process Automation es la tecnología que permite automatizar procesos informáticos y digitales mediante la configuración de robots software que emulan e integran las acciones de un operador humano, interactuando dentro de los sistemas digitales para llevar a cabo diversos procesos. Los robots RPA pueden utilizar la interfaz de usuario para recopilar datos y administrar aplicaciones, al igual que un usuario humano. Robots RPA entre captura información, desencadena respuestas y se comunica con otros sistemas, especialmente para realizar una amplia variedad de tareas repetitivas (CRS: 2020).

Automatización de procesos robóticos Las tecnologías son útiles para los procesos de recolección, procesamiento, diseminación y gestión de inteligencia porque permiten la automatización de tareas recurrentes mediante el procesamiento e indexación de grandes volúmenes de datos, asegurando también las correlaciones entre bases de datos, destinatarios, canales de comunicación y otras entidades (Miller: 2015).

3.4. Tecnologías de cadena de bloques

Las tecnologías de cadena de bloques se basan en una cadena de bloques de datos vinculados criptográficamente, cada bloque contiene una clave criptográfica ("hash") del bloque anterior, una marca de tiempo y datos de transacción. Por lo tanto, la tecnología Block Chain no

permitir cualquier alteración de los datos. Una vez grabados, los datos de un bloque no pueden modificarse retroactivamente sin la modificación de todos los bloques posteriores. La tecnología utiliza un libro mayor distribuido y no un libro mayor único.

Block Chain Technologies permitirá una implementación eficiente de las políticas relativas a los permisos y derechos de acceso a información clasificada, incluido el acceso remoto a sistemas y datos en condiciones de alta seguridad (The Economist – Intelligence Unit: 2019).

3.5. Otras tecnologías Web

Scraping se utiliza para extraer datos de sitios web. Usando varios protocolos, el software accede directamente a las páginas web a través de procesos automatizados, un bot o un Web Crawler, para recopilar datos específicos (de una base de datos) que se almacenan y posteriormente se utilizan (Pinto, et al: 2018). Web Scraping implica descargar el contenido de una página y luego extraer los datos para su posterior procesamiento. Así, el contenido de una página se puede almacenar, estructurar y analizar posteriormente. El Web crawler, el Spider o el Spider-bot es un robot que navega sistemáticamente por la web. Los rastreadores copian las páginas para su procesamiento inmediato o posterior.

Los rastreadores también pueden mapear la web identificando la información relevante para secuencias de búsqueda específicas.

Todas estas tecnologías son esenciales para la recopilación porque permiten la recopilación y el almacenamiento de datos web (Katz: 2020).

El convertidor de analógico a digital es un sistema que convierte una señal analógica (sonido, luz, etc.) en una señal digital. Un convertidor también puede proporcionar el valor digital de una medida, por ejemplo, el valor del voltaje en un circuito. Estas tecnologías son críticas para OSINT porque permiten la conversión de información analógica, como grabaciones de audio, grabaciones de video o imágenes, en información digital. La información digital tiene la ventaja de que puede ser almacenada, indexada (a la información digital se le pueden asignar atributos), agregada y posteriormente utilizada en acciones de inteligencia. También se pueden incluir en la clase de convertidores algunas tecnologías específicas de la comunidad de inteligencia que permiten cierta conversión digital requerida para una adecuada indexación de la información (Williams, Blum: 2018). Por ejemplo, la conversión automática de una grabación de audio en texto o la conversión de una grabación de video digital en audio y luego en texto y la correlación del texto.

con los marcos. De manera similar, la información impresa se puede convertir en información digital. Además, utilizando tecnologías de Inteligencia Artificial, los sujetos pueden ser automáticamente

identificados en fotografías, así como las acciones realizadas, territorios y otra información que puede ser indexada, permitiendo posteriormente una adecuada explotación (Williams, Blum: 2018).

El software de análisis de redes sociales facilita la red social. análisis en términos de cantidad o calidad, describiendo las características de la red y mediante representación numérica o visual. Las redes pueden consistir en cualquier cosa, desde familias, equipos, vectores de enfermedades y membresía en sitios web de redes sociales y redes web (Pinto, et al: 2018). Las redes están formadas por conexiones directas entre nodos o vínculos indirectos basados en atributos compartidos, asistencia compartida a eventos o membresías comunes.

Los paquetes de software de alto rendimiento utilizan bases de datos relacionales para importar y almacenar algunas funciones de red y utilizan algoritmos avanzados de inteligencia artificial para análisis estadísticos, análisis de sentimientos, tráfico, lenguaje y predicción (Katz: 2020).

el electronico correo

Las aplicaciones son críticas, porque son vulnerables principalmente en lo que respecta a la seguridad de las transferencias de datos. Los requisitos de seguridad, como la identificación de la persona y el dispositivo relacionado, el cifrado y la seguridad de los datos, la seguridad de la red y los paquetes de datos, son cuestiones críticas que deben garantizar estas aplicaciones. También,

las aplicaciones pueden configurarse para estar de acuerdo con las matrices de distribución, para agregar beneficiarios o, para ciertos temas, para sugerir al usuario que también debe informar a otras entidades que podrían enfrentar el riesgo (Brown: 2019).

4. OSINT - TENDENCIAS FUTURAS Y TECNOLOGÍAS

Nos referiremos a continuación a OSINT mediante el análisis de las fases del ciclo de inteligencia: recopilación, procesamiento, análisis y difusión. tenga en cuenta que nuestro enfoque será de alguna manera teórico, organizado por fases individuales. De hecho, las fases del ciclo de inteligencia a menudo se superponen o, en algunos casos, no son todas parte del proceso.

En cuanto a todas las fases enumeradas a continuación, es relevante mencionar que para todo el ciclo de inteligencia, los asuntos relacionados con la seguridad de las bases de datos, dispositivos y redes, envíos de datos y paquetes son puntos centrales en la agenda de los servicios de inteligencia (Katz: 2020) (CRS: 2020) (Tabatabaei, Wells: 2016). En la mayoría de los casos se están desarrollando módulos o aplicaciones dedicadas, pero también se han desarrollado soluciones eficientes en el sector comercial, como las proporcionadas por grandes empresas como Microsoft, IBM, Cisco, Fortinet, etc. u otros proveedores de nicho, como

SolarWinds, Intruder, Bitdefender, Malwarebytes, etc.

4.1. Recopilación

En cuanto a la recopilación, primero nos referimos a la configuración del sistema fuente para todos los temas de inteligencia sistemáticos (recurrentes). Como tal, con base en los intereses nacionales, la mayoría de los servicios de inteligencia también monitorean constantemente otros territorios objetivo. En muchos casos, el monitoreo implica el establecimiento de un sistema de fuentes, una correlación inicial de la información relevante disponible en esas fuentes, seguida de la recopilación sistemática de nueva información.

Dicha recopilación puede planificarse en varios intervalos o puede tener lugar al mismo tiempo que la publicación.

Una vez que se establece una frecuencia óptima, las fuentes se escanean y monitorean sistemática y sistemáticamente: se recopila nueva inteligencia, se identifican las diferencias que surgen en las bases de datos, se evalúan las variaciones de volumen o cualitativas en el flujo de noticias o se registran y marcan las desviaciones de ciertos indicadores. (Katz: 2020). Tan pronto como se establece y valida la base de recopilación, las fuentes se mantienen relativamente estables, lo que significa que, una vez configuradas, las tecnologías utilizadas para la recopilación funcionan sin requerir otros ajustes significativos, a menos que se ajuste la estructura de la fuente (ODNI, DNS: 2018) .

Sin embargo, la aparición de temas asimétricos puede requerir una recalibración del sistema fuente.

Si bien mediante las actividades de vigilancia y monitoreo los servicios de inteligencia pretenden estar alertas y anticiparse oportunamente a todas las posibles amenazas, pueden presentarse situaciones disruptivas atípicas que no han sido cubiertas por dichos mecanismos. Estas situaciones atípicas requieren que se integren nuevas fuentes en la base de recolección. La integración de nuevas fuentes requiere en la mayoría de los casos que se encuentren soluciones tecnológicas fiables lo antes posible. Como tal, se recomienda para la base de recolección mencionada anteriormente poder asegurar el marco informativo capaz de proporcionar alertas tempranas y responder a todo tipo y categoría de amenazas posibles y probables (CRS: 2020).

Por lo tanto, la recolección recurrente de inteligencia es un proceso preponderantemente tecnológico sistémico cuyo propósito es asegurar una base de información exhaustiva.

La recopilación de información por solicitud también es un enfoque tecnológico pero no sistémico y no sistemático, destinado a garantizar una base de información para un tema específico.

El escenario ideal para cualquier centro OSINT es operar apoyándose únicamente en la recopilación de inteligencia sistémica y sistemática, pero debido a la volatilidad

y asimetrías del entorno actual, los profesionales a menudo se ven obligados a ajustar dinámicamente el sistema de fuentes y necesitan encontrar nuevas soluciones tecnológicas para manejar solicitudes específicas de información (Katz: 2020).

Si bien en la actualidad las fuentes que se explotan de manera preponderante son aquellas que permiten una recolección sistemática, los avances tecnológicos de las fuentes abiertas e identificar más fácilmente las soluciones tecnológicas que permitan la extracción.

de información de estas fuentes. Se confirma así la tendencia según la cual los procesos para establecer los límites del sistema fuente y calibrar la base de recolección en función de las necesidades de información son dinámicos (Brown: 2019). Esto será posible porque, con la excepción de los medios impresos, habrá nuevas tecnologías para permitir una identificación y un seguimiento eficientes de las fuentes de la web, los medios, las redes sociales y la web oscura.

(Ortega: 2019) (Pastor-Galindo et al. 2016). Por un lado, existen nuevas soluciones que permiten la recolección sistémica de ciertas categorías de fuentes y, por otro lado, las plataformas existentes se desarrollan para incluir y procesar nuevas categorías de fuentes (Brown: 2019).

Para identificar las fuentes abiertas de la web, las redes sociales y la oscuridad

web, los centros OSINT actualmente utilizan soluciones similares a motores de búsqueda web que son de alguna manera similares a Qwiki, Wolfram Alpha, Wowd o Recorded Future.

Las tendencias futuras indican el uso de soluciones de búsqueda elástica, mejoradas por tecnologías de automatización de procesos robóticos, soluciones que permitirían un escaneo eficiente de las redes sociales (Kanakaris et al., 2018). Otra herramienta de ayuda es la tecnología de inteligencia artificial específica, que mediante algoritmos estadísticos especiales, naturales

el procesamiento del lenguaje y el aprendizaje automático, permiten una identificación adecuada de las fuentes. Además, las soluciones de software se ejecutarán en infraestructuras de hardware continuamente actualizadas. El aumento de la velocidad de operación y potencia de cómputo promoverá el desarrollo de algoritmos cada vez más complejos y refinados (CRS: 2020).

El robot central más conocido Las soluciones de automatización de procesos son: UiPath, blueprism, Automation Anywhere, etc.

Es difícil dar ejemplos de soluciones de inteligencia artificial ya que su campo de aplicación es extremadamente amplio. Grandes corporaciones, como Microsoft, IBM, Google, Adobe, OpenAI, etc., junto con empresas de nicho, como Starmind, Vesttorly, Braina o Footprints, se encuentran entre los proveedores más conocidos.

Para la extracción de datos, los centros de la OSINT actualmente utilizan soluciones "spider", "scrap", "crawl", "geolocalización" u otras similares, potenciadas por inteligencia artificial y capacidades de automatización de procesos robóticos (Williams, Blum: 2018) (Kanakariset al., 2018) (Pastor-Galindo et al., 2016). Las soluciones utilizadas por los centros OSINT son similares a

soluciones como: Scrapy, HTTrack, OutWit Hub, Visual Scraper, Google Dorks, Spyse, Creepy, etc.

Las tendencias futuras indican el uso de este tipo de soluciones (Crawlers – Spiders – Scrapers) para la extracción de datos, pero dentro de ellas, el peso de la inteligencia artificial y la automatización de procesos robotizados será significativamente mayor.

4.2. Procesamiento e indexación de inteligencia Tanto la

información recopilada sistemática como no sistemáticamente (para un tema específico) debe normalizarse, agregarse, indexarse (asignación de atributos) y almacenarse, de modo que pueda identificarse fácilmente cuando sea necesario (Katz: 2020).

Normalización medio
convertir y llevar toda la información recopilada al mismo formato (por ejemplo, toda la información debe estar en formato de texto digital, en el mismo idioma y todas las imágenes en un formato digital específico) (Moliner: 2015). La eficiencia de

El software de conversión es crítico aquí. Luego se agregan datos idénticos y similares que se recopilan de diferentes fuentes (Williams, Blum: 2018).

Posteriormente, en la fase de indexación, junto con la asignación de metadatos y atributos (temas, lugares, eventos, materias, acciones, verticales temáticos), dependiendo de las tecnologías utilizadas, los riesgos potenciales relacionados y las contramedidas recomendadas pueden

también se pueden correlacionar, o se pueden enumerar otros casos similares, etc. (Katz: 2020) (Pastor-Galindo et al., 2016). Cuantos más atributos y metadatos se asignada, mayor será la probabilidad de aprovechar la información en una fase u operación posterior. Para estas categorías de aplicaciones, es relativamente difícil identificar ejemplos de software comercial (Williams, Blum: 2018). Sin embargo, ciertas funcionalidades se encuentran en aplicaciones como CRMs o MATLAB, SPSS, Wolfram Mathematica, etc. En cuanto a las bases de datos, destacan las soluciones que aportan las grandes corporaciones como IBM, Oracle, Microsoft, etc. o para la analítica parte, IBM SPSS, Elasticsearch, SAP Hana, MicroStrategy, SAS Visual Analytics, Forestpin Analytics, etc.

Además, los derechos de acceso pueden configurarse tecnológicamente en gran medida, de acuerdo con las políticas de clasificación de la información. Para

Por ejemplo, los derechos se pueden asignar correlacionando los niveles de acceso a la información con los de un sujeto y con los niveles de acceso que se han asignado a las fuentes y, posteriormente, ajustando los permisos en función de los metadatos relacionados con el información o el clúster donde la información fue distribuida (Katz: 2020). Aquí también podemos encontrar soluciones desarrolladas por Oracle, Microsoft, Cisco, etc.

Además de los aspectos relacionados con la indexación y configuración de los derechos de acceso, el procesamiento y la indexación de las bases de datos web y dark web disponibles son otros desafíos que se plantean en este punto. Las dificultades surgen ya que cada fuente puede utilizar estructuras e indexaciones arbitrarias para sus bases de datos y la normalización, agregación e indexación de las mismas requiere un gran esfuerzo inicial (Ortega: 2019). Por ejemplo, un parámetro simple, como la distancia entre dos puntos, puede expresarse en kilómetros. O una fuente puede confiar en la distancia entre los dos puntos, mientras que otra fuente puede relacionarse con el tiempo promedio necesario para cruzar esa distancia. (Katz: 2020). Hay casos en los que el mantenimiento también puede ser difícil porque las fuentes pueden cambiar voluntariamente la estructura de las bases. Además, sería ideal para todas las bases de datos recopiladas de varios fuentes y relacionadas con un tema determinado

para ser agregado en una sola base. Solo después de la normalización y la agregación se pueden determinar los indicadores (niveles) de alerta y alerta temprana. La agregación y normalización preceden a la generación automatizada y semiautomatizada de productos informativos recurrentes presentados a determinados beneficiarios. Un ejemplo de productos

informativos que se emiten automáticamente en base a series de datos son aquellos que reflejan las fluctuaciones de las monedas en determinados

territorios (Katz: 2020).

Las tendencias actuales indican que el procesamiento se realizará preponderantemente mediante tecnología. Los avances en las aplicaciones de conversión, las soluciones ajustadas de normalización y agregación asistidas por la automatización de procesos robóticos permitirán que los algoritmos y tecnologías específicos de inteligencia artificial (aprendizaje automático y procesamiento de lenguaje natural) realicen con éxito estas categorías de tareas.

4.3. Análisis

Un primer desafío en el análisis OSINT es la validación de la información. Además de lo real análisis de la información, se debe prestar atención a las fuentes y autores para evitar toda

posibles intentos de manipulación o desinformación (Nacci: 2020). Hay publicaciones o autores que consiguen

voluntariamente involucrados en la manipulación o la desinformación y los autores que sin querer han sido atrapados en los arreglos de manipulación, sin saberlo, asumiendo ciertas ideas distorsionadas en sus artículos.

(Katz: 2020). Además, la información incompleta y la información fragmentada

sin embargo, puede compensarse en una fase posterior, analizando todas las fuentes (integrando también otros tipos de fuentes: HUMINT, IMINT, SIGINT, MASINT, etc. en el enfoque analítico) (Katz: 2020)

(Marrón: 2019). Para el análisis de la información, las soluciones de Inteligencia Artificial basadas en el procesamiento del lenguaje natural y el aprendizaje automático se vuelven cada vez más eficientes, lo que permite detectar cualquier intento de manipulación, propaganda o fragmentación de la información (Brown: 2019) (Nacci: 2020). En este sentido, existen soluciones comerciales como IBM i2, Palantir, Siren, Cogito, 6th Sense, etc.

El segundo desafío en el análisis OSINT consiste en determinar patrones de difusión de inteligencia, dado que muchas veces la información se toma sin citar la fuente. En la fase analítica, es fundamental determinar la fuente de información y el momento de la publicación, porque también se pueden analizar posibles intereses relacionados con la fuente o el autor

(Katz: 2020) (Marrón: 2019). Esta operación es aún más difícil en el caso de las redes sociales y, con toda probabilidad, solo puede llevarse a cabo utilizando herramientas tecnológicas de alto rendimiento (Williams, Blum: 2018) - (Kanakaris, et al., 2018). El impacto de la inteligencia artificial y la automatización de procesos robóticos también se siente cada vez más en este caso. En la actualidad, los algoritmos de aprendizaje automático y los mecanismos de automatización de procesos robóticos permiten en ciertos casos identificar automáticamente la fuente (Miller: 2015) (Brown: 2019). Paralelamente también se han desarrollado aplicaciones de análisis de redes sociales, como NetMiner, NetworkX, Centrifuge, SocNetV, etc.

El impacto de la Inteligencia Artificial también se notará en el caso del análisis. Las correlaciones quién, qué, por qué, dónde, cómo, con quién, etc. serán cada vez más precisas, proporcionando al analista pistas significativas (Brown: 2019). Las analogías relacionadas con determinados patrones de actuación, perfilado, análisis del habla, gestión de evidencias, etc. serán procesadas en mayor medida de forma automática, proporcionando al analista supuestos de trabajo fiables (Katz: 2020).

En este sentido, jugarán un papel importante los ordenadores cuánticos, que acelerarán el desarrollo de la inteligencia artificial y revolucionarán determinados patrones de programación (Miller: 2015).

4.4. Difusión de inteligencia

En el caso de OSINT, la creación de productos informativos da lugar a varias situaciones. Así, ciertos productos informativos pueden ser creados automáticamente (usando tecnología), con una frecuencia preestablecida específica. Ejemplos de tales productos informativos incluyen la revista de prensa o un informe resumido o gráfico sobre las transacciones bursátiles relativas a las empresas en las que el Estado tiene participación accionaria.

Asimismo, en ciertos casos los informes se generan automáticamente y el analista realiza una revisión final del documento antes de ser presentado al beneficiario (Nacci: 2020). Un tercer caso es aquel en el que el informativo

los productos son elaborados en su totalidad por analistas de inteligencia, de acuerdo con las prácticas comunes, en la mayoría de los casos según un enfoque que implica el análisis de todas las fuentes (Katz: 2020).

Con respecto a la indexación y clasificación de inteligencia, todos los documentos se indexan y almacenan de acuerdo con los principios establecidos en la fase de procesamiento, porque es muy importante poder acceder a ellos en cualquier momento.

necesario.

En términos de difusión de inteligencia, los productos informativos se difunden al beneficiario designado o

beneficiarios. Sin embargo, las tecnologías actuales facilitan la creación de matrices de distribución, lo que posibilita también difundir esta información a otros beneficiarios (Katz: 2020). Las matrices de distribución permiten elaborar las mejores listas de beneficiarios, teniendo en cuenta los permisos de acceso a la información y los intereses

de beneficiarios. En función de los metadatos adjuntos al informativo productos, los productos informativos se correlacionan automáticamente con otros posibles beneficiarios que pueden aprovechar dicha información, lo que mejora significativamente la eficiencia de este enfoque informativo (Williams, Blum: 2018).

Posteriormente, los beneficiarios podrán solicitar aclaraciones o información adicional. También podrán presentar sugerencias en cuanto a la forma de presentación (texto, tabla, gráficos, imágenes, etc.), calibrando así la comunicación al mejor nivel (Williams, Blum: 2018).

Existen numerosas aplicaciones diseñadas para los servicios de correo electrónico, incluyendo aquí jugadores como Microsoft, IBM, Apple y otros jugadores de nicho, como eM, Inky o Hiri. En cuanto a los próximos pasos, aquí se confirman una vez más las tendencias de un impacto creciente de la Inteligencia Artificial y la Automatización de Procesos Robóticos. Además, bloquea

la tecnología de cadena juega un papel importante en lo que respecta a la seguridad de las transacciones (Brown: 2019). Aquí también hay proveedores conocidos, como IBM, Microsoft, Oracle, etc., pero también empresas más pequeñas, como Ripple, NEO, Stellar, etc.

5. LOS PRÓXIMOS PASOS DE OSINT

Las cinco tendencias ya identificadas se confirman aún más con los resultados de cada paso OSINT, de la siguiente manera:

1. El volumen de inteligencia de fuente abierta crece continuamente, a un ritmo exponencial, una tendencia confirmada por el desarrollo de la web, la dark web y las redes sociales.

2. El número de fuentes aumenta continuamente, y sus tipos son cada vez más diversos, tendencia que se sustenta tanto en la diversificación de tecnologías utilizadas en web y bases de datos, como en la aparición de plataformas de contenidos.

3. Los avances tecnológicos y las nuevas tecnologías permiten la recogida y recogida automatizada procesamiento de grandes volúmenes de datos y su integración desde diversos tipos de fuentes, tendencia sostenida por las ventajas tecnológicas relacionadas con la Inteligencia Artificial y la Automatización de Procesos Robóticos.

4. Los procesos para establecer los límites del sistema fuente y calibrar

la base de recolección en relación a las necesidades de información son dinámicas y pueden ser asistidas tecnológicamente por algoritmos de Inteligencia Artificial.

5. La recolección y procesamiento

OSINT avanza hacia un enfoque preponderantemente tecnológico, como lo confirma cada fase del ciclo de inteligencia. Como tal, la tendencia 5 puede reformularse de la siguiente manera: OSINT avanza hacia un enfoque preponderantemente tecnológico.

5.1. La fusión entre OSINT y las

nuevas Tecnologías

OSINT avanza hacia un enfoque tecnológico.

Cada fase utiliza sus propias tecnologías, Crawlers – Spiders – Scrapers en caso de Recolección, convertidores en caso de Procesamiento o Blockchain en caso de difusión. Es relevante mencionar que la Inteligencia Artificial y la Automatización de Procesos Robóticos contribuyen en todas las fases. Además, los avances en el desarrollo de las computadoras cuánticas, el aumento de la potencia de cómputo, el desarrollo continuo de varios tipos de redes influirán significativamente en la recopilación, al mismo tiempo que impulsarán y brindarán soluciones, lo que también traerá algunos beneficios directos, como una mejor velocidad de procesamiento, un mayor volumen de datos procesados y mejores formas de procesamiento y

analizar información (Katz: 2020).

Asimismo, el cifrado y descifrado cuántico podría cambiar radicalmente este campo. Las computadoras cuánticas podrían acelerar el desarrollo y aumentar las capacidades de la Inteligencia Artificial, transformando las capacidades de procesamiento (Nacci: 2020). El desarrollo de la tecnología 5G y los dispositivos IoT desencadenarán cambios en dónde y cómo se recolecta la información, la “conectividad omnipresente”, creando nuevas oportunidades para el campo de la recolección (Katz: 2020) (Nacci: 2020).

En conclusión, los avances tecnológicos respaldan el desarrollo de OSINT. En la práctica, el desarrollo tecnológico acelerado conduce inevitablemente a un desarrollo acelerado de OSINT.

5.2. El impacto OSINT en los sistemas nacionales de inteligencia

El crecimiento sostenido de OSINT se reflejará en consecuencia en los pesos de base de recolección y posteriormente, en los de base de inteligencia. Las ventajas proporcionadas por la automatización de las fases de recopilación, procesamiento y difusión y el importante soporte técnico brindado a los analistas realzan la importancia de la recopilación de código abierto. Además, el hecho de que la información se recopile de forma remota, sin exponer al recolector humano, es un importante

ventaja (Ivanjko, Dokman: 2020).

Por lo tanto, debido al aumento en el volumen de inteligencia de fuente abierta, debido al hecho de que los procesos OSINT están automatizados, lo que reduce significativamente los recursos necesarios y, como la adquisición de fuente abierta no expone a los recolectores humanos, OSINT seguirá jugando una parte central dentro de los ecosistemas de servicios de inteligencia.

5.3. Los Próximos

Pasos Podemos concluir que en el futuro cercano el ciclo ONSINT será un enfoque preponderantemente tecnológico.

En cuanto a la recopilación, en los próximos diez años los avances tecnológicos permitirán mapear la mayoría de las fuentes abiertas e identificar fácilmente, muchas veces automáticamente, las soluciones tecnológicas para extraer información de estas fuentes. Se automatizarán los procesos de establecimiento de límites del sistema fuente y calibración de la base de recolección en relación con las necesidades de información, ya que, salvo para los medios impresos, las soluciones tecnológicas permitirán una eficiente identificación y monitoreo de fuentes web, medios, redes sociales y web oscura. Las futuras tendencias indican que Crawlers – Arañas – Las soluciones scrapers se utilizarán para la extracción de datos, pero dentro de ellas,

el peso de la inteligencia artificial y la automatización de procesos robóticos será significativamente mayor. Además, se utilizarán soluciones de "búsqueda elástica" y se mejorarán con tecnologías de automatización de procesos robóticos, lo que conducirá a un escaneo eficiente de las redes sociales. La inteligencia artificial promoverá una identificación adecuada de las fuentes.

Procesamiento voluntad ser

realizado preponderantemente con tecnología. Las aplicaciones de conversión, normalización y soluciones de agregación asistidas por tecnologías de automatización de procesos robóticos permitirán que las tecnologías y algoritmos de inteligencia artificial específicos lleven a cabo con éxito estas categorías de tareas.

El análisis de inteligencia se basará en el procesamiento eficiente del lenguaje natural y los algoritmos de aprendizaje automático, que detectarán automáticamente cualquier intento de manipulación, propaganda y fragmentación de la inteligencia. Las correlaciones quién, qué, por qué, dónde, por qué, con quién, etc. procesadas por la Inteligencia Artificial serán cada vez más precisas. El análisis de escenarios, análisis de hipótesis concurrentes, análisis de voz, gestión de evidencias, etc. serán procesados automáticamente, proporcionando al analista una información fiable.

supuestos de trabajo. Las aplicaciones de análisis de red mejoradas por algoritmos de aprendizaje automático y mecanismos de automatización de procesos robóticos conducirán a una identificación automática de la fuente.

La difusión utilizará protocolos avanzados de encriptación y transferencia segura de información, probablemente usando computación cuántica. Además, las matrices de distribución permitirán la difusión de información a listados optimizados de beneficiarios.

6. CONCLUSIONES

Cómo los servicios de inteligencia ajustarán y sincronizarán OSINT con el proceso tecnológico será un factor de éxito esencial. cuatro
Los niveles deben señalarse

aquí: - Uso de tecnologías de inteligencia artificial en las fases específicas del ciclo de inteligencia y en la mayoría de las plataformas de software específicas; - Uso de tecnologías de automatización de procesos robóticos en las fases específicas del ciclo de inteligencia y en las plataformas de software más específicas; - Adopción de tecnologías 5G; - Adopción de tecnologías cuánticas.

Estos niveles podrían marcar la diferencia entre un servicio eficiente y eficaz y un menor servicio de rendimiento.

AGRADECIMIENTOS Este

artículo fue supervisado por la profesora Irena Chiru, PhD.

REFERENCIAS

- [1] Bereziuk, B., (2016) *El modus operandi de la inteligencia china*, Ottawa: Universidad de Carleton, págs. 3-6.
- [2] Brown, ZT, (2019) *Inteligencia adaptativa para una era incierta*, Washington: Universidad Nacional de Inteligencia, págs. 15-188.
- [3] Hamilton, B., (2011) *No More Secrets - Open Source Information and the Reshaping of US Intelligence*, Santa Barbara: Praeger Security International, pp. 3-84.
- [4] Herman, M., (1999) *Intelligence Power in Peace and War*, Cambridge: Cambridge University Press, págs. 259-268.
- [5] Huges-Wilson, J., (2018) *Serviciile Secrete*, Bucarest: Meteor Publishing, págs. 29-46.
- [6] Ivanjko, T., Dokman T., (2020), *Open Source Intelligence (OSINT): problemas y tendencias*, Zagreb: Universidad de Zagreb, pp 6-9. Gate Publishing Company, Farnham, págs. 304-306.
- [7] Johnson, LK, (2010) *Inteligencia de Seguridad Nacional*, Oxford: Oxford Handbooks, págs. 12-14.
- [8] Kanakaris, V., Bandekas, DV, Tzovelekis, K., Geolocalización en Twitter e Instagram basada en técnicas OSINT: un estudio de caso, en: *International Journal of Advanced Research*, febrero de 2018, págs. 780-789.
- [9] Katz, B., (2020) *The Collection Edge*, Washington: CSIS Briefs, págs. 2-8.
- [10] Miller DT, (2015) *Defense 2045*, Washington: Rowan & Littlefield, págs. 21-52.

- [11] Nacci, G., (2017) *Appunti sulla architettura sistemica delle Fonti in OSINT*, ResearchGate, Working Paper, pp. 7-10
- [12] Nacci, G., (2020) *OSINT e COVID-19*, Roma : Società Italiana di Intelligence Press, pp. 04-07.
- [13] Ortega, JM, (2019) *OSINT + PYTHON: Extrayendo información de TORnetwork y Darkweb*, Alicante: Universidad de Alicante, pp. 12-77.
- [14] Pastor-Galindo, J., et al, (2016), *La mina de oro aún no explotada de OSINT: Oportunidades, retos abiertos y tendencias de futuro*, Murcia: Universidad de Murcia, pp. 6-8.
- [15] Pinto, RA, Hernández Medina, MJ, Pinzón, CC, Díaz, D. O., García, JC, Inteligencia de fuentes abiertas (OSINT) para operaciones de ciberseguridad. Aplicación de OSINT en un contexto colombiano y análisis de sentimientos, In: *Revista Vínculos: Ciencia, Tecnología y Sociedad*, vol. 15, nº 2, 2016, pp. 19-21.
- [16] Tabatabaei F., Wells, D., (2016) *Investigación de inteligencia de código abierto - OSINT en el contexto de la ciberseguridad*, de Polaris Spring 2016, pp. 1-15.
- [17] Williams, HJ, Blum I., (2018) *Definición de OSINT de segunda generación para la empresa de defensa*, Santa Mónica: RAND Corporation, págs. 1-14.
- [18] ***Informe CRS, (2020) *Inteligencia Artificial y Seguridad Nacional*, Washington: Servicio de Investigación del Congreso, págs. 2-29. [19] ***iee.es - Instituto Español de Estudios Estratégicos, (2013) *La inteligencia económica en un mundo global*, Madrid: Ministerio de Defensa de España - Dossier Estratégico 162, pp. 118-119.
- [20] ***Ministerio de Defensa de Japón, (2020) *2020 Defensa de Japón*, Tokio: Ministerio de Defensa, p. 23
- [21] ***Ministerio de Relaciones Exteriores de Japón, (2013) *Estrategia de Seguridad Nacional*, Tokio: Ministerio de Relaciones Exteriores de Japón, p. 18
- [22] ***OTAN, (2011) *Manual de inteligencia de fuente abierta de la OTAN*, SACEUR, pp. 2-4.
- [23] ***ODNI, DNS, (2018) *Tecnología Emergente y Seguridad Nacional*, Washington: Gobierno de EE.UU., pp. 14-27.
- [24] ***Presidente de la República Francesa, (2017) *Revisión Estratégica de Defensa y Seguridad Nacional*, París: Presidente de la República Francesa, pp. 63-72.
- nacional ruso Security Strategy*, Moscú: Presidente de la Federación Rusa, págs. 6-28.
- [25] ***Federación de Rusia Presidente, (2015).
*** El Economista – [26] Unidad de Inteligencia (2019), *Un mundo completamente nuevo: cómo la tecnología impulsa la evolución de la banca inteligente*, Londres, págs. 3-25.
- [27] ***The Economist – Intelligence Unit, (2020) *Un libro de jugadas estratégicas de C-suite para navegar por el mundo 5G*, Londres, págs. 10-12.
- [28] *** Ministerio de Relaciones Exteriores de la Federación Rusa, (2016) *Doctrina de Seguridad de la Información de la Federación Rusa*, Moscú: Ministerio de Relaciones Exteriores de la Federación Rusa, pp. 5-12.
- [29] ***Casa Blanca, (2017) *Estrategia de Seguridad Nacional*, Washington: Casa Blanca, 2017, pp. 32-35.