Universidad Zaragoza
1542

Trabajo Fin de Grado

El desarrollo de la capacidad de guerra electrónica "spoofing" aplicado a las señales "sistema de identificación automática"

Caballero Alférez Cadete D. Alejandro Izquierdo Nacarino

Director académico: Coronel D. José Manuel Vicente Gaspar y Dra. Gema Martínez Martínez

Director militar: Capitán D. Carlos Barquín Portillo

Centro Universitario de la Defensa-Academia General Militar

2022

Agradecimientos

Quiero dedicar este trabajo al Capitán D. Carlos Barquín Portillo, por su ayuda y hospitalidad durante mi período de prácticas en el Regimiento de Guerra Electrónica nº31, situado en el acuartelamiento “Zarco del Valle”, en Madrid.

El presente trabajo no podría haber sido realizado sin el acogimiento y amabilidad de los oficiales, suboficiales y tropas del regimiento.

Finalmente, me gustaría agradecer el apoyo de mi familia; Alejandro, María Isabel y Ana Isabel.

A mis amigos, por contar siempre y ayudarme en mis momentos difíciles; Sergio, Jorge, Alberto y Manuel.

RESUMEN

El presente trabajo ha sido realizado para compilar los distintos usos y aplicaciones del *spoofing* aplicado a señales de identificación automática (AIS), a petición del Regimiento de Guerra Electrónica nº31 y del Centro Universitario de la Defensa, en Zaragoza.

En este trabajo se exponen los principales conceptos a utilizar: *spoofing* y *jamming* y se realiza una introducción histórica desde los inicios de la aplicación de la guerra electrónica en el campo de batalla hasta nuestros días. También se contempla la literatura internacional sobre el tema en cuestión. Finalmente se describe la importancia de la tecnología *spoofing* en los conflictos armados que se están desarrollando actualmente.

El desarrollo del tema propuesto se ha llevado a cabo través de una serie de herramientas metodológicas como son, encuestas y pruebas de campo, y de laboratorio informático. Se han realizado pruebas de campo prácticas, así como estudios y análisis de la doctrina actual del Ejército de Tierra en el ámbito de la Guerra Electrónica. Como principales conclusiones, se destaca, que con los medios disponibles en el Regimiento de Guerra Electrónica nº 31 se puede realizar ataques tipo *spoofing* con señales AIS con ciertas limitaciones.

Finalmente, se incluye una propuesta de empleo táctica en guerra electrónica, así como, propuestas de uso de medios y materiales.

ABSTRACT

This paper is written to compile various uses and applications of spoofing applied to automatic detection signals (AIS). This electronic warfare has been requested by *“Regimiento de Guerra Electrónica nº31”*, as well as the Centro Universitario de la Defensa, in Zaragoza.

In this work the main concepts of spoofing and jamming, as well as a historical introduction and state of the art to date are described. It is also highlighted the rules on the topic in question, counting in turn with the international literature, and the importance of spoofing technology in ongoing armed conflicts.

The proposed topic has been developed through a range of methodological tools, such as, surveys or field and computer laboratory tests. Practical field tests have been carried out. Additionally, the current theory of the army in the field of electronic warfare has been described and analyzed.

As the main conclusion, it is highlighted that with the means available in “*The Regimiento de Guerra Electrónica nº31”*, are able to carry out spoofing attacks with AIS signals with certain limitations. Finally, electronic warfare includes a proposal for strategic use, as well as proposals for the use of means and materials.

INDICE DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

Tabla 1. ABREVIATURAS, SIGLAS Y ACRÓNIMOS

PALABRA	SIGNIFICADO
AIS	Sistema de Identificación Automática
GPS	Sistema de Posicionamiento Global
SDR	Radio Definida por Software
REW 31	Regimiento de Guerra Electrónica nº31
GNSS	Sistema Global de Navegación por Satélite
INTRANET	Red Informática Interna
FFAA	Fuerzas Armadas
HF	High Frequency
VHF	Very High Frequency
UHF	Ultra High Frequency
EW	Guerra Electrónica
EWL	Guerra Electrónica Ligera
BMR	Blindado Medio sobre Ruedas
GNSS	Sistema Global de Navegación por Satélite
EMCON	Emissions Control

INTRODUCCIÓN

Desde mediados del siglo pasado y hasta nuestros días, en pleno S.XXI, se ha avanzado significativamente en la interconexión y dependencia de las telecomunicaciones. Todo esto ha mejorado nuestro estilo de vida, haciendo más rápidos y accesibles los recursos disponibles. No obstante, el avance en este sentido también ha posibilitado que estos recursos puedan ser utilizados con fines malignos e ilegales. Consecuentemente, el desarrollo de la seguridad en las redes y telecomunicaciones es cada día más importante y crítico.

La guerra electrónica, desde la aparición de las telecomunicaciones, ha sido imprescindible en el campo de batalla. Existen multitud de sistemas que poseen dicha capacidad: estaciones terrestres, aéreas, marítima, etc. Todas ellas posibilitan la detección del enemigo en el espectro electromagnético, interceptando, interrumpiendo y modificando acciones.

Por otro lado, al igual que en el resto de los ámbitos de defensa, nunca se debe subestimar al enemigo, la constante renovación y desarrollo de la tecnología para la guerra electrónica es vital para la supervivencia y cumplimiento de la misión

En los últimos años, la rapidez de la innovación se ha acentuado de forma exponencial. El desarrollo de la tecnología en el siglo XX ha sido crucial en multitud de crisis y eventos nacionales e internacionales, por lo tanto, es primordial situarse a la vanguardia en investigación y desarrollo de las nuevas tecnologías aplicadas a la guerra electrónica.

El conjunto de métodos para la innovación consta de software, hardware, algoritmos y demás elementos, y técnicas para lograr dicho objetivo; así como la colaboración entre distintas empresas y agentes sociales que interactúen con el Ministerio de Defensa.

Dentro del ámbito de la guerra electrónica, existen fundamentalmente dos técnicas para atacar al enemigo: s*poofing* y *jamming*.

Spoofing es el conjunto de técnicas a través de las cuales un determinado usuario o identidad se hace pasar por una fuente de confianza para acceder a una serie de datos o conocimientos [13].

Jamming es todo conjunto de técnicas que consisten en la interrupción o inhibición de una determinada señal [14].

En el actual conflicto de Ucrania, las fuerzas especiales ucranianas, están usando equipos portátiles con capacidad *jamming,* que bloquean la señal Global Position System (*GPS)*, las redes de datos móviles, la Frecuencia Modulada (FM), la Amplitud modulada (AM), etc. Ello permite a las FFAA ucranianas atacar objetivos militares rusos, sin que estos puedan comunicar el ataque sufrido.

Los tres pilares básicos de la seguridad en cualquier tipo de telecomunicación son la disponibilidad, la confidencialidad y la integridad. El *spoofing* propiamente dicho, ataca a este último pilar, la integridad de la información a través de señales de sistemas de identificación automática.

Debido a la dependencia mundial de los sistemas de información, la influencia del *spoofing* con señales AIS influye tanto en el ámbito civil como en el militar. Cabe destacar también su

influencia en el ámbito de la logística, tal y como sucedió el 23 de marzo de 2021 en el canal de Suez.

Ese día el navío “Ever Given” colapsó al quedar atravesado en el canal de Suez durante seis semanas, lo que supuso una pérdida de diez mil millones de dólares al día. Como consecuencia, el tráfico mundial marítimo tuvo que ser desviado sufriendo multitud de retrasos [15].

El estudio de los ataques con componente *spoofing* es de especial relevancia en las unidades de guerra electrónica de las Fuerzas Armadas, debido a que su uso, se está empleando de forma recurrente en los conflictos armados.

OBJETIVOS Y METODOLOGÍA

El **objetivo principal** de este trabajo es confirmar, con los medios existentes en Unidades de Guerra Electrónica y Ciberdefensa del Ejército, la posibilidad de realizar ataques de AIS *spoofing*, los cuales, a pesar de interesar en gran medida como ventaja táctica, no están desarrollados en técnica y procedimiento en el Ejército de Tierra (ET)

En caso de una inexistencia efectiva de medios y coordinación para ejecutarlos, será necesario presentar unas propuestas técnicas y organizativas que sirvan como punto de partida a pruebas de campo e instrucción en el ET, dando prioridad a los Sistemas de Navegación AIS de plataformas navales sobre objetivos-víctima. Además, será necesario poder investigar y auditar, las capacidades del Regimiento de Guerra Electrónica nº 31, en torno a la realización de *spoofing* a señales AIS con los medios disponibles.

Los objetivos específicos son:

- Describir y definir la capacidad *spoofing*, así como diferenciarla de otros conceptos.
- Estudiar los distintos usos y capacidades del *spoofing* aplicado a señales AIS (Sistema de Identificación Automática).
- Estudiar los medios y doctrina del empleo de dicha tecnología en las Fuerzas Armadas Españolas.
- Compilar distintos casos y ejemplos reales del uso de dicha tecnología.
- Auditar el uso de dicha tecnología con los medios del Regimiento de Guerra Electrónica nº 31.

El cronograma propuesto para conseguir estos objetivos se detalla en la ilustración 1.

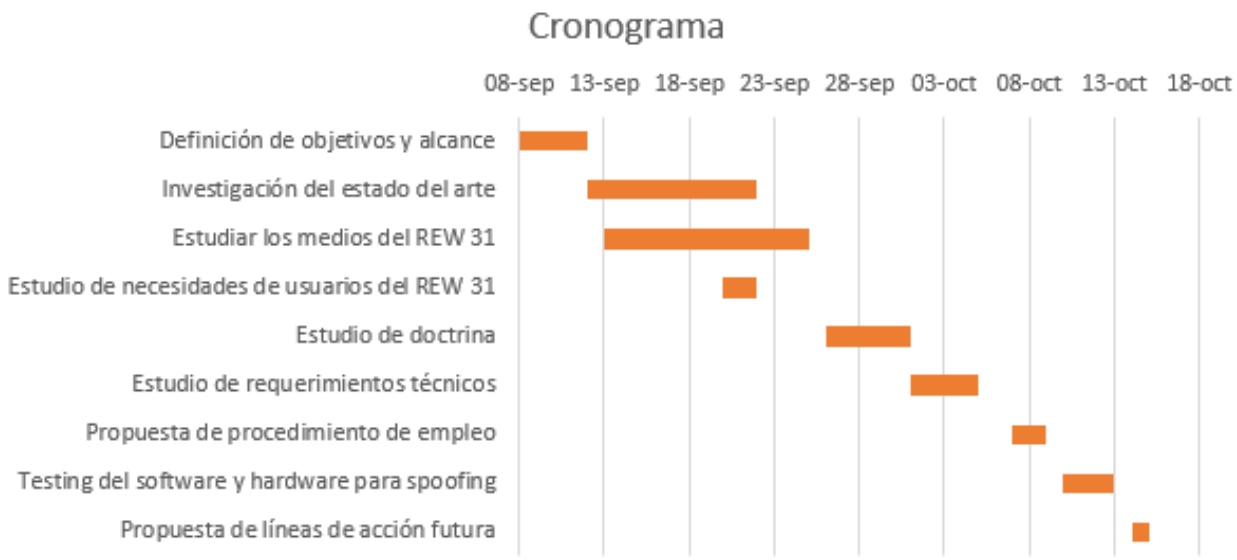


Ilustración 1. Cronograma. Elaboración propia.

El **alcance** de este trabajo final de grado, está dirigido hacia los usuarios de guerra electrónica encuadrados en las siguientes unidades:

1. Regimiento de Guerra Electrónica nº 31.
2. Regimiento de Guerra Electrónica nº 32.
3. Unidades de maniobra de la Armada e Infantería de Marina, que mediante el conocimiento del avance de este tipo de técnicas, pudiesen hacer mejoras en su Plan *Emissions Control* (*EMCON*).

Dado que el principal ámbito de trabajo se desarrolla en la línea de costa, se requiere amplia colaboración entre el Ejército de Tierra y la Armada Española. Esta colaboración que ya se ha dado en ocasiones anteriores, como en el ejercicio “Aquiles” 2020 desarrollado en Algeciras (Cádiz), supone la demostración de la integración de medios, en primer lugar, por parte de los Regimientos de Guerra Electrónica nº 31 y nº 32 entre sí, y de forma conjunta, con la Unidad de Guerra Electrónica de la Brigada de Infantería de Marina.

Entre los resultados más notorios de este ejercicio, destacan:

- Integración de materiales:

Los materiales y recursos de las Fuerzas Armadas están plenamente capacitados para su interconexión y máxima compatibilidad entre sí. De esta forma, no existe distinción de capacidad de tecnologías y se asegura el éxito en la misión.

- Coordinación de procedimientos:

Toda operación se basa en la coordinación, especialmente de procedimientos. La falta de coordinación, produce que el esfuerzo y las fuerzas presentes en una determinada misión, sean dispares y que no se asegure la máxima eficacia.

- Explotación en un medio real:

Todos los medios, procedimientos y personal, deben ser situados y entrenados en las acciones más cercanas a una situación de combate real. Actualmente, el escenario más próximo a un conflicto convencional se encuentra en la región del Mediterráneo/Sahel, de ahí la localización del ejercicio Aquiles 2020.

Como conclusiones del ejercicio “Aquiles” 2020 y posibles líneas de acción futuras, destacan las futuras escuelas prácticas para intercambio de conocimiento y tecnología, el aumento de experiencia y mejora en los procedimientos de empleo de guerra electrónica, y los apoyos mutuos y fuentes de interoperabilidad.

En cuanto a las tareas para completar el alcance, destacan las siguientes:

- **Diálogo con DIRACA y DIRMIL:**

La conversación y apoyo de los tutores académicos y civiles es clave para la realización del proyecto, tanto para presentar una guía, como para refuerzo en contenido y forma.

- **Entrevistas con el personal del Regimiento de Guerra Electrónica nº 31:**

Durante el periodo de estancia compartido con el personal del Regimiento de Guerra Electrónica nº 31, se contó con el apoyo incondicional tanto de Oficiales como de Suboficiales y Tropa.

- **Comparación de métodos de estudio e investigación:**

En el momento de emprender un trabajo de estudio a nivel universitario, es de primera necesidad contar con una estructuración y cumplimentación de objetivos, tanto de forma temporal como secuencial.

- **Búsqueda de tecnologías existentes en la actualidad a nivel mundial:**

Es Fundamental a la hora de desarrollar un trabajo científico revisar la bibliografía y literatura existentes hasta el momento.

- **Auditoria de medios disponibles:**

La presencia y prácticas de mando, en el Regimiento de Guerra Electrónica nº 31, otorga la capacidad de auditar y comprobar los distintos medios sobre los cuales, el Regimiento de Guerra Electrónica nº 31, debe apoyarse para desarrollar la capacidad sobre la que se centra el presente trabajo.

- **Optimización de recursos**:

La eficacia y el empleo de los recursos, tanto en el mundo civil como militar, es clave no solo por el ahorro económico, sino también, por la sencillez y simplicidad a la hora de emplear los recursos.

- **Pruebas de campo:**

A la hora de completar y desarrollar el alcance del trabajo, las pruebas de campo y técnicas son imprescindibles, tanto por comprobación como por definición del progreso.

En cuanto a los recursos disponibles utilizados, destacan los siguientes:

- **SDR:**

  Dispositivo que conectado junto a una Radio Definida por Software y una antena, permite emitir una señal.

- **Antena:**

  Sistema que posibilita el estudio de las diferentes señales en pruebas de laboratorio.

- **GNU Radio:**

  Software con licencia gratuita, que permite diseñar una Radio Definida por Software.

- **SDR Angel:**

  Software que permite la recepción de señales en un amplio espectro de frecuencias y bandas, para su posterior procesamiento y lectura de estas.

- **Portátil Personal**

  Ordenador cuyas características mínimas serán tener 16 GB de RAM, un procesador Intel de la serie 5 y un disco duro sólido.

- **Intranet:**

  Red interna del ejército, que contiene documentos y manuales tanto de instrucción como de perfeccionamiento.

- **Doctrina sobre Guerra Electrónica:**

  Manuales que describen y ejemplifican el empleo de la Guerra Electrónica tanto en operaciones convencionales como de combate.

METODOLOGÍA

Como **método cualitativo** se han utilizado las entrevistas, destacando el capital humano de los entrevistados, tanto personal de tropa como de suboficiales y oficiales. Estas entrevistas, se han realizado en ejercicios de instrucción en el campo de maniobras (caso de “*El Palancar*”), como en las instalaciones del acuartelamiento Zarco del Valle (Madrid). Con las entrevistas personales, se pueden desarrollar herramientas como:

1. Encuestas.
2. Cronogramas.
3. Gráficos.

Mediante las entrevistas se pretende observar y evaluar el funcionamiento de la tecnología disponible en el Regimiento de Guerra Electrónica nº 31, para auditar la tecnología y proponer las correspondientes mejoras. Así como estudiar las capacidades y el alcance que tiene el propio material, ya que transformándolo o actualizándolo se pueden conseguir capacidades nuevas. Por último, analizar varios casos públicos del empleo del *spoofing* con señales AIS realizados hasta la fecha. Todos estos estudios quedarán reflejados en el estado del arte.

En cuanto a **métodos cuantitativos**, destacan las encuestas realizadas al personal de tropa, suboficiales y oficiales sobre el funcionamiento de dicha tecnología.

Esta metodología, permitirá medir y definir los resultados en cuanto al empleo de dicha tecnología, y de esta forma, auditar los medios de guerra electrónica de que dispone el Regimiento de Guerra Electrónica nº 31.

ANTECEDENTES Y MARCO TEÓRICO

ANTECEDENTES

Como suceso de *spoofing* en el ámbito civil, cabe destacar lo sucedido en el año 2013. Ese año, Un grupo de estudiantes de la Universidad de Texas fue invitado a bordo de un yate para comprobar *in situ* la posibilidad de realizar un ataque tipo *spoofing* con señales AIS a través de unas antenas de tamaño reducido, y un software operado desde un portátil personal.

Los estudiantes emitieron una señal GPS para hacerse con el control del navío, ya que el sistema de navegación del propio barco captaba mejor las señales generadas por el grupo de estudiantes. Con el ordenador portátil, emitieron unas señales falsas de GPS, consiguiendo que la tripulación, sin percatarse de la acción, modificara la trayectoria del navío [1], y A través de un incremento significativo de la potencia definida por software y emitida con su radio, consiguieron realizar un *spoofing* con señales GPS, como se muestra en la ilustración 2.

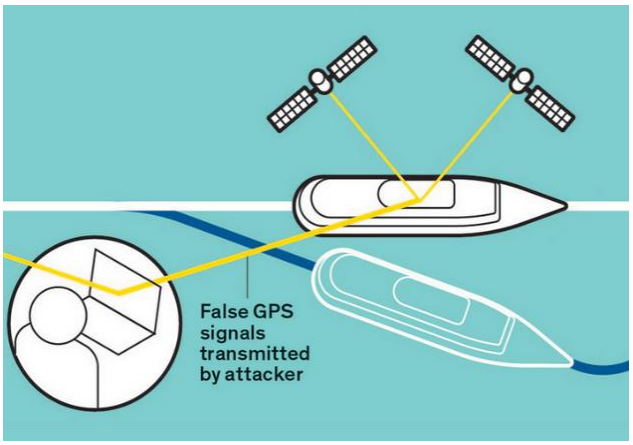


Ilustración 2. Spoofing con señales AIS a una embarcación. Digital Yatch

Otro suceso destacable de *spoofing* en el ámbito miliar tuvo lugar en junio de 2017. En este caso, La administración marítima de los Estados Unidos de América realizó un parte de incidencias en el mar Negro (mar ubicado entre Europa Oriental y Asia Occidental). El capitán, jefe de un navío mercante, amarrado en el puerto ruso de *Novorossiysk,* informó que su transmisor AIS situaba a su navío a 32 kilómetros tierra adentro [2]. El capitán para cerciorarse del posicionamiento, contactó con navíos próximos y pudo comprobar que sus señales AIS indicaban posiciones en la misma zona que la del navío mercante. Finalmente, los expertos corroboraron que se trataba del primer caso de *spoofing* con señales GPS que afectó a un total de 20 navíos (ilustración 3).

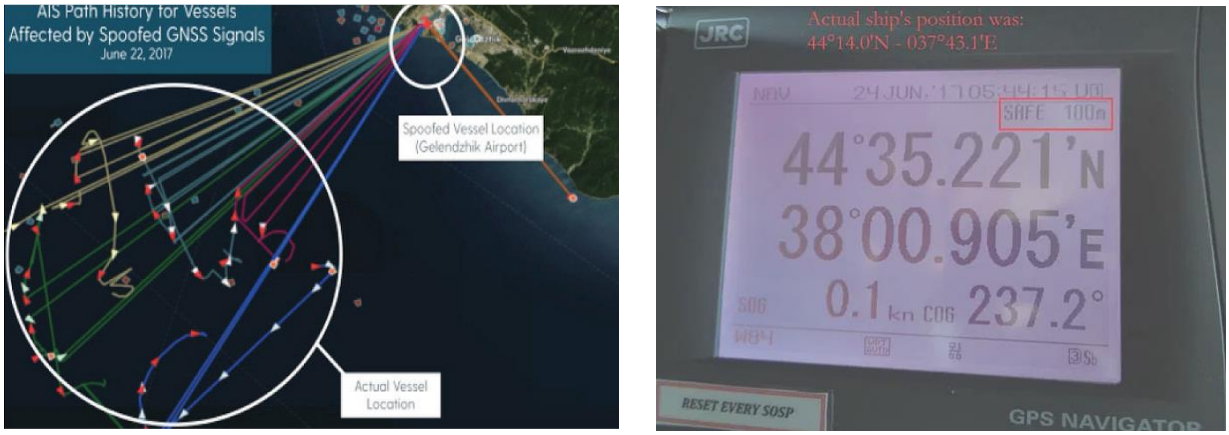


Ilustración 3. Incidente del 22 de junio de 2017. Research Gate.

Todos estos hechos dieron lugar a la realización de los siguientes análisis por parte de la comunidad científica:

1.- “*AIS Data Vulnerability Indicated by a Spoofing Case-Study”*, financiado por los gobiernos de Croacia y Eslovenia. Es un Estudio que muestra el AIS como la principal fuente de información del ambiente marítimo, tanto de embarcaciones privadas como de defensa, así como su vulnerabilidad y desafío para la seguridad marítima y de navegación.

Este estudio refleja que la industria marítima no es inmune a los ciber ataques y que no se encuentra preparada para hacer frente a los riesgos asociados con el uso de los sistemas digitales del siglo XXI. Finalmente, asocia las señales AIS junto a una serie de estándares y recomendaciones para su empleo. Concluye que la estandarización es clave para la unificación de protocolos y de seguridad colectiva en este ámbito [3].

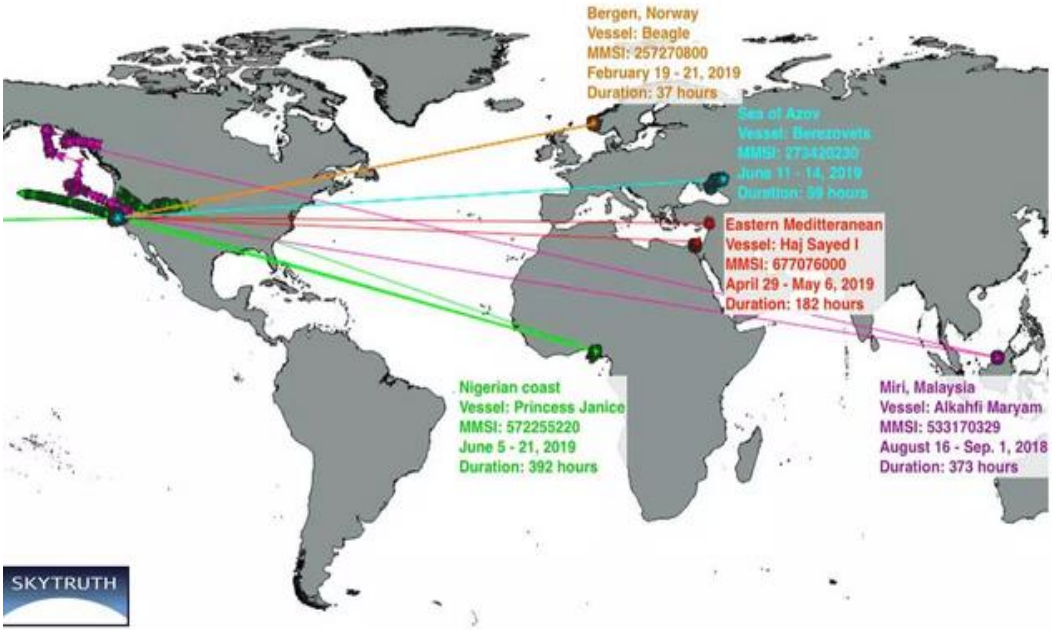


Ilustración 4. Navegación mediante AIS. Adsl zone

2.- “DeAIS Project: Detection of AIS spoofing and resulting risks”. Este trabajo describe cómo detectar el *spoofing* a través de señales AIS, así como sus potenciales riesgos. Fue realizado por el instituto francés de investigación naval (IRENav) contando con multitud de investigadores tanto franceses como de otros países europeos.

En los últimos años, el incremento del transporte marítimo ha favorecido la aparición y generalización de los sistemas de información y seguridad de los trayectos entre navíos. Entre estos sistemas, destaca el AIS como principal recurso para dicho fin. Recientemente se ha demostrado que la falsificación de AIS es posible, de tal forma, que podría enmascarar o beneficiar, actividades ilegales tales como la piratería, el narcotráfico, etc. [4]

3.- “Detection of malicious AIS position spoofing by exploiting radar information “. Este estudio describe el concepto *AIS* como un sistema de seguimiento basado en los mensajes enviados desde los buques y embarcaciones, que contienen un transpondedor *AIS*. El mensaje tipo AIS, contiene información sobre la posición de la embarcación, velocidad, etc. El principal problema de los transpondedores AIS, es que se basan en un autoinforme, en lugar de en las mediciones de un sensor. De esta forma, usando el radar como sensor se puede detectar información AIS maliciosa. [5]

Ilustración 5. Hardware con soporte AIS. Promo nautica

4.- “Detection of AIS Spoofing in Fishery Scenarios”. Este trabajo comienza con una descripción del concepto *AIS*, argumentando que funciona como una radio VHF, e intercambiando información de forma automática vía *broadcast*. A su vez, el estudio se basa en detectar el *spoofing* con señales *AIS* en aquellos escenarios o situaciones, donde los navíos cuya principal actividad sea la pesca, puedan ser objeto de *spoofing*. Finalmente, propone crear una base de datos de todos los incidentes reportados hasta la fecha, para mejorar la seguridad, y proponer un nuevo formato de envío de paquetes AIS, como se refleja en la Ilustración 6. El nuevo sistema de envío de paquetes, está basado principalmente, en su división o reparto en el tiempo, como reflejan sus autores. [6]

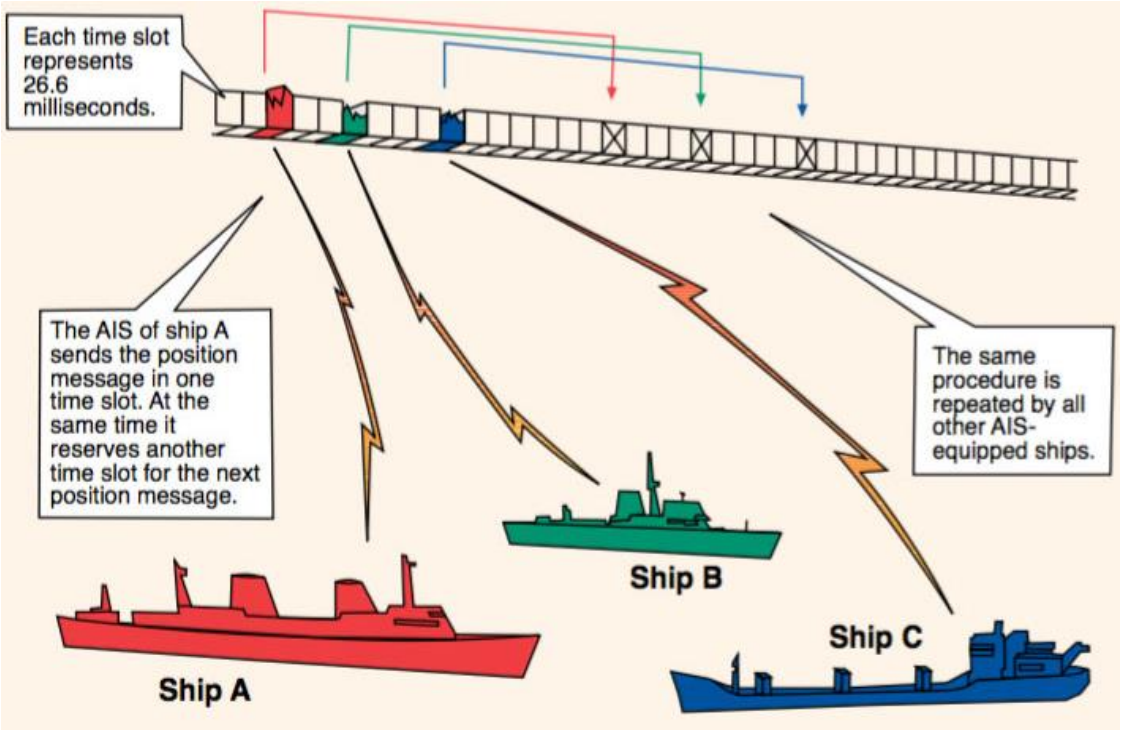


Ilustración 6. Envío de paquetes AIS. Gmd stesters

5.- “Algorithms for detecting vessel spoofing of space-based AIS data”. Este estudio comienza con una breve introducción acerca del gran movimiento y transporte que existe por los mares. Como En determinados incidentes, como en derrames de petróleo o secuestros, el AIS ha servido para mejorar la coordinación y cooperación para superar problemas. No obstante, también se ha demostrado, que la falsificación de los mensajes AIS es posible, por lo que podría favorecer las acciones ilegales, provocar perturbaciones de los sistemas de monitoreo, y otra multitud de riesgos, muchos de ellos aún por estudiar. [7]

6.-: “Sistema de identificación automática de buques AIS”. Este estudio propone un algoritmo para detectar la suplantación de identidad, ya que compara el desplazamiento y la distancia del buque con otros elementos. El resultado gráfico de este algoritmo se muestra en la ilustración 8, en ella, se observan diferentes navíos agrupados en códigos de colores, según el interés o preferencias, que haya denostado el usuario o comandante de la embarcación en cuestión. [8]

Ilustración 7. Algoritmo de funcionamiento de AIS. Vessel tracking

DESARROLLO: ANÁLISIS Y RESULTADOS

CRONOGRAMA

El cronograma que se muestra en la ilustración 8, define las actividades que se podían realizar en el Regimiento de Guerra Electrónica nº 31.

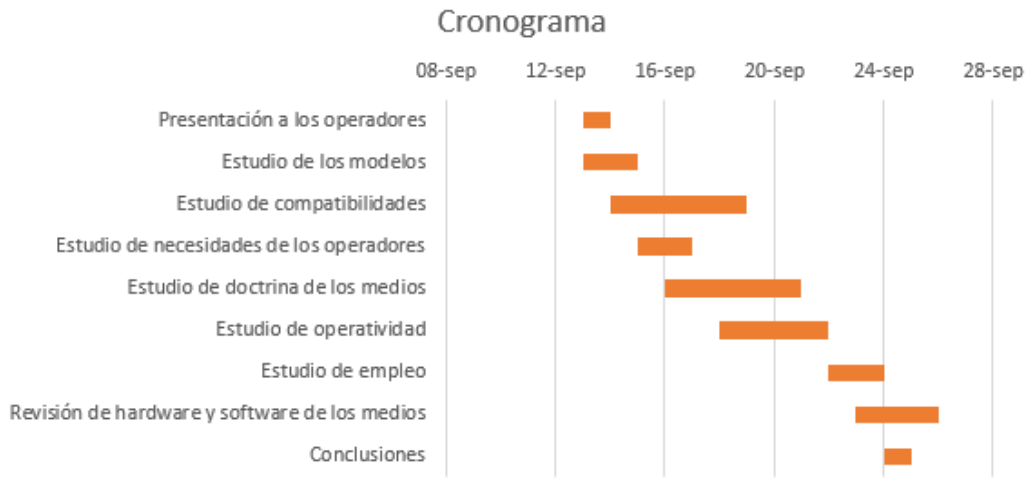


Ilustración 8. Cronograma. (Elaboración propia).

La necesidad de la elaboración del cronograma es crucial en los documentos científicos, debido a que, la planificación temporal es clave para el éxito del estudio. A través del presente diagrama [Ilustración 8], se reúnen las actividades definidas previamente, así como su orden planificado y sucesión temporal.

ESTUDIO DE NECESIDADES DE USUARIOS DE GUERRA ELECTRÓNICA

La encuesta realizada según el **Anexo [1]** fue dirigida hacia los siguientes expertos de guerra electrónica:

- Oficial jefe de la Compañía de Telecomunicaciones; con experiencia en ciber defensa, coordinación de operaciones, situaciones críticas y gestión de crisis.
- Oficial jefe de la Sección de Sigilo; con experiencia en ciber defensa y operaciones en el exterior.
- Sargento encuadrado en la Sección de Sigilo; con experiencia en programación, ciber defensa y operaciones en el exterior.
- Sargento encuadrado en la Sección de Sigilo; con experiencia en gestión de medios de guerra electrónica y operaciones en el exterior.
- Sargento encuadrado en la Sección de Sigilo; con experiencia en gestión de la perturbadora BMR (Blindado Medio sobre Ruedas) M1 y operaciones en el exterior.
- Soldado encuadrado en la Sección de Sigilo; con experiencia en programación.
- Soldado encuadrado en la Sección de Sigilo; con experiencia en captación de señales.
- Soldado encuadrado en la Sección de Sigilo; con experiencia en análisis de señales.

A la hora de describir y reunir las necesidades de usuarios de guerra electrónica, tuvo gran importancia las maniobras reunidas “Alpha”, realizadas en el campo de maniobras “*El Palancar*” (Hoyo de Manzanares), en la semana del 19 al 23 de septiembre de 2022.

En esa semana, se desplegaron los principales medios con los que cuenta el Batallón de Guerra Electrónica I/31, y de forma más específica, las siguientes secciones:

Sección de sigilo:

Que realizó diferentes pruebas de captación y emisión de señales a frecuencias comprendidas entre 30 a 300 MHz. A su vez, también se registraron ruidos e interferencias anómalos para su posterior análisis

Sección de perturbación:

A través del despliegue de la perturbadora móvil “BMR M1 EW”, se desplegaron las perturbadoras en diferentes puntos del terreno para captar y triangular fuentes a frecuencias comprendidas entre 20 y 400 MHz. En la ilustración 9 se refleja una triangulación de objetivos captada el 22 de septiembre de 2022.

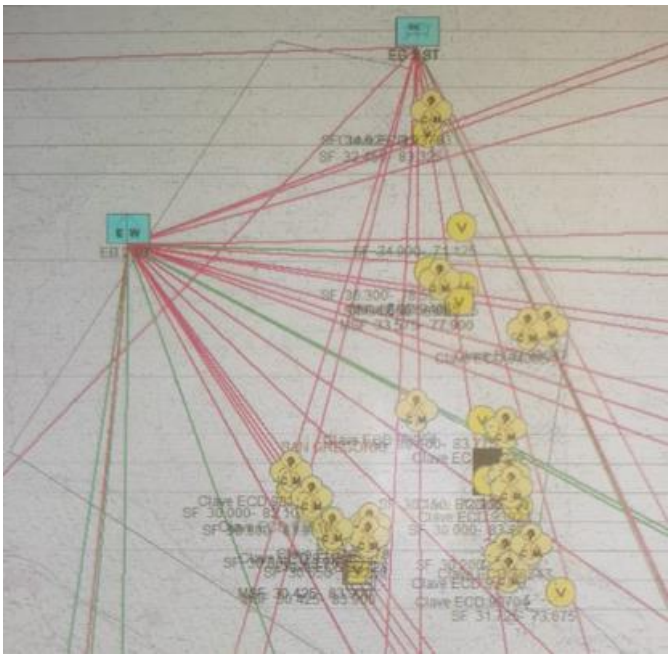


Ilustración 9. Triangulación de las perturbadoras en “El Palancar”. Elaboración propia.

El objeto de las maniobras previamente citadas era conocer las necesidades más importantes, ya que de esta forma se podría trabajar de manera más persistente y clara sobre ellas. En la ilustración 10 se muestran las necesidades de los usuarios de guerra electrónica.

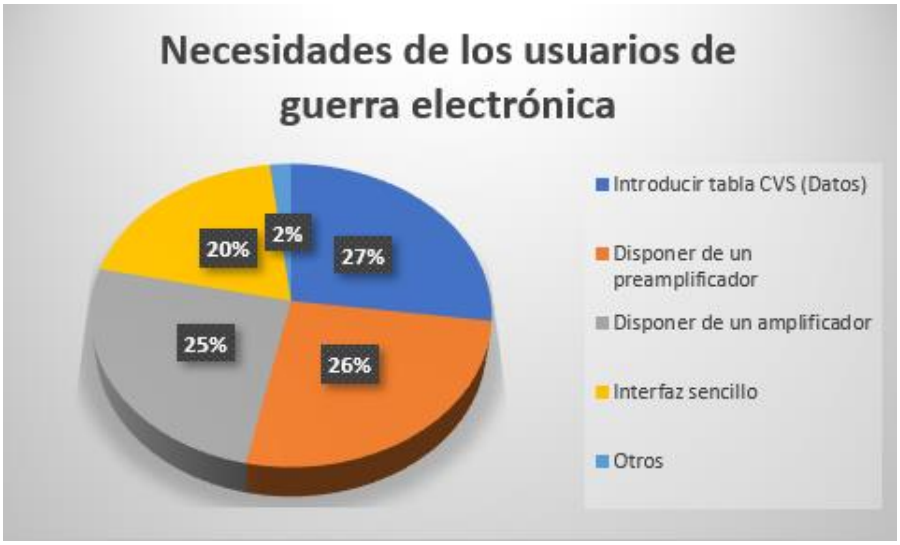


Ilustración 10. Resultados de las encuestas. Elaboración propia.

A continuación, se enumeran y detallan cada una de las necesidades reflejadas:

1.- Introducir tabla CVS. A la hora de realizar una interferencia con señales AIS, se necesita introducir una tabla con una serie de datos para poder emitir con mayor frecuencia (Ilustración 11). En el desarrollo del proyecto, se ha utilizado “GNURadio” para poder emitir una señal AIS a través de un SDR y una antena, que es carente de información como tal. Es por ello por lo que se debe proporcionar una herramienta que permita emitir los datos precisos para la interferencia. La Ilustración 11, muestra los datos más relevantes que se introducen en una tabla CVS, entre ellos el nombre, latitud, longitud, etc.

Ubicación	43.369N, 1.786W
Velocidad	0.0 Km/h
Rumbo	0.0°
Hora de actualización	26/5/16 22:55:03
Clase	Velero/Recreo
País	España
MMSI	224232960
Callsign	EB2788
Eslora	12.0 m.

Ilustración 11. Tabla CVS. Vigo sonar

2.- Disponer de un Preamplificador. Es una necesidad a destacar por los usuarios, ya que sin un preamplificador lo suficientemente potente, la señal no podrá ser recibida por las demás embarcaciones, o por la embarcación objetivo en un *spoofing* con señales AIS. A su vez, el preamplificador debe tener ganancia suficiente para conseguir que el amplificador funcione en un rango de frecuencias aceptable para su correcto empleo. Por otro lado, el preamplificador debe trabajar a 162 MHz. En el mercado civil existen multitud de preamplificadores que trabajan a dicha frecuencia.

Estos preamplificadores fueron analizados con el Sargento encuadrado en la Sección de Sigilo, con experiencia en programación, ciberdefensa y operaciones en el exterior, en base a sus características técnicas, y requisitos específicos de los medios del Regimiento de Guerra Electrónica nº 31. [Ver Anexo 2].

3.- Disponer de un amplificador. El amplificador es un componente que se encuentra a continuación del preamplificador, y que aporta la ganancia más considerable al sistema electrónico en conjunto. Del mismo modo que con el preamplificador, hay que buscar un amplificador, que trabaje en el rango de frecuencias que deseamos, para un mayor aprovechamiento de la capacidad de guerra electrónica:

De la multitud de amplificadores que se encuentran en el mercado, destacamos el que figura en la ilustración 12, ya que su ganancia a 162 Mhz es máxima, aproximadamente 11 dB.

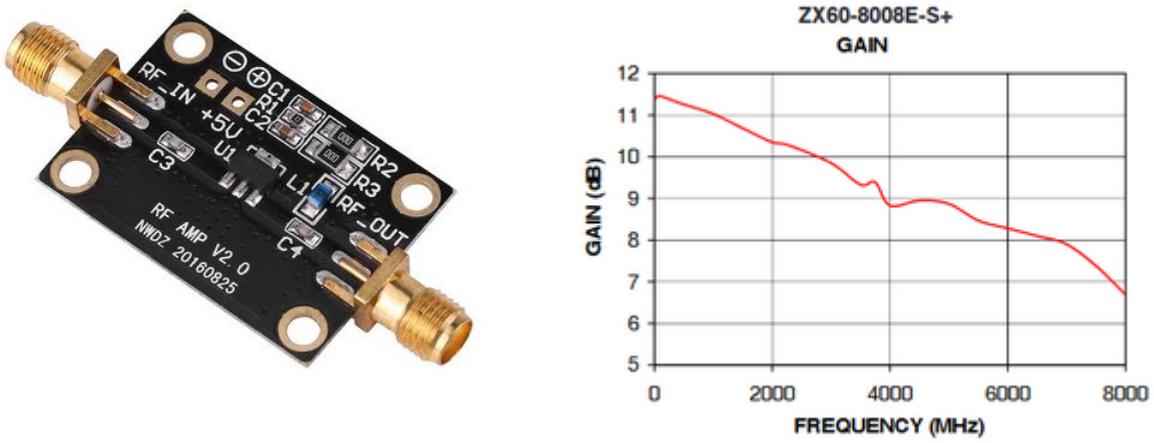


Ilustración 12. Amplificador. Amazon

4.- Interfaz sencilla.

La Ilustración 13 muestra entre otras funciones: la transmisión de la antena, la posición GPS, la antena AIS, el sistema de reporte de la antena AIS, el estado del sistema, el tiempo de espera, encendido/apagado, las transmisiones enviadas, las transmisiones recibidas y por último el voltaje suministrado.

Ilustración 13. Interfaz del software AIS. Digital yacht

También sería conveniente que los indicadores y la distribución del interfaz se desarrollasen junto a los operadores de guerra electrónica, con el objetivo fundamental de que el software y hardware sean diseñados para los usuarios, lo que aumentaría de forma considerable la eficacia y eficiencia.

En la ilustración 14 se muestran distintos parámetros como las dimensiones de la embarcación, el nombre de la embarcación y el tipo de embarcación. Los valores de los parámetros pueden ser modificados introduciéndolos manualmente o bien cargándolos de un fichero o archivo que contenga las características previamente solicitadas.

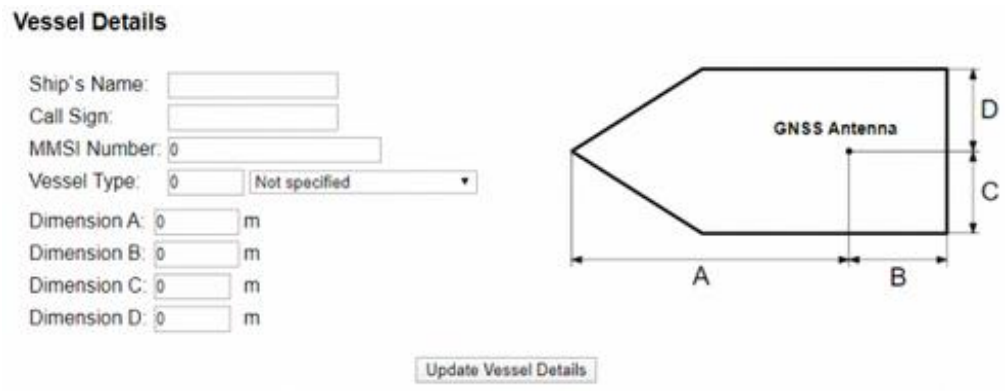


Ilustración 14. Interfaz AIS. Digital yacht

ESTUDIO DE NECESIDADES: DOCTRINA DE EMPLEO TÁCTICA.

En las últimas décadas, las fuerzas militares han incrementado de forma considerable el uso y la dependencia del espectro electromagnético. El control de este entorno es clave para garantizar el cumplimiento de la misión, de esta forma, todo jefe de una determinada operación debe de integrar la guerra electrónica en los planes y órdenes de operaciones de toda maniobra. El empleo de la guerra electrónica, según la doctrina presente en las Fuerzas Armadas, se basa en tres pilares fundamentales: Ataque electrónico, Defensa y Vigilancia electrónica.

- **Ataque electrónico**:

Consiste en el uso de la energía electromagnética con propósitos ofensivos. Se emplea para destruir, neutralizar, negar, degradar, interrumpir o engañar las capacidades de mando y ~~el~~ control del enemigo. También para reducir las oportunidades que puedan modificar o explotar el entorno operativo. La energía electromagnética no se emplea de forma aislada, sino como un elemento más de ataque, siendo habitual que se complemente con otros apoyos. Cuando se combina con el ataque físico se consigue el mayor poder de destrucción.

- **Defensa electrónica**:

Consiste en el uso de la energía electromagnética para proporcionar protección. Se utiliza para proteger las operaciones propias, como por ejemplo, inteligencia en ataques electrónicos del adversario, etc. Así como colaborar con otras capacidades físicas a la protección de fuerzas de plataformas de los sistemas y de determinadas áreas de la zona de acción. La defensa electromagnética también desempeña un papel clave en la lucha contra los artefactos explosivos improvisados controlados por radiofrecuencia, proporcionando protección a la patrulla que se desplaza en las áreas que existe este riesgo. La energía dirigida y la perturbación electrónica pueden considerarse como defensa electrónica cuando se emplean defensivamente.

- **Vigilancia electrónica:**

Es el empleo de la energía electromagnética para obtener conocimiento de la situación con objeto de reconocer la amenaza de acuerdo con los indicadores y alertas que determinan la actividad operativa en el entorno inmediato. Por lo que, no se circunscribe solo a telecomunicaciones, sino a cualquier emisión electromagnética.

Además de los sensores y los sistemas de guerra electrónica en los niveles operacional y táctico de las grandes unidades, existen una gran cantidad de equipos desplegados por las fuerzas terrestres. Estos son capaces de detectar la actividad electromagnética del enemigo, incluso en los escalones más bajos.

Así, la capacidad de intercambiar información entre todos los componentes del espectro electromagnético (sensores, plataformas de armas, órganos de decisión, fuerzas participantes,

etc.) es clave para las operaciones. De esta forma se permite disponer en tiempo real de la información necesaria para desarrollar la misión. El funcionamiento en red (o en común) proporciona ventajas operativas, como las siguientes:

- Conocimiento común de la situación operativa.
- Trabajo coordinado entre distintas unidades o plataformas.
- Optimización del empleo de los recursos disponibles.
- Mejora en el proceso de toma de decisiones, al disponer de una visión más completa del entorno operativo.

Con la guerra electrónica en red, se consigue la optimización del empleo de los recursos disponibles, al poder compartir la información captada por los distintos medios de guerra electrónica, radar e infrarrojos. Estos medios, son desplegados en otras áreas con el objetivo de realizar actividades electromagnéticas desde plataformas de unidades distintas, para actuar con más eficacia sobre un objetivo determinado.

La información sobre el adversario es clave, debido a que es necesario conocer ciertas características, tales como:

Entidad enemiga: Es necesario conocer y/o estimar la entidad enemiga ya que las fuerzas propias actuarán de distinta manera dependiendo de si la unidad es pequeña o grande. Así, se utilizarán medios más discretos si la entidad enemiga es tipo sección o batallón.

Inteligencia de las fuerzas enemigas: La inteligencia de las fuerzas enemigas determina su capacidad para procesar información y convertirla a conocimiento sobre su adversario. Esto también se traslada a la tecnología disponible y el uso que se le dé a ella.

Medios que dispone la fuerza enemiga: No sólo se debe investigar acerca de los medios que puedan irradiar o captar radiación electromagnética, sino que además habrá que tener en cuenta la capacidad y alcance del fuego enemigo. Esto es debido a que, a la hora de emitir una determinada señal, esta se tiene que hacer de forma rápida, para evitar ser detectados por el enemigo y de esta manera ser alcanzados.

Vehículos enemigos: Los posibles medios de guerra electrónica pueden ser usados desde vehículos, por ello es fundamental que se conozcan para el beneficio propio.

Frecuencias utilizadas por el enemigo: A la hora de realizar una acción de guerra electrónica, como por ejemplo perturbar, se debe tener en cuenta todos aquellos rangos de frecuencias y demás parámetros de interés para tal fin. Esto es debido a que no servirá, en este caso, inhibir un cierto rango de frecuencias, que además puede incidir sobre las fuerzas propias.

Autonomía logística: Como se ha podido observar en los conflictos a lo largo de la historia, la autonomía logística es clave para el éxito de la misión. Para ello, habrá que cerciorarse de los diferentes elementos entre los que cabe destacar:

- Combustible
- Alimentos
- Agua
- Repuestos vehiculares
- Munición

Tipo de jerarquía militar: A la hora de que el adversario responda ante una determinada acción y decisión, el tipo de jerarquía y estructuración que tenga será clave para el empleo de ~~los~~ medios, recursos y personal propios.

- *Aumento de potencia de combate propia:* impidiendo el uso del espectro electromagnético por parte del enemigo, y complementando esta acción con el uso de fuegos propios.

- *Seguridad y protección de unidades:* la mayoría de los sistemas de armas y tipos de munición, se basan y guían en el espectro electromagnético para la adquisición y eliminación de objetivos.

Siendo el procedimiento operativo:

- *Independencia:* los procedimientos operativos deben regular la necesaria homogeneización del planeamiento y la ejecución de las actividades de guerra electrónica necesarias para el adecuado apoyo independientemente de la situación y la misión encomendada. Estos solo se sustentan con los condicionantes que el propio sistema de guerra electrónica establezca.
- *Permanencia de los sistemas operativos:* necesario si se quiere llegar a disponer de un sistema de guerra electrónica. Los continuos cambios en los mismos llevan consigo una disminución de la efectividad del sistema.
- *Flexibilidad:* esta característica permite que los procedimientos puedan adaptarse a los cambios para una perfecta adecuación a la situación. No hay planeamiento que aguante una situación cambiante muy brusca, es por ello que los operadores y usuarios de guerra electrónica deben de ser capaces de tomar decisiones de forma rápida y acertada.
- *Globalidad:* los procedimientos que se determinen deben ser válidos independientemente del escalón de mando de que se trate, y deben ser perfectamente utilizables desde el más alto hasta el más bajo escalón de la cadena de mando. En cualquier situación los procedimientos deben ser conocidos y operables por todos los usuarios de guerra electrónica, de tal forma, que si falla un escalón de mando la misión no se interrumpa.
- *Agilidad:* esta característica permite que el sistema ofrezca un apoyo adecuado en tiempo y forma para lograr la mayor efectividad de acuerdo con la misión y ~~a~~ la situación. A su vez, se ve potenciada hoy en día por el amplio uso de sistema de información para el mando y control dentro de las grandes unidades.
- *Sencillez:* las operaciones actuales requieren poder aplicar toda la potencia de combate de una gran unidad, en un tiempo oportuno y en el momento que se determine.

Para que en una guerra electrónica se pueda llegar a favorecer la jerarquía militar, el sistema debe sustentarse en unos procedimientos fáciles de emplear en toda situación. Esta característica será fundamental a la hora del desarrollo de estos.

En el nivel táctico, las grandes unidades pueden ser apoyadas por unidades de guerra electrónica, normalmente en cuerpo de ejército o de división. La variedad de los espacios en los que se despliegan las Fuerzas Armadas hace cada vez más frecuente la presencia de unidades ligeras, con una gran dispersión y movilidad. A su vez, implica que actualmente sea normal llevar a cabo el apoyo de guerra electrónica hasta los escalones de ejecución más bajos. Por lo tanto, se cumple el principio de oportunidad y se obtiene el máxima efecto de las acciones de guerra electrónica.

- **Guerra electrónica en movimiento/ Guerra electrónica en apoyo al combate próximo**

Se basa en dotar de diferentes medios y recursos a las unidades desplegadas para proteger a convoyes y unidades ligeras de diferentes artefactos y perturbaciones electromagnéticas.

La variedad de escenarios interconectados, hace cada vez más común la presencia de unidades ligeras con una gran dispersión en su despliegue, una gran movilidad y desconocimiento de la amenaza. Esto implica que actualmente sea normal llevar a cabo el apoyo de guerra electrónica hasta los escalones de ejecución más bajos. De este modo, se cumple el principio de oportunidad y se obtiene el máximo efecto de las acciones de guerra electrónica.

Como consecuencia de ello, han surgido en estos años los siguientes conceptos de guerra electrónica:

- **Guerra electrónica contra IED (Improvised Explosive Device)**

Las operaciones que se llevan a cabo en escenarios con conflictos no convencionales, están sujetas a modificaciones y adaptaciones del equipo y material. Una de las principales amenazas es la lucha contra los artefactos IED, mediante el uso de inhibidores y otros recursos que se encuentran principalmente en convoyes móviles. Existen dos tipos:

- Activados por radio: engloba tantos las acciones encaminadas a impedir la activación y detonación de los IED, como las encaminadas a detectar dichas emisiones.
- Activados por infrarrojos: engloba las acciones encaminadas a impedir la activación y detonación de los IED activados por infrarrojos (perturbación), y las encaminadas a detectar dichas emisiones.

Protección de bases

Las Fuerzas Armadas desplegadas fuera de las fronteras españolas necesitan protección tanto física como en el espacio electromagnético, es por ello por lo que se requiere de diversos recursos para lograr tal fin.

Se denomina contramedida electrónica a todas aquellas medidas que emplean la energía electromagnética para impedir o reducir el uso por parte del enemigo del espectro electromagnético. El ataque de tipo *Spoofing* con señales AIS es un tipo de contramedida electromagnética. En general existen cuatro tipos de contramedidas electromagnéticas:

1. **Guerra electrónica en apoyo al combate próximo:**

Integra elementos de guerra electrónica dentro de unidades de combate en el escalón más bajo de mando, proporcionando el principio de oportunidad a la guerra electrónica en combates asimétricos.

El operador de guerra electrónica, además de operar los equipos e informar de la situación directamente al jefe de la unidad apoyada, es un combatiente más.

2. **Perturbación electromagnética:**

Es toda aquella radiación liberada en forma de onda electromagnética con intención de dificultar o impedir por parte del enemigo el espectro electromagnético. El uso de un dispositivo tipo *jammer* que inutilice un determinado rango de frecuencias sería un ejemplo de este tipo de contramedida electromagnética.

3. **Decepción electromagnética:**

Es toda radiación liberada en forma de onda electromagnética con intención de confundir, distraer o engañar al enemigo. El uso de la técnica *spoofing* con señales AIS es un ejemplo de este tipo de contramedida electromagnética.

4. **Neutralización electromagnética:**

Es toda radiación liberada en forma de onda electromagnética con intención de dañar temporal o permanentemente los equipos enemigos.

SOFTWARE Y HARDWARE

A la hora de implementar estas herramientas, se dispone de los siguientes medios:

A- <u>Software</u>

- **GNU Radio:** es un software diseñado por “Proyecto GNU”, implementado con C++ y Python. Permite crear sistemas de radio diseñados por software.

El programa cuenta con multitud de herramientas consistentes en elementos y cajones para representar los distintos módulos que componen cualquier elemento de transmisión con frecuencia modulada. Para trabajar con GNU Radio, es conveniente utilizar Linux o una distribución similar.

Por asesoramiento y recomendación del Sargento experto en captación y tratamiento de señales encuadrado en el gabinete de Sigilo es necesario utilizar la distribución Ubuntu. Se trata de una distribución de Linux que permite programar y trabajar de forma sencilla gracias a su interfaz. Para ello, conviene formatear un portátil o hacer una partición de disco duro y así no tener problemas de compatibilidad. La ilustración 15 muestra la interfaz correspondiente a Ubuntu.

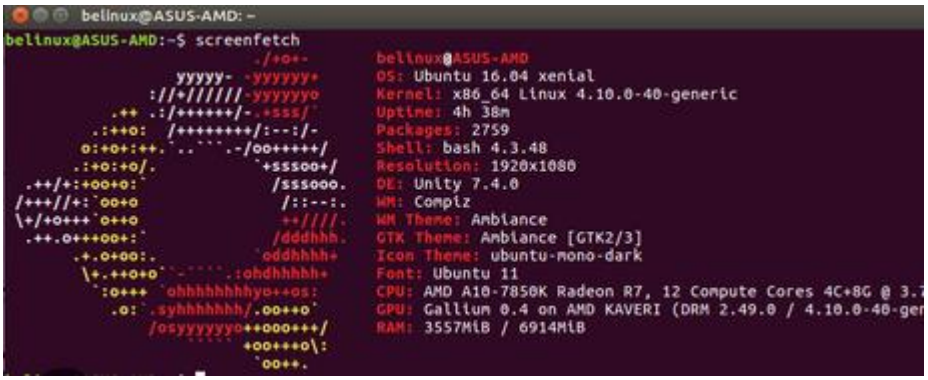


Ilustración 15. Interfaz de inicio de ubuntu. Ubuntu Log.

En el anexo 3 se especifica detalladamente cómo se debe instalar GNU Radio con la interfaz de Ubuntu.

Una vez realizados los pasos especificados en el anexo 3, se abrirá el programa. En la propia web se pueden encontrar ejemplos de diagramas y manuales de uso (Ilustración 16).

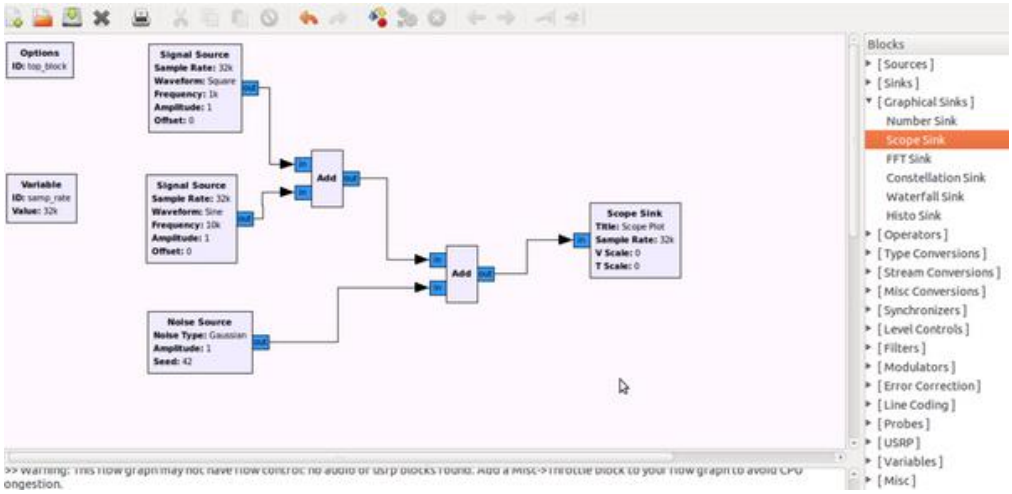


Ilustración 16. Presentación del interfaz del programa. GNU Radio

A su vez, para obtener el esquema del transmisor que permitirá mandar la señal AIS, se debe buscar en el repositorio GitHub el código específico. GitHub es una página web a través de la cual los usuarios pueden subir códigos y fuentes de software propios en Linux para compartirlo con el resto de la comunidad.

Para buscar el código deseado, se introduce en el navegador “AIS GitHub”.

Tras un estudio prolongado junto con el Sargento experto en captación y tratamiento de señales encuadrado en la Sección de Sigilo, se comprobó que el código que otorga la radio definida por software para enviar la señal AIS, está en “aistx”, en la página web de GitHub (Ilustración 17).

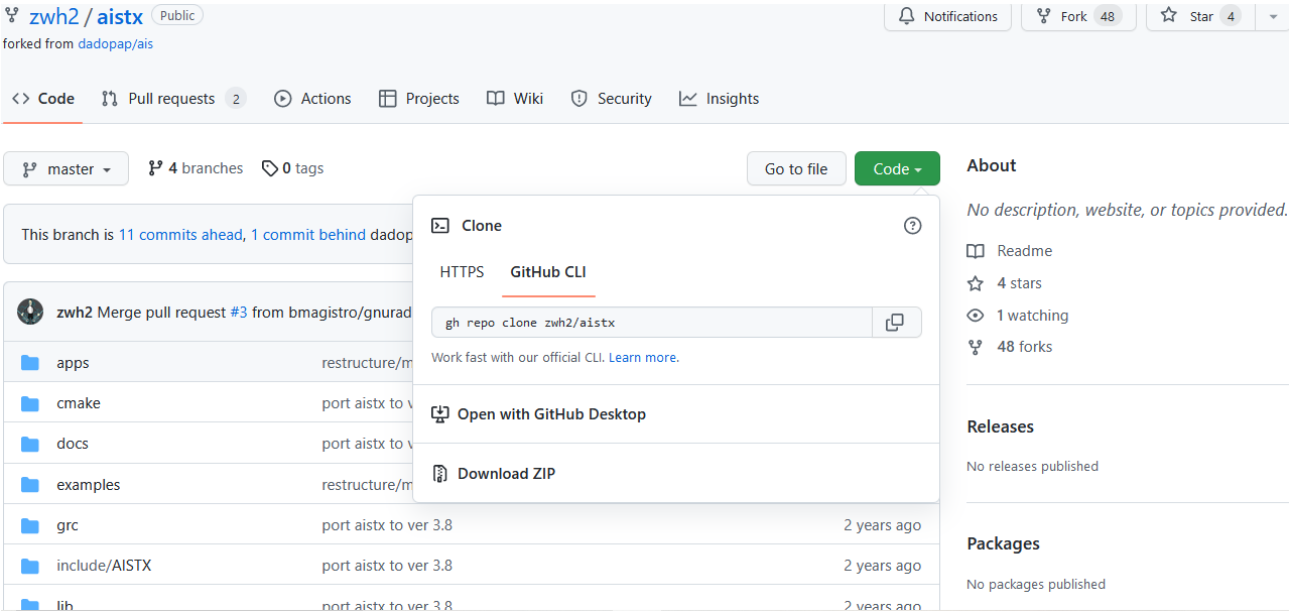


Ilustración 17. Interfaz de código de aistx. GitHub

Para poder descargar el código y la configuración en GNU Radio, hay que pinchar en el recuadro verde "*Code"* (Ilustración 17), y a continuación se copia el comando que aparece en GitHub CLI: *"gh repo clone zwh2/aistx".*

El comando citado se introduce en la terminal de Ubuntu, siguiendo los pasos descritos previamente. Después, el programa se ejecuta con los módulos ya instalados. La interfaz a la que se llega se muestra en la ilustración 18, mostrando el siguiente interfaz:

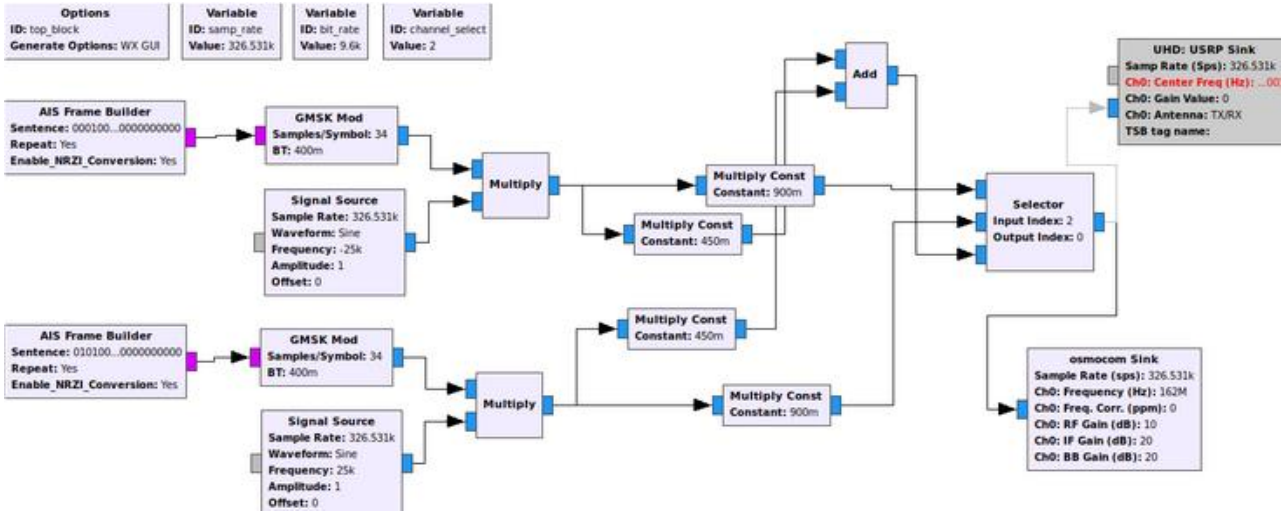
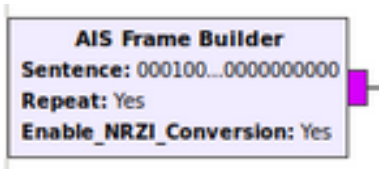


Ilustración 18. Esquema del interfaz de la prueba de laboratorio. Elaboración propia.

Se puede observar que el esquema del interfaz sigue una sucesión lógica de izquierda a derecha, siendo los módulos "*AIS Frame Builder*" las entradas, y "*osmocom Sink"* la salida de la radio definida por software.

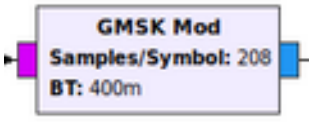
- **AIS Frame Builder**



Este módulo genera un código binario que es la base de la señal AIS. y Refleja todas las características del posicionamiento de la embarcación o navío. Como se puede observar, está configurado en modo periódico y la conversión "No retorno a cero invertido" (NRZI), se encuentra activada.

NRZI es uno de los métodos más comunes para convertir una señal binaria en una señal digital para poder transmitirla por el medio. Una de las características más comunes de esta codificación, es que es bastante inmune a los efectos del ruido y a otras interferencias. [11]

- **GMSK Mod**

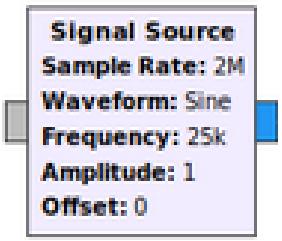


Es un modulador por desplazamiento mínimo gaussiano, que tiene como principal característica reducir el ancho de banda necesario para transmitir una señal. Esta modulación, en

concreto, se utiliza en otros ámbitos diferentes a los Sistemas de Identificación Automática como pueden ser:

a. Sistema global para las comunicaciones móviles.
b. Control de estaciones base.
c. Códigos estándar en redes.
d. Control de hogar.
e. Banda ancha sobre líneas eléctricas.

- **Signal Source**



Genera una señal base, que junto al multiplicador y al “AIS Frame Builder” mezclan la señal para obtener el producto deseado. Entre otros parámetros, se puede observar que la forma de la onda es de tipo “seno”, la frecuencia es de 25000 Hz, el valor de la amplitud es igual a 1, la frecuencia de muestreo equivale a 2 MHz, y la desactivación programada “Offset” equivale a 0.

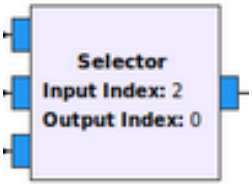
- **Multiply**

Multiplica dos señales de entrada, obteniéndose una señal de salida. Este módulo es necesario en las radios definidas por software, debido a que es un simplificador de circuitos, que minimiza la complejidad del circuito y maximiza su sencillez, y por lo tanto su eficacia.

- **Multiply Constant**

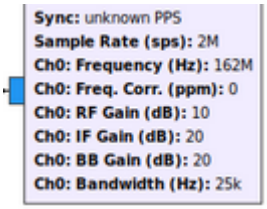
Multiplica la señal de entrada por una determinada constante. Este módulo es común ya que, en muchas radios definidas por software, se requiere de una constante para completar los circuitos debido a las pérdidas que estos sufren.

- **Selector**



El usuario decide qué entradas desea que sigan procesándose en el circuito. A la hora de seleccionar un determinado modo, función o constante es de vital importancia, ya que permite aumentar el ámbito de aplicación y/o agrupar distintas características en un mismo software, como es el caso propio.

- **Transmisor**



Representa todos los valores que se van a emitir, entre los que se encuentran la sincronización (Sync), frecuencia (Frequency), frecuencia acumulada (Freq. Corr), intensidad de señal que llega al emisor (RF Gain), frecuencia intermedia (IF Gain), frecuencia base (BB Gain) y ancho de banda (Bandwidth) [12]

- **SDR Angel:**

Junto con un *SDR* permite recibir señales en multitud de frecuencias y formatos. En este caso, es esencial para detectar las señales AIS. SDR Ángel puede ser descargado desde su página web, permitiendo el análisis de multitud de señales, y que según el propio programa, puede trabajar en los siguientes modos:

Tabla 3. Capacidades de SDR Angel.

Analógico	**Digital**
AM	802.15.4
APT	AIS
FM	ADS-B
DSB	APRS
NTSC	DAB
PAL	DAB+
SSB	DCF77
VOR	DMR

A su vez, el programa cuenta con multitud de herramientas e interfaces que permiten una visión rápida y cómoda de los datos. En la ilustración 19 se muestra un ejemplo de dicha interfaz obtenida de la página principal.

Ilustración 19. Presentación del software sdrangel. SDR Angel

Finalmente, cabe destacar que todo el software descrito hasta la fecha es de dominio público y civil, por lo tanto, no cuenta actualmente con las normas de seguridad en las tecnologías de información y comunicación del Centro Criptológico Nacional (CCN-STIC)

B- Hardware:

A continuación, se describirán los dispositivos hardware utilizado en las pruebas de campo, y en el laboratorio del Regimiento de Guerra Electrónica nº 31. Destacar que todos los materiales y recursos físicos que se expondrán se pueden obtener desde multitud de páginas de Internet. Actualmente, la tecnología aun teniendo menor nivel técnico que el expresado en el presente documento, es de fácil adquisición para cualquier usuario vía Internet.

A su vez, existen multitud de gamas económicas, por lo tanto, siempre habrá un modelo que pueda ser adquirido por un determinado usuario. La mayoría de los modelos vienen importados de la República Popular de China, por lo que no se respetan los estándares europeos en cuanto a seguridad y potencia que genera un riesgo añadido.

Entre los dispositivos más característicos, se destacan los siguientes:

- **Hack RF**

Este dispositivo, que contiene una Radio Definida por Software, es capaz de operar desde el rango de 1 MHz hasta los 6 GHz. [9] Además de ser ampliamente usado por radioaficionados, puede ser empleado para los siguientes usos:

1. Ingeniería Inversa.
2. Captar paquetes Wifi.
3. Digitalizar ondas de radio.
4. Captar comunicaciones no cifradas.

Ilustración 20. Hardware HackRF One. Great Scott Gadgets

- **Antena**

Con soporte magnético la cual conectada mediante puerto USB al ordenador y otro SDR, puede captar la señal y analizarla con SDR Angel. Una antena como esta, se encuentra en el gabinete de sigilo en el Regimiento de Guerra Electrónica nº 31.

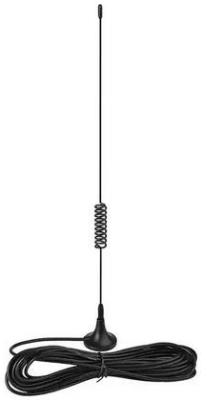


Ilustración 21. Antena. Amazon

- **RTL-SDR**

Es un dispositivo mucho más compacto, sencillo y económico que el SDR, mostrado previamente el Hack RF.

El rango de frecuencias en el que puede sintonizar comprende desde los 500 KHz hasta los 1.7 GHz. El sistema operativo se encuentra programado en Linux, la tecnología del sintonizar es digital y apenas pesa 30 gramos.

Ilustración 22. SDR. Amazon

ESTUDIO DE MEDIOS

Este estudio de medios se centra en la perturbadora BMR M1 de “guerra electrónica” (Ilustración 23), y que servirá para trasladar las pruebas realizadas en el gabinete de sigilo al propio campo de batalla.

Ilustración 23. BMR R1. Defensa

Esta estación perturbadora cuenta con las siguientes antenas dependiendo de la frecuencia deseada:

- Antena HF (High Frequency): 3-30 MHz
- Antena V/UHF (Very/ Ultra High Frequency): 30-3000 MHz

En la **Antena HF** se distinguen las siguientes ondas para transmitir o recibir señales.

Onda de superficie (Ground Wave):

Al desplegarla tiene una longitud de 15 metros, y una frecuencia de trabajo de 1.6 a 30 MHz. Como se observa en la Ilustración 24 la onda de superficie sigue la curvatura de la tierra, por lo tanto, es necesario que posea una frecuencia baja y una longitud de onda elevada.

Ilustración 24. Propagación de onda de superficie. Centro Andaluz

Onda ionosférica (Sky Wave)

La ilustración 25 muestra una onda ionosférica. Tiene una longitud de 12 metros y una frecuencia de trabajo de 1.6 a 30 Mhz.

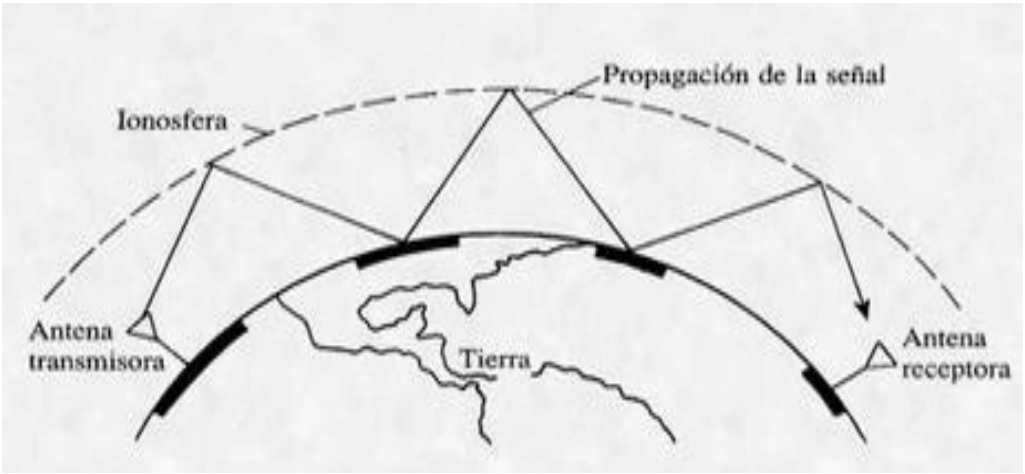


Ilustración 25. Propagación de onda a través de la ionosfera. Centro andaluz

La onda ionosférica depende principalmente de las condiciones meteorológicas de la zona de emisión ya que las precipitaciones, nubosidades y fluctuaciones en la densidad del ambiente, alterarán y/o hacen variar su capacidad de la onda de propagación a través del medio.

Las antenas HF cuentan con amplificadores entre los que cabe destacar los siguientes:

1. Amplificación y filtrado.
2. Conmutación entre transmisión y recepción.
3. Combinación de señales de recepción.
4. Control de períodos de transmisión y recepción.

Por otro lado, la estación de contramedidas **V/UHF** cuenta con las siguientes características:

1. Frecuencia de trabajo entre 20 y 30000 MHz.
2. Exploración en V/UHF.
3. Monitorización de una señal en V/UHF.
4. Clasificación de una señal en V/UHF.
5. Perturbación sobre una frecuencia.
6. Control remoto desde estación.

Y la estación perturbadora de **V/UHF** cuenta con cinco antenas cuyas frecuencias de detallan en la tabla 4.

Tabla 4. Frecuencias y capacidades de la perturbadora en V/UHF.

Antena	**MHz**
1	20-130
2	130-500
3	500-1000
4	1000-1700
5	1700-3000

Todas las antenas descritas previamente cuentan con una ganancia de cinco decibelios, y al desplegarlas cuentan con una altura de 3.8 - 4 metros. Además, los amplificadores cuentan con los siguientes rangos de frecuencia:

Tabla 5. Amplificadores de la estación perturbadora V/UHF, y frecuencias operables de estos

Amplificador	**MHz**
1	20-130
2	130-500
3	500-1010
4	1010-1700
5	1700-3000

Consecutivamente se dispone el explorador en **VHF**, que cuenta con las siguientes características:

1. Sintonía de la señal a medir.
2. Digitalización de la señal sintonizada.
3. Proceso digital sobre la señal sintonizada.
4. Control de todos los procesos.
5. Comunicación con el exterior.
6. Autocomprobación.
7. Inhibición para autoprotección.
8. Comunicación con dos radios PR4G suministradas por el Ministerio de Defensa.

Finalmente, se encuentran dos tipos de refrigeración en la estación perturbadora BMR M1 que son:

1. Aire Acondicionado/ Calefacción.
2. Refrigeración líquida: Amplificador, filtros y cargas.

Es especialmente útil la refrigeración líquida debido a que el sobrecalentamiento satura los componentes siendo posible su pérdida y/o inhabilitación. Además, dentro de la estación perturbadora BMR M1 se deberían introducir los siguientes recursos:

1. Portátil, con las siguientes características: 16 GB de RAM, 1 TB de almacenamiento en disco duro, procesador equivalente a un Intel i5 y una tarjeta gráfica de NVIDIA.
2. HackRF.
3. Preamplificador.
4. Cableado para conectar todo el sistema a la perturbadora.

PRUEBA DE FUNCIONAMIENTO

La prueba de funcionamiento tuvo lugar en el Gabinete de Sigilo (Sección de sigilo) el día 29 de septiembre de 2022 a las 11:35 horas. Emitiendo señal AIS con el siguiente sistema:

Portátil Personal (I) + Máquina virtual de Ubuntu con GNU Radio + HackRF+ Antena.

De forma inmediata el sistema compuesto por: Portátil Personal (II) + SDR Angel + RTL-SDR+ Antena recibió la señal AIS, con la interfaz en SDR Angel que se muestra en la ilustración 26:

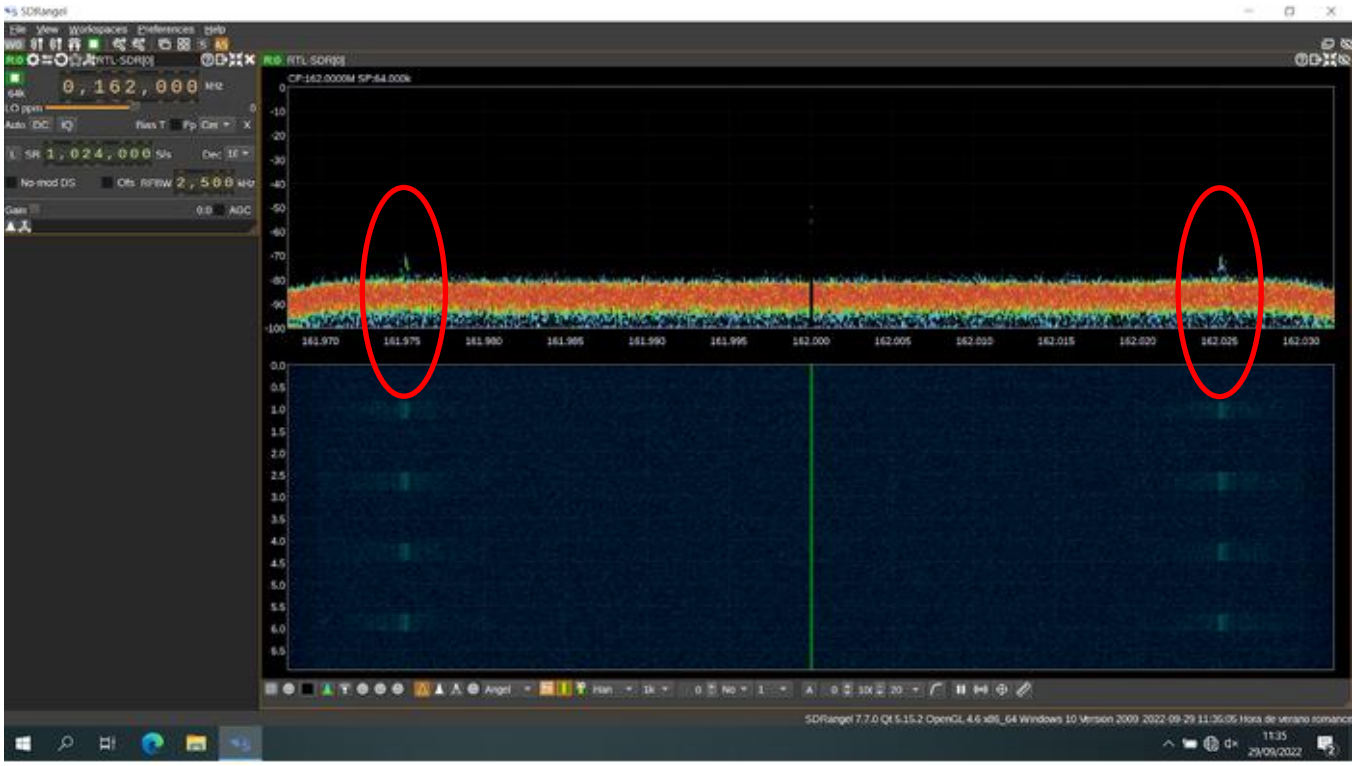


Ilustración 26. Recepción de señal AIS. Elaboración propia.

Se pueden observar dos frecuencias principales en 162.025 MHz y 161.975 MHz característicos de la señal AIS. La principal razón por la que se emiten dos señales es que el estándar AIS requiere de forma normalizada dos frecuencias, el canal 87 B (161.975 MHz) y el canal 88 B (162.025 MHz). [8]

El funcionamiento de la práctica de laboratorio es el siguiente:

A través del software GNU Radio y el correspondiente esquema del transmisor de AIS, se envía la señal al “Hack RF”. Este, interpreta la señal digital y la transforma en impulsos eléctricos que son enviados a la antena portátil. Seguidamente, la antena portátil envía la señal a través del medio y es captada por el SDR del receptor.

El SDR del receptor transforma la señal analógica en digital, y Finalmente, el programa “SDR Angel” interpreta la señal.

Como se puede ver, en la parte superior izquierda aparecen las siguientes pestañas: “File”, “View”, “Workspaces”, “Preferences” y “Help”.

Para la realización de las prácticas de campo, solo se usó la pestaña “File” para realizar una grabación de pantalla. La pestaña “Workspaces” es de gran utilidad, ya que permite desplegar varios elementos de estudio, bien de recepción o de transmisión.

La estructura horizontal naranja, representa el ruido que capta la antena.

La barra vertical verde delgada, indica la frecuencia central a la que recibe el software.

En la parte inferior de la ilustración, aparecen distintas herramientas que permiten redondear o aproximar la onda hasta un valor determinado. (En este estudio no ha sido necesario).

PROPUESTA DE PROCEDIMIENTO DE EMPLEO EN EW

El procedimiento de empleo en EW, una vez que se tienen todos los recursos (software y hardware), se lleva a cabo según se describe a continuación.

Entre los parámetros que se deben otorgar a los usuarios de la estación perturbadora BMR M1 para proceder a emplearla, destacan los siguientes:

- Frecuencia.
- Modulación.
- Ancho de banda.
- Potencia.
- Duración.

Una vez que se han definido los principales parámetros para operar de forma correcta en la estación perturbadora, se realiza el siguiente procedimiento:

1. Búsqueda:

Es la exploración continua y sistemática del espectro electromagnético para descubrir cualquier actividad de interés.

Los sistemas modernos de guerra electrónica permiten realizar exploraciones automáticas de anchos de banda limitados del espectro, dando como resultado datos, y conteniendo aquellas frecuencias en las que se ha detectado actividad, además de determinados datos técnicos en relación con la misma.

2. Interceptación:

Es el análisis de la emisión descubierta con el fin de extraer la información técnica y de contenido preciso para proceder a su posterior identificación y explotación. Esta actividad se lleva a cabo en los centros de interceptación. En el caso de que la misión interceptada fuera considerada de alto interés será necesario realizar el seguimiento de la misma.

3. Localización:

Es la determinación de la situación geográfica del emisor interceptado (en este caso marina), mediante el empleo de medios de radiogoniometría, utilizando técnicas de triangulación basadas en la determinación del ángulo de llegada del frente de ondas a distintos receptores situados en posiciones conocidas.

Esta actividad será llevada a cabo por los centros de inteligencia con el apoyo de las bases radio goniométricas. Las acciones de exploración e interceptación llevarán normalmente aparejadas las localizaciones correspondientes.

A continuación, se deben introducir las medidas de tipo táctico, que Son aquellas que aprovechan los dispositivos técnicos que están incorporados a los sistemas electrónicos propios para oponerse a las acciones de guerra electrónica de los posibles adversarios.

Consisten en:

- Utilizar equipos de banda ancha.
- Utilizar equipos de salto de frecuencia.

- Utilizar equipos de salto temporal.
- Aprovechar la diversidad de frecuencia.
- Utilizar control de interferencia.
- Cambiar los parámetros de emisión.
- Utilizar antes especial muy direccionales que eliminen lóbulos laterales.
- Utilizar conexiones multienlace que proporcionen vías alternativas.

Por otro lado, están las medidas de tipo táctico, que son aquellas que aplican los jefes de unidad asesorados por oficiales de transmisiones, tanto aplicadas al despliegue de medios electrónicos, como de establecimiento del régimen general de empleo de los medios.

Son las siguientes:

- Establecer la ubicación y empleo de los medios de mando y control para reducir el riesgo de detección.
- Instalar las antenas adecuadamente, de forma que el terreno haga de pantalla y atenúe las emisiones de radiofrecuencia.
- Conseguir que las antenas que se utilicen no ofrezcan, por sus características, mayores alcances de los planeados.
- Utilizar en lo posible, en las frecuencias de la banda V/UHF, la mínima potencia necesaria para asegurar la comunicación.

Finalmente, están las medidas de procedimiento. Que Son aquellas que regulan el empleo y manejo de los medios electrónicos que deben aplicar los operadores para reducir los efectos de las posibles contramedidas de guerra electrónica del adversario.

Consisten en las siguientes acciones:

- Cambios de frecuencias.
- Empleo de cifrado cuando sea posible.
- Cambio de los tipos de modulación
- Ausencia de transmisiones que no estén autorizadas y evitar las señales de prueba y de sintonía.
- Utilización de la mínima potencia necesaria.
- Reducción de transmisiones a las mínimas necesarias y seguimiento riguroso del proceso de transmisión.
- Reducción de las emisiones de no telecomunicaciones a lo estrictamente necesario.
- Cumplimiento del plan de control de emisiones.

También se debe tener en cuenta, que el enemigo puede intentar introducirse en nuestro sistema de telecomunicaciones y simular tráfico propio para confundir y engañar a nuestras fuerzas. El éxito del enemigo, por la tanto, depende en gran parte de la despreocupación o imprevisión del personal relacionado con el empleo de los medios de guerra electrónica.

Para proteger los sistemas y medios de guerra electrónica, hay que tener en cuenta los siguientes aspectos:

- Utilización rigurosa de los procedimientos de transmisión.
- Conocimiento de los operadores, para reconocer irregularidades en los procedimientos y en las características de tono o manipulación.
- Determinación en la demora de transmisiones de origen dudoso.
- Hacer poco uso del lenguaje en claro, en sistemas no protegidos (por cifra o medidas de tipo técnico).
- Uso de procedimiento de autenticación ante el menor indicio de intrusión y con relativa frecuencia para garantizar la seguridad.

CONCLUSIONES

Este trabajo confirma la viabilidad del uso de la tecnología *spoofing* con señales AIS con los medios disponibles en el Regimiento de Guerra Electrónica nº 31, con la limitación de introducir un módulo en GNU Radio para poder mandar una señal AIS con información en el espectro electromagnético. Gracias a los diferentes casos de uso de forma temporal, se ha podido definir la capacidad de *spoofing* y diferenciarlo del término *jamming*. Además, aportar claridad en definiciones, así como experiencia a la comunidad científica.

El estudio de los medios y doctrina del Regimiento de Guerra Electrónica nº 31, del material y equipo, de la observación en el campo de maniobras, de los diversos manuales y reglamentos sobre guerra electrónica, han permitido concluir que esta es una disciplina que avanza de forma significativa, afectando prácticamente a cualquier ámbito social.

En este trabajo ha resultado clave el trabajo de oficiales, suboficiales y tropa, proponiendo mejoras en las medidas y procedimientos para aplicar esta tecnología en las operaciones y misiones en las que las Fuerzas Armadas se encuentran actualmente presentes, a fin de aprovechar con plenitud la capacidad de guerra electrónica *spoofing* a señales AIS en un entorno cambiante y fluido.

Para terminar de alcanzar el objetivo deseado, sería conveniente poder disponer de tiempo semanal suficiente en el gabinete de sigilo (Sección de Sigilo, Compañía de Telecomunicaciones). Y Una vez desarrollado el software al completo, proceder a instalar el portátil personal, con la radio definida por software y los elementos de cableado en la perturbadora móvil “BMR R1 EW”.

REFERENCIAS BIBLIOGRÁFICAS

[1] http://nauta360.expansion.com/2013/08/14/muy_exclusivo/1376492751.html

[2] https://insidegnss.com/reports-of-mass-gps-spoofing-attack-in-the-black-sea-strengthen-calls-for-pnt-backup/

[3] https://www.mdpi.com/2076-3417/11/11/5015

[4] https://ieeexplore.ieee.org/abstract/document/7271729

[5]https://ieeexplore.ieee.org/abstract/document/6641132?casa_token=A7yS2LTLfacAAAAA:94gXWnOc8FqkYrSr5ICY7iSnFB0LKGKtGne9X6DGBJ-tHUv2fo1zzj0IIqpNKVU9fGKkYllY.

[6] https://ieeexplore.ieee.org/abstract/document/9011328

[7] https://aip.scitation.org/doi/abs/10.1063/5.00604288

[8] https://www.azimutmarine.es/seguridad-ais

[9] https://www.jtsec.es/es/entrada-blog/111/usos-comunes-y-puesta-en-marcha-de-una-hackrf-one

[10] https://ejercito.defensa.gob.es/noticias/2020/12/8224_unidades_aquiles_20.html

[11] https://www.uv.es/~hertz/hertz/Docencia/teoria/codificacion.pdf

[12]https://www.edaboard.com/threads/how-we-can-decide-for-set-bb-gain-if-gain-rf-gain.364402/

[13] https://www.redseguridad.com/actualidad/cibercrimen/spoofing-que-es-y-como-prevenir-la-suplantacion-de-identidad_20220120.html

[14] https://ajax.systems/es/blog/what-is-jamming/

[15] https://www.nytimes.com/es/2021/07/19/espanol/canal-suez-evergiven.html

ILUSTRACIONES

Ilustración [26] Elaboración Propia.

ANEXOS

[1] Encuesta realizada a los usuarios de Guerra Electrónica

1. ¿Qué necesitaría para desarrollar la capacidad de guerra electrónica “*Spoofing”* con señales AIS?

2. ¿Le gustaría disponer de alguna funcionalidad software para desarrollar la capacidad de guerra electrónica “*Spoofing”* con señales AIS?

3. ¿Le gustaría disponer de algún elemento hardware para desarrollar la capacidad de guerra electrónica “*Spoofing”* con señales AIS?

[2] Preamplificadores pertenecientes a la Sección de Sigilo, Regimiento de Guerra Electrónica nº31.

. Preamplificador. Amazon.

. Preamplificador. Amazon

Característica:

1. El amplificador de RF está hecho de materiales de alta calidad, con baja figura de ruido y buena durabilidad.
2. Con carcasa blindada, el rendimiento es más estable y se puede utilizar durante mucho tiempo.
3. El ancho de banda es de 1MHz a 2GHz, 64DB de alta ganancia, la ganancia es diferente a diferentes frecuencias.
4. Cuando se requieren diferentes valores de ganancia, la tensión de alimentación puede reducirse.
5. Fabricación profesional, mano de obra exquisita, fácil instalación y desmontaje.

Especificación:

Condición: 100% nuevo
Tipo de artículo: Amplificador de bajo ruido
Material: metal
Voltaje de la fuente de alimentación: 12V CC (corriente 70MA)
Ganancia: 64DB
Impedancia de entrada y salida: 50 ohmios
Potencia de salida máxima: 10dBm (bajo 2VPP \ 50 ohm de carga)
Señal de entrada: <= - 54DBM (la señal de salida se ha distorsionado cuando la entrada es mayor que -54 dBm)
Ancho de banda: 1MHz - 2GHz (La ganancia es diferente en diferentes frecuencias, consulte el índice de curva S21 para más detalles)
Figura de ruido: 2dB (medido a 0,5 GHz)
Ganancia del método de frecuencia de puntos:
F = 30.29MHZ GAIN = 63.41 dB
F = 310.2MHZ GAIN = 66.43 dB
F = 620.2MHZ GAIN = 64.54dB
F = 880.1MHZ GAIN = 59.08 dB
F = 1.210GHZ GAIN = 55.59 dB
F = 1.590GHZ GAIN = 48.18 dB
F = 1.810GHZ GAIN = 38.44 dB
F = 2.000GHZ GAIN = 39.58 dB

Lista de paquetes:

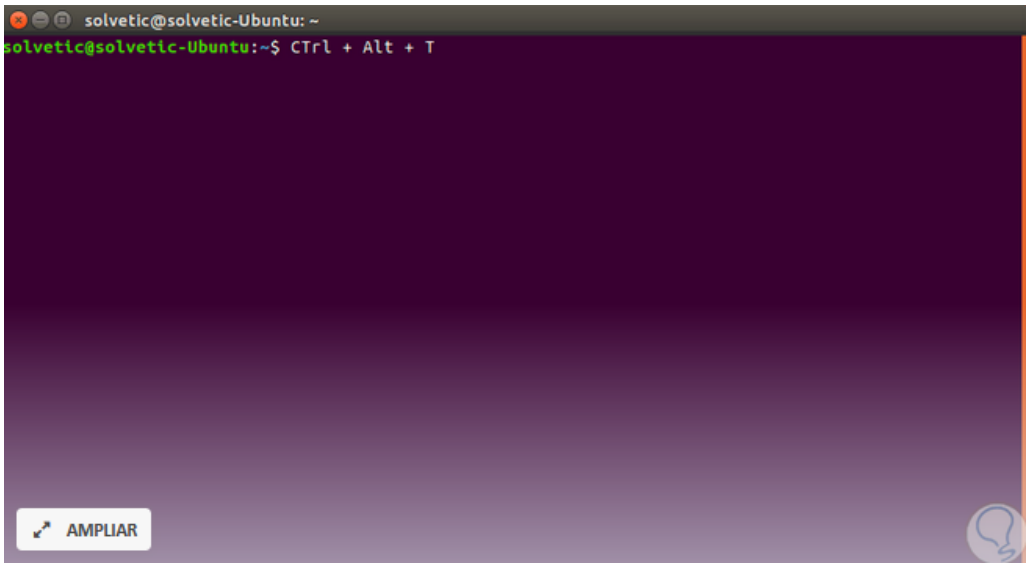
1 x amplificador de bajo ruido

Características técnicas del preamplificador. Amazon.

[3] Instalación de GNU Radio en la Interfaz de Ubuntu

A la hora de descargar un programa determinado en una distribución de Linux, no se puede hacer de forma directa; sino que hay que introducir una serie de comandos para llegar al programa en cuestión; los cuales son los siguientes.

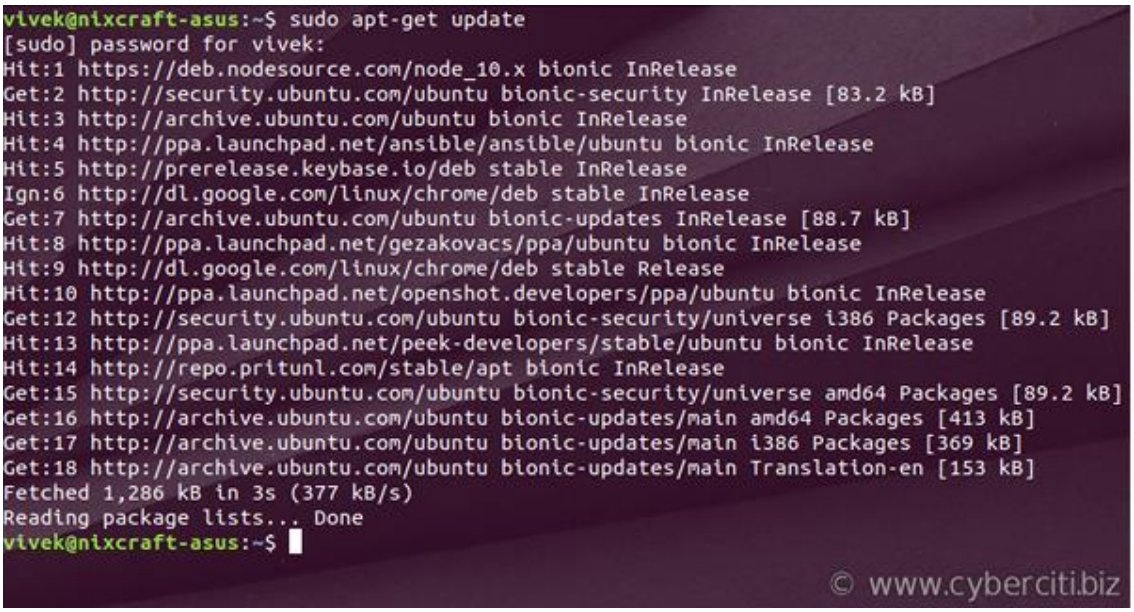
1. Abrir la terminal, para ello introducir el siguiente comando: *Control + Alt + Suprimir.*



Terminal de ubuntu. 1. Solvetic

2. Teclear en la terminal: “*sudo apt-get update”*

De esta forma, la terminal buscará en las librerías de Linux todas las actualizaciones y paquetes disponibles. Esto es especialmente importante y no debemos eliminar este paso ya que de forma contrario aparecerán multitud de errores y problemas en el terminal.

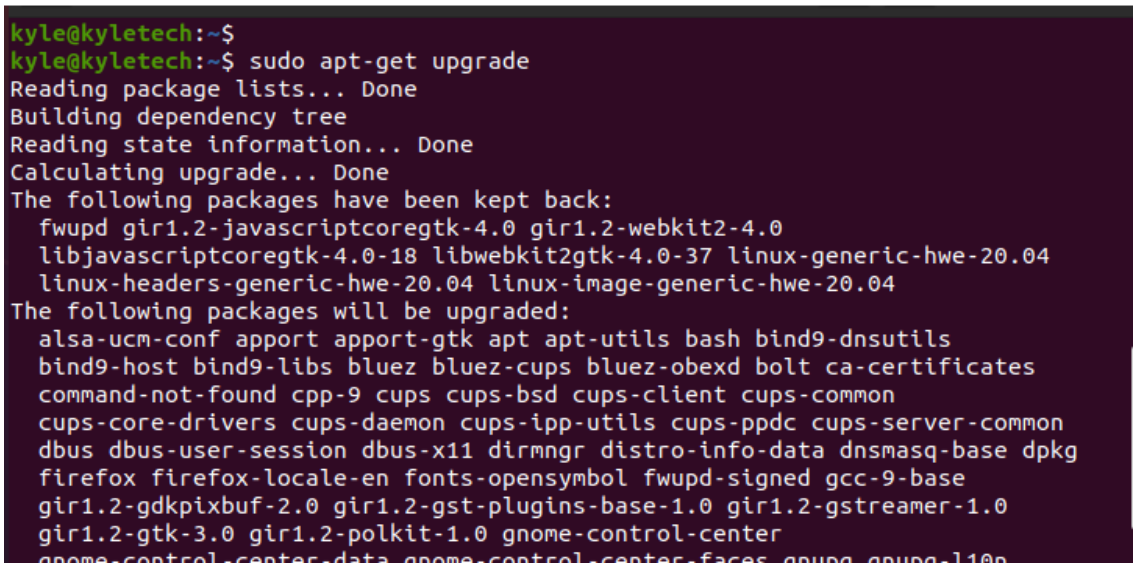


Interfaz de actualización de paquetes. Cybercity

Como podemos ver en la ilustración, la terminal busca las actualizaciones más recientes de los paquetes a utilizar.

3. Teclear en la terminal el comando: “*sudo apt-get upgrade”*

Este comando permitirá instalar todas las actualizaciones realizadas hasta el momento, completando finalmente la instalación. Cabe recalcar que el comando “*sudo*” debe ser introducido, ya que entraremos en modo privilegiado y no habrá problemas de instalación y/o compatibilidad.



Interfaz de instalación de paquetes de ubuntu. linuxhint.com

Una vez finalizada la instalación, la terminal devolverá la palabra “*Done*”.

1. Finalmente, reiniciar el ordenador para asegurar que se hayan guardado todas las actualizaciones.

   A continuación, instalar GNU Radio. Para ello, introduciremos los siguientes comandos, desde la terminal previamente abierta.

2. Introducir en la terminal el comando: “*sudo apt-get install gnuradio”.*

De esta forma, la terminal descargará todos los paquetes correspondientes para que GNU Radio funcione de manera correcta.

Ilustración 22. Interfaz de descarga de GNU Radio. YouTube

Presionar la tecla “*Enter*” y la terminal comenzará a descargar paquetes. Una vez descargados, nos preguntará si quieremos continuar, de la siguiente forma.

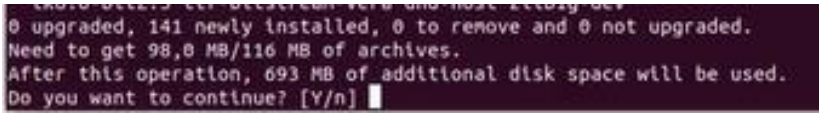


Ilustración 23. Interfaz de descarga de GNU Radio. YouTube

Presionaremos la tecla “*y”* y esperaremos a que la descarga se realice por completo.

1. Ejecución de la aplicación

   Una vez que la instalación se haya completado, se introducirá el comando: “*gnuradio-companion”*, tras lo cual la terminal abrirá el programa.

Ilustración 24. Interfaz de inicio de GNU Radio. YouTube