



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Análisis de la capacidad SIGINT en la red de receptores WebSDR y similares

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Sergio Alarcón Morales

DIRECTOR: José María Núñez Ortuño

CURSO ACADÉMICO: 2025-2026

Universida_{de}Vigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Análisis de la capacidad SIGINT en la red de receptores WebSDR y similares

Máster Universitario en Dirección TIC para la Defensa
Especialidad de Sistemas y Tecnologías de la Información

Universida_{de}Vigo

RESUMEN

El presente trabajo analiza la capacidad de las redes distribuidas de receptores WebSDR, KiwiSDR y OpenWebRX para llevar a cabo funciones de Inteligencia de Señales (SIGINT). En el contexto actual de democratización del acceso al espectro radioeléctrico, se evalúa técnica y operativamente si estas infraestructuras públicas pueden replicar las capacidades de obtención de los sistemas militares tradicionales.

El estudio examina la cobertura global, las especificaciones de los receptores y las limitaciones de estas redes bajo la doctrina de Guerra Electrónica. Los resultados demuestran que, si bien constituyen herramientas eficaces para la vigilancia estratégica de comunicaciones (COMINT) y la geolocalización en HF, carecen de la capacidad técnica necesaria para la inteligencia electrónica (ELINT) moderna y presentan vulnerabilidades críticas de seguridad operativa en confidencialidad, integridad y disponibilidad. Como solución, se propone una arquitectura de despliegue de una red privada en la nube, basada en hardware COTS y gestión centralizada, diseñada para constituir un sistema de inteligencia soberano, seguro y escalable.

ABSTRACT

This thesis analyzes the capacity of distributed WebSDR, KiwiSDR, and OpenWebRX receiver networks to perform Signals Intelligence (SIGINT) functions. In the current context of democratized access to the radio spectrum, the study evaluates, both technically and operationally, whether these public infrastructures can replicate the collection capabilities of traditional military systems.

The study examines the global coverage, receiver specifications, and limitations of these networks under Electronic Warfare doctrine. The results demonstrate that, while they are effective tools for strategic communications surveillance (COMINT) and HF geolocation, they lack the technical capacity required for modern electronic intelligence (ELINT) and present critical operational security vulnerabilities regarding confidentiality, integrity, and availability. As a solution, a deployment architecture for a private cloud network is proposed, based on COTS hardware and centralized management, designed to establish a sovereign, secure, and scalable intelligence system.

PALABRAS CLAVE

SIGINT – COMINT – ELINT – SDR – WebSDR – EW

AGRADECIMIENTOS

A mi mujer Noelia y a mis hijos Sergio y Alejandro, por su paciencia y apoyo durante el tiempo dedicado a cursar este máster, muy especialmente a la hora de elaborar este trabajo, restándole tiempo al ocio familiar.

A mis superiores y compañeros del Cuartel General de la Comandancia General de Melilla, en especial a la Sección CIS, que han permitido que dedique la atención necesaria para culminar esta tarea.

Finalmente, a mis compañeros del Batallón de Guerra Electrónica I/32, que a lo largo de mis años de servicio han fomentado que adquiriera los conocimientos, la experiencia y, sobre todo, la pasión por la Guerra Electrónica, claves para finalizar este trabajo.

Y muy especialmente a ti, Mai; gracias por tus enseñanzas y asesoramiento siempre. Seguro que, allí donde estés, sigues analizando señales.

Contenido

Índice de Figuras	4
Índice de Tablas	6
1 Introducción y objetivos.....	7
1.1 Introducción.	7
1.2 Contexto y motivación del estudio.	8
1.3 Propósito.	8
1.4 Objetivos.....	9
1.5 Metodología de investigación.....	9
1.6 Organización de la memoria.	10
2 Fundamentos teóricos.	11
2.1 Marco doctrinal.....	11
2.1.1 Inteligencia de señales.....	11
2.1.2 Guerra Electrónica.....	12
2.1.3 Relación SIGINT y EW. Operaciones electromagnéticas.....	13
2.1.4 Actividades ESM y SIGINT.	15
2.2 Arquitectura y Funcionamiento de WebSDR clásica y redes similares.	17
2.2.1 Receptor Radio Definido por Software.	17
2.2.2 Arquitectura del modelo WebSDR.	18
2.2.3 Redes distribuidas de receptores SDR.	20
2.2.4 Aplicaciones de las redes WebSDR y similares.....	20
3 Estado del Arte.....	21
3.1 Evolución y estado actual de las redes SDR distribuidas.	21
3.1.1 La Infraestructura de WebSDR y el Modelo de la Universidad de Twente.....	21
3.1.2 KiwiSDR: Hardware Embebido y Sincronización Global.	23
3.1.3 OpenWebRX y OpenWebRX+.	24
3.1.4 Receptores habituales.	24
3.1.5 Iniciativas académicas y experimentales.....	25
3.2 SIGINT.	25
3.2.1 Arquitecturas de Hardware SIGINT de Próxima Generación.....	26
3.2.2 La Plataforma USRP X410.	26
3.2.3 Per Vices Cyan.	26
3.2.4 Tecnologías de Radiogoniometría y Geolocalización Híbrida.....	27
3.3 Inteligencia Artificial Aplicada al Análisis de Señales.	27

3.4 Arquitecturas en la Nube y Procesamiento de Big Data para SIGINT.....	27
4 Análisis de capacidad SIGINT de las redes WebSDR.....	29
4.1 Cobertura de los nodos SDR.....	29
4.1.1 Cobertura espectral.....	30
4.1.2 Cobertura espacial.	30
4.2 Capacidades técnicas de recepción aplicadas a las funciones SIGINT/ESM.....	31
4.2.1 Análisis de información técnica de los fabricantes.	31
4.2.2 Búsqueda.	33
4.2.3 Interceptación.	33
4.2.4 Identificación.....	36
4.2.5 Localización.	36
4.3 Almacenamiento de toda la información.	36
4.4 Análisis de Seguridad.	36
4.4.1 Confidencialidad.	36
4.4.2 Integridad.	37
4.4.3 Disponibilidad.	37
4.5 Control de configuraciones.....	37
5 Conclusiones, propuesta de despliegue y líneas futuras.	39
5.1 Conclusiones sobre las redes WebSDR.	39
5.1.1 Herramientas válidas para COMINT, ineficaces para ELINT “moderno”.	39
5.1.2 ELINT “clásico” posible objetivo.	40
5.1.3 Limitaciones críticas en el ciclo de obtención.	40
5.1.4 Capacidad de Localización.....	41
5.1.5 Cobertura Estratégica sin proyección Táctica.	41
5.1.6 Vulnerabilidad Operativa: Seguridad y Fiabilidad.....	41
5.2 Limitaciones del trabajo realizado.....	42
5.3 Propuesta de despliegue.....	42
5.3.1 Arquitectura del Nodo Sensor.	42
5.3.2 Segmento de Captación: Tipología de Nodos Sensores.....	42
5.3.3 Segmento de Procesamiento: Edge Computing y Nube.....	44
5.3.4 Segmento de Red y Seguridad.	44
5.4 Estrategia de Despliegue Encubierto (Red "Zona Gris").....	44
5.5 Capacidad de Decepción Electrónica.	45
5.6 Líneas futuras.....	45
5.7 Conclusión final.....	45
6 Bibliografía	47

7 Anexo I: Distribución de Nodos WebSDR.....	51
7.1 WebSDR.....	52
7.2 KiwiSDR.....	54
7.3 OpenWebRx.	56
8 Anexo II: Criterio de evaluación de receptores SDR.....	59
8.1 Parámetros técnicos considerados.	59
8.2 Tabla de Cuantificación.....	61
8.2.1 Tabla de cuantificación COMINT.....	61
8.2.2 Tabla de cuantificación ELINT.....	62
9 Anexo III: Características de receptores SDR analizados	63
10 Anexo IV: Características de receptores SDR propuestos.....	75

ÍNDICE DE FIGURAS

Figura 2-1 Guerra Electrónica (Fuente: elaboración propia)	13
Figura 2-2 Operaciones Electromagnéticas (Fuente: MADOC).....	14
Figura 2-3 El entorno electromagnético (Fuente: AJP-3.6 <i>Allied Joint Doctrine for EW</i>).....	15
Figura 2-4 Proceso de análisis en interceptación COMINT (Fuente: Elaboración propia con IA GEMINI)	16
Figura 2-5 DF con antena direccional rotatoria (Fuente: Elaboración propia con IA GEMINI).....	16
Figura 2-6 Localización TDoA (Fuente: Elaboración propia con IA GEMINI)	17
Figura 2-7 Diagrama de bloques de receptor SDR genérico (Fuente: elaboración propia).....	18
Figura 2-8 Distribución de nodos SDR en la red WebSDR (Fuente: websdr.com).....	19
Figura 2-9 Nodos del 1 al 6 de la WebSDR. Fuente: websdr.com	19
Figura 3-1 Nodo 34 de la WebSDR (Fuente: websdr.com).....	22
Figura 3-2 Nodo 34 de la WebSDR en mapa (Fuente: websdr.com)	22
Figura 3-3 Interfaz nodo 34 de la WebSDR. (Fuente: EA4RCR)	22
Figura 3-4 Extensión de localización TDoA en KiwiSDR (Fuente: HB9RE).....	23
Figura 3-5 Extensión de localización TDoA en KiwiSDR (Fuente: HB9RE).....	23
Figura 3-6 Decodificación de posicionamiento aeromóviles en OpenWebRX+ (Fuente: EA7KQR) ...	24
Figura 4-1 Decodificación de llamadas selectiva en OpenWebRX+ (Fuente: fms.komkon.org/OWRX/).....	35
Figura AI-1 Distribución de nodos SDR (Fuente: receiverbook.de [32]).....	51
Figura AI-2 Distribución de nodos HF WebSDR (Fuente: receiverbook.de [32]).....	52
Figura AI-3 Distribución de nodos VHF WebSDR (Fuente: receiverbook.de [32]).....	52
Figura AI-4 Distribución de nodos UHF WebSDR (Fuente: receiverbook.de [32]).....	53
Figura AI-5 Distribución de nodos SHF WebSDR (Fuente: receiverbook.de [32]).....	53
Figura AI-6 Distribución de nodos HF KiwiSDR (Fuente: receiverbook.de [32])	54
Figura AI-7 Distribución de nodos VHF KiwiSDR (Fuente: receiverbook.de [32]).....	54
Figura AI-8 Distribución de nodos UHF KiwiSDR (Fuente: receiverbook.de [32]).....	55
Figura AI-9 Distribución de nodos SHF KiwiSDR (Fuente: receiverbook.de [32])	55
Figura AI-10 Distribución de nodos HF OpenWebRx (Fuente: receiverbook.de [32])	56
Figura AI-11 Distribución de nodos VHF OpenWebRx (Fuente: receiverbook.de [32])	56
Figura AI-12 Distribución de nodos UHF OpenWebRx (Fuente: receiverbook.de [32])	57
Figura AI-13 Distribución de nodos SHF OpenWebRx (Fuente: receiverbook.de [32]).....	57
Figura AIII -1 AirSpy HF+ Discovery (Fuente: airspy.com)	64
Figura AIII -2 AirSpy R2 (Fuente: airspy.com)	65
Figura AIII -3 HackRF One (Fuente: greatscottgadgets.com/).....	66

Figura AIII-4 KiwiSDR (Fuente: kiwisdr.com).....	67
Figura AIII -5 LimeSDR USB (Fuente: limemicro.com)	68
Figura AIII -6 Perseus SDR (Fuente: microtelecom.it)	69
Figura AIII-7 RTL-SDR.COM Blog V4 (Fuente: rtl-sdr.com)	70
Figura AIII-8 SDRplay RSP1B (Fuente: sdrplay.com)	71
Figura AIII-9 SDRplay RSPdx-R2 (Fuente: sdrplay.com).....	72
Figura AIV-1 Cyan (Fuente: pervices.com)	76
Figura AIV-1 USRP B210 (Fuente: ettus.com)	77
Figura AIV-2 WEB-888 (Fuente: rx-888.com)	78
Figura AIV-3 KrakenSDR (Fuente: krakenrf.com)	79

ÍNDICE DE TABLAS

Tabla 3-1 Resumen de parámetros técnicos de fabricante (Fuente: elaboración propia)	25
Tabla 4-1 Valores cuantificados COMINT (Fuente: elaboración propia)	32
Tabla 4-2 Valores cuantificados ELINT (Fuente: elaboración propia)	32
Tabla AII-1 Criterios para evaluación cuantitativa de receptores en COMINT (Fuente: Elaboracion propia)	62
Tabla AII-2 Criterios para evaluación cuantitativa de receptores en ELINT (Fuente: Elaboracion propia)	62
Tabla AIII-1 Receptores a analizar (Fuente: Elaboracion propia)	63
Tabla AIII -2 Datos técnicos AirSpy HF+ Discovery (Fuente: Elaboracion Propia)	64
Tabla AIII -3 Datos técnicos AirSpy R2 (Elaboracion Propia)	65
Tabla AIII -4 Datos técnicos HackRF One (Elaboracion Propia)	66
Tabla AIII -5 Datos técnicos KiwiSDR (Elaboracion Propia).....	67
Tabla AIII -6 Datos técnicos LimeSDR USB (Elaboracion Propia)	68
Tabla AIII -7 Datos técnicos Perseus SDR (Elaboracion Propia)	69
Tabla AIII -8 Datos técnicos RTL-SDR Blog V4 (Fuente: Elaboracion Propia)	70
Tabla AIII-9 Datos técnicos SDRplay RSP1B (Elaboracion Propia)	71
Tabla AIII-10 Datos técnicos SDRplay RSPdx-R2 (Elaboracion Propia).....	72
Tabla AIII-11 Comparativa 1/2 de datos técnicos de receptores SDR (Elaboracion Propia).....	73
Tabla AIII-11 Comparativa 2/2 de datos técnicos de receptores SDR (Elaboracion Propia).....	74
Tabla AIV-1 Receptores a analizar (Fuente: Elaboracion propia).....	75
Tabla AIV-2 Datos técnicos Cyan (Elaboracion Propia).....	76
Tabla AIV-3 Datos técnicos USRP B210 (Elaboracion Propia).....	77
Tabla AIV-4 Datos técnicos WEB-888 (Elaboracion Propia)	78
Tabla AIV-5 Datos técnicos KrakenSDR (Elaboracion Propia).....	79

1 INTRODUCCIÓN Y OBJETIVOS.

1.1 Introducción.

El concepto de inteligencia ha estado históricamente ligado a la capacidad de obtener y analizar información relevante para la toma de decisiones estratégicas, tanto en contextos civiles como militares. Desde el inicio de la telegrafía y la radio, la observación del espectro electromagnético se ha convertido en una de las principales fuentes de información, hasta el punto de que, dentro de este marco, la Inteligencia de Señales (SIGINT – del inglés *Signal Intelligence*) y la Guerra Electrónica (EW – del inglés *Electronic Warfare*) han evolucionado como disciplinas fundamentales en el ámbito de la defensa, la ciberseguridad y la gestión de infraestructuras tecnológicas [1].

A lo largo del siglo XX, las capacidades SIGINT estuvieron tradicionalmente reservadas a potencias militares y agencias gubernamentales con acceso a costosos sistemas de interceptación y redes de sensores distribuidos. Estas infraestructuras, basadas en equipamiento especializado y enlaces dedicados, requerían inversiones significativas y estaban sujetas a fuertes restricciones legales y de confidencialidad. Sin embargo, la interconexión global mediante Internet y el desarrollo de la radio definida por software (SDR – del inglés *Software Defined Radio*) han propiciado un cambio de paradigma que abre nuevas posibilidades para la observación y el análisis del espectro radioeléctrico, ya no sólo en entornos militares y de defensa, sino también en entornos civiles y académicos [2].

De esta forma, la aparición de plataformas WebSDR¹ –sistemas que permiten la recepción remota de señales de radio a través de navegadores web– ha democratizado el acceso al espectro radioeléctrico global. Estas plataformas, gestionadas de manera descentralizada por radioaficionados, universidades o entidades privadas, actúan como nodos de recepción distribuidos que cubren amplias zonas geográficas. Mediante interfaces accesibles y protocolos abiertos, los usuarios pueden sintonizar frecuencias, visualizar espectrogramas en tiempo real y, en algunos casos, descargar muestras de señal para su análisis [3][4][5].

En este sentido, la naturaleza abierta de la red WebSDR –desarrollada originalmente por la Universidad de Twente–, su cobertura global y diversidad de configuraciones técnicas, la convierten

¹ Para una mejor comprensión, cuando en el trabajo se emplee el término Red WebSDR se hace referencia exclusiva a la red desarrollada originalmente por la Universidad de Twente. En el caso de emplear el término Redes WebSDR, se incluye a todas las redes distribuidas de nodos SDR.

en un objeto de estudio relevante para analizar hasta qué punto podrían evolucionar hacia arquitecturas orientadas a la inteligencia de señales [2].

El presente trabajo pretende evaluar si las redes WebSDR son capaces de replicar las capacidades de los modernos y complejos sistemas de obtención de inteligencia militar. Este análisis no se realizará desde una perspectiva exclusivamente técnica, pues ya existen diversos trabajos que demuestran las bondades de estos sistemas para fines similares [6][7][2], sino también desde un punto de vista operativo, evaluando si cumplen con los requisitos necesarios para ser explotados para el fin descrito.

Desde esta perspectiva, el trabajo explora la hipótesis de que una red SIGINT basada en tecnologías WebSDR integradas en una red privada podría ofrecer una alternativa de bajo coste, modular y escalable para la captación, almacenamiento y análisis de señales, con potencial aplicación no sólo en sectores civiles, como la investigación académica, la gestión del espectro o la detección de interferencias, sino también en ámbitos de seguridad y defensa y, más concretamente, en el de la Inteligencia.

1.2 Contexto y motivación del estudio.

El contexto actual de la sociedad digital se caracteriza por una creciente densidad espectral y una proliferación de tecnologías de comunicación inalámbrica. Desde sistemas 5G y enlaces satelitales hasta redes IoT, la cantidad de emisiones electromagnéticas activas en cualquier momento es extraordinaria. Este fenómeno incrementa la necesidad de disponer de mecanismos eficientes de vigilancia y gestión del espectro radioeléctrico, no solo con fines regulatorios, sino también para garantizar la seguridad y la integridad de los sistemas de información [5].

En paralelo, el paradigma de la nube privada ha transformado la manera en que las organizaciones gestionan sus infraestructuras TIC. La virtualización, la contenedorización y la automatización han permitido desplegar entornos de cómputo seguros, escalables y adaptables a múltiples necesidades. En el contexto de la inteligencia de señales, la nube privada representa una oportunidad para centralizar la gestión de receptores distribuidos, procesar grandes volúmenes de datos de manera paralela y asegurar el cumplimiento normativo en el tratamiento de la información [6].

La motivación de este trabajo radica en la confluencia de ambas tendencias: la expansión de las redes WebSDR como fuentes de datos distribuidos y el auge de la computación en la nube como entorno de consolidación y análisis. El objetivo último es proponer una arquitectura conceptual que permita aprovechar el potencial SIGINT de redes WebSDR bajo un modelo de gestión TIC centralizada, en el que la seguridad, la gobernanza de datos y la eficiencia operativa sean elementos clave.

A diferencia de los estudios centrados exclusivamente en el rendimiento técnico de los receptores o en la decodificación de señales específicas, este trabajo adopta un enfoque más holístico, que abarca no sólo aspectos técnicos, sino operativos, de gestión y seguridad.

El análisis se fundamenta en la revisión crítica de literatura técnica, estándares y casos de uso documentados, junto con una modelización arquitectónica basada en buenas prácticas de ingeniería de sistemas, ciberseguridad y administración de infraestructuras distribuidas.

1.3 Propósito.

El objetivo principal de este Trabajo Fin de Máster es analizar la capacidad SIGINT de las redes WebSDR, evaluando su potencial técnico y operativo para la recolección, tratamiento y análisis de señales radioeléctricas.

Este objetivo busca determinar hasta qué punto las infraestructuras WebSDR públicas pueden constituir una base viable para la observación estructurada del espectro electromagnético, tanto desde una perspectiva tecnológica (capacidades de recepción, ancho de banda, sensibilidad, cobertura) como

organizativa/operativa (gestión, seguridad y gobernanza de los datos). Para ello se considera que los nodos SDR son explotados remotamente a través de las redes WebSDR sin más herramientas que un PC a través del navegador de Internet. Adicionalmente, se puede considerar que se disponen de herramientas de análisis de señales instaladas ese u otro equipo.

Finalmente, se pretende proponer una posible arquitectura para el despliegue de una red distribuida de receptores radio SDR, a través de una red privada.

1.4 Objetivos.

Tomando como base el propósito del trabajo se definen una serie de objetivos específicos:

- **Definir el marco conceptual y teórico de la inteligencia de señales (SIGINT)** y su relación con la guerra electrónica (EW), abarcando las subdisciplinas principales COMINT y ELINT y su evolución hacia entornos digitales distribuidos.
- **Analizar la red global de receptores WebSDR y plataformas similares**, identificando su distribución geográfica, características técnicas y nivel de interoperabilidad.
- **Evaluar la viabilidad técnica y operativa** de las redes WebSDR como herramientas para actividades SIGINT.
- **Proponer una arquitectura conceptual de red WebSDR privada**, desplegable sobre infraestructura de red privada o híbrida, que permita explotar las capacidades SIGINT identificadas bajo un entorno controlado.

En síntesis, este trabajo parte del análisis exhaustivo de la capacidad SIGINT existente en las redes WebSDR, y evoluciona hacia la definición de un modelo arquitectónico privado, que permita maximizar dicha capacidad en un entorno de gestión TIC seguro y eficiente.

1.5 Metodología de investigación.

El enfoque metodológico del trabajo es descriptivo, analítico y propositivo, orientado al análisis sistemático de las redes WebSDR y a la formulación de un modelo arquitectónico de referencia para su explotación controlada.

La metodología se compone de cuatro fases complementarias:

- Fase 1: Revisión teórica y documental.

En esta primera fase se realiza una revisión exhaustiva de literatura doctrinal sobre la inteligencia de señales (SIGINT) y la guerra electrónica (EW), incluyendo sus subdisciplinas, componentes históricos y su adaptación al ámbito digital.

Se estudian igualmente las tecnologías SDR y WebSDR, sus arquitecturas, protocolos de comunicación, y los proyectos abiertos más relevantes (WebSDR, KiwiSDR, OpenWebRX).

- Fase 2: Análisis de las redes WebSDR.

En esta etapa se realiza un análisis estructurado de las capacidades de las redes WebSDR. Se recopilan y analizan datos sobre:

- Número y ubicación de nodos activos.
- Bandas de frecuencia cubiertas y rango espectral efectivo.
- Características técnicas de los receptores empleados (resolución, sensibilidad, protocolos).
- Accesibilidad, disponibilidad temporal y conectividad de los nodos.
- Otros aspectos de relevancia.

Este análisis se basa en fuentes abiertas, catálogos técnicos y documentación de proyectos de investigación, con el fin de determinar las capacidades actuales y potenciales de las redes WebSDR y similares para fines SIGINT.

En este trabajo no se considerarán aspectos legales de la interceptación de señales, suponiendo que su empleo se realizará con las debidas autorizaciones de las autoridades administrativas y/o judiciales, así como dentro del marco de la Seguridad Nacional y de las Operaciones Militares.

- Fase 3: Evaluación de la capacidad SIGINT.

Con la información obtenida, se procede a una evaluación teórica y técnica de la capacidad de las redes WebSDR para realizar actividades de observación del espectro que puedan enmarcarse dentro de las funciones de SIGINT. El estudio considera aspectos como:

- Resolución temporal y frecuencia de muestreo.
- Limitaciones en ancho de banda y ruido.
- Sincronización entre nodos y precisión geográfica.
- Integración potencial de fuentes heterogéneas.
- Fiabilidad y seguridad de la información recibida.

El resultado de esta fase permite identificar los principales factores limitantes (técnicos, organizativos y normativos) que condicionan el uso operativo de las redes WebSDR con fines de inteligencia de señales.

- Fase 4: Propuesta arquitectónica.

Como derivada del análisis de capacidades SIGINT de las redes WebSDR y similares, se formulará una propuesta conceptual de arquitectura privada en nube, diseñada para maximizar la capacidad SIGINT observada en las redes WebSDR.

Esta arquitectura no constituye un sistema SIGINT plenamente operativo ni una implementación experimental, sino un modelo teórico de referencia para líneas de trabajo e investigación posteriores.

1.6 Organización de la memoria.

Con la finalidad de alcanzar los objetivos ya definidos, esta memoria se organiza de la siguiente manera:

- **Capítulo 1: Introducción.** Presenta el contexto, la motivación, los objetivos y la metodología del estudio, centrando el foco en el análisis de la capacidad SIGINT de las redes WebSDR y en la propuesta de una posible arquitectura de red WebSDR en nube privada.
- **Capítulo 2: Fundamentos teóricos.** Desarrolla los conceptos de SIGINT, EW y sus subdisciplinas (COMINT, ELINT, FISINT), y analiza los principios técnicos de los sistemas SDR y WebSDR.
- **Capítulo 3: Estado del arte.** Examina las principales plataformas WebSDR, las tecnologías SDR asociadas, las herramientas de análisis disponibles y los estudios previos en el ámbito de la observación distribuida del espectro.
- **Capítulo 4: Análisis de la red WebSDR y sistemas similares.** Presenta un estudio descriptivo de la red global de receptores WebSDR, evaluando su cobertura, capacidades técnicas y limitaciones para tareas SIGINT.
- **Capítulo 5: Conclusiones, propuesta de despliegue y líneas futuras** de investigación.

2 FUNDAMENTOS TEÓRICOS.

2.1 Marco doctrinal.

2.1.1 Inteligencia de señales.

Inteligencia es el proceso de integrar, interpretar, analizar y evaluar información relevante sobre un determinado asunto que representa una amenaza o una oportunidad para una organización o un Estado, orientado a la toma de decisiones y a la acción [8][9].

En el ámbito de las operaciones terrestres, la función de combate Inteligencia comprende el conjunto de actividades encaminadas a satisfacer las necesidades de conocimiento del jefe, relativas al entorno operativo y la situación táctica, necesarias para el planeamiento y ejecución de las operaciones, así como para la identificación de las amenazas contra las fuerzas propias y el cumplimiento de la misión [10].

Las disciplinas de inteligencia comprenden los medios, sistemas y procedimientos utilizados para observar, explotar, almacenar y difundir información referente a la situación, amenazas y otros factores del entorno operativo. Por la naturaleza de la fuente o del órgano de obtención que la explota, y la especialización de su personal, clásicamente se clasifican en: Inteligencia Humana (HUMINT), Inteligencia Geográfica (GEOINT), Inteligencia de Imágenes (IMINT), Inteligencia de Fuentes Abiertas (OSINT), Inteligencia Técnica (TECHINT), Inteligencia Acústica (ACINT), Inteligencia Sanitaria (MEDINT) e Inteligencia de Señales (SIGINT), definida esta última como el conjunto de actividades técnicas y analíticas orientadas a la obtención de información mediante la interceptación, el procesamiento y la interpretación de señales electromagnéticas [11][12].

A lo largo de la historia militar moderna, el SIGINT ha sido una herramienta esencial para alcanzar la superioridad informativa. El desarrollo de los sistemas de inteligencia de señales ha acompañado constantemente la evolución tecnológica de las comunicaciones y de los sistemas electrónicos, demostrando siempre el poder estratégico de la información obtenida a través del espectro electromagnético, como la procedente de los programas de descifrado de códigos Enigma o *Purple* durante la Segunda Guerra Mundial [13].

La SIGINT se subdivide en dos ramas complementarias [11][14]:

- COMINT (*Communications Intelligence* – Inteligencia de Comunicaciones): orientada al estudio de las comunicaciones electromagnéticas y de los sistemas de comunicaciones.

- **ELINT** (*Electronic Intelligence* – Inteligencia electrónica): dedicada al análisis de las radiaciones electromagnéticas procedentes de emisores que no son de telecomunicaciones, como radares o sensores.

En la doctrina de los Estados Unidos se define además un tercer componente [9][15]:

- **FISINT** (*Foreign Instrumentation Signals Intelligence*): enfocada al análisis técnico de datos interceptados procedentes de equipos y sistemas de control, como telemetría, telecontrol y guiado, armado y disparo y enlaces de datos o data-links.

2.1.2 Guerra Electrónica.

La doctrina terrestre [14][16] define la Guerra Electrónica (EW) como la acción militar que explota la energía electromagnética para proporcionar conocimiento de la situación y lograr efectos ofensivos y defensivos, con la finalidad de obtener la superioridad sobre el adversario en el empleo del entorno electromagnético (EEM²), para reducir o impedir su uso hostil y asegurar su uso eficaz por parte de las fuerzas propias y aliadas. Atendiendo al efecto que pretenden obtener, las acciones de EW se clasifican en:

- **Vigilancia Electrónica** (ES – *Electronic Surveillance*): Empleo de la energía electromagnética para obtener conocimiento de la situación, entendiéndose como tal la identificación y localización de las fuerzas propias y del adversario.
- **Ataque Electrónico** (EA – *Electronic Attack*): Empleo de la energía EM con propósitos ofensivos. Se emplea para destruir, neutralizar, negar, degradar, interrumpir o engañar las capacidades de mando y control (C2) y de empleo del espectro por parte del adversario.
- **Defensa Electrónica** (ED – *Electronic Defense*): Uso de la energía EM para proporcionar protección y asegurar el empleo efectivo del EMS por las fuerzas propias o aliadas, frente los ataques electrónicos del adversario, así como para colaborar con otras capacidades físicas a la protección de las fuerzas, de las plataformas, de los y de determinadas áreas de la zona de acción.

Esta clasificación facilita al mando y a sus órganos de apoyo el planeamiento y conducción de las operaciones mediante el empleo de la EW para conseguir unos efectos deseados. Para una tipificación de las actividades de EW desde un punto de vista técnico, es decir planeadas y ejecutadas en su mayoría por personal especialista en EW para conseguir los efectos vistos anteriormente, se introduce el concepto de medidas de EW:

- **Medidas de apoyo electrónico** (ESM - *Electronic Support Measures*): Son aquellas medidas que se realizan para buscar, interceptar, identificar y localizar la emisión EM y su fuente con una doble finalidad, por un lado proporcionar información al escalón que apoya y por otro lado proporcionar información técnica para posibilitar la ejecución de otras medidas. De hecho, su participación es fundamental en la toma decisiones inmediatas que impliquen ECM, EPM y otras acciones tácticas.
- **Contramidasas electrónicas** (ECM - *Electronic Counter Measures*): Son aquellas que emplean la energía EM para impedir o reducir el uso eficaz del espectro electromagnético por parte del enemigo mediante:
 - Perturbación electrónica: Uso de la energía electromagnética para dificultar o impedir la utilización que el enemigo pueda hacer de sus equipos o sistemas electrónicos.

² Entorno Electromagnético (EEM) se define como la combinación de la energía electromagnética procedente de fuentes naturales o artificiales, a la cual un sistema o equipo será expuesto en la realización de su función. Abarca la totalidad de los fenómenos o actividades electromagnéticas que existen en un lugar determinado

- **Decepción electrónica:** Uso de la energía electromagnética con la finalidad de confundir, distraer o engañar al enemigo o a sus sistemas electrónicos.
- **Neutralización electrónica:** Es el uso deliberado de energía electromagnética para dañar temporal o permanentemente los dispositivos enemigos que utilizan el espectro electromagnético para su funcionamiento.
- **Medidas de protección electrónicas (EPM - *Electronic Protective Measures*):** Son aquellas medidas que aseguran el uso eficaz del espectro electromagnético por las fuerzas propias, a pesar del uso hostil que de la energía electromagnética pueda hacer el enemigo. Pueden ser activas o pasivas mediante el empleo de técnicas, tácticas o procedimientos. Estas medidas no son exclusivas del personal especialista de EW.

En la Figura 2-1 se muestra de forma genérica la relación entre las acciones y las medidas de EW.



Figura 2-1 Guerra Electrónica (Fuente: elaboración propia)

2.1.3 Relación SIGINT y EW. Operaciones electromagnéticas.

Tanto la SIGINT como la EW, junto a la gestión del espectro (SM), NAVWAR (*Navigation Warfare*), las operaciones en el ciberespacio y otras que se consideren; forman parte de las Operaciones Electromagnéticas (EMO), definidas como el conjunto de acciones militares dirigidas a conformar y vigilar el EME y garantizar la superioridad en él mediante el empleo de la energía electromagnética con fines ofensivos y defensivos[16][17].

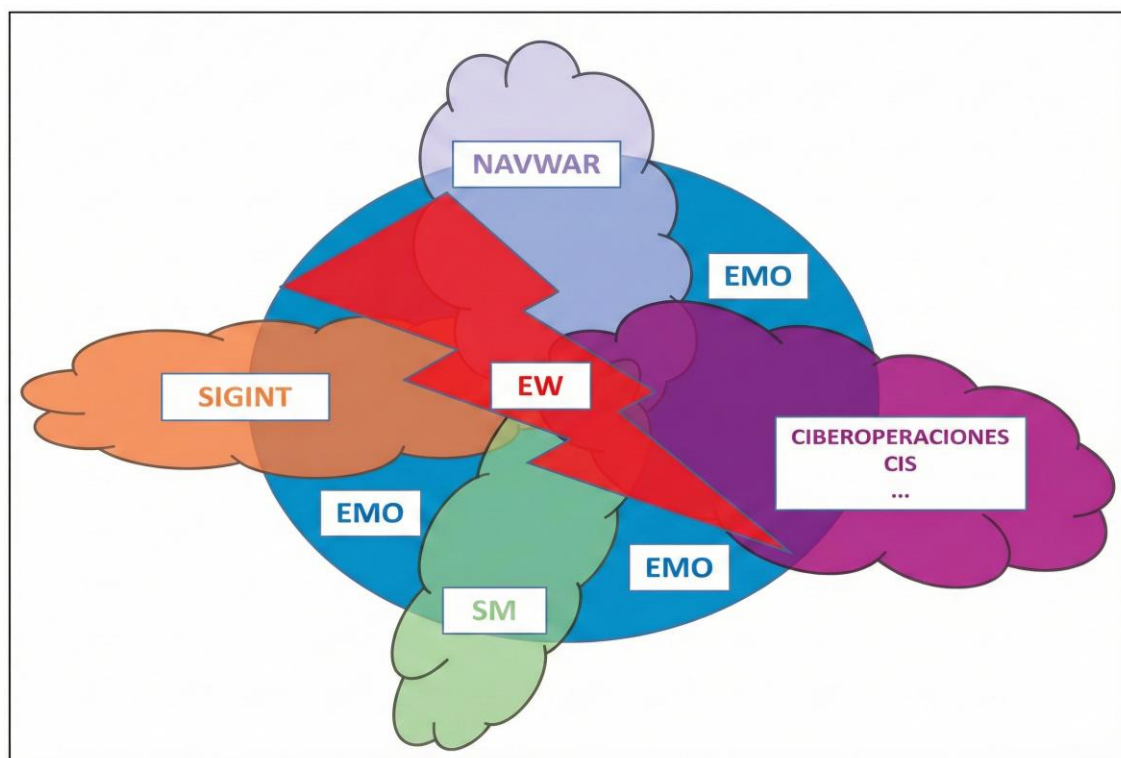


Figura 2-2 Operaciones Electromagnéticas (Fuente: MADOC)

De la lectura de las definiciones expuestas en los apartados anteriores se desprende que las ESM constituyen la intersección operativa entre SIGINT y EW y su misión principal es mantener actualizado el Orden de Batalla Electrónico (OBE), definido como el listado de emisores usados por una fuerza o empleados en un escenario, con información específica sobre sus características electromagnéticas, parámetros, localización, plataforma asociada, uso y cualquier otro dato considerado de relevancia. En el área de operaciones, las ESM son la fuente principal de información para la elaboración de la SIGINT [18]. Las diferencias entre ellas estriban en la finalidad, en el uso de la información obtenida y en el marco temporal de desarrollo de sus actividades.

La SIGINT proporciona apoyo de inteligencia a todos los niveles, desde el gobierno hasta los mandos combatientes, tanto al planeamiento a largo plazo como a las operaciones de combate más inmediatas, incluso a las de guerra electrónica. La información obtenida sirve para mantener actualizado el OBE de todos los países que se consideren de interés y sus actividades se realizan desde tiempo de paz [14].

Las ESM proporcionan información tanto para la conducción de la guerra electrónica y de las acciones tácticas como para la actualización de los OBE de los teatros de operaciones, mientras éstas tienen lugar [14].

De esta forma, el EEM se convierte en una dimensión intangible del campo de batalla incluida en el dominio ciberespacial, en el que los diferentes actores de un conflicto armado tratan de obtener la superioridad [19].



Figura 2-3 El entorno electromagnético (Fuente: AJP-3.6 *Allied Joint Doctrine for EW*)

2.1.4 Actividades ESM y SIGINT.

Dado que, tal y como se ha visto anteriormente, la finalidad de las ESM es en gran parte coincidente con las de la SIGINT, serán las actividades de las primeras las que se utilizarán para analizar la capacidad SIGINT de la red WebSDR y similares.

Las actividades desarrolladas dentro de las ESM son [14]:

- **Búsqueda:** sondeo continuo y sistemático del espectro para descubrir cualquier actividad electromagnética. Esta actividad se puede realizar:

Sobre una banda de frecuencia con la finalidad de descubrir nuevas frecuencias de emisiones. Posteriormente se determinará si son útiles o no. Es conocida como exploración electromagnética o simplemente exploración.

Sobre frecuencias que ya han sido declaradas de interés, con la finalidad de explotar sus emisiones. Es lo que se conoce como vigilancia electromagnética.

- **Intercepción:** análisis de la emisión captada con el fin de extraer la información técnica y de contenido. Esta actividad es diferente según se trate de COMINT y ELINT.

Se pueden diferenciar dos procesos independientes: la grabación/captura de la señal y su tratamiento o análisis para extraer la información técnica y de contenido.

Mientras que en COMINT, la señal captada se clasifica y en función de si es conocida y es posible su demodulación y decodificación, por lo que se obtiene toda la información técnica y

de contenido, o por el contrario no se conoce, procediendo a realizar un análisis de señales para tratar de clasificarla y determinar proceso de demodulación y decodificación.



Figura 2-4 Proceso de análisis en interceptación COMINT (Fuente: Elaboración propia con IA GEMINI)

En ELINT, la señal interceptada es analizada para extraer todos los parámetros técnicos posibles.

- **Identificación:** estudio de los parámetros técnicos y de contenido obtenidos en la fase de interceptación para asociar la emisión al sistema que la origina, reconocer si es hostil, determinar su grado de amenaza, la alerta que representa o, simplemente, para determinar si es o no de interés.
- **Localización:** determinación de la ubicación geográfica del origen de la emisión interceptada mediante el empleo de medios de radiogoniometría para determinar el ángulo de llegada del frente de ondas a distintos receptores estáticos o a un único receptor en movimiento geolocalizados, y utilizando técnicas de triangulación basadas para determinar el punto o zona donde probablemente se ubique el emisor.

La localización se puede llevar utilizando diferentes técnicas:

Dirección (DF) por antena direccional y rotación mecánica o electrónica. Normalmente tratando de definir la dirección por la que la recepción es más potente. Con la dirección obtenida de 3 receptores se determina una zona de probabilidad de emisión.

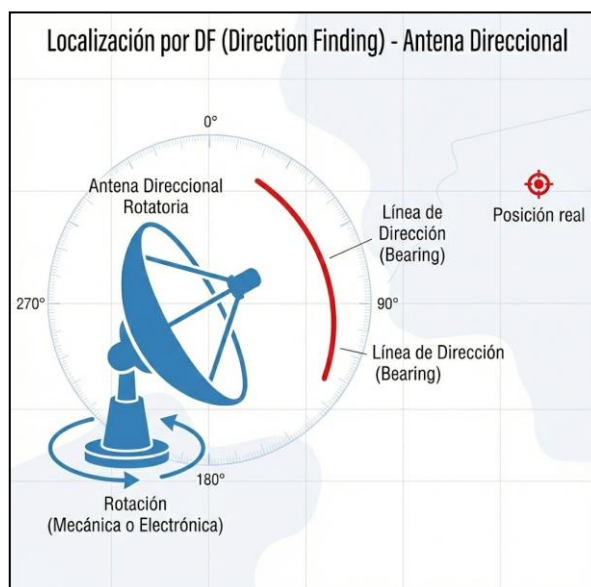


Figura 2-5 DF con antena direccional rotatoria (Fuente: Elaboración propia con IA GEMINI)

- **TDoA (*Time Difference of Arrival*)**: requiere sincronización temporal precisa entre nodos (GPS/PTP) y buffering temporal de IQ. Compara la diferencia temporal con que varios pares de receptores sincronizados reciben una misma emisión, de forma que se puede calcular la diferencia de distancia del emisor a cada uno de los receptores de cada par, obteniendo hipérbolas. Estudian cómo se entrecortan estas hipérbolas, se puede determinar una zona de probabilidad de emisión.
- **RSSI multilateración**: menos preciso pero útil en condiciones de sincronización imperfecta.
- **Angle of Arrival (AoA)** mediante array de antenas y procesamiento de fase.

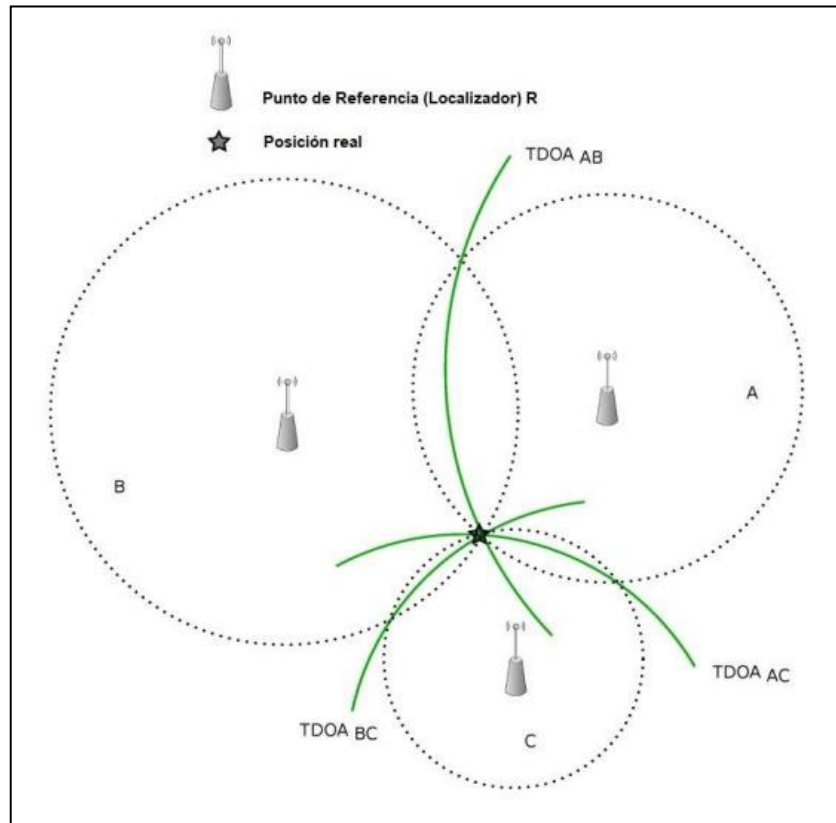


Figura 2-6 Localización TDoA (Fuente: Elaboración propia con IA GEMINI)

Un factor determinante para la eficacia de las actividades ESM es el tipo de emisión sobre el que se trabaja (HF, VHF, UHF, SHF, etc.), ya que factores como atenuación, potencia de emisión y terreno, entre otros, condicionan la capacidad de detección de la señal objetivo y determinan el rango del alcance de los medios de radiogoniometría.

2.2 Arquitectura y Funcionamiento de WebSDR clásica y redes similares.

2.2.1 Receptor Radio Definido por Software.

Una Radio Definida por Software (SDR – del inglés) consiste en una radio en la que algunas (o todas) funciones realizadas por elementos físicos en radios convencionales están definidas por software. [20]

En este sentido, un receptor radio definido por software (SDR Rx) es una arquitectura en la que las funciones clásicas (generalmente las de filtrado, demodulación y decodificación) se implementan mediante software en lugar de hardware fijo, pudiendo contar adicionalmente con una cadena de transmisión.

Un sistema SDR Rx se compone de los siguientes elementos fundamentales, repartidos en cuatro bloques funcionales [21][22]:

- Bloque de Radiofrecuencia (RF):
 - **Frontend:** encargado de la sintonización y conversión de la RF a Frecuencia Intermedia.
- Bloque de Frecuencia Intermedia (FI):
 - **Conversor analógico-digital** (ADC – *Analog to Digital Converter*): digitaliza la señal recibida.
 - **Conversor Digital Descendente** (DDC – *Digital Down Converter*): Traslada a Banda Base (BB) la señal en FI procedente del paso anterior.
- Bloque de Banda Base:
 - **Procesador digital** (DSP – *Digital Signal Processor*): aplica algoritmos de filtrado y demodulación.
- Bloque de Control:
 - **Interfaz de hombre-máquina:** proporciona la comunicación entre el usuario y el sistema.

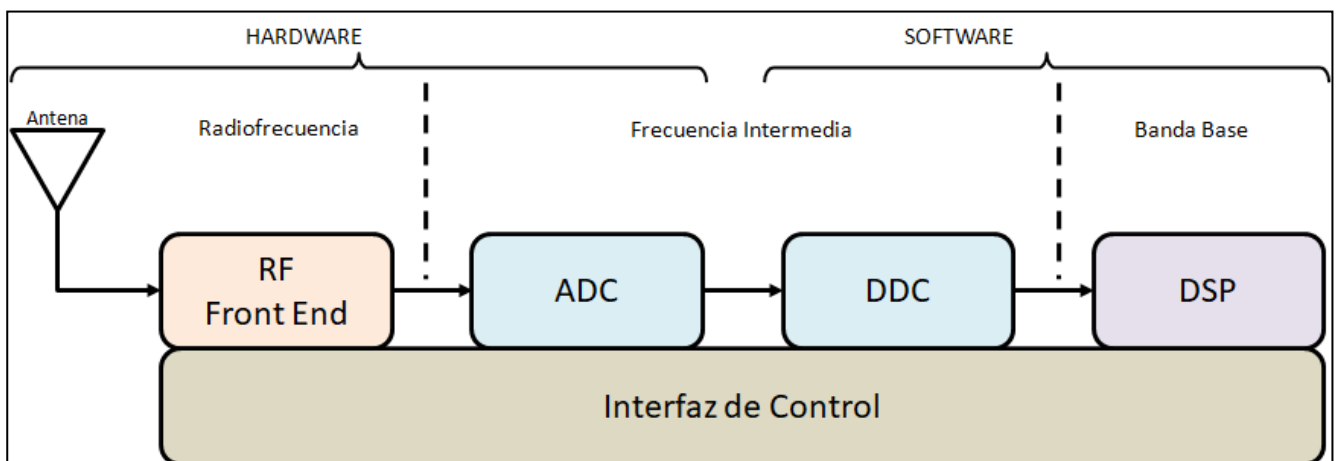


Figura 2-7 Diagrama de bloques de receptor SDR genérico (Fuente: elaboración propia)

Su principal ventaja radica en la flexibilidad: un mismo hardware puede adaptarse a múltiples tipos de señales o formas de onda, simplemente modificando el software.

2.2.2 Arquitectura del modelo WebSDR.

El WebSDR es una evolución del concepto SDR Rx que permite el acceso remoto y simultáneo a receptores de radio a través de Internet. Fue desarrollado inicialmente en 2007 por la Universidad de Twente, con el propósito de facilitar el acceso al radiotelescopio *Dwingeloo* a multitud de radioaficionados. Hoy en día, el software está disponible para cualquier persona que disponga de un receptor SDR y quiera proporcionar acceso remoto al mismo [3].

Su funcionamiento se basa en la digitalización continua de un ancho de banda, que se retransmite por medio de un servidor web. Cada usuario puede seleccionar una frecuencia y modo de demodulación de forma independiente, lo que convierte al sistema en una plataforma multiusuario. [3]

Actualmente, existe una red de servidores o nodos SDR desplegados a lo largo de todo el planeta, como se muestra en el mapa de la Figura 2-5, a través de los cuales se pueden sintonizar emisiones en diferentes bandas de frecuencia [3].



Figura 2-8 Distribución de nodos SDR en la red Websdr.com (Fuente: websdr.com)

En la figura 2-6 se puede observar el listado de los 6 primeros nodos SDR. En ella se puede ver claramente como los nodos no son iguales entre sí, sino que están configurados con diferente hardware, cubriendo además distintas bandas de frecuencias.

WebSDR at the University of Twente, Enschede, NL http://websdr.ewi.utwente.nl:8901/ JO32KF; 772 users	0.000 - 29.160 MHz	Mini-Whip	1
WebSDR Maasbree Netherlands (Low): rural low noise level, 160m/80m/60m/40m/30m/20m/17m/15m band, CW segments included http://sdh.websdrmaasbree.nl:8901/ JO31ai59; 124 users	1.799 - 1.991 MHz 3.468 - 3.852 MHz 5.277 - 5.469 MHz 6.908 - 7.292 MHz 10.054 - 10.246 MHz 13.983 - 14.367 MHz 18.022 - 18.214 MHz 20.841 - 21.609 MHz	Low noise active receiving loop and GPS locked RX888MKII	2
BATC & AMSAT-UK QO-100 (Es/Hail-2) Geostationary Satellite WebSDR http://eshail.batc.org.uk:8901/ IO70JB; 95 users	10489.500 - 10490.000 MHz	1.3m Dish -> GPS-locked Octagon LNB -> Aisrpy Receiver	3
Northern Utah WebSDR, Corinne, Utah, U.S.A. - WebSDR #1 (Yellow) - Landing Page http://websdr1.sdrutah.org:8901/ DN31uo; 59 users	0.125 - 0.317 MHz 0.318 - 0.510 MHz 1.708 - 2.092 MHz 0.516 - 2.564 MHz 3.366 - 4.134 MHz 4.816 - 5.584 MHz 6.741 - 7.509 MHz	Omnidirectional E-Field whip at 6.5 Meters TCI 530 Omni Log Periodic	4
WebSDR Maasbree Netherlands (High): rural low noise level, 40m/30m/20m/17m/15m/12m/10m band, CW segments included http://sdh.websdrmaasbree.nl:8902/ JO31ai57; 30 users	6.908 - 7.292 MHz 10.054 - 10.246 MHz 13.983 - 14.367 MHz 18.022 - 18.214 MHz 20.841 - 21.609 MHz 24.844 - 25.036 MHz 27.966 - 28.734 MHz 28.716 - 29.484 MHz	Low noise active receiving loop and GPS locked RX888MKII	5
- Ham - Bordeaux (France) 80m / 40m / 20m / 15m / 10m / 144 MHz / 433 MHz / Es Hail-2 ; QO-100 Satellite geostationnaire 26 Est http://ham.websdrbordeaux.fr:8000/ IN94RP; 44 users	3.408 - 3.792 MHz 6.446 - 7.214 MHz 14.008 - 14.392 MHz 20.866 - 21.634 MHz 27.976 - 30.024 MHz 144.026 - 146.074 MHz 431.996 - 434.044 MHz 10489.400 - 10490.100 MHz	Delta Loop 83m Vector 4000 - 6/8 Diamond X200 - 4*5/8 Parabole 85cm ; Lnb Bullseyes ;	6

Figura 2-9 Nodos del 1 al 6 de la WebSDR. Fuente: websdr.com

Los principales componentes de un nodo WebSDR son [3]:

- Un **receptor SDR** conectado a una antena local.
- Un **PC** con Linux que proporciona:
- **Servidor WebSDR:** software que gestiona la digitalización y transmisión de la señal.
- **Interfaz web** (cliente HTML/JavaScript) para: acceso, control de hardware, visionado de espectrograma, salida audio y, en algunas ocasiones, grabar el audio.

- Una conexión a internet.

Esta red de receptores SDR, configurados inicialmente como el nodo original de Pieter-Tjerk de Boer (PA3FWM) pero que en la actualidad dispone de receptores SDR a medida.

A partir de este modelo han surgido otras implementaciones similares como OpenWebRX [4] y KiwiSDR [5], que amplían las capacidades de administración, registro y acceso remoto mediante APIs REST o *WebSocket*.

Estos sistemas son los precursores de la idea de redes SDR distribuidas, que permiten la captación de señales de manera cooperativa desde múltiples ubicaciones geográficas.

2.2.3 Redes distribuidas de receptores SDR.

A escala global existen centenares de nodos WebSDR y similares interconectados y operados por universidades, radioaficionados y centros de investigación. Su distribución geográfica cubre prácticamente todos los continentes, ofreciendo acceso en tiempo real a bandas que van desde HF hasta SHF [3].

El conjunto de estos nodos constituye una infraestructura distribuida de observación del espectro, con características singulares:

- Cobertura global y redundancia geográfica.
- Diversidad tecnológica de hardware y software.
- Acceso público mediante protocolos web estándar.
- Capacidad de análisis multibanda en tiempo real.

Estas propiedades convierten a las redes WebSDR y similares en entornos distribuidos con potenciales capacidades SIGINT, aunque también presentan limitaciones técnicas y operativas que serán analizadas posteriormente, como ausencia de sincronización temporal precisa, variabilidad de calibración entre nodos y falta de cifrado en las comunicaciones [11].

2.2.4 Aplicaciones de las redes WebSDR y similares.

Los receptores SDR y las plataformas WebSDR y similares posibilitan la recepción y análisis de señales en amplios rangos de frecuencia mediante equipamiento asequible y software de código abierto [6][7].

Estas tecnologías se emplean actualmente en:

- Gestión del espectro radioeléctrico y detección de interferencias.
- Investigación científica en campos como la radioastronomía, meteorología o geolocalización.
- Ciberseguridad e identificación de anomalías en entornos industriales o IoT.

3 ESTADO DEL ARTE.

La arquitectura de las comunicaciones inalámbricas y la vigilancia del espectro electromagnético han experimentado una gran evolución en las últimas décadas, pasando de infraestructuras de hardware rígidas y monolíticas hacia sistemas dinámicos basados en software. Este paradigma, denominado Radio Definida por Software (SDR), ha permitido no solo una mayor flexibilidad operativa en el ámbito militar, sino también la democratización del acceso al espectro a través de redes globales distribuidas.

En el año 2025, el estado del arte se define por la convergencia de receptores SDR accesibles vía web y sistemas profesionales de Inteligencia de Señales que integran de forma nativa inteligencia artificial (IA) y procesamiento en la nube.

3.1 Evolución y estado actual de las redes SDR distribuidas.

El concepto de red SDR distribuida se basa en la premisa de que un receptor físico puede ser compartido por múltiples usuarios a través de una interfaz de red, permitiendo el monitorización remota del espectro sin la necesidad de que el usuario final posea hardware especializado.

Tal y como se adelanto en el apartado 2, el panorama actual está dominado por tres arquitecturas principales: WebSDR, KiwiSDR y OpenWebRX (y su nueva versión OpenWebRX+).

3.1.1 *La Infraestructura de WebSDR y el Modelo de la Universidad de Twente.*

WebSDR, el precursor de los receptores compartidos en línea, mantiene una relevancia crítica debido a su capacidad única de permitir que cientos de usuarios sintonicen frecuencias independientes simultáneamente dentro de una misma banda de paso. Sin embargo, su desarrollo ha sido históricamente centralizado, ya que el creador del software ha limitado la distribución del código del servidor, entregándolo principalmente a radioaficionados que garantizan una conexión a internet de alta velocidad y hardware adecuado para ser listado en el portal centralizado [3].

A pesar de esta restricción, el sitio de la Universidad de Twente continúa siendo el estándar de oro para la monitorización de la banda de onda corta, demostrando que una arquitectura optimizada puede soportar una carga masiva de usuarios sin degradar la calidad de la señal procesada [3].

Actualmente existen receptores desplegados por todo el mundo. A través de la web de la aplicación se puede seleccionar el nodo al que conectarse, de forma gráfica o a través de listado, obteniendo diversos detalles sobre el hardware y software instalado.

En la Figura 3-1 se pueden ver los datos de un nodo SDR que trabaja en dos bandas, con sendos receptores SDR.

 ROMA2 WEBSDR RADIO Italy Rome CB HF VHF UHF http://roma2.sdr.ddns.net/ JN61FW; 9 users	2.866 - 4.914 MHz	Windom (80100) + RSP1	33
	26.831 - 28.879 MHz	Half Wave Vertical Antenna	
 WEB-SDR en Madrid - Spain REM-ESP http://rem-esp.sdrns.org:8901/ IN80BH; 6 users	429.976 - 432.024 MHz		34
	143.976 - 146.024 MHz	RTL-SDR + OSJ Antenna	
	13.026 - 15.074 MHz		
	5.976 - 8.024 MHz	RSP1 + Long Wire	
	2.751 - 4.799 MHz		
	0.000 - 0.096 MHz	Mini-whip like antenna on 4 m well grounded metal pipe, located ~50 m far from any buildings.	
	1.588 - 2.612 MHz	FOOAAA antenna with "High Z" preamp. Antenna is located ~50m far from any buildings - low QRM, great S/N! DSP filters,	
	2.938 - 3.962 MHz	dschuster integration and soon possibility to switch antennas. 24 b/7 FT8	

Figura 3-1 Nodo 34 de la WebSDR (Fuente: websdr.com)

Y como se puede ver en la selección gráfica sobre mapa en la Figura 3-2:

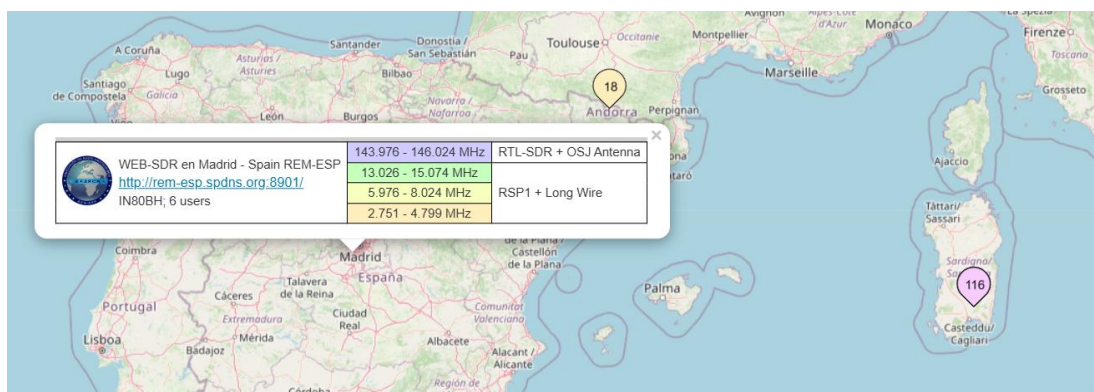


Figura 3-2 Nodo 34 de la WebSDR en mapa (Fuente: websdr.com)

En la figura 3-3 se muestra la interfaz de control de los receptores del nodo.

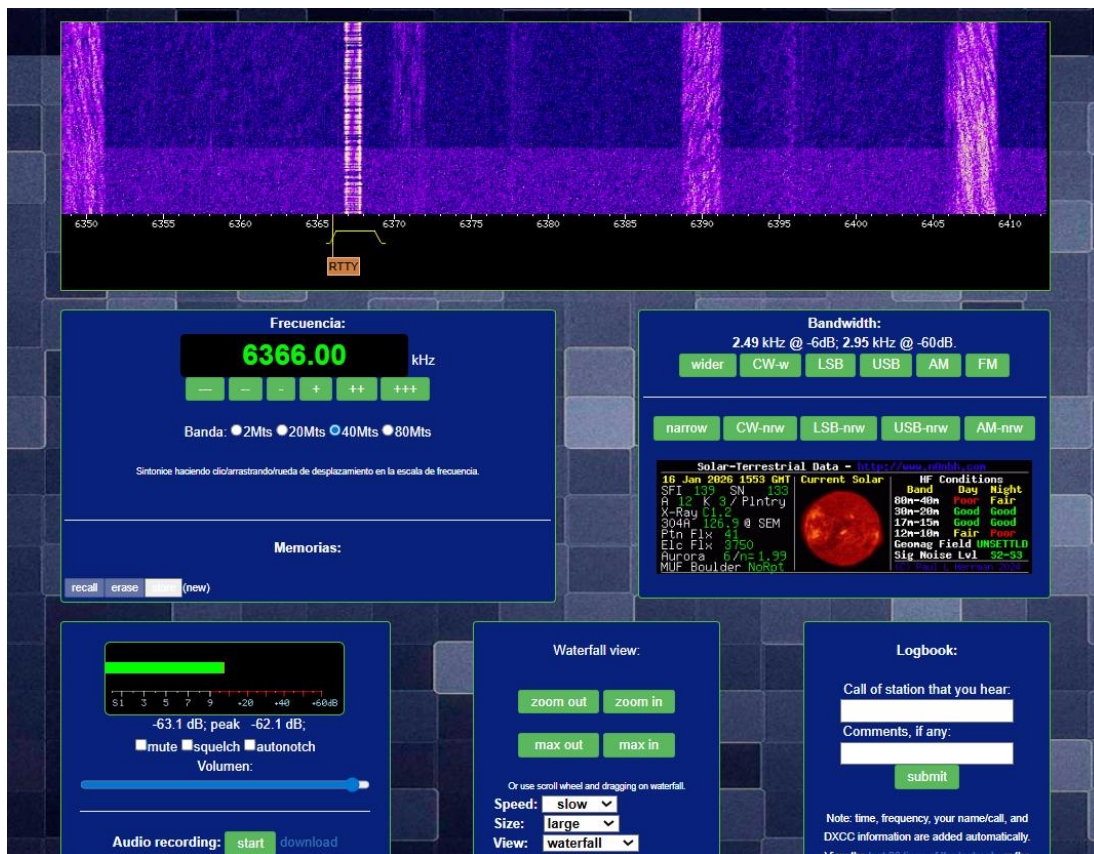


Figura 3-3 Interfaz nodo 34 de la WebSDR. (Fuente: EA4RCR)

3.1.2 KiwiSDR: Hardware Embebido y Sincronización Global.

El receptor KiwiSDR ofrece una solución de hardware "llave en mano" basada en la placa *BeagleBone Black* y un FPGA personalizado. En su versión más reciente para 2025, el KiwiSDR 2 ha introducido mejoras significativas en el diseño físico y la conectividad [5].

La importancia técnica del KiwiSDR radica en su oscilador de cristal disciplinado por GPS (GPSDO) que permite que los receptores de la red KiwiSDR mantengan una sincronización temporal extremadamente precisa. Esta sincronización es lo que facilita la localización de emisores en cualquier parte del mundo mediante técnicas de TDoA (Diferencia de Tiempo de Llegada).

Las interfaces de las aplicaciones WebSDR son muy similares y permiten actuar sobre los típicos parámetros de receptores radio. La red KiwiSDR proporciona una funcionalidad para localizar el emisor. Como se ve en la Figura 3-4, se han seleccionado 5 receptores SDR que muestrean la señal de de forma sincronizada.

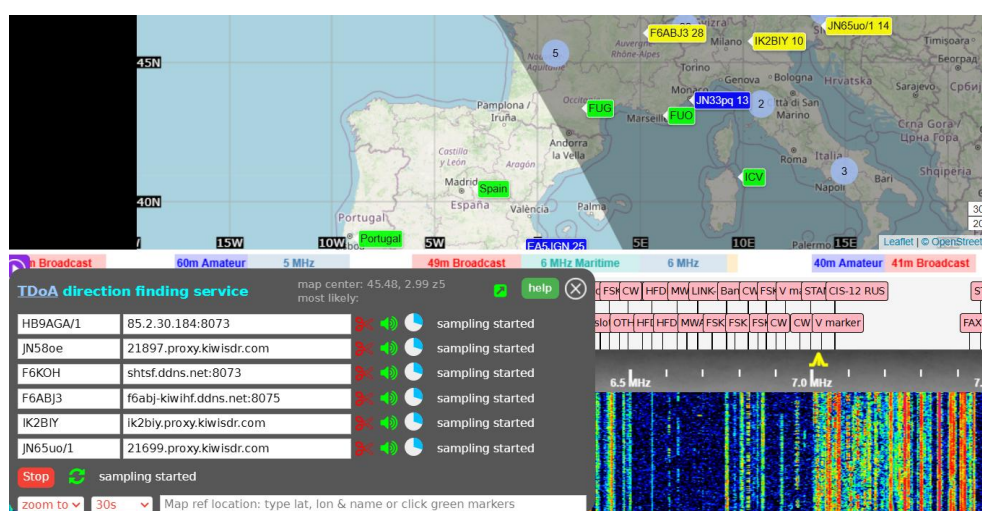


Figura 3-4 Extensión de localización TDoA en KiwiSDR (Fuente: HB9RE)

En la Figura 3-5, se observa cómo se obtienen zonas de probabilidad de ubicación del emisor, señalando las coordenadas aproximadas de la ubicación más probable.

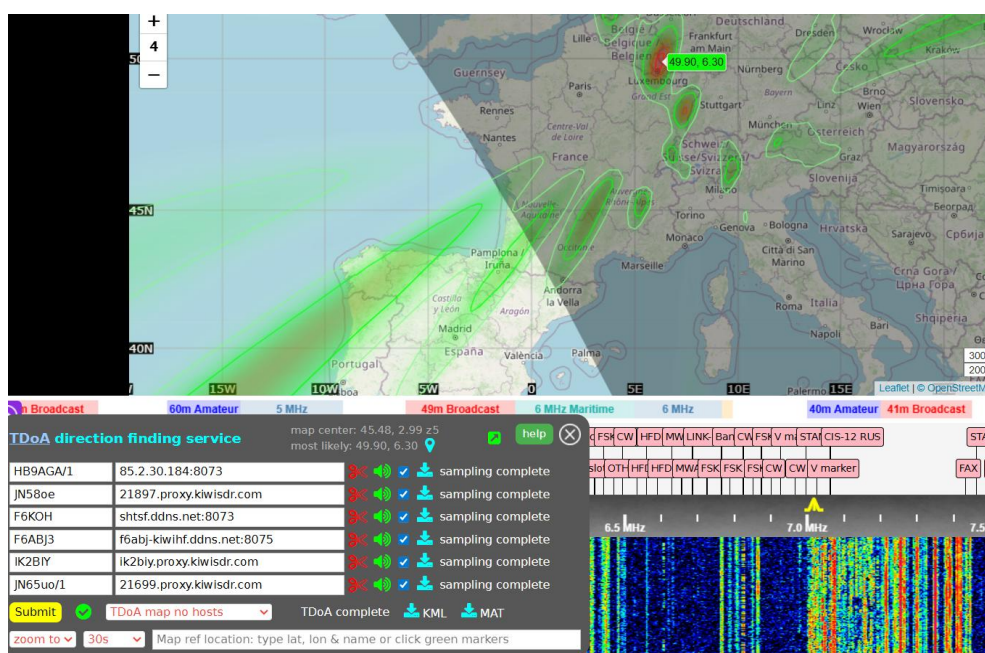


Figura 3-5 Extensión de localización TDoA en KiwiSDR (Fuente: HB9RE)

La Tabla AIII-1 muestra un resumen de las características de los receptores relacionados, de acuerdo a lo indicado en el [Anexo III](#).

Receptor	Rango de Frecuencia	RTBW (Ancho de Banda Instantáneo)	Tasa de Muestreo (Sample Rate)	Resolución ADC	Sensibilidad (MDS/NF)	Rango Dinámico (SFDR/BDR)	Linealidad (IIP3)	Canales y Coherencia	Sincronización (GPS/Clock)
Airspy HF+ Disc.	0.5 kHz - 260 MHz	0.66 MHz	0.768 MSPS	18 bit	-140 dBm MDS	110 dB BDR	+15 dBm	1 Canal	0.5 ppm TCXO
Airspy R2	24 - 1700 MHz	10 MHz	10 MSPS	12 bit	3.5 dB NF	95 dB SFDR	35 dBm	1 Canal	1 RTC / Ext Clock
HackRF One	1 MHz - 6 GHz	20 MHz	20 MSPS	8 bit	-15 dBm (Max in)	~50 dB SFDR	Baja	1 Canal	Ext In/Out
KiwiSDR 2	10 kHz - 30 MHz	30 MHz	66.67 MSPS	14 bit	Alta (Oda. Corta)	Elevado	NO DEFINIDO	4-8 Ch Virt.	GPSDO Integrado
LimeSDR USB	0.1 MHz - 3.8 GHz	61.44 MHz	61.44 MSPS	12 bit	NO DEFINIDO	NO DEFINIDO	LMS7002M	2x2 MIMO	Sync externa
Perseus SDR	10 kHz - 30 MHz	1.6 MHz (I/Q)	80 MSPS	14 bit	-131 dBm MDS	110 dB SFDR	>31 dBm	1 Canal	1 ppm
RTL-SDR V4	0.5 MHz - 1766 MHz	2.56 MHz	2.56 MSPS	8 bit	Mejorada HF	~50 dB SFDR	Superior V3	1 Canal	1 ppm TCXO
SDRplay RSP1B	1 kHz - 2 GHz	10 MHz	10.66 MSPS	14 bit	18 dB NF @2MHz	Elevado	11 Filtros	1 Canal	0.5 ppm TCXO
RSPdx-R2	1 kHz - 2 GHz	10 MHz	10.66 MSPS	14 bit	2.1 dB NF @200M	Mejorado HDR	Alta	1 Canal	Reloj Ext. MCX

Tabla 3-1 Resumen de parámetros técnicos de fabricante (Fuente: elaboración propia)

3.1.5 Iniciativas académicas y experimentales.

Entre los proyectos abiertos más relevantes para el estudio de capacidades SIGINT distribuidas destacan:

- GlobalSDR (MIT, 2019): red experimental de receptores SDR conectados por Internet para el estudio de propagación y tráfico en HF.
- KiwiTDoA Project (2020–2024): red de receptores KiwiSDR empleada para la geolocalización de señales mediante diferencia de tiempo de llegada [24].

Estos proyectos, aunque de naturaleza civil, proporcionan un marco valioso para el desarrollo conceptual de redes SIGINT cooperativas, validando modelos de sincronización, fusión de datos y control remoto de nodos.

3.2 SIGINT.

La Inteligencia de Señales se ha convertido en la piedra angular de la defensa nacional moderna. El mercado global de SIGINT se valoró en 16.8 mil millones de dólares en 2024 y se estima que crecerá a una tasa compuesta anual (CAGR) de más del 5.4% hasta 2034.[25] Otras proyecciones sitúan el tamaño del mercado en 18.51 mil millones de dólares para 2025, alcanzando los 28.51 mil millones en 2033 [25].

El crecimiento del sector SIGINT está impulsado por el aumento de los presupuestos de defensa en las principales potencias mundiales, la proliferación de amenazas cibernéticas y la necesidad de

contrarrestar el terrorismo global. Estados Unidos lidera la inversión, asignando más fondos a defensa que los siguientes 10 países combinados [26].

En Europa, países como España están reforzando sus capacidades navales con sistemas de Indra que detectan señales de radar y comunicaciones en buques de guerra, integrándolos automáticamente con redes de sensores avanzados.

3.2.1 Arquitecturas de Hardware SIGINT de Próxima Generación.

El rendimiento de un sistema SIGINT está intrínsecamente ligado a la capacidad de su hardware para procesar datos IQ a velocidades extremas. La tendencia actual es la adopción de plataformas RFSoc (*Radio Frequency System on Chip*), que integran conversores analógico-digitales (ADC) y digital-analógicos (DAC) directamente en el mismo silicio que la lógica del FPGA y los procesadores ARM.

3.2.2 La Plataforma USRP X410.

El NI Ettus USRP X410 [27] representa el estado del arte en radios definidas por software de alto rendimiento, destacando las siguientes características: Utiliza el SoC Xilinx Zynq UltraScale+ ZU28DR, que proporciona una densidad de canales sin precedentes en un factor de forma de medio rack.

- **Rango de Frecuencia:** Cubre un rango de 1 MHz a 7.2 GHz, sintonizable hasta 8 GHz.
- **Ancho de Banda:** Ofrece 400 MHz de ancho de banda instantáneo por canal a través de sus 4 canales independientes de transmisión y recepción.
- **Procesamiento Interno:** Incluye un subsistema de procesamiento de cuatro núcleos Cortex-A53 a 1.2 GHz y una unidad de tiempo real de doble núcleo Cortex-R5.
- **Conectividad de Datos:** Cuenta con dos puertos QSFP28 capaces de soportar interfaces de 10 GbE, 100 GbE y protocolos Aurora, esenciales para el movimiento masivo de datos IQ hacia sistemas de almacenamiento o análisis externo.

3.2.3 Per Vices Cyan.

El Per Vices Cyan [28][29] se posiciona como la solución COTS (*Commercial Off-The-Shelf*) de mayor rendimiento en el mercado, diseñada específicamente para aplicaciones críticas como guerra electrónica, radar y vigilancia espectral masiva. Utiliza una arquitectura basada en el SoC FPGA Intel Stratix 10, permitiendo una capacidad de procesamiento y una densidad de canales de altas prestaciones.

- **Rango de Frecuencia:** Opera desde casi DC (100 kHz) hasta 18 GHz, con opciones que permiten extender la sintonización hasta 20 GHz, cubriendo un espectro masivo sin necesidad de convertidores externos.
- **Ancho de Banda:** Proporciona un ancho de banda instantáneo estándar de 1 GHz por canal, con una opción de "alto ancho de banda" (Cyan HB) que alcanza los 3 GHz por cadena de radio, soportando hasta 16 canales independientes de transmisión o recepción para una vigilancia persistente del espectro.
- **Procesamiento Interno:** Integra un SoC FPGA Intel Stratix 10 con un procesador ARM Cortex-A53 MPCore, ofreciendo recursos extensivos para DSP a bordo, lo que permite realizar operaciones complejas como *beamforming*, demodulación y análisis de señales en tiempo real directamente en el dispositivo.
- **Conectividad de Datos:** Dispone de un *backhaul* digital masivo a través de 4 puertos ópticos qSFP+, configurables para 4x 40 Gbps (estándar) o actualizables a 4x 100 Gbps (versión HB),

permitiendo un flujo de datos agregado de hasta 400 Gbps hacia sistemas de almacenamiento o procesamiento externos.

3.2.4 Tecnologías de Radiogoniometría y Geolocalización Híbrida.

La localización precisa de un emisor es fundamental para las misiones de los gestores de espectro y las agencias de inteligencia. En 2025, el estándar industrial ha pasado de sistemas que empleaban un solo método de localización a soluciones de geolocalización híbrida que combinan AoA (*Angle of Arrival*) y TDOA (*Time Difference of Arrival*).

El método AoA utiliza arrays de antenas para determinar la dirección de la onda incidente basándose en la fase del frente de onda. Es excelente para señales de banda estrecha o señales no moduladas (CW), pero su precisión disminuye en entornos con múltiples reflexiones [30].

Por el contrario, el TDoA se basa en medir el retraso temporal exacto de una señal recibida en tres o más sitios distribuidos geográficamente. Dado que las ondas electromagnéticas viajan a la velocidad de la luz ($\approx 300,000$ km/s), la precisión del sistema debe estar en el rango de los nanosegundos[30].

3.3 Inteligencia Artificial Aplicada al Análisis de Señales.

El volumen masivo de datos generado por los sistemas SIGINT modernos ha hecho que el análisis manual sea obsoleto. La integración de la IA ha transformado el proceso de "señal a decisión", permitiendo la automatización de tareas de clasificación, detección de anomalías y decodificación [31].

La Clasificación Automática de Modulaciones es un subcampo crítico de la radio cognitiva. Las investigaciones actuales exploran el uso de redes neuronales híbridas que combinan la capacidad de extracción de características locales de las Redes Neuronales Convolucionales (CNN) con la capacidad de modelado de contexto global de los Transformadores (*Transformers*) [31].

Un avance significativo es el uso de la Descomposición Empírica de Modos (EMD) o su versión mejorada BEMD. Al descomponer una señal IQ en sus componentes intrínsecos antes de alimentarla a una CNN, los investigadores han logrado mejorar la precisión de reconocimiento en un 13% en condiciones generales, llegando hasta un 36% en secuencias de datos largas [31].

3.4 Arquitecturas en la Nube y Procesamiento de Big Data para SIGINT.

La escala actual de la vigilancia electrónica requiere infraestructuras de procesamiento de datos que puedan manejar petabytes de información. La integración de herramientas de "Big Data" comerciales en el ámbito militar ha permitido la creación de plataformas de inteligencia escalables y resilientes.

4 ANÁLISIS DE CAPACIDAD SIGINT DE LAS REDES WEBSDR.

Este capítulo analiza la red WebSDR y sistemas SDR similares desde la perspectiva operativa y funcional de la Vigilancia Electrónica (*Electronic Surveillance*) y SIGINT. El objetivo no es sólo describir el hardware y software que disponen los nodos SDR, sino examinar cómo las funciones básicas de un sistema SIGINT/EW —búsqueda, interceptación, identificación y localización— pueden realizarse (o no) sobre una red distribuida de nodos WebSDR, con las necesarias garantías.

Aunque uno de los factores determinantes de la capacidad SIGINT de estas redes son los receptores SDR, no se deben olvidar otros aspectos que también determinan su utilidad en este sentido. Así, se van a analizar aspectos como la distribución geográfica de los nodos, su distribución espectral y otros aspectos que como las condiciones de seguridad, en sus dimensiones principales: confidencialidad, integridad y disponibilidad.

Finalmente, siempre se debe tener en cuenta, a la hora de evaluarlos, que estos equipos no han sido diseñados para la realización de SIGINT/ESM, por lo que difícilmente pueden competir con los modernos sistemas que compañías especializadas fabrican para el ámbito de la seguridad y defensa.

4.1 Cobertura de los nodos SDR.

En este apartado se analizará la cobertura de los nodos SDR de las redes WebSDR, KiwiSDR y OpenWebRX desde dos puntos de vista:

- **Cobertura espectral.** Referida a las bandas de frecuencia en las que los nodos WebSDR operan. No se entra a valorar la mayor o menor cobertura dentro de la banda, sino simplemente que operan en esas bandas, ya que se tratará en detalle en el análisis de los receptores SDR.
- **Cobertura espacial.** En este caso se refiere a la distribución geográfica de los nodos, que condicionará también su capacidad SIGINT.

Para analizar estos parámetros, se ha consultado la web www.receiverbook.de [32], donde están refundidos todos los nodos de las tres redes WebSDR principales. La se puede filtrar el listado por banda de trabajo y/o por red. Los nodos se pueden ver gráficamente sobre un plano o en un listado, mostrando las características principales del nodo.

Cabe destacar, que este tipo de páginas que funcionan a modo de directorio de nodos WebSDR, suelen mostrar sólo los nodos que estén en ese momento conectados a la red, por lo que el número y distribución total podría variar.

4.1.1 Cobertura espectral.

A la vista del estudio de las figuras del Anexo I, se puede observar lo siguiente respecto a las bandas de uso en las tres redes WebSDR analizadas:

- Que el global de nodos está ampliamente distribuido en las bandas VHF e inferiores, mientras que su número se reduce a medida que se aumenta la banda de frecuencia, siendo en SHF inferior a 50 nodos.
- Que la distribución de WebSDR, a pesar de ser la red con menos nodos de las tres, abarca todas las bandas de frecuencias, desde VLF hasta SHF.
- Que en el caso de la red KiwiSDR, la distribución de nodos en las bandas HF e inferiores es la misma³, siendo la red más usada en estas bandas.
- Que la red OpenWebRX tienen gran cantidad de nodos en todas las bandas de frecuencias, hasta SHF. Esta red se puede considerar la más extendida.

Las bandas predominantes en número de nodos son VLF, HF y VHF, por lo que la capacidad de la red se orienta hacia COMINT, permitiendo la monitorización eficaz de comunicaciones vocales y datos de banda estrecha (comunicaciones marítimas, aeronáuticas en ruta y radioaficionados).

Gracias a la excelente cobertura en HF, se facilita la realización de actividades SIGINT de largo alcance, aprovechando la reflexión ionosférica. Sin embargo, en el caso de bandas superiores, donde la visión directa es fundamental, la utilidad de estas redes depende estrictamente de la relativa coincidencia geográfica entre ambos, limitando su uso táctico.

La escasez de nodos que trabajen en frecuencias superiores a 1 GHz hace que estas redes sean menos efectivas para la interceptación de señales procedentes sistemas de comunicaciones de banda ancha, telefonía móvil, comunicaciones satelitales o de señales procedentes de radar, como radares asociados a sistemas de armas.

4.1.2 Cobertura espacial.

En este apartado se vuelven a analizar las imágenes contenidas en el Anexo I, pero en esta ocasión el factor que determinante es la distribución geográfica de los nodos en función de la red que se esté analizando.

De esta forma se puede concluir que:

- Aunque existen nodos en los 5 continentes, su uso es extendido en Europa occidental y América del Norte. En menor medida en América del Sur, Oceanía, Asia y con casi nula presencia en África y Europa oriental.
- La red más extendida geográficamente es KiwiSDR, siendo la única con cobertura global.
- La menos extendida es WebSDR, prácticamente esta acotada a Europa occidental y América.

El disponer de un elevado número de nodos distribuidos contribuye a conseguir una mejor localización de emisores, ya sea mediante técnicas TDoA o mediante triangulación de AoA, donde se

³ Aunque aparecen nodos en el mapa para frecuencias superiores a 30MHz, no es real y cuando uno entra en el nodo sólo permite sintonizar hasta esa frecuencia. Esto es lógico, ya que esta red fue diseñada para emplearla con el receptor KiwiSDR, cuyo sintonizador opera entre 0,1 KHz y 30MHz. Además, la aplicación tampoco permite sintonizar frecuencias superiores a 30 MHz.

requiere de varias estaciones sincronizadas que reciban simultáneamente la misma señal para ubicarla geográficamente.

En las zonas de alta densidad de nodos, la red ofrece una alta disponibilidad, ya que si un nodo queda inoperativo, existen múltiples alternativas cercanas para mantener la vigilancia sobre el objetivo. Esta redundancia operativa no existe en el resto del globo, donde la caída de un nodo único puede significar la pérdida total de cobertura sobre una zona de interés.

Por el contrario, en el caso de África y Europa oriental, zonas con conflictos actualmente activos, la escasa presencia de nodos en bandas de VHF/UHF hace que cualquier actividad electromagnética en estas regiones sea invisible para la red. En HF, aunque la señal puede llegar por reflexión ionosférica a nodos lejanos, se pierde la capacidad de análisis de la onda de superficie.

Por todo lo anterior, la cobertura actual favorece la vigilancia estratégica en tiempos de paz, permitiendo la monitorización de fronteras propias o tráfico marítimo y aéreo global, pero carece de proyección para operaciones expedicionarias en zonas hostiles.

4.2 Capacidades técnicas de recepción aplicadas a las funciones SIGINT/ESM.

4.2.1 Análisis de información técnica de los fabricantes.

En este apartado se procederá a evaluar la capacidad técnica para realizar SIGINT que poseen una serie de receptores relacionados en la Tabla AIII-1. Dados los diferentes requisitos técnicos que deben cumplir los receptores COMINT y ELINT, se analizarán por separado, basándose estrictamente en las especificaciones de las fuentes proporcionadas

Para analizar la capacidad técnica de los receptores SDR, primero se verificarán las características especificadas por los fabricantes, determinando su capacidad en función de lo establecido en la Tabla AIII-11.

Posteriormente, se han creado dos tablas de cuantificación, una para COMINT y otra para ELINT, que definen 5 niveles de idoneidad de cada una de las características técnicas analizadas para SIGINT. Las tablas AII-1 y AII-2 contienen los valores de cuantificación para COMINT y ELINT.

Todas las tablas señaladas anteriormente, así como la justificación de su definición, están detalladas en el Anexo II.

El resultado de aplicar las tablas de cuantificación a la tabla de parámetros técnicos de los receptores nos da una idea de capacidad tiene cada receptor para realizar SIGINT. Aplicando un código de colores, se consigue que a la simple vista de la tabla se obtenga una primera aproximación de la capacidad SIGINT de los receptores. El código de colores empleado es el siguiente:

- **Rojo**: Valores 0 y 1. Capacidad SIGINT nula o baja.
- **Amarillo**: Valores 2 y 3. Capacidad SIGINT media.
- **Verde**: Valores 4 y 5: Capacidad SIGINT alta/excelente.

Receptor	Sens								Ruido		Can		
	RF	RTBW	Sample	POI	NF	SFDR	IIP3	ADC	Fase	Coh	GNSS	I/Q	Interfaz
Airspy HF+ Discovery	2	1	1	4	5	5	3	5	4	1	0	4	2
Airspy R2	4	3	3	4	3	4	5	3	3	2	1	4	2
HackRF One	5	4	4	5	0	1	0	1	2	1	1	4	2
KiwiSDR 2	2	5	5	5	4	4	3	4	5	5	4	5	3
LimeSDR USB	4	5	5	3	1	1	3	3	4	4	2	5	4
Perseus SDR	2	1	5	5	4	5	5	4	3	1	0	4	2
RTL-SDR Blog V4	4	2	2	2	2	2	2	1	3	1	0	4	2
SDRplay RSP1B	4	3	2	2	2	4	3	4	4	1	0	4	2
SDRplay RSPdx-R2	4	3	2	4	4	4	4	4	4	2	2	4	2
USRP B210	5	5	5	5	3	3	2	3	5	4	3	5	4

Tabla 4-1 Valores cuantificados COMINT (Fuente: elaboración propia)

Receptor					Sens			Ruido		Can			
	RF	RTBW	Sample	POI	NF	SFDR	IIP3	ADC	Fase	Coh	GNSS	I/Q	Interfaz
Airspy HF+ Discovery	0	0	0	0	3	3	3	5	4	0	0	3	0
Airspy R2	1	1	1	1	3	3	4	3	3	0	1	3	0
HackRF One	3	2	2	4	0	1	0	1	2	0	1	3	0
KiwiSDR 2	0	3	3	2	2	2	1	4	5	3	4	3	1
LimeSDR USB	2	5	4	2	1	1	2	3	4	3	2	5	2
Perseus SDR	0	0	3	1	2	3	4	4	3	0	0	3	0
RTL-SDR Blog V4	1	1	0	1	1	2	2	1	3	0	0	3	0
SDRplay RSP1B	1	1	0	1	1	2	3	4	4	0	0	3	0
SDRplay RSPdx-R2	1	1	0	2	2	2	3	4	4	1	2	3	0
USRP B210	3	4	4	5	3	3	2	3	4	3	3	5	2

Tabla 4-2 Valores cuantificados ELINT (Fuente: elaboración propia)

Si se observan las Tablas 4-1 y 4-2, se pueden extraer unas consideraciones generales, sin particularizar en modelos y características:

- Los receptores SDR estudiados podrían ser empleados en tareas COMINT, pues los colores verdes y amarillos
- No ocurre lo mismo con estos receptores y su posible empleo para ELINT. En este caso los colores rojo y amarillos son los que mayoritariamente se pueden ver; mientras la mayoría de receptores obtienen puntuaciones medias/altas en COMINT (color verde/amarillo), fracasan sistemáticamente en ELINT (color rojo).
- La principal causa es la falta de *Ancho de Banda Instantáneo* (RTBW) suficiente para capturar pulsos de radar rápidos y a la carencia de *coherencia de fase* necesaria para llevar a cabo una radiogoniometría de precisión.

- Se pueden distinguir entre una gama de receptores “de aficionado” (RTL-SDR, por ejemplo) y otros “semiprofesionales/científicos” (USRP, KiwiSDR, Aircspy) en función de la capacidad SIGINT.

Hay que destacar que es imposible encontrar un receptor que sea adecuado para realizar todas las actividades en COMINT y ELINT, incluso bastante difícil en una de ellas exclusivamente. Hasta los grandes sistemas de EW y SIGINT no emplean receptores “todo tareas”, sino que dependiendo de la función que se pretende realizar, se emplean receptores con las características adecuadas, por lo que el análisis anterior sólo da una visión general. Por ejemplo, los sistemas ELINT disponen de un receptor para la actividad de búsqueda y otro para interceptación, realizando la localización con la conjunción de ambos. Los sistemas COMINT disponen de tres bloques diferenciados para búsqueda, interceptación y localización.

A continuación, se analizará la capacidad técnica aplicada a cada una de las actividades SIGINT/ESM, teniendo en cuenta, no sólo el receptor sino el resto del nodo WebSDR.

4.2.2 Búsqueda.

La actividad de búsqueda en ESM requiere un sondeo sistemático del espectro para descubrir actividad electromagnética, lo que demanda receptores con un alto ancho de banda en tiempo real (RTBW) o, en su defecto, una elevada velocidad de escaneo. Mientras que en el COMINT normalmente se buscan emisiones persistentes, para ELINT el objetivo son a menudo pulsos de radar breves, lo que impone requisitos técnicos mucho más estrictos de Probabilidad de Intercepción (POI) y velocidad de escaneo.

En las redes WebSDR encontramos los nodos basados en KiwiSDR que ofrecen una capacidad de búsqueda excelente en la banda de HF (0-30 MHz). Estos receptores procesan simultáneamente toda la banda, permitiendo una "Probabilidad de Intercepción" (POI) muy alta para señales en esa banda de frecuencias.

En el caso de las bandas de VHF/UHF, la red depende mayoritariamente de dispositivos como el RTL-SDR, cuyo RTBW está limitado a aproximadamente 2.56 MHz. Esto implica que, para cubrir amplios rangos de frecuencia, el sistema debe realizar barridos secuenciales. Si la velocidad de barrido no es suficiente, aumenta el riesgo de no detectar señales de corta duración, pulsadas o con agilidad de frecuencia.

En el caso de ELINT, el valor de Ancho de Banda Instantáneo o de velocidad de escaneo es crítico, ya que habitualmente, las señales procedentes de modernos emisores radar pueden requerir 500 – 1000 MHz para su captación, como es el caso de los radares de apertura sintética que, para resoluciones de 0,5 m., el ancho de banda necesario es de al menos 300 MHz.

Además, la mayoría de los radares modernos de alerta temprana y de control de tiro trabajan en bandas S, C y X (superiores a 3 GHz), por lo que su recepción estaría acotada a los menos de 50 nodos en toda la red global capaces de escuchar en SHF.

Sin embargo, a priori, estas redes son perfectamente válidas para búsqueda a radares OTH en HF o radares de vigilancia aérea antiguos en VHF/UHF.

4.2.3 Interceptación.

La interceptación, incluida entre las actividades ESM, no se limita a la simple escucha, o grabación de la señal, sino que constituye un proceso complejo que abarca desde la digitalización de la señal captada hasta la extracción de toda la información técnica y de contenido posible, incluyendo información de metadatos en comunicaciones, que proporcionen información relevante sobre el funcionamiento de la red de comunicaciones objetivo (corresponsales, jerarquías, patrones horarios...).

Este proceso se divide en dos áreas funcionales bien diferenciadas: la captura y grabación de la señal, y el posterior análisis, decodificación, demodulación y extracción de la información.

Captura y Grabación.

La calidad de la inteligencia obtenida de señales depende de la información deducida y extraída de las capturas realizadas, y por tanto, de la fidelidad con la que se digitaliza la señal en el nodo. Para fines SIGINT, el objetivo es obtener muestras en formato I/Q (Fase y Cuadratura), que preservan toda la información de amplitud y fase de la señal, permitiendo un post-procesado avanzado.

Todos los receptores permiten el acceso al dato crudo (*Raw I/Q*), sin embargo, la arquitectura estándar de las redes WebSDR (como el software original de la Universidad de Twente) está diseñada para optimizar el ancho de banda de internet, enviando al usuario final audio demodulado o espectrogramas visuales comprimidos, en lugar del flujo de datos I/Q completo. Esto representa una limitación severa para la interceptación técnica, ya que impide la aplicación de algoritmos avanzados de recuperación de señal o análisis de fase posterior. Solo iniciativas específicas o configuraciones avanzadas (como ciertas implementaciones de OpenWebRX) permiten la transmisión de I/Q, pero requieren un ancho de banda de red significativo, a menudo inviable para nodos domésticos con conexiones ADSL/4G.

En ELINT, son especialmente críticos los parámetros de velocidad de muestreo (*sample rate*) y la resolución (número de bits) a la hora de reconstruir el pulso radar, que es más demandante a medida que se reduce su duración. A medida que se reduce un pulso, su ancho de banda aumenta y, según el criterio de Nyquist, la velocidad de muestreo debe ser al menos del doble del ancho de banda muestrear; sin embargo, para reconstruir pulsos ELINT, este límite no es suficiente, ya que para no perder detalles de las rampas de subida del pulso que desemboquen en detecciones erróneas, se debe sobremuestrear la señal, siendo lo habitual que la velocidad de muestreo sea de 2.5 veces el ancho de banda. Además, la resolución del ADC, que determina la precisión con la que se mide la amplitud de la señal, es crítica para el rango dinámico y la calidad final de la compresión del pulso. Una mayor resolución (más bits) reduce el ruido de cuantificación, lo que permite al receptor detectar ecos muy débiles incluso en presencia de señales fuertes interferentes, porro que habitualmente se estima en 12 el número mínimos de bits necesario para sistemas ELINT [33].

Según lo expresado en el párrafo anterior, en el caso del receptor el receptor Lime SDR USB[34], cuya tasa de muestreo es de 61,44 MSPS, es capaz de muestrear pulsos de hasta 24.5 MHz de ancho de banda (sobremuestreo de 2,5) o 40,7 ns de duración de pulso (transmitido sin compresión o de pulso comprimido en el caso de radares de compresión de pulso). Esto lo hace insuficiente para los modernos radares, teniendo en cuenta además que su rango de frecuencias superior solo alcanza los 3.8 MHz, inferior a lo deseable.

En cuanto a los parámetros de Resolución y Rango Dinámico, la capacidad de captura varía drásticamente según el hardware empleado como receptor en cada nodo. Los receptores de "de aficionados" (RTL-SDR con ADC de 8 bits) poseen un rango dinámico limitado (~50 dB), lo que provoca que señales débiles de interés queden ocultas por el ruido o por la saturación de emisores comerciales cercanos. Por el contrario, nodos equipados con hardware como KiwiSDR o SDRplay (12-14 bits) ofrecen un rango dinámico superior (>85 dB), permitiendo una captura de alta fidelidad necesaria para distinguir señales complejas en entornos electromagnéticos saturados.

Una carencia crítica de los nodos de redes WebSDR públicas es la ausencia de un buffer de almacenamiento local. En un sistema SIGINT operativo, el sensor graba continuamente en un bucle cerrado (por ejemplo, los últimos 30 segundos) para permitir la recuperación retroactiva de una señal tras una alerta de detección. En la red WebSDR, si el analista no está grabando manualmente en el momento exacto de la emisión, la información se pierde irremediamente, afectando drásticamente a la interceptación de señales LPI (*Low Probability of Intercept*).

Análisis (Clasificación, Demodulación y Decodificación).

Una vez capturada la señal, el sistema debe permitir extraer la información técnica y de contenido. En las redes SDR distribuidas, esta capacidad reside fundamentalmente en el software, realizándose la computación en el servidor del nodo y el navegador del cliente.

En lo que a **demodulación y decodificación** COMINT se refiere, las redes muestran una alta capacidad para tratar con protocolos civiles estándar. Plataformas como OpenWebRX+ han integrado robustas bibliotecas de decodificación (como DSD+ o *direwolf*) que permiten demodular no solo voz analógica (AM/FM/SSB), sino también modos digitales complejos como DMR, P25, YSF, FT8, APRS y protocolos aeronáuticos (ACARS, ADS-B) directamente en la interfaz web. Esto convierte a ciertos nodos en estaciones COMINT muy capaces para la monitorización de comunicaciones no cifradas.

La capacidad disminuye drásticamente en tareas de **clasificación** técnica. A diferencia de los sistemas militares que emplean Inteligencia Artificial para clasificar automáticamente una modulación desconocida o caracterizar un pulso de radar (análisis intrapulso), los nodos WebSDR dependen de la interpretación visual del espectrograma (*waterfall*) por parte del operador humano, o emplear herramientas externas utilizando la captura del canal IQ.



Figura 4-1 Decodificación de llamadas selectiva en OpenWebRX+ (Fuente: fms.komkon.org/OWRX/)

Tal y como se mostró en la Tabla 4.2, la falta de ancho de banda instantáneo y de herramientas de análisis de pulsos impide que la red realice funciones de análisis ELINT (como medir el PRI o el ancho de pulso de un radar), limitando su función analítica casi exclusivamente al ámbito de las señales de comunicaciones.

En cuanto al descifrado, Las redes públicas carecen de capacidades de criptoanálisis. Cualquier señal cifrada (comunicaciones militares seguras, tetra o encriptado, por ejemplo) se percibe meramente como ruido digital, sin posibilidad de explotación de contenido, salvo que se exporte la señal para su tratamiento en sistemas externos dedicados.

4.2.4 Identificación.

El proceso de identificación conlleva la correlación de la información técnica y de contenido obtenida en la fase anterior con información almacenada en Bases de Datos de Referencia (BDR). Estas bases de datos suelen estar clasificadas, por lo que no pueden estar alojadas en cualquier red de datos. Ésta es una de las mayores debilidades de las redes WebSDR públicas. No existe una estandarización en los metadatos de las señales recibidas ni un repositorio centralizado de "firmas" accesible por los nodos para realizar una identificación automática.

4.2.5 Localización.

La localización precisa exige técnicas como la Diferencia de Tiempo de Llegada (TDoA) o el Ángulo de Llegada, las cuales dependen críticamente de la sincronización temporal y la coherencia de fase.

La heterogeneidad del hardware de las redes WebSDR define dos realidades opuestas. Por un lado, gracias a la integración de GPS en los receptores de la red KiwiSDR, los nodos mantienen una sincronización temporal precisa, permitiendo realizar TDoA con éxito global para localizar emisores en HF.

En las redes que trabajan en bandas VHF/UHF, la mayoría de los nodos (RTL-SDR, SDRPlay) carecen de relojes GPS integrados y de arrays de antenas coherentes necesarios para AoA. Por tanto, la localización en estas bandas se limita a estimaciones groseras basadas en la proximidad del receptor a la fuente (RSSI) o a la direccionalidad de antenas rotatorias simples, insuficiente para la geolocalización táctica precisa para fines militares y de inteligencia.

4.3 Almacenamiento de toda la información.

Un sistema SIGINT operativo debe gestionar volúmenes masivos de datos con criterios de seguridad y almacenamiento para consultas posteriores o análisis forense.

En las redes WebSDR actuales, los datos se transmiten en *streaming* y rara vez se almacenan localmente en el nodo, debido a las limitaciones de almacenamiento en los dispositivos anfitriones (generalmente Raspberry Pi o PCs convencionales).

Tampoco existen políticas de retención de datos I/Q, ni mecanismos de indexado de eventos históricos.

Por todo lo expresado anterior, las redes WebSDR no son aptas para SIGINT a menos que se establezca un sistema de almacenamiento con las suficientes medidas de seguridad.

4.4 Análisis de Seguridad.

La capacidad SIGINT de una red no depende solo de la recepción de la señal, sino de la garantía de que la información obtenida es fiable, de que el sistema y la información están disponibles cuando se requiere y de que la propia actividad de inteligencia no es detectada por el adversario. A continuación, se evalúa la seguridad de las redes WebSDR públicas.

4.4.1 Confidencialidad.

La mayoría de los nodos (WebSDR, KiwiSDR, OpenWebRX) están alojados en domicilios particulares o instituciones académicas sin medidas de seguridad física estrictas. Esto permite que un actor malintencionado con acceso físico pueda manipular el hardware o comprometer el sistema operativo.

Gran parte del tráfico de las redes WebSDR tradicionales se transmite mediante protocolo HTTP estándar o WebSockets sin cifrar. Esto expone la información a ataques de *Man-in-the-Middle* (MitM), permitiendo a un observador en la red interceptar el flujo de audio o datos I/Q.

Finalmente, al conectar un terminal propio a un nodo público, la dirección IP del analista y, crucialmente, la frecuencia sintonizada, quedan registradas en los logs del servidor remoto. Aunque tal y como se ha dicho anteriormente, los nodos no suelen almacenar información, el propietario del nodo (o quien tenga acceso a él) puede deducir el interés de la inteligencia sobre los objetivos en seguimiento (frecuencias monitorizadas, localizaciones). Esto constituye una fuga de información que podría alertar al adversario de que sus comunicaciones están siendo vigiladas, vulnerando el principio de confidencialidad de la operación SIGINT.

4.4.2 Integridad.

Una vez se ha producido un ataque MitM, el atacante podría manipular el flujo de datos para que la información técnica y de contenida no corresponda con la realidad. Existe por tanto un riesgo técnico elevado de *Spoofing* o suplantación de señales. Un nodo comprometido podría estar programado para insertar señales fantasmas (objetivos falsos) en el espectro o filtrar frecuencias específicas, entregando una visión distorsionada de la realidad electromagnética al analista, sin que este tenga medios para verificar la autenticidad de la captura en el origen.

Esto permite que un actor malintencionado con acceso físico pueda manipular el hardware (inyectar señales falsas directamente en el cable de antena) o comprometer el sistema operativo (generalmente distribuciones Linux en Raspberry Pi o PCs convencionales) que a menudo carecen de parches de seguridad actualizados o *hardening* militar, por lo que las redes SDR carecen de integridad.

Además, como los nodos no están ubicados en instalaciones propias, carecen de las suficientes garantías de integridad del propio nodo, pudiendo ser dañado.

4.4.3 Disponibilidad.

Por la naturaleza de las redes WebSDR, en la que los nodos son desplegados y mantenidos por personas o entidades voluntarias, no existe un Acuerdo de Nivel de Servicio (SLA).

La disponibilidad está sujeta a fallos de alimentación doméstica, cortes de internet o la simple voluntad del propietario de apagar el equipo, lo cual es inaceptable para operaciones críticas de vigilancia continua.

4.5 Control de configuraciones.

En ningún momento se dispone de control sobre la configuración de los nodos:

- Ubicaciones.
- Receptores empleados.
- Antenas desplegadas y dirección de apuntamiento.
- Software.

Por lo que es muy posible que se dispongan de numerosos nodos con el equipamiento adecuado en zonas donde no se interceptan emisiones de interés, mientras que en otras zonas donde se requiera disponer de sensores, no existan.

5 CONCLUSIONES, PROPUESTA DE DESPLIEGUE Y LÍNEAS FUTURAS.

Tras el análisis técnico y operativo realizado en los capítulos precedentes, se concluye que las redes WebSDR y similares (KiwiSDR, OpenWebRX) presentan una capacidad SIGINT asimétrica y condicionada: asimétrica porque si para COMINT puede ser una herramienta con gran potencial, no lo es tanto para ELINT; condicionada porque depende en gran medida del objetivo sobre el que se quiere extraer información y el nodo seleccionado

Si bien constituyen una herramienta formidable de acceso global al espectro, su utilidad como sistema de inteligencia militar está severamente limitada por restricciones arquitectónicas y de seguridad.

A continuación se detallan las conclusiones específicas sobre su capacidad.

5.1 Conclusiones sobre las redes WebSDR.

Las redes WebSDR públicas actuales constituyen una potente fuente de información complementaria (OSINT/SIGINT) para tareas de instrucción, vigilancia de espectro civil y monitorización estratégica en HF, comunicaciones “tácticas” en bandas VHF y UHF y ciertas señales de no comunicaciones. Sin embargo, tal y como están planteadas actualmente, **no pueden sustituir a los sistemas SIGINT/EW dedicados** debido a su incapacidad para procesar señales radar modernas (ELINT), la falta de acceso a datos crudos (I/Q) y, sobre todo, la ausencia de seguridad operativa.

Para mitigar estas vulnerabilidades, derivadas todas del carácter público de las redes, y aprovechar la capilaridad de esta tecnología, se hace necesario evolucionar hacia un modelo de arquitectura privada, tal y como se introducirá en la propuesta de despliegue.

5.1.1 Herramientas válidas para COMINT, ineficaces para ELINT “moderno”.

Existe una clara dicotomía en la utilidad de estas redes según la disciplina de inteligencia:

- **Capacidad COMINT:** Los receptores analizados demuestran ser eficaces para la interceptación de comunicaciones de voz y datos de banda estrecha. La alta densidad de nodos en las bandas HF, VHF y UHF garantiza una vigilancia eficaz de las comunicaciones marítimas, aéreas y de radioaficionados. La integración de decodificadores digitales en

plataformas como OpenWebRX+ facilita la explotación de protocolos estándar sin necesidad de hardware adicional.

- **Capacidad ELINT:** Las redes públicas carecen de la capacidad técnica mínima para la inteligencia electrónica de radares modernos. Los receptores empleados (tipo RTL-SDR o SDRplay) no disponen del Ancho de Banda Instantáneo (RTBW) necesario para capturar pulsos de radar rápidos ni de la coherencia de fase requerida para el análisis intrapulso.

Por ejemplo, para capturar pulsos de un radar de apertura sintética con una resolución de 0,5 m., el ancho de banda instantáneo del receptor debe ser de 300 MHz y la velocidad de muestreo (con un sobremuestreo de 2,5) debería ser de 750 MSPS, muy por encima de las características de los receptores SDR presentes en las redes WebSDr.

Además, la escasa presencia de nodos en bandas superiores a 3 GHz (bandas S, C, X) hace imposible la detección de la mayoría de radares de control de tiro y alerta temprana.

Por lo tanto, estos receptores son ineficaces ante:

- **Radares sobre plataforma aéreas de combate** (cazas): Como los instalados en los F-16, F-35, Su-35, Eurofighter, Rafale. Casi todos los radares de control de tiro aerotransportados operan en Banda X (8-10 GHz).
- **Radares de Navegación:** Los radares rotatorios típicos de las plataformas navales (Banda X) están fuera de alcance.
- **Control de Tiro de Alta Gama:** quedan fuera de rango sistemas críticos como el radar principal del Patriot (Banda C), los iluminadores del S-300/S-400 (Banda X), y muchos radares de dirección de tiro naval (Banda X/Ku).

5.1.2 ELINT “clásico” posible objetivo.

Aunque tal y como se ha visto, estas redes no son adecuadas para la interceptación de radares modernos, en los que la compresión de pulso es una característica habitual, si que puede ser empleado para ELINT sobre unos determinados tipos de radares, en general, radares con pulsos largos que trabajen en las bandas S-Band (bajo) e inferiores. Por ejemplo, para el receptor Lime SDR USB que se ha puesto de ejemplo en ELINT, los posibles objetivos serían:

- **Radares de Vigilancia Aérea de Largo Alcance** (L-Band / S-Band bajo): Estos se convierten en los objetivos principales, por ejemplo.
- **Radares de Vigilancia Aérea 3D de Largo Alcance.** Suelen operar entre 1.2 GHz y 3.5 GHz, utilizando pulsos largos con compresión moderada, usualmente entre 5 y 20 MHz
- **Radares Navales Multifunción.**
- **Radares de Control de Tráfico Aéreo** (ATC) primarios: Casi todos operan en Banda L o S baja.
- **Radares OTH.**
- **Radares de onda continua.**

5.1.3 Limitaciones críticas en el ciclo de obtención.

El modelo de distribución de datos de las redes WebSDR públicas, diseñado para el consumo de audio por internet de particulares, principalmente, suponen unas limitaciones técnicas insalvables para una explotación SIGINT profunda. De esta forma:

- **Falta de acceso a datos I/Q crudos:** A pesar de que los receptores SDR estudiados si permiten el acceso a este canal, la mayoría de los nodos transmiten audio demodulado o espectrogramas comprimidos para ahorrar ancho de banda. Esto impide al analista realizar

demodulaciones avanzadas, análisis de fase o recuperación de señales ocultas bajo el ruido, limitando la inteligencia obtenida a lo que el demodulador estándar del nodo permite escuchar. Es posible que el nodo óptimo para actuar sobre un objetivo carezca de esta opción, siendo imposible cumplir con la misión.

- **Ausencia de "Buffering" y capacidad forense:** A diferencia de los sistemas EW militares que graban en bucle (buffer circular), permitiendo acceder a toda la transmisión aunque haya transcurrido cierto tiempo hasta que el operador o el sistema detecte actividad, los nodos WebSDR funcionan en tiempo real estricto. Si una señal (especialmente las de baja probabilidad de interceptación o LPI) no es grabada manualmente por el operador en el instante exacto de su emisión, la información se pierde irremediablemente, impidiendo su posterior análisis.
- **Identificación manual:** El sistema, no solo carece de automatización de esta actividad, sino que no dispone de bases de datos de firmas espectrales integradas, obligando a una identificación visual y manual que no es escalable para operaciones de vigilancia continua, o a exportar la información necesaria para correlar con bases de datos externas.

5.1.4 Capacidad de Localización.

La capacidad de localizar emisores es esencial en sistemas SIGINT/ESM, pues de nada sirve identificar un emisor y su plataforma, determinando incluso que es una potencial amenaza, si no puedo geolocalizarla. Esta capacidad en las redes WebSDR públicas es desigual y dependiente de la tecnología del nodo:

- **Excelente en HF (Red KiwiSDR):** Gracias a la integración de GPSDO en los receptores KiwiSDR, la red logra una sincronización temporal precisa que permite realizar geolocalización por **TDofA (Diferencia de Tiempo de Llegada)** a nivel global con gran efectividad en pocos minutos.
- **Ineficaz en VHF/UHF:** La mayoría de nodos en estas bandas carecen de sincronización GPS y de arrays de antenas coherentes. Por tanto, no es posible aplicar técnicas de TDofA ni de AoA con precisión, limitándose la localización a estimaciones groseras por proximidad (RSSI) cuando el nodo dispone de esta capacidad, que tampoco es habitual.

5.1.5 Cobertura Estratégica sin proyección Táctica.

La distribución geográfica de los nodos ofrece una **vigilancia estratégica persistente** en zonas de estabilidad (Europa Occidental, Norteamérica), siendo el sistema ideal para monitorización de fronteras propias o vigilancia del espectro global en HF.

Sin embargo, la red presenta "zonas ciegas" en regiones de conflicto como África y Europa Oriental. Esto invalida su uso como apoyo directo a unidades desplegadas en Zona de Operaciones, donde la cobertura local en V/UHF es imprescindible.

5.1.6 Vulnerabilidad Operativa: Seguridad y Fiabilidad.

Finalmente, se concluye que las redes públicas actuales **no cumplen los requisitos de seguridad** básicos para operaciones SIGINT debido a tres factores críticos analizados en el Capítulo 4:

- **Falta de Confidencialidad:** El uso de la red expone la dirección IP del analista y la frecuencia sintonizada, revelando al adversario los objetivos de interés de la inteligencia propia.
- **Falta de Integridad:** La falta de control sobre el hardware del nodo sobre el que estamos trabajando permite que un actor malintencionado inyecte señales falsas en el nodo, entregando una visión distorsionada del entorno electromagnético (**Riesgo de Spoofing**).

No se puede dejar de lado que alguna nación sobre la que estemos realizando SIGINT a través de este tipo de redes pueda conocer esta situación y despliegue nodos “trampa” (**Honeypots**) para monitorizar nuestra actividad y tratar de deducir nuestros objetivos. Estos nodos también se podrían utilizar para realizar ataque ciber sobre nuestros sistemas locales de operación de nodos WebSDR.

- **Falta de Disponibilidad:** Al depender de voluntarios sin Acuerdos de Nivel de Servicio (SLA), los nodos pueden desconectarse arbitrariamente, no estando garantizado su empleo en momentos críticos.

5.2 Limitaciones del trabajo realizado

El presente estudio se ha desarrollado dentro del marco académico, con un enfoque analítico, técnico y estratégico, sin incorporar una fase experimental sobre red operativa real.

La información sobre cobertura, rendimiento o precisión se ha basado en fuentes abiertas verificadas y en modelos de simulación teóricos.

Tampoco se han abordado en profundidad aspectos de interoperabilidad OTAN ni de integración con sistemas C2 (*Command and Control*), aunque la arquitectura propuesta prevé su inclusión futura.

Finalmente, el análisis de ciberseguridad se ha limitado a la capa TIC de la red, sin extenderse a contramedidas de guerra electrónica activa (ECM) ni ataques electromagnéticos intencionados (EA), que requerirían un marco doctrinal más amplio.

5.3 Propuesta de despliegue.

Partiendo del análisis realizado, donde se ha puesto de manifiesto la falta de seguridad operativa de las redes WebSDR públicas, que además carecen de capacidad técnica para llevar a cabo acciones ELINT avanzadas, se propone el despliegue de una Red WebSDR SIGINT, basada en una arquitectura de red privada.

Esta propuesta está basada en el empleo de nodos sensores propios ("nodos soberanos") gestionados y operados de forma centralizada. A diferencia de la heterogeneidad de la red pública, esta arquitectura estandariza el hardware para garantizar la coherencia de fase, la sincronización temporal y la cobertura de bandas. Además, se prioriza la seguridad operativa, la soberanía del dato y la capacidad de acción en todo el espectro de electromagnético de interés.

5.3.1 Arquitectura del Nodo Sensor.

Basándose en el análisis de capacidades y limitaciones realizado, se propone el despliegue de una red de inteligencia distribuida bajo un modelo de Nube Privada.

La red se estructura en una topología de nodos heterogéneos, adaptando el hardware del sensor al perfil de la misión (estratégica, táctica o encubierta).

5.3.2 Segmento de Captación: Tipología de Nodos Sensores.

Para poder llevar a cabo cometidos COMINT y ELINT, se propone un el despliegue de 3 tipos de nodos empleando hardware COTS, seleccionados por su rendimiento en bandas específicas.

El software para controlar los receptores y elementos sería de desarrollo propio, similar al de las redes WebSDR.

Los nodos podrían contar con hardware adicional para control de antenas, como conmutadores y rotores.

Nodo de Vigilancia COMINT HF.

Este nodo permitiría la interceptación de comunicaciones de largo alcance y la geolocalización global mediante TDoA (Diferencia de Tiempo de Llegada), empleando receptores con sincronización temporal precisa y acceso directo a la banda de HF.

- **Hardware propuesto:** KiwiSDR 2 o WEB-888.
- **Justificación:** Ya se ha estudiado que el receptor KiwiSDR integra un GPSDO que garantizaría el cumplimiento de los cometidos en esa banda. Alternativamente, el receptor WEB-888 [35] se presenta como una evolución capaz de procesar hasta 60 MHz de ancho de banda, cubriendo toda la banda HF y parte de VHF de forma instantánea, en un factor de forma compacto, ideal para despliegues desatendidos. Ambos permitirían la monitorización de múltiples usuarios simultáneos sin degradación de la señal.

Nodo de Vigilancia COMINT V/UHF.

Para la vigilancia de comunicaciones en bandas VHF y UHF, se requiere hardware capaz de operar en configuraciones coherentes de fase para permitir la localización por Ángulo de Llegada (AoA) y soportar anchos de banda suficientes para capturar emisores de corta duración y en saltos de frecuencia.

- **Hardware propuesto:** LimeSDR o Ettus USRP B210.
- **Justificación:** A diferencia de los dongles RTL-SDR básicos, el LimeSDR [34] y el USRP B210 [36] ofrecen arquitecturas MIMO (2x2) y anchos de banda instantáneos de hasta 61.44 MHz. Esto permite implementar arrays de antenas para radiogoniometría y capturar señales de banda ancha que escapan a los receptores convencionales. Además, gracias a su capacidad Full Duplex, permitiendo transmisión, habilita funciones de Ataque Electrónico.

Nodo de Localización.

Para la localización de emisores en banda HF e inferiores, se utilizará la TDoA que proporciona directamente KiwiSDR.

Para las bandas VHF/UHF (baja) se propone el uso de un hardware diseñado específicamente para este fin.

- **Hardware propuesto:** KrakenSDR.
- **Justificación:** Tal y como se ha indicado, este receptor SDR ha sido diseñado específicamente para la localización de emisores[37].

Nodo ELINT.

Para solucionar la principal carencia ya mencionada de los receptores empleados en las redes WebSDR públicas (la incapacidad de capturar señales radar modernas en bandas S, C, X o Ku), se propone un nodo de alto rendimiento que extendería su cobertura hasta esas bandas.

- **Hardware propuesto:** Cyan.
- **Justificación:** Aunque es un receptor de altas prestaciones y coste, comparado con el resto de receptores de la propuesta, su coste es mucho más bajo que los modernos sistema ELINT y cumple con todos los requisitos en un solo equipo.

Las fuentes analizadas caracterizan esta plataforma como una solución de altas capacidades capaz de operar desde 0 Hz hasta 18 GHz, con un ancho de banda instantáneo de 1 GHz por cadena. Esto elimina la necesidad de *down-converters* externos complejos, permitiendo la interceptación directa y el análisis intrapulso de radares de Control de tiro y Sistemas de armas modernos, una capacidad inexistente en la infraestructura WebSDR pública.

En caso de requerir ampliar la cobertura hasta banda superiores (40 GHz), se podrían emplear los *down-converters*.

5.3.3 Segmento de Procesamiento: Edge Computing y Nube

Dado el volumen masivo de datos I/Q generado por los nodos de alto rendimiento (especialmente el nodo ELINT), la transmisión cruda de forma permanente a un centro de datos central es inviable. Para solucionar esto se propone una arquitectura de procesamiento en el borde (*Edge Computing*):

1. **Pre-procesado Local** (Edge): Cada nodo contará con una unidad de cómputo local (basada en FPGA o GPU) encargada de la canalización, demodulación y filtrado inicial. En el caso de señales conocidas (COMINT), solo se transmitirá el audio o los metadatos decodificados. Para ELINT, se emplearán algoritmos de detección de pulsos (PDW - *Pulse Descriptor Words*) en el nodo, enviando al centro de mando únicamente los parámetros del pulso y no el espectro completo.
2. **Fusión en Nube Privada**: Un clúster centralizado recibirá los flujos de datos depurados para ejecutar tareas de alto nivel: correlación TDoA entre nodos dispersos, fusión de datos ELINT/COMINT y alimentación de modelos de Inteligencia Artificial para la clasificación automática de emisores desconocidos.

5.3.4 Segmento de Red y Seguridad.

La interconexión de estos nodos se realizará exclusivamente a través de una Red Privada Virtual (VPN) sobre enlaces satelitales o fibra óptica dedicada. Esta VPN debe ser propietaria y no estar sujeta a servicios de terceros, para garantizar la soberanía de la información. Se debe tener en cuenta el coste temporal de este elemento, que aumenta la latencia y podría afectar búsqueda, interceptación y localización de las señales. Manteniendo la línea “*low cost*” de la propuesta,

En zonas donde sea imposible el empleo de estos soportes de comunicaciones, normalmente en despliegues transfronterizos, se emplearán técnicas que permitan el empleo de Internet con las debidas garantías (Túneles VPN y Terminadores TLS, por ejemplo). Esto garantiza:

- **Confidencialidad**: Se oculta la dirección IP de origen y, lo más importante, se cifra el tráfico de control, impidiendo que terceros conozcan qué frecuencias está sintonizando el centro de inteligencia (mitigando el riesgo de contrainteligencia expuesto en el apartado 4.4.1).
- **Integridad de los datos**: Al controlar físicamente el hardware y lógicamente el canal de comunicaciones, se elimina el riesgo de spoofing o inyección de señales falsas por parte de los administradores del nodo, garantizando la veracidad de la inteligencia obtenida.

En los despliegues en terceros países, se evitará el uso de cifradores o productos que pongan de manifiesto el empleo con fines de Inteligencia.

Con el fin de garantizar la **disponibilidad** del nodo, éste dispondrá de Sistemas de Alimentación Ininterumpida y generadores auxiliares.

5.4 Estrategia de Despliegue Encubierto (Red "Zona Gris").

Aprovechando la naturaleza comercial y el bajo coste de ciertos receptores, comparados con los grandes sistemas ELINT convencionales, se propone una capa de despliegue de "sensores desechables" en zonas de interés que se pueden emplear sin problema en la denominada Zona Gris del espectro de los conflictos [38]⁴.

⁴ Zona Gris: Es el espacio difuso entre la paz y la guerra, donde actores estatales y no estatales usan tácticas no convencionales (económicas, legales, cibernéticas, informativas) para lograr objetivos estratégicos sin llegar a un conflicto militar abierto.

Estos dispositivos, con costes muy inferiores a los sistemas SIGINT/EW convencionales, pueden instalarse en entornos urbanos camuflados como equipamiento informático o puntos de acceso Wi-Fi. Su pérdida o captura no compromete tecnología sensible para la nación.

Su bajo coste permite un despliegue masivo para saturar una zona con sensores de alerta temprana.

5.5 Capacidad de Decepción Electrónica.

Finalmente, la propuesta contempla explotar la capacidad de transmisión que proporcionan los SDR seleccionados para evolucionar hacia una red pasiva (SIGINT) que en caso de necesidad puede evolucionar rápidamente a una red activa (EW) y actuar en apoyo a operaciones militares.

Los nodos pueden configurarse para generar objetivos falsos, simular tráfico de radio para confundir al análisis de tráfico enemigo, realizar spoofing GPS en áreas localizadas e incluso volver a emitir señales interceptadas para confundir a los sistemas enemigos en momentos clave de las operaciones.

Riesgo: Se debe tener en cuenta que el uso de estas funciones activas compromete la posición del nodo, por lo que se recomienda su uso exclusivo en caso de necesidad.

5.6 Líneas futuras.

A partir de los resultados obtenidos, se identifican diversas líneas de trabajo que podrían enriquecer y ampliar el presente estudio:

- Desarrollo detallado de la arquitectura propuesta.
- Desarrollo de un prototipo operativo SIGINT en entorno controlado.
- Integración de capacidades SIGINT y CYBERINT.

Explorar la convergencia entre la inteligencia de señales y la inteligencia cibernética, especialmente en entornos donde las comunicaciones radio y los enlaces IP se superponen (por ejemplo, IoT militar y redes tácticas mesh).

- Extensión hacia la guerra electrónica ofensiva y de apoyo.
 - Estudiar la viabilidad de sensorización masiva del campo de batalla con fines de EW, mediante la instalación de receptores SDR en todos los vehículos bajo el paraguas de una red WebSDR EW, de forma que cada vehículo se convierta en un sensor autónomo mediante *Edge Computing* para autoprotección y contribuyendo a las ESM y SIGINT.
 - Estudiar cómo la información obtenida por la red WebSDR EW puede alimentar sistemas de contramedidas electrónicas (ECM) o de engaño electromagnético (DECM).
 - Estudiar si los equipos SDR de la red WebSDR EW instalados en los vehículos pueden formar ser empleado como inhibidores para EPM.
- Análisis de costes, escalabilidad y sostenibilidad.
 - Realizar estudios de coste-beneficio para definir la viabilidad económica de desplegar una red WebSDR SIGINT basada en SDR, evaluando opciones de mantenimiento, formación, licencias y ciclo de vida del sistema.

5.7 Conclusión final

El presente estudio ha demostrado que, si bien las redes WebSDR públicas actuales ofrecen una cobertura global sin precedentes, carecen de la seguridad operativa y las prestaciones técnicas necesarias —especialmente en ancho de banda y coherencia— para sustituir a los sistemas de inteligencia militar dedicados en el ámbito ELINT. No obstante, la validación de sus excelentes

capacidades para COMINT y geolocalización en HF confirman que el paradigma de recepción distribuida basada en SDR es tecnológicamente maduro. La verdadera oportunidad estratégica no reside, por tanto, en el consumo de la red pública, sino en la adopción de su arquitectura para desplegar una **red soberana de bajo coste**, basada en hardware COTS estandarizado y gestionada bajo un modelo de Nube Privada que garantice la confidencialidad, integridad y disponibilidad del dato de inteligencia.

En definitiva, la implementación de una arquitectura propia permite transformar la "escucha de aficionado" en un **sistema de armas dual**, capaz de integrar la vigilancia persistente pasiva con capacidades avanzadas de **decepción electrónica** en zonas de interés, gracias a la facilidad de ocultación de los nodos. Esta solución híbrida democratiza el acceso a la superioridad electromagnética, permitiendo proyectar capacidades de obtención y negación en escenarios complejos sin la huella logística de los grandes sistemas de EW, alineando así la inteligencia de señales con los requisitos de flexibilidad, escalabilidad y eficiencia económica que exigen los conflictos modernos.

6 BIBLIOGRAFÍA

- [1] J. L. Hernández Garvi, «Muy Interesante,» 22 05 2025. [En línea]. Available: <https://muyinteresante.okdiario.com/historia/evolucion-inteligencia-militar-a-lo-largo-de-la-historia.html>. [Último acceso: 10 09 2025].
- [2] F. Radu, P. A. Cotfas, M. Alexandru, T. C. Bălan, V. Popescu y D. T. Corfas, «Signals Intelligence System with Software-Defined Radio,» *Applied Sciences*, 21 04 2023. [En línea]. Available: <https://www.mdpi.com/2076-3417/13/8/5199>. [Último acceso: 25 10 2025].
- [3] «WebSDR,» [En línea]. Available: <http://websdr.org/>.
- [4] «OpenWebRX Documentation,» OpenWebRX Project, [En línea]. Available: <https://openwebrx.de/>.
- [5] KiwiSDR, «KiwiSDR Operating Information,» KiwiSDR, [En línea]. Available: <http://kiwisdr.com/info/>.
- [6] R. Calvo Palomino, H. Cordobés, M. Engel, M. Fuchs, P. Jain, M. Liechti, S. Rajendran, M. Schäfer, B. Van den Bergh, S. Pollin, D. Giustiniano y V. Lenders, «Electrosense+: Crowdsourcing Radio Spectrum Decoding using IoT Receivers,» *arxiv.org*, 11 05 2020. [En línea]. Available: <https://arxiv.org/pdf/1811.12265>. [Último acceso: 20 10 2025].
- [7] M. B. Perotoni y K. M. G. dos Santos, «SDR-Based Spectrum Analyzer Based in,» *Journal of Microwaves, Optoelectronics and Electromagnetic Applications*, 09 2021. [En línea]. Available: <https://www.scielo.br/j/jmoea/a/TCg4wdgNMmHZVK9TGZKZS8C/?lang=en>. [Último acceso: 30 09 2025].
- [8] J. J. Jordán Enamorado, «Introducción a la inteligencia en el ámbito de seguridad y defensa,» 09 12 2015. [En línea]. Available: <https://www.ugr.es/~gesi/analisis/26-2015.pdf>. [Último acceso: 20 09 2025].
- [9] U.S. Departament of the Army, ADP 2-0. Inteligencia, 2012.
- [10] MADOC, PD1-001 (2ª Ed.). Empleo de las fuerzas terrestres., Ejército de Tierra, 2021.

- [11] MADOC, PD3-308. Inteligencia, Ejército de Tierra, 2014.
- [12] P. Boland, «CyberCOL,» [En línea]. Available: <https://sites.google.com/view/cibercol/tipos-de-osint/tipos-de-osint/sigint>.
- [13] C. Andrew, The Secret World: A history of intelligence, Yale University Press, 2018.
- [14] MADOC, PD3-312. Guerra Electrónica, Ejército de Tierra, 2014.
- [15] U.S. Joint Chief of Staff, JP 2-0. Joint Intelligence, 2013.
- [16] MADOC, PD4-504 (2ª Ed.). Empleo de las unidades de guerra electronica desplegadas, Ejército de Tierra, 2025.
- [17] MADOC, Nota Doctrinal 01/23. Actividades en el ciberespacio y electromagnéticas (CEMA), Ejército de Tierra, 2023.
- [18] MADOC, PR-01. Glosario de términos militares, Ejército de Tierra, 2023.
- [19] D. L. Adamy, EW 104: Electronic Warfare Against a New Generation of Threats, Artech House, 2015.
- [20] Wireless Innovation, «What is a Software Defined Radio?,» [En línea]. Available: https://www.wirelessinnovation.org/Introduction_to_SDR. [Último acceso: 20 08 2025].
- [21] D. García gómez, J. M. Riera Salís y P. García del Pino, «Implementación y configuración de un receptor de radio definido por software (SDR) para estudios de propagación,» Universidad Politécnica de Madrid, 2012. [En línea]. Available: https://oa.upm.es/22874/1/INVE_MEM_2012_153627.pdf.
- [22] M. Tábara Carbajo, «Radiocomunicaciones con radio definida por software y GNU Radio,» Universidad de Valladolid, 2023. [En línea]. Available: <https://uvadoc.uva.es/bitstream/handle/10324/50027/TFG-G5208.pdf>.
- [23] «OpenWebRX+ Feature Report,» [En línea]. Available: <https://websdr.nikdale.me/features>.
- [24] RTL-SDR.COM, «KiwiSDR TDoA Direction Finding Now Freely Available for Public Use,» RTL-SDR.COM, 07 2018. [En línea]. Available: <https://www.rtl-sdr.com/kiwisdr-tdoa-direction-finding-now-freely-available-for-public-use/>.
- [25] Global Market Insights, «Signal Intelligence Market Size,» Global Market Insights, 02 2025. [En línea]. Available: <https://www.gminsights.com/industry-analysis/signals-intelligence-sigint-market>.
- [26] The Business Research Compan, «Signals Intelligence (SIGINT) Market Report 2025,» The Business Research Compan, 02 2025. [En línea]. Available: <https://www.researchandmarkets.com/reports/5767367/signals-intelligence-sigint-market-report>.
- [27] Ettus Research, «USRP X410,» Ettus Research, [En línea]. Available: <https://www.ettus.com/all-products/usrp-x410/>.
- [28] Per Vices, «Using SDRs for Signals Intelligence (SIGINT),» Microwave Product Digest (MPD), 2022. [En línea]. Available: <https://www.mpdigest.com/2022/08/22/using-sdrs-for-signals-intelligence-sigint/>.
- [29] Per Vices Corporation, «CYAN TECHNICAL SPECIFICATIONS,» Per Vices Corporation, [En línea]. Available: <https://www.pervices.com/wp-content/uploads/2021/10/pervices-tm-cyan>

datasheet.pdf.

- [30] Rohde&Schwarz, «TDOA and AOA hybrid geolocation systems,» Rohde&Schwarz, [En línea]. Available: https://www.rohde-schwarz.com/de/loesungen/critical-infrastructure/spectrum-monitoring/tdoa-and-aoa-hybrid-geolocation-systems_232792.html.
- [31] A. Gros, V. Moeyaert y P. Mégret, «Signal Surface Augmentation for Artificial Intelligence-Based Automatic Modulation Classification,» MDPI, 03 12 2025. [En línea]. Available: <https://doi.org/10.3390/electronics14234760>.
- [32] «Receiver Book,» [En línea]. Available: <https://www.receiverbook.de/>. [Último acceso: 01 10 2025].
- [33] J. Grajal de la fuente y F. Pérez Martínez, «ESM en Sistemas de No Telecomunicaciones,» de *I Curso Avanzado de EW*, Academia de Ingenieros del Ejército / Escuela Politécnica de Madrid, 2005.
- [34] Lime microsystems, «LimeSDR USB,» Lime microsystems, 2019. [En línea]. Available: <https://limemicro.com/sdr/limesdr-usb/>.
- [35] Rx-888, «Web-888 SDR,» Rx-888, [En línea]. Available: <https://www.rx-888.com/web/>.
- [36] Ettus Research, «B200-B210_spec_sheet.pdf,» Ettus Research, [En línea]. Available: https://www.ettus.com/wp-content/uploads/2019/01/b200-b210_spec_sheet.pdf.
- [37] Passion-Radio.com, «KrakenSDR 5-channel receiver for direction finding and radio triangulation,» Passion-Radio, [En línea]. Available: <https://www.passion-radio.com/sdr-receivers/kraken-sdr-3012.html>.
- [38] A. Rodriguez Gómez, «Conflictos en la zona gris: la nueva amenaza universal,» European Public & Social Innovation Review, 17 02 2025. [En línea]. Available: <https://doi.org/10.31637/epsir-2025-1603>.
- [39] F. Pérez Martínez, «ESM en Sistemas de Comunicaciones,» de *I Curso Avanzado de EW*, Academia de Ingenieros del Ejército / Escuela Politécnica de Madrid, 2005.
- [40] R. A. Poisel, *Electronic Warfare Receivers and Receiving Systems*, Artech House, 2014.
- [41] Avionics Department, *Electronic Warfare and Radar Systems - Engineering Handbook*, Naval Air Warfare Center Weapons Division, 2013.
- [42] AirSpy, «Try our Award Winning HF/VHF Receiver!,» AirSpy, [En línea]. Available: <https://airspy.com/airspy-hf-discovery/>. [Último acceso: 2025].
- [43] Shoc, «AirSpy HF+ / R2/ Mini HF/VHF/UHF,» Shoc, [En línea]. Available: <https://www.shoc.ch/airspy.html>. [Último acceso: 2026].
- [44] AirSpy, «The dependable VHF/UHF Radio for your projects,» AirSpy, [En línea]. Available: <https://airspy.com/airspy-r2/>. [Último acceso: 2025].
- [45] HackRF, «Hardware Components,» HackRF, 2021. [En línea]. Available: https://hackrf.readthedocs.io/en/latest/hardware_components.html.
- [46] HackRf Wiki, «HackRF-One.md,» GitHub, [En línea]. Available: <https://github.com/dodgymike/hackrf-wiki/blob/master/HackRF-One.md>.
- [47] Great Scott Gadgets, «HackRF One,» Great Scott Gadgets, [En línea]. Available:

- <https://greatscottgadgets.com/hackrf/one/>. [Último acceso: 2025].
- [48] KiwiSDR, «SDR comparison,» KiwiSDR, [En línea]. Available: <http://kiwisdr.com/ks/compare.1.1.pdf>. [Último acceso: 01 10 2025].
- [49] J. Seamons, «KiwiSDR design review,» KiwiSDR, 02 2016. [En línea]. Available: <http://kiwisdr.com/docs/KiwiSDR/KiwiSDR.design.review.pdf>. [Último acceso: 09 2025].
- [50] KiwiSDR, «KiwiSDR: Wide-band SDR + GPS cape for the BeagleBone Black,» KiwiSDR, 08 01 2026. [En línea]. Available: <http://www.kiwisdr.com/>. [Último acceso: 08 01 2026].
- [51] MyriadRF, «LimeSDR-USB,» MyriadRF, 2019. [En línea]. Available: <https://wiki.myriadrf.org/LimeSDR-USB>.
- [52] MicroTelecom, «Perseus Receiver User Manual,» MicroTelecom, [En línea]. Available: https://www.microtelecom.it/get-file?path=microtelecom%2FPerseus%2FUser_manuals%2Fperseususermanual-en14.pdf. [Último acceso: 2025].
- [53] RTL-SDR Blog, «RTL-SDR Blog V4 Dongle Initial Release!,» RTL-SDR Blog, 16 08 2023. [En línea]. Available: <https://www.rtl-sdr.com/rtl-sdr-blog-v4-dongle-initial-release/>.
- [54] RTL-SDR Blog, «RTL-SDR Blog V4 Datasheet,» RTL-SDR Blog, 2024. [En línea]. Available: https://www.rtl-sdr.com/wp-content/uploads/2024/12/RTLSDR_V4_Datasheet_V_1_0.pdf.
- [55] Lichfield Radio Astronomy Observatory, «Comparison between the RTL-SDR Blog V3 and RTL-SDR Blog V4,» Lichfield Radio Astronomy Observatory, 04 10 2025. [En línea]. Available: <https://www.astronomy.me.uk/comparison-between-the-rtl%E2%80%91sdr-blog-v3-and-rtl%E2%80%91sdr-blog-v4>. [Último acceso: 02 12 2025].
- [56] SDRPlay, «RSP1B,» SDRPlay, 2024. [En línea]. Available: <https://www.sdrplay.com/rsp1b/>.
- [57] RigPix, «RSP1B,» RigPix, 2024. [En línea]. Available: https://www.rigpix.com/miscrx/sdrplay_rsp1b.htm.
- [58] SDRPlay, «RSPdx-R2,» SDRPlay, 2024. [En línea]. Available: <https://www.sdrplay.com/rspdxR2/>.
- [59] RigPix, «SDRplay RSPdx R2,» RigPix, 2024. [En línea]. Available: https://www.rigpix.com/miscrx/sdrplay_rspdxr2.htm.
- [60] KrakenRF Inc., «KrakenSDR,» KrakenRF Inc., 2022. [En línea]. Available: <https://www.krakenrf.com/product-page/krakensdr>.
- [61] Mouser Electronics, «KrakenRF Software Defined Radio,» Mouser Electronics, 13 06 2024. [En línea]. Available: <https://www.mouser.es/new/krakenrf/krakenrf-software-defined-radio/>.

7 ANEXO I: DISTRIBUCIÓN DE NODOS WEBSDR.

En este anexo se muestra la distribución de los nodos de las tres principales redes WebSDR en las bandas de frecuencia de HF, VHF, UHF y SHF.

En primer lugar se muestra la imagen de todos los nodos de las redes analizadas en todas las bandas de frecuencia.



Figura AI-1 Distribución de nodos SDR (Fuente: receiverbook.de [32])

7.1 WebSDR.



Figura AI-2 Distribución de nodos HF WebSDR (Fuente: receiverbook.de [32])



Figura AI-3 Distribución de nodos VHF WebSDR (Fuente: receiverbook.de [32])



Figura AI-4 Distribución de nodos UHF WebSDR (Fuente: receiverbook.de [32])



Figura AI-5 Distribución de nodos SHF WebSDR (Fuente: receiverbook.de [32])

7.2 KiwiSDR.



Figura AI-6 Distribución de nodos HF KiwiSDR (Fuente: receiverbook.de [32])



Figura AI-7 Distribución de nodos VHF KiwiSDR (Fuente: receiverbook.de [32])



Figura AI-8 Distribución de nodos UHF KiwiSDR (Fuente: receiverbook.de [32])



Figura AI-9 Distribución de nodos SHF KiwiSDR (Fuente: receiverbook.de [32])

7.3 OpenWebRx.



Figura AI-10 Distribución de nodos HF OpenWebRx (Fuente: receiverbook.de [32])



Figura AI-11 Distribución de nodos VHF OpenWebRx (Fuente: receiverbook.de [32])



Figura AI-12 Distribución de nodos UHF OpenWebRx (Fuente: receiverbook.de [32])



Figura AI-13 Distribución de nodos SHF OpenWebRx (Fuente: receiverbook.de [32])

8 ANEXO II: CRITERIO DE EVALUACIÓN DE RECEPTORES SDR

La metodología de evaluación se basa en un análisis de "caja negra" en base a los parámetros técnicos proporcionados por fabricantes o distribuidores de los receptores SDR comúnmente utilizados en las redes WebSDR.

El proceso comienza con la definición de parámetros críticos para, posteriormente, definir una matriz de cuantificación que asigna a cada parámetro una puntuación de 0 a 5 en función de su valor para determinar su contribución a la capacidad SIGINT del receptor.

8.1 Parámetros técnicos considerados.

Las características técnicas que se van a evaluar de los receptores SDR desplegados en redes WebSDR y similares para determinar su capacidad SIGINT son los siguientes [39][33][28][40][41]:

- **Rango de Frecuencia** (Cobertura): Es la porción de espectro electromagnético que el receptor puede sintonizar (ej. 8 KHz a 40 GHz). Determina las bandas y el tipo de emisores que puede interceptar, desde comunicaciones navales VLF hasta radares de ondas milimétricas Ka.
- **Ancho de Banda en Tiempo Real** (RTBW): El ancho de banda máximo que el receptor procesa de forma instantánea y continua. Es vital en exploración o búsqueda de emisiones y permite capturar señales de baja probabilidad de interceptación (LPI) y radares con agilidad de frecuencia que saltan dentro de una banda ancha.
- **Velocidad de Escaneo** (*Scan*): Es la velocidad a la que el receptor recorre el espectro electromagnético, medida en Hz/s. En SIGINT, la velocidad determina la capacidad de dominar el espectro y encontrar emisores esporádicos o de corta duración.

Nota: En los receptores modernos que tienen gran ancho de banda en tiempo real, este valor no tiene importancia, pues incluso pueden llegar a observar toda la banda de forma simultánea, sin necesidad de desplazar la sintonía del receptor. Este valor se tendrá en cuenta en casos en los que se tiene un RTBW bajo respecto a la Cobertura, pues en ese caso, para explorar toda la banda, la velocidad a la que el receptor recorre toda la banda si determina ciertas capacidades SIGINT/EW.

- **Frecuencia o Tasa de Muestreo** (*Sample Rate*): Es el número de muestras del ADC por unidad de tiempo. En COMINT permite analizar señales complejas y en ELINT permite medir con precisión parámetros de interpulsos e intrapulso de radar.
- **Probabilidad de Intercepción** (POI): Es la probabilidad de detectar una señal basándose en su duración mínima. Por ejemplo: 100% POI para señales de 75 ns. Los radares modernos usan pulsos extremadamente cortos; si el receptor no garantiza una POI alta, estas amenazas pasarán desapercibidas.
- **Sensibilidad** (MDS) y **Figura de Ruido** (NF): Es la capacidad para detectar señales débiles. Está limitada por el ruido térmico y el ruido añadido por el propio receptor. Una NF baja permite interceptar emisores lejanos o de baja potencia que de otro modo quedarían ocultos en el ruido.
- **Rango Dinámico Libre de Espurias** (SFDR): Es la diferencia entre el nivel mínimo de señal detectable y el nivel donde aparecen distorsiones de intermodulación (IMD3). Este parámetro es crucial en entornos electromagnéticos saturados (por ejemplo, zonas costeras o campos de batalla); evita que señales potentes cercanas generen señales "fantasmas" que enmascaren señales de interés débiles.
- **Linealidad** (IIP3): Es el punto de intercepción de tercer orden referido a la entrada; mide la tolerancia a la distorsión por señales fuertes. Define la robustez del receptor ante interferencias co-localizadas (como radares propios o torres 5G cercanas).
- **Resolución del ADC y Número Efectivo de Bits** (ENOB): La primera es el número de bits por muestra digitalizada. Este parámetro determina la capacidad de extraer contenido de señales débiles junto a señales fuertes.
- El ENOB es un indicador de la "verdadera" resolución de un digitalizador, reflejando la calidad de la señal más allá de su especificación nominal de bits reales tras considerar ruido y jitter. Por ejemplo, un ADC de 14 bits con un ENOB bajo perderá fidelidad en señales complejas de banda ancha.
- **Ruido de Fase** (*Phase Noise*): Estabilidad a corto plazo del oscilador local que afecta la pureza de la señal mezclada. Un ruido de fase elevado provoca "mezcla recíproca", donde una señal fuerte cercana ensancha su base y oculta señales débiles adyacentes.
- **Número de Canales y Coherencia de Fase**: Es la cantidad de rutas de recepción paralelas que mantienen la relación de fase exacta entre sí. Es el requisito para realizar Radiogoniometría (DF – *Direction Finding*) y localización precisa mediante técnicas de Ángulo de Llegada (AoA – *Angle of Arrival*).
- **Sincronización GNSS** (Time-Stamping): Es la capacidad de sincronizar el reloj con un patrón de tiempos (GPS/Galileo) y de estampar marcas temporales ultra precisas en los datos capturados. Este parámetro es indispensable para la localización multi-plataforma mediante Diferencia de Tiempo de Llegada (TDoA – *Time Difference of Arrival*) entre receptores geográficamente separados.
- **Acceso a I/Q**. Disponibilidad de muestras complejas en fase y cuadratura para post procesado. Esencial para demodulación avanzada y clasificación de señales en SIGINT.
- **Interfaz de Datos y Throughput** (*I/Q Streaming*): Es la capacidad del receptor de volcar datos digitales (IQ – *In-phase/Quadrature*) a la red (procesadores externos o FPGAs). En arquitecturas de muestreo directo, el flujo puede superar los 500 Gbit/s; la interfaz determina si el sistema puede analizar toda la banda capturada por el receptor o si debe descartar datos.

Estos parámetros permiten caracterizar de forma integral la capacidad del receptor SDR para detectar, interceptar, identificar y localizar emisiones electromagnéticas.

8.2 Tabla de Cuantificación.

Para transformar las especificaciones técnicas en datos comparables, se establece a continuación una Tabla de Cuantificación de Variables. Este marco de valoración asigna una puntuación objetiva del 0 al 5 a cada parámetro, en función de su valor.

Esta escala permite medir el rendimiento absoluto de cada receptor SDR, clasificando desde dispositivos básicos de bajo coste —comunes en redes como OpenWebRX— hasta sistemas de alto rendimiento y muestreo directo. La cuantificación es el paso previo esencial para normalizar las capacidades del hardware antes de aplicar los criterios de prioridad según la misión específica.

Dado que los requisitos de los receptores COMINT y ELINT no son los mismos, se definirá una tabla de cuantificación para medir la capacidad COMINT y otra para medir la capacidad ELINT.

Para una mejor comprensión, los valores de las tablas, una vez aplicados a los datos técnicos de los receptores, se agruparan de la siguiente forma:

- 0-1: Capacidad SIGINT baja (color rojo).
- 2-3: Capacidad SIGINT media (color amarillo).
- 4-5: Capacidad SIGINT alta (color verde).

Una vez se aplique la matriz de cuantificación a la tabla con características técnicas de los fabricantes y al objeto de una mejor compresión gráfica, las celdas se colorearan según el código indicado.

8.2.1 Tabla de cuantificación COMINT.

El enfoque prioritario para COMINT es el rango dinámico, la resolución de bits y la linealidad para extraer información de señales de voz o datos en entornos ruidosos.

De esta forma, el éxito depende de la capacidad de detectar y muestrear señales débiles junto a otras muy potentes, lo que exige un ADC de alta resolución (14-18 bits) y un SFDR elevado (>100 dB) para evitar que las espurias enmascaren la comunicación.

Parámetro	1	2	3	4	5
Rango de Frecuencia	Solo una banda	< 500 MHz	< 1.5 GHz	< 3 GHz	> 6 GHz
RTBW (Ancho de Banda)	< 1 MHz	1 - 5 MHz	5 - 10 MHz	10 - 25 MHz	> 25 MHz
Tasa de Muestreo	< 2 MSPS	2 - 10 MSPS	10 - 30 MSPS	30 - 60 MSPS	> 60 MSPS
POI (Prob. Intercep.)	Muy baja	Baja	Moderada	Alta	Persistente (Banda completa)
Sensibilidad (MDS)	> -100 dBm	-100 a -115 dBm	-115 a -125 dBm	-125 a -135 dBm	< -135 dBm
SFDR (Rango Dinámico)	< 50 dB	50 - 70 dB	70 - 85 dB	85 - 100 dB	> 100 dB
Linealidad (IIP3)	< -20 dBm	-20 a 0 dBm	0 a +15 dBm	+15 a +30 dBm	> +30 dBm
Res. ADC / ENOB	8 bit / < 7	10 bit / ~9	12 bit / ~10.5	14 bit / ~12.5	16-18 bit / > 14

Ruido de Fase	No definido	>1ppm	Bueno 1 ppm	0.5 ppm	Ultra bajo (TCXO/GPSDO)
Canales / Coherencia	1 Canal	1 Canal (ext. clk)	2 Canales	2 Canales (Coherente)	> 4 Canales (Coherente)
Sincronización GNSS	Ninguna	Solo externa	Soporta GPSDO	GNSS Integrado	Estampado de tiempo nanoseg.
Acceso a I/Q	No disponible	Solo audio	IQ limitado	IQ Completo	IQ Full (Multi-streaming)
Interfaz / Throughput	USB 2.0 (Lento)	USB 2.0 (Fast)	Ethernet 100M	USB 3.0 / GigE	Fibra / > 5 Gbps

Tabla AII-1 Criterios para evaluación cuantitativa de receptores en COMINT (Fuente: Elaboracion propia)

8.2.2 Tabla de cuantificación ELINT.

En el caso de ELINT, los parámetros claves son io es el Ancho de Banda en Tiempo Real, la Probabilidad de Intercepción y la Tasa de Muestreo permitiendo la captura de pulsos de corta duración.

Parámetro	1	2	3	4	5
Rango de Frecuencia	< 30 MHz	< 1.7 GHz	< 3.8 GHz	< 6 GHz	> 18 GHz
RTBW (Ancho de Banda)	< 2 MHz	2 - 10 MHz	10 - 30 MHz	30 - 60 MHz	> 60 MHz
Tasa de Muestreo	< 10 MSPS	10 - 25 MSPS	25 - 50 MSPS	50 - 100 MSPS	> 100 MSPS
POI (Prob. Intercep.)	Casual	Por barrido lento	Por barrido rápido	Salto de frec.	Intercep. Pulso Único
Sensibilidad (NF)	> 20 dB	15 - 20 dB	10 - 15 dB	5 - 10 dB	< 5 dB
SFDR (Rango Dinámico)	< 45 dB	45 - 55 dB	55 - 70 dB	70 - 80 dB	> 80 dB
Linealidad (IIP3)	< -30 dBm	-30 a -15 dBm	-15 a 0 dBm	0 a +15 dBm	> +15 dBm
Res. ADC / ENOB	< 8 bit	8 bit / ~7	10 bit / ~9	12 bit / ~11	14-16 bit / > 12
Ruido de Fase	> 10 ppm	5 - 10 ppm	1 - 5 ppm	0.5 - 1 ppm	< 0.5 ppm (GPSDO)
Canales / Coherencia	1 RX	1 RX (ext. ref)	2 RX (MIMO)	2 RX (Coherente)	Array Coherente (>4)
Sincronización GNSS	Ninguna	NTP/Software	PPS Externo	GPSDO Opcional	GPSDO Integrado/Rubidio
Acceso a I/Q	No disponible	Filtrado	Muestras brutas	Streaming total	Acceso a FPGA/VHDL
Interfaz / Throughput	USB 2.0	Ethernet 1G	USB 3.0	PCIe / 10 GigE	QSFP / > 40 Gbps

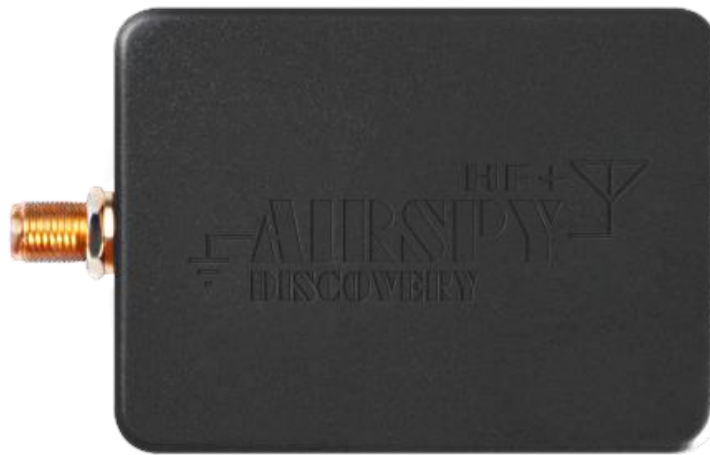
Tabla AII-2 Criterios para evaluación cuantitativa de receptores en ELINT (Fuente: Elaboracion propia)

9 ANEXO III: CARACTERÍSTICAS DE RECEPTORES SDR ANALIZADOS

A continuación se rellenará una ficha con los parámetros relacionados en el apartado 10.1 del Anexo I para cada uno de los siguientes receptores:

Receptor
Airspy HF+ Disc.
Airspy R2
HackRF One
KiwiSDR 2
LimeSDR USB
Perseus SDR
RTL-SDR Blog V4
SDRplay RSP1B
SDRplay RSPdx-R2

Tabla AIII-1 Receptores a analizar (Fuente: Elaboracion propia)

AirSpy HF+ Discovery [42][43]**Figura AIII -1 AirSpy HF+ Discovery (Fuente: airspy.com)**

Parámetro	Detalle
Rango de Frecuencia	0.5 kHz - 31 MHz / 60 MHz - 260 MHz
Ancho de Banda (RTBW)	660 kHz (libre de alias)
Velocidad de Escaneo	NO DEFINIDO
Tasa de Muestreo	0.768 MSPS (Salida IQ)
POI	NO DEFINIDO
Sensibilidad (MDS) / NF	-140.0 dBm (HF) / -141.5 dBm (VHF)
SFDR	110 dB (HF) / 95 dB (VHF)
Linealidad (IIP3)	+15 dBm (HF) / +13 dBm (VHF)
Resolución ADC / ENOB	18 bits / 18 bits (DDC interno)
Ruido de Fase	-110 dBc/Hz @ 1kHz (100 MHz)
Canales / Coherencia	1 Canal / No nativa
Sincronización GNSS	Ajuste de frecuencia 1 PPB (No sincronización GNSS interna)
Acceso a I/Q	Sí
Interfaz y Throughput	USB 2.0 / 480 Mbps
Precio aproximado	250 €

Tabla AIII -2 Datos técnicos AirSpy HF+ Discovery (Fuente: Elaboracion Propia)

AirSpy R2 [43] [44]

Figura AIII -2 AirSpy R2 (Fuente: airspy.com)

Parámetro	Detalle
Rango de Frecuencia	24 MHz - 1700 MHz
Ancho de Banda (RTBW)	10 MHz (9 MHz libre de alias)
Velocidad de Escaneo	NO DEFINIDO
Tasa de Muestreo	10 MSPS (hasta 80 MSPS custom)
POI	NO DEFINIDO
Sensibilidad / NF	3.5 dB NF (42 a 1002 MHz)
SFDR	95 dB
Linealidad (IIP3)	35 dBm (RF front-end)
Resolución ADC / ENOB	12 bits / 10.4 bits
Ruido de Fase	0.5 ppm
Canales / Coherencia	1 Canal (Entrada reloj externo)
Sincronización GNSS	1 reloj RTC
Acceso a I/Q	Sí
Interfaz y Throughput	USB 2.0 / 480 Mbps
Precio aproximado	200 €

Tabla AIII -3 Datos técnicos AirSpy R2 (Elaboracion Propia)

HackRF One [45][46][47][48]



Figura AIII -3 HackRF One (Fuente: greatscottgadgets.com/)

Parámetro	Detalle
Rango de Frecuencia	1 MHz - 6000 MHz
Ancho de Banda (RTBW)	20 MHz
Velocidad de Escaneo	NO DEFINIDO
Tasa de Muestreo	20 MSPS
POI	NO DEFINIDO
Sensibilidad / NF	NO DEFINIDO (Máx. entrada -15 dBm)
SFDR	NO DEFINIDO
Linealidad (IIP3)	NO DEFINIDO
Resolución ADC / ENOB	8 bits / NO DEFINIDO
Ruido de Fase	NO DEFINIDO
Canales / Coherencia	1 Canal (Half-duplex)
Sincronización GNSS	Entrada/Salida SMA para reloj externo
Acceso a I/Q	Sí
Interfaz y Throughput	USB 2.0 / 480 Mbps
Precio aproximado	900 €

Tabla AIII -4 Datos técnicos HackRF One (Elaboracion Propia)

KiwiSDR [48][49][50]

Figura AIII-4 KiwiSDR (Fuente: kiwisdr.com)

Parámetro	Detalle
Rango de Frecuencia	3 Hz - 30 MHz
Ancho de Banda (RTBW)	30 MHz (Procesamiento simultáneo de toda la banda de HF)
Velocidad de Escaneo	Monitorización persistente (sin necesidad de escaneo por saltos HF)
Tasa de Muestreo	66.67 MSPS
POI	NO DEFINIDO
Sensibilidad / NF	NO DEFINIDO
SFDR	NO DEFINIDO
Linealidad (IIP3)	NO DEFINIDO
Resolución ADC / ENOB	14 bits / NO DEFINIDO
Ruido de Fase	Estabilizado mediante oscilador disciplinado por GPS (GPSDO)
Canales / Coherencia	4 a 8 canales virtuales simultáneos; coherencia temporal para TDOA
Sincronización GNSS	Integrada; incluye receptor GPS para estampado de tiempo preciso
Acceso a I/Q	Sí, acceso remoto a espectro y cascada (waterfall) vía web
Interfaz / Throughput	Ethernet (RJ45); streaming de datos para múltiples usuarios
Precio aproximado	600 €

Tabla AIII -5 Datos técnicos KiwiSDR (Elaboracion Propia)

LimeSDR USB [34][51]

-
-



Figura AIII -5 LimeSDR USB (Fuente: limemicro.com)

Parámetro	Detalle
Rango de Frecuencia	100 kHz - 3.8 GHz
Ancho de Banda (RTBW)	61.44 MHz
Velocidad de Escaneo	NO DEFINIDO
Tasa de Muestreo	61.44 MSPS
POI	NO DEFINIDO
Sensibilidad / NF	NO DEFINIDO
SFDR	NO DEFINIDO
Linealidad (IIP3)	Arquitectura LMS7002M
Resolución ADC / ENOB	12 bits
Ruido de Fase	Reloj Rakon @ 30.72 MHz
Canales / Coherencia	2 TX, 2 RX (MIMO 2x2)
Sincronización GNSS	NO DEFINIDO
Acceso a I/Q	Sí (Bidireccional)
Interfaz y Throughput	USB 3.0 / 5 Gbps
Precio aproximado	500 €

Tabla AIII -6 Datos técnicos LimeSDR USB (Elaboracion Propia)

Perseus SDR[52]**Figura AIII -6 Perseus SDR (Fuente: microtelecom.it)**

Parámetro	Detalle
Rango de Frecuencia	10 kHz - 30 MHz (Hasta 40 MHz)
Ancho de Banda (RTBW)	0.4 MHz (Visual) / 1.6 MHz (Grabación)
Velocidad de Escaneo	Analizador de espectro hasta 40 MHz
Tasa de Muestreo	80 MSPS (Muestreo directo)
POI	NO DEFINIDO
Sensibilidad (MDS)	0.39 uV SSB / -131 dBm MDS
SFDR	110 dB
Linealidad (IIP3)	> 31 dBm
Resolución ADC / ENOB	14 bits / NO DEFINIDO
Ruido de Fase	NO DEFINIDO (Estabilidad +/- 1 ppm)
Canales / Coherencia	1 Canal (Preselección de 10 bandas)
Sincronización GNSS	NO DEFINIDO
Acceso a I/Q	Sí (muestras de 24 bits)
Interfaz y Throughput	USB 2.0 / 480 Mbps
Precio aproximado	900 €

Tabla AIII -7 Datos técnicos Perseus SDR (Elaboracion Propia)

RTL-SDR Blog V4 [53][54][55]

Figura AIII-7 RTL-SDR.COM Blog V4 (Fuente: rtl-sdr.com)

Parámetro	Detalle
Ancho de Banda (RTBW)	2.56 MHz
Velocidad de Escaneo	~2.56 MHz por salto estable
Tasa de Muestreo	2.56 MSPS
POI	NO DEFINIDO
Sensibilidad / NF	Mejorada en HF mediante upconverter SA612
SFDR	NO DEFINIDO
Linealidad (IIP3)	Superior a V3 en HF por filtrado triplexor
Resolución ADC / ENOB	8 bits / NO DEFINIDO
Ruido de Fase	Reducido por fuente de alimentación optimizada
Canales / Coherencia	1 Canal / No nativa
Sincronización GNSS	NO DEFINIDO
Acceso a I/Q	Sí, flujo de datos por USB
Interfaz y Throughput	USB 2.0 / 480 Mbps
Ancho de Banda (RTBW)	2.56 MHz
Precio aproximado	35 €

Tabla AIII -8 Datos técnicos RTL-SDR Blog V4 (Fuente: Elaboracion Propia)

SDRplay RSP1B [56][57]**Figura AIII-8 SDRplay RSP1B (Fuente: sdrplay.com)**

Parámetro	Detalle
Rango de Frecuencia	1 KHz - 2 GHz (Sin brechas)
Ancho de Banda (RTBW)	10 MHz (Visualización instantánea)
Velocidad de Escaneo	NO DEFINIDO
Tasa de Muestreo	2 - 10.66 MSPS
POI	NO DEFINIDO
Sensibilidad / NF	18 dB @ 2 MHz; 3.3 dB @ 100 MHz
SFDR	NO DEFINIDO
Linealidad (IIP3)	Optimizada mediante 11 filtros de preselección frontales
Resolución ADC / ENOB	14 bits nativos (Hasta 6.048 MSPS)
Ruido de Fase	Estabilidad de reloj de 0.5 ppm TCXO
Canales / Coherencia	1 Canal RX
Sincronización GNSS	NO DEFINIDO
Acceso a I/Q	Sí, a través de SDRuno y APIs documentadas
Interfaz / Throughput	USB 2.0 / 480 Mbps
Precio aproximado	160 €

Tabla AIII-9 Datos técnicos SDRplay RSP1B (Elaboracion Propia)

SDRplay RSPdx-R2 [58][59]**Figura AIII-9 SDRplay RSPdx-R2 (Fuente: sdrplay.com)**

Parámetro	Detalle
Rango de Frecuencia	1 kHz – 2 GHz
Ancho de Banda (RTBW)	10 MHz
Velocidad de Escaneo	NO DEFINIDO
Tasa de Muestreo	2 - 10.66 MSPS
POI	Mejorada en bandas bajas mediante modo HDR
Sensibilidad / NF	19 dB @ 300 kHz; 18 dB @ 2 MHz; 2.1 dB @ 200 MHz
SFDR	NO DEFINIDO
Linealidad (IIP3)	NO DEFINIDO
Resolución ADC / ENOB	14 bits
Ruido de Fase	0.5 ppm TCXO (ajustable a 0.01 ppm)
Canales / Coherencia	1 Canal RX (3 puertos de antena)
Sincronización GNSS	Entrada de reloj externo (MCX) para GPSDO
Acceso a I/Q	Sí
Interfaz y Throughput	USB 2.0 / 480 Mbps
Precio aproximado	280 €

Tabla AIII-10 Datos técnicos SDRplay RSPdx-R2 (Elaboracion Propia)

Receptor	Rango de Frecuencia	RTBW (Ancho de Banda Tiempo Real)	Tasa de Muestreo (Sample Rate)	Probabilidad de Intercepción (POI)	Sensibilidad (MDS) / Figura de Ruido (NF)	SFDR (Rango Dinámico)
Airspy HF+ Disc.	0.5 kHz - 260 MHz	0.66 MHz	0.768 MSPS	Excelente en HF	-141 dBm MDS	110 dB (HF)
Airspy R2	24 - 1700 MHz	10 MHz	10 MSPS	Alta en VHF/UHF	3.5 dB NF	95 dB
HackRF One	1 MHz - 6 GHz	20 MHz	20 MSPS	Elevada (señales ágiles)	Max input -15 dBm	~48-50 dB
KiwiSDR 2	10 kHz - 30 MHz	30 MHz	66.67 MSPS	Muy alta en HF	Alta sensibilidad HF	Elevado (14 bits)
KrakenSDR	24 - 1766 MHz	2.56 MHz	2.56 MSPS (x5)	NO DEFINIDO	Max input +10 dBm	~50 dB (estimado)
LimeSDR USB	0.1 MHz - 3.8 GHz	61.44 MHz	61.44 MSPS	NO DEFINIDO	NO DEFINIDO	NO DEFINIDO
Perseus SDR	10 kHz - 30 MHz	0.4 MHz (Vis) / 1.6 MHz (IQ)	80 MSPS	Muy alta (HF persistente)	-131 dBm MDS (CW)	110 dB
RTL-SDR Blog V4	0.5 MHz - 1766 MHz	2.56 MHz	2.56 MSPS	Limitada por RTBW	Mejorada en HF (SA612)	~50 dB
SDRplay RSP1B	1 kHz - 2 GHz	10 MHz	2 - 10.66 MSPS	Limitada por RTBW	18 dB NF (@ 2MHz)	Elevado (14 bits)
SDRplay RSPdx-R2	1 kHz - 2 GHz	10 MHz	2 - 10.66 MSPS	Alta (Mejorada en HDR)	2.1 dB NF (@ 200MHz)	Mejorado en Modo HDR
USRP B210	70 MHz - 6 GHz	56 MHz	61.44 MSPS	Excelente (Banda ancha)	<8.5 dB NF	78 dB

Tabla AIII-11 Comparativa 1/2 de datos técnicos de receptores SDR (Elaboracion Propia)

Receptor	Linealidad (IIP3)	Resolución ADC / ENOB	Ruido de Fase	Canales / Coherencia	Sincronización GNSS	Acceso a I/Q	Interfaz / Throughput
Airspy HF+ Disc.	+15 dBm (HF)	18 bit (DDC)	-110 dBc/Hz @ 1kHz	1 Canal	NO DEFINIDO (0.5 ppm TCXO)	Sí	USB 2.0 / 480 Mbps
Airspy R2	35 dBm	12 bit (16 dec.)	0.5 ppm estabilidad	1 Canal (Coherencia ext.)	1 RTC (Time-stamp)	Sí	USB 2.0 / 480 Mbps
HackRF One	Baja (Front-end abierto)	8 bit / ~7 bits	Estándar comercial	1 Canal (Half-duplex)	Reloj externo in/out	Sí	USB 2.0 / 480 Mbps
KiwiSDR 2	NO DEFINIDO	14 bit / ~12 bits	Estabilizado por GPSDO	4-8 Canales virtuales	Integrada (GPS)	Sí (Remoto)	Ethernet (RJ45)
KrakenSDR	NO DEFINIDO	8 bit / ~7 bits	1 PPM / 0.5 PPM	5 Canales Coherentes	GPS vía dispositivo host	Sí	USB-C (3.0)
LimeSDR USB	LMS7002M	12 bit	Reloj Rakon 30.72MHz	2 TX, 2 RX (MIMO 2x2)	Hardware externo	Sí (Bidireccional)	USB 3.0 / 5 Gbps
Perseus SDR	>31 dBm	14 bit / ~12.5 bits	1 ppm estabilidad	1 Canal	NO DEFINIDO	Sí	USB 2.0 / 480 Mbps
RTL-SDR Blog V4	Superior a V3	8 bit / ~7 bits	Reducido (PSU optimizada)	1 Canal	No integrada	Sí	USB 2.0 / 480 Mbps
SDRplay RSP1B	Optimizada (11 filtros)	14 bit	0.5 ppm TCXO	1 Canal	No integrada	Sí	USB 2.0 / 480 Mbps
SDRplay RSPdx-R2	Alta	14 bit	0.5 ppm TCXO	1 Canal (3 puertos)	Entrada reloj (MCX)	Sí	USB 2.0 / 480 Mbps
USRP B210	-20 dBm	12 bit / 12 bits	-102 dBc/Hz @ 10kHz	2 TX, 2 RX (MIMO)	Soporta GPSDO opcional	Sí	USB 3.0 / 5 Gbps

Tabla AIII-12 Comparativa 2/2 de datos técnicos de receptores SDR (Elaboracion Propia)

10 ANEXO IV: CARACTERÍSTICAS DE RECEPTORES SDR PROPUESTOS

A continuación se rellenará una ficha con los parámetros relacionados en el apartado 10.1 del Anexo I para cada uno de los siguientes receptores, empleados en el modelo de red WebSDR SIGINT y que no han sido incluidos en el Anexo III:

Receptor
Cyan
USRP B210
WEB-888
Kraken SDR

Tabla AIV-1 Receptores a analizar (Fuente: Elaboracion propia)

Cyan [29]



Figura AIV-1 Cyan (Fuente: pervices.com)

Parámetro	Detalle
Rango de Frecuencia	DC - 18 GHz
Ancho de Banda (RTBW)	1 GHz (por canal),
Velocidad de Escaneo	Muy Alta (Soporta BW de 1-3 GHz)
Tasa de Muestreo	Extrema (Captura banda ultra ancha)
POI	Muy Alta (Grado EW/Militar)
Sensibilidad / NF	Excelente (Grado Estratégico)
SFDR	Alta
Linealidad (IIP3)	16 bits
Resolución ADC / ENOB	Muy bajo (Relojes de precisión)
Ruido de Fase	16 Cadenas Indep. RX/TX,
Canales / Coherencia	Externa/Interna (Alta precisión)
Sincronización GNSS	Sí (Backhaul masivo)
Acceso a I/Q	100G Ethernet (QSFP28),
Interfaz y Throughput	DC - 18 GHz
Precio aproximado	20000 €

Tabla AIV-2 Datos técnicos Cyan (Elaboracion Propia)

USRP B210[36]

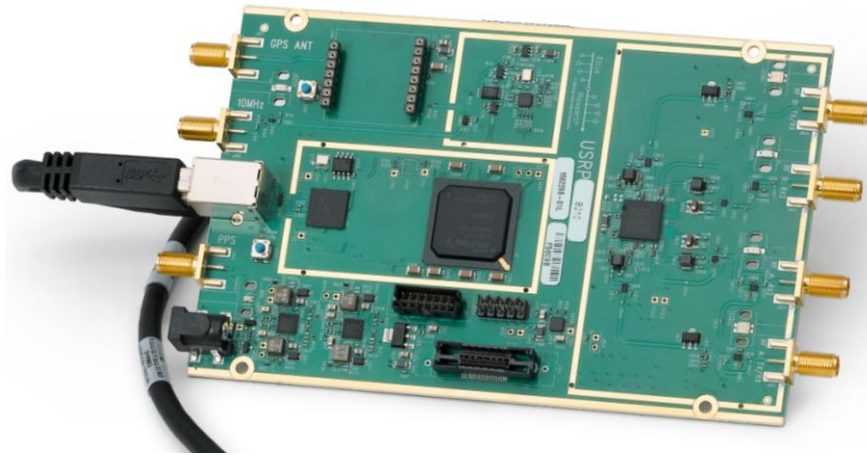


Figura AIV-2 USRP B210 (Fuente: ettus.com)

Parámetro	Detalle
Rango de Frecuencia	70 MHz - 6 GHz,
Ancho de Banda (RTBW)	56 MHz (hasta 61.44 MHz),
Velocidad de Escaneo	61.44 MSPS
Tasa de Muestreo	Alta (en ventana de 56 MHz)
POI	< 8 dB (Típico AD9361)
Sensibilidad / NF	Bueno (12-bit ADC > 75 dB)
SFDR	Media (+ dBm variables)
Linealidad (IIP3)	12 bits
Resolución ADC / ENOB	Bueno (2 ppm est., opción GPSDO)
Ruido de Fase	2x2 MIMO (Coherente)
Canales / Coherencia	Externa (Opcional GPSDO)
Sincronización GNSS	Sí (UHD Driver)
Acceso a I/Q	USB 3.0
Interfaz y Throughput	70 MHz - 6 GHz,
Precio aproximado	2500 €

Tabla AIV-3 Datos técnicos USRP B210 (Elaboracion Propia)

WEB-888 [35]



Figura AIV-3 WEB-888 (Fuente: rx-888.com)

Parámetro	Detalle
Rango de Frecuencia	0 - 60 MHz (HF/VHF bajo) + 118-150 MHz (Airband),
Ancho de Banda (RTBW)	60 MHz (Toda la banda HF),
Velocidad de Escaneo	122.88 MSPS (HF) / 130 MSPS (Max),
Tasa de Muestreo	100% en banda HF (Muestreo directo)
POI	Alta (Optimizada con LNA+LPF+ATT)
Sensibilidad / NF	Alto (Diseño basado en LTC2208/RX-888)
SFDR	Alta (Front-end optimizado)
Linealidad (IIP3)	16 bits,
Resolución ADC / ENOB	Bajo (0.5ppm TCXO + PLL disciplinado),
Ruido de Fase	1 RX físico (Multi-usuario virtual)
Canales / Coherencia	GPS integrado (GPSDO por software),
Sincronización GNSS	Sí (Procesado en FPGA/Zynq)
Acceso a I/Q	Gigabit Ethernet (Autónomo),
Interfaz y Throughput	0 - 60 MHz (HF/VHF bajo) + 118-150 MHz (Airband),
Precio aproximado	500 €

Tabla AIV-4 Datos técnicos WEB-888 (Elaboracion Propia)

KrakenSDR [60][61][37]

Figura AIV-4 KrakenSDR (Fuente: krakenrf.com)

Parámetro	Detalle
Rango de Frecuencia	24 MHz a 1766 MHz. (radiogoniometría: 100 MHz a 1000 MHz)
Ancho de Banda (RTBW)	2.56 MHz por canal
Velocidad de Escaneo	No especificado explícitamente
Tasa de Muestreo	2.56 MSPS (Muestras por segundo) por canal (RTL-SDR)
POI	(Limitado por el ancho de banda estrecho de 2.56 MHz)
Sensibilidad / NF	R820T2, 3.5 dB NF
SFDR	No especificado
Linealidad (IIP3)	No especificado.
Resolución ADC / ENOB	8 bits. (Basado en 5 chips RTL2832U).
Ruido de Fase	Estabilidad del oscilador local (LO): 0.5 PPM (TCXO).
Canales / Coherencia	5 Canales RX. Coherentes en fase
Sincronización GNSS	Externa.
Acceso a I/Q	Sí
Interfaz y Throughput	USB 3
Precio aproximado	1500 €

Tabla AIV-5 Datos técnicos KrakenSDR (Elaboracion Propia)