2.8

La radio definida por software (SDR) como herramienta para integrar la guerra electrónica y la ciberguerra en la capacitación del personal

Por el CR Com (R) OIM Rafael Olivieri (*)
Co-autores: CR Com (R) OIM Adrián Buscaglia, Ing. Ignacio Raffo Triaca
e Ing. Ignacio Omaechavarría

Temario

Introducción.
Desarrollo y propuesta.
Componentes de Software.
Software probado.
¿Qué podemos hacer con estas herramientas?
Conclusiones.

Resumen

La Ciberguerra se ocupa de asegurar el propio uso del ciberespacio y de negar su uso al enemigo u oponente mediante el software y las redes de datos en genera, y podemos decir que su dominio es el ciberespacio, mientras que la Guerra Electrónica (EW)[1] hace lo propio en el espectro electromagnético, siendo éste su dominio.

Pero sabemos que muchas redes emplean el espectro electromagnético, y vemos aquí un nexo entre ambos dominios. Por lo tanto existe una posibilidad de colaboración entre la ciberguerra y la guerra electrónica, tanto en el ataque como en la defensa.

Desafortunadamente existen diferencias importantes que impiden la integración o al menos la colaboración entre ambos dominios. No hay muchos expertos que operen en los dos dominios, la ciberguerra está en el ámbito de la informática mientras que la guerra electrónica dentro de la electrónica y las comunicaciones.

1 Electronic Warfare – EW.

Los sistemas de radio definidos por software (SDR)[2] se basan en interfaces de software y computadoras. Las funciones que desarrollaban los circuitos electrónicos se hacen por software y los avances son mayores. Mientras que las redes de datos emplean cada vez más el espectro electromagnético, y, por lo tanto, los sistemas basados en SDR ofrecen un enorme potencial para fomentar la colaboración ciberguerra – guerra electrónica.

Queda entonces proponer proyectos que promuevan esa integración, en principio basados en software libre y dispositivos de bajo costo. El principal rédito de ésto es el incremento en el nivel de capacitación del personal, que estará en mejores condiciones de crear medidas y contramedidas en un entorno cada vez más innovador y cambiante.

El resultado será un mejor nivel de entrenamiento y personal preparado para responder en un escenario que presenta indistintamente a la guerra electrónica y a la ciberguerra en forma común.

PALABRAS CLAVE: SOFTWARE DEFINED RADIO – RADIO DEFINIDA POR SOFTWARE (SDR). CIBERGUERRA. CIBERDEFENSA. GUERRA ELECTRÓNICA. ESPECTRO ELECTROMAGNÉTICO. CIBERESPACIO.

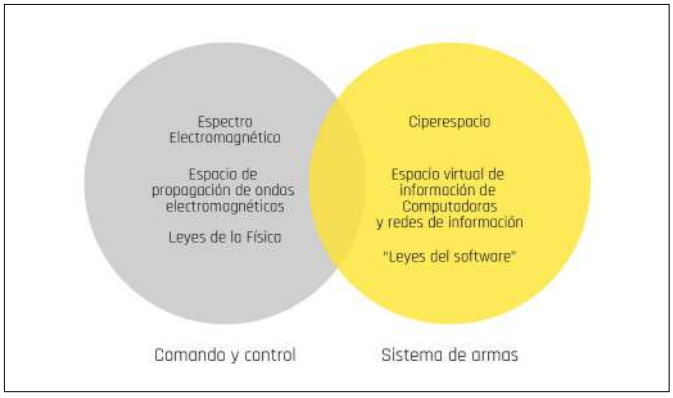
Introducción

La guerra electrónica se desarrolla en el espectro electromagnético, mientras que la ciberguerra lo hace en el ciberespacio. Ambas desarrollan actividades defensivas, para proteger los recursos propios, y ofensivas para negar el empleo de los espacios (espectro electromagnético y ciberespacio) al enemigo u oponente.

Lo mismo podemos decir del desarrollo de actividades pasivas, no detectadas por el enemigo u oponente, destinadas a obtener información, y activas, que involucran el ataque a los sistemas del enemigo u oponente.

En consecuencia, ambas actividades son similares, y además comparten factores comunes, como el software y el espectro electromagnético.[3]

FIGURA 1: ESPECTRO ELECTROMAGNÉTICO Y CIBERESPACIO



Se ha divulgado ya el uso de sistemas de radio definidos por software (SDR) para empleo educativo y también se ha propuesto como un medio para permitir a los profesionales cibernéticos y de EW comprender mejor las similitudes y diferencias entre ambos dominios e identificar formas de colaboración.

SDR presenta la oportunidad más importante, que es la posibilidad de proporcionar a todos

2 Software Defined Radio – SDR.

3 TEC1000 – edición 2024 "La Guerra Electrónica y la Ciberguerra en el conflicto de Ucrania"

y cada uno de los alumnos un sistema que les permita explorar el espectro electromagnético, animándoles así a desarrollar una mejor comprensión de este entorno único. También poder analizar señales de datos y disectar y analizar protocolos de redes. Existen muchas posibilidades más destacando la disponibilidad de hardware SDR de bajo costo y paquetes de software SDR gratuitos y de código abierto. Estas oportunidades incluyen permitir a los alumnos construir y examinar modelos de sistemas complejos y la implementación de sistemas EW y ciberguerra avanzados.

La propuesta entonces es desarrollar un proyecto que permita acercar ambos dominios mediante la capacitación. Obviamente habrá expertos en guerra electrónica y en ciberguerra, pero necesitamos contar con personal que entienda la intersección de ambos dominios para dar respuesta a las necesidades que plantea la guerra moderna, como hemos visto en los conflictos recientes y en desarrollo, como la Guerra de Ucrania. Debemos capitalizar la experiencia ajena, la propia llegará tarde, y hoy podemos ver lo que sucede con relación a los conflictos modernos:

a Paradojas, como tecnologías modernas que otorgan precisión a sistemas de armas, como el guiado de munición por GPS no pueden emplearse cuando la guerra electrónica del enemigo no lo permite, y se prefieren sistemas antiguos, menos precisos pero no vulnerables.
b El software embebido en diferentes dispositivos, que potencia sus prestaciones, puede resultar inoperante y hasta producir efectos en contra propia si es vulnerable a la ciberguerra del enemigo.
c Las infraestructuras críticas ya no son solo vulnerables a los ataques por fuego o sabotaje (ataques cinéticos), sino también por ciberataques, en la medida en que cada vez dependen más de las tecnologías de la información y las comunicaciones.
d En general las tecnologías avanzadas que potencian sistemas de armas, para que sean más eficaces, eficientes y ocasionen el mayor efecto sobre el enemigo, pueden resultar inocuas y obsoletas frente a acciones inteligentes de guerra electrónica y ciberguerra.

Las soluciones tecnológicas, medidas y contramedidas ya no se esperan tanto de los proveedores de sistemas de armas o servicios tecnológicos, deben obtenerse en el campo de batalla. Deben ser inmediatas, la dinámica de la guerra moderna no puede esperar los tiempos administrativos de nuevas adquisiciones. Los expertos en tecnología deben estar ahora en las unidades de combate.[4]

Desarrollo - Propuesta

Nuestra propuesta consiste en el desarrollo de una plataforma basada en software libre y dispositivos SDR de bajo costo para vigilar el espectro electromagnético en busca de amenazas a la seguridad de los sistemas propios, tanto militares como de infraestructuras críticas, con foco en la capacitación y entrenamiento del personal dedicado a guerra electrónica y ciberguerra. Se trata del proyecto SIGINT, "Inteligencia de señales de radiofrecuencia para guerra electrónica y ciberdefensa".

Si bien se han empleado dispositivos de bajo costo en operaciones militares, como la Guerra de Ucrania, nuestro objetivo es la capacitación exclusivamente.[5]

Este desarrollo permite introducir nuevas tecnologías de bajo costo que permiten analizar e interpretar señales del espectro electromagnético, junto con el aporte de las tecnologías de la infor-

4 https://www.fie.undef.edu.ar/ceptm/?p=8116 - "El Ejército de EEUU evalúa incorporar programadores en unidades de guerra electrónica y ciberguerra en operaciones"

5 https://www.fie.undef.edu.ar/ceptm/?p=11227.

mación que permitan interpretar la información obtenida, y si fuera posible desencriptarla cuando estuviera cifrada a fin de extraer la información que se transmite.

Estas últimas tecnologías tienen la potencialidad de incrementar cuantitativa y cualitativamente la vigilancia y análisis que se puede realizar del espectro electromagnético para detectar y prevenir amenazas, particularmente con el aporte de la minería de datos y la inteligencia artificial.

La capacitación del personal de ciberguerra y guerra electrónica se incrementa con la posibilidad de ejecutar prácticas en situaciones reales, a la vez que aporta motivación, calidad y posibilidad de crecimiento con el desarrollo de nuevos proyectos.

Los recursos computacionales aportan productividad y calidad en la ejecución de actividades de guerra electrónica y ciberguerra, a la vez que son mas accesibles desde el punto de vista económico, al menos para la capacitación y el desarrollo de proyectos específicos aplicados a la ciberguerra y guerra electrónica.

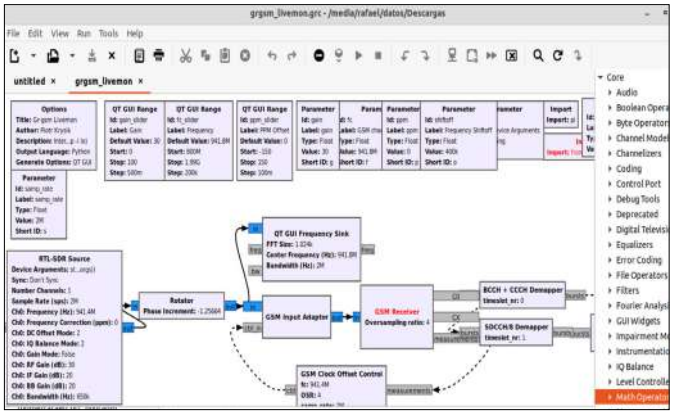
El conocimiento y experiencia obtenidos estarán disponibles al empleo militar y civil de manera dual, puesto que al ser de libre disponibilidad, no implica ningún tipo de restricción ni secreto, y por lo tanto se pueden emplear en forma dual. La comunidad en general, la industria y el sector estatal, cuentan con recursos e infraestructuras críticas vulnerables, que también se deben proteger al igual que los recursos humanos abocados a esa tarea necesitan medios para capacitarse y entrenarse, entre los cuales los productos de este proyecto sin duda contribuyen.

Componentes de Software

Empleamos únicamente código abierto y probamos software basado en GNU. GNU Radio que es un conjunto de herramientas de desarrollo de software gratuito y de código abierto que proporciona bloques de procesamiento de señales para implementar radios definidas por software (SDR). Se puede utilizar con hardware de radiofrecuencia (RF) externo de bajo costo y disponible para crear radios definidas por software, o sin hardware en un entorno similar a una simulación. Se utiliza ampliamente en entornos de investigación, industria, academia, gobierno y aficionados para respaldar tanto la investigación de comunicaciones inalámbricas como los sistemas de radio del mundo real.

FIGURA 2: PROYECTO GNU RADIO

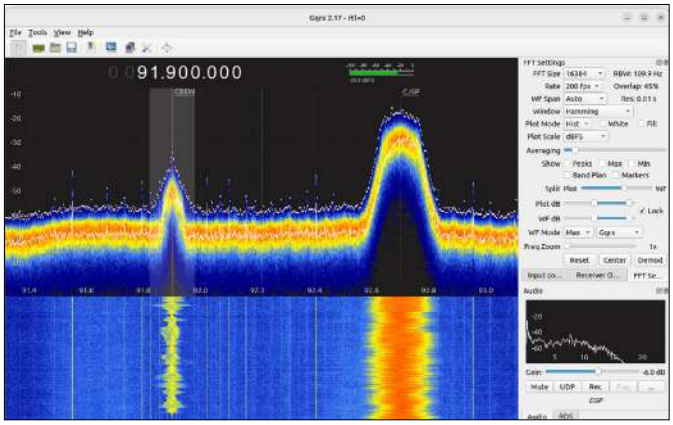
FIGURA 3: INTERFAZ DE GNU RADIO



A todo esto, podemos decir que la radio definida por software (SDR) es un sistema de radio que realiza el procesamiento de señales requerido en software en lugar de utilizar circuitos integrados dedicados en hardware. El beneficio es que, dado que el software se puede reemplazar fácilmente en el sis-

tema de radio, el mismo hardware se puede usar para crear muchos tipos de radios para muchos estándares de comunicaciones diferentes; por lo tanto, una radio definida por software se puede utilizar para una variedad de aplicaciones, incluso se puede modificar, perfeccionar sin cambiar el dispositivo de hardware. Esto es particularmente importante, puesto que en guerra electrónica permite implementar características o propiedades a requerimiento, como nuevas modulaciones, formas de onda y hasta medidas de seguridad o Contra Contra Medidas Electrónicas, tanto en el ataque como en la defensa.

FIGURA 4: RECEPTOR GQRX



Como receptor probamos GQRX el cual es un receptor de radio definido por software (SDR) de código abierto impulsado por GNU Radio y el kit de herramientas gráficas Qt.

Gqrx admite muchos de los dispositivos de hardware SDR disponibles, incluidos Airspy, Funcube Dongles, rtl-sdr, HackRF y dispositivos USRP. De estos, probamos Dongle y HackRFOne.

Por otra parte funciona en varias plataformas: Windows, Linux y Mac, empleando en nuestro caso la versión para Linux.

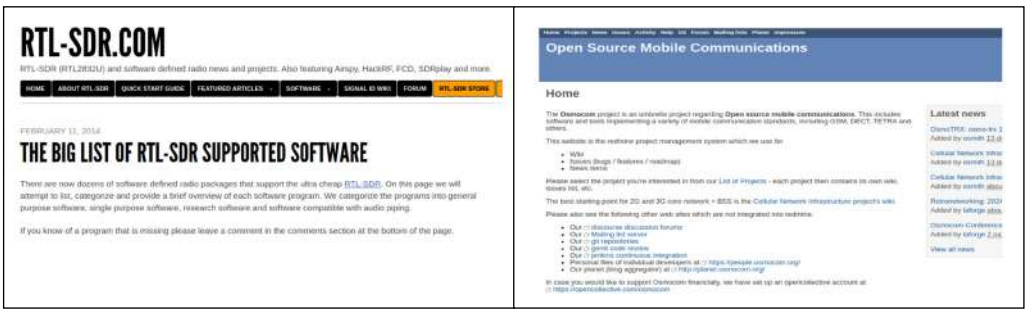
Además de todo esto cuenta con un analizador o visor del espectro de la señal recibida, una herramienta muy importante a la hora de analizar diferentes señales recibidas y esto es particularmente muy importante para la capacitación.

Software probado

En la red existen numerosos sitios mantenidos por comunidades entusiasta del software y la radio SDR donde se puede obtener información y recursos relacionados a las plataformas basadas en SDR y software libre.

Uno de los principales es www.rtl-sdr.com basado en los dispositivos RTL-SDR Dongle, los mas baratos y fáciles de usar, pero también incluye información de muchos mas.

FIGURA 5. PROYECTO RTL-SDR



Pero tal vez la parte más interesante de este sitio, a los fines educativos es la wikipedia de señales, dónde se pueden observar capturas de señales de diferentes equipos civiles y militares, de comunicaciones o no, exponiendo cómo se ven esas señales en el analizador de espectro y como se escuchan. Esto constituye una base de datos muy importante a la hora de capacitar personal, desde lo más básico, como reconocer si una señal es analógica o digitar y hasta reconocer otros parámetros más complejos como el propio equipo emisor.

Otra fuente importante, en este caso para comunicaciones móviles, es el sitio https://osmocom.org/ que presenta noticias, foro y repositorio de código fuente de aplicaciones que empleamos.

Podemos obtener información sobre comunicaciones móviles GSM (Global System Mobile) y LTE (Long Term Evolution – 4G LTE) y aún 5G.

Probamos aplicaciones como grgsm_livemon, que es un receptor de canales GSM, demodulador y captura tramas de protocolo, con una interfaz UDP que permite entregar esas tramas a la aplicación Wireshark dónde se pueden analizar.

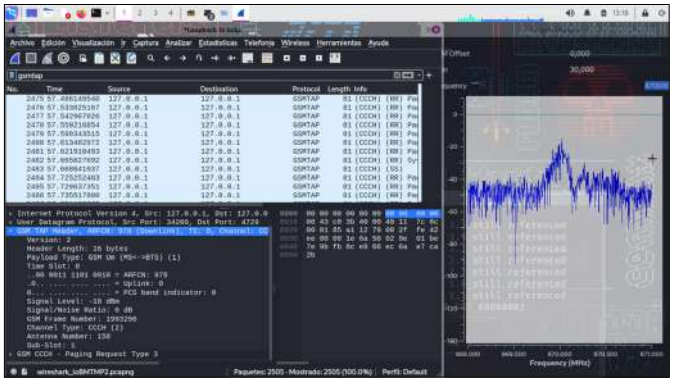
Esta aplicación se basa también en GNURadio. También fue probada con Linux como sistema operativo.

Por la parte de ciberseguridad, contamos, como ya adelantamos, con Wireshark, que permite analizar protocolos de datos.

Wireshark, además de escuchar sobre las interfases de red físicas de la computadora, puede escuchar sobre la interfaz de loopback del host y por algún puerto TCP/UDP que configuremos, y así, cualquier aplicación, en este caso un receptor SDR puede enviar datos por un canal UDP sobre esa interfaz, y entonces Wireshark puede mostrar las tramas de varios protocolos de wireless, además de Ethernet, como pueden ser LTE y GSM.

FIGURA 6: WIRESHARK - ANALIZADOR DE PROTOCOLOS

FIGURA 7: CAPTURA DE TRAMAS DE DATOS GSM OBTENIDOS POR EL RECEPTOR GRGSM_LIVEMON EN LA BANDA DE TELEFONÍA MÓVIL GSM850



¿Qué podemos hacer con estas herramientas?

El propósito es la capacitación. Contar con herramientas en las unidades de guerra electrónica y ciberdefensa facilita el entrenamiento, familiarizarse con la forma y parámetros de las señales de los sistemas de armas y comando y control, tanto para detectar actividades del enemigo, como también poder detectar en forma temprana vulnerabilidades propias. Podemos enumerar algunas posibilidades con estas herramientas como:

- > Conocer la forma y parámetros de diversas señales empleadas en sistemas de armas, sensores y comunicaciones.
- > Detectar vulnerabilidades propias.
- > Ensayar contra medidas para proteger los sistemas propios.
- > Investigar / innovar sobre el espectro electromagnético.
- > Reconocer parámetros de identificación de los sistemas en el espectro y en los datos capturados.
- > Vigilar el espectro electromagnético.
- > Ejecutar y practicar el control de emisiones propias (CONEM).

Conclusión

Con lo analizado y probado al momento podemos ser optimistas en cuanto a que esto puede realmente emplearse en la capacitación del personal que se desempeña en funciones de ciberdefensa y guerra electrónica. De hecho en muchos ejércitos y en el nuestro en particular, esas funciones ya están agrupadas por una misma unidad y bajo un comando único.

Los elementos doctrinarios, los fundamentos y la conciencia ya están sembradas, solo pretendemos ofrecer herramientas disponibles a bajo costo, probadas y compiladas en una unidad estandarizada, como herramienta para capacitar al personal.

Fuentes

1. SDR en el ámbito militar y aeroespacial: más allá de las radios tácticas – Microwave Journal – 2020. https://www.microwavejournal.com/articles/34577-sdr-in-military-and-aerospace---beyond-tactical-radios
2. Military Embedded Systems - Ampliando la versatilidad de la radio definida por software para el campo de batalla digital – 2020. https://militaryembedded.com/radar-ew/signal-processing/expanding-software-defined-radio-versatility-for-the-digital-battlefield
3. Electronic-Warfare (EW) Training with Software-Defined Radio (SDR) - Warren Paul du Plessis – Conference Paper 2018 - University of Pretoria.
4. Noticias y proyectos sobre radio definida por software y RTL-SDR www.rtl-sdr.com
5. Comunicaciones móviles de código abierto https://osmocom.org/
6. Proyecto Radio Definida por Software https://www.gnuradio.org/

(*) **Rafael Mario Olivieri** es Coronel del Ejército Argentino en situación de retiro, promoción 116, Arma de Comunicaciones, Ingeniero Militar especialidad Informática, Especialista en Redes de Datos, Analista del Centro de Estudios de Prospectiva Tecnológica Militar "Grl Mosconi" de la FIE. Se desempeñó en diferentes proyectos de desarrollo de software y comunicaciones en el Ejército Argentino, profesor de Sistemas Operativos, Comunicaciones, Redes y Teoría de Control; ha realizado publicaciones sobre su especialidad.