Microwaves&RF

Alejandro Buritica, Product Manager, RF & Wireless,
Tektronix, https://www.tek.com/en

The Intelligent Future of Spectrum Visibility (Part 1)

Discover how artificial intelligence is revolutionizing spectrum operations, offering unparalleled speed, precision, and adaptability. AI will change the way we "see" RF.

On the morning of December 7, 1941, radar operators at Opana Point, Hawaii, detected an unusually large blip on their radar screen: a large group of aircraft heading for Pearl Harbor. Despite this early warning, a series of miscommunications and assumptions about the blip being friendly aircraft led to a catastrophic defensive failure.

The incoming planes were, of course, Japanese fighters, launching what would become one of the most infamous surprise attacks in military history. This incident starkly highlights the perils of underestimating the value of cutting-edge radar technology and its integration with other sensors and quick-response mechanisms.

Large-scale adoption of artificial intelligence (AI) marks a revolutionary shift in the field of spectrum operations, promising to transform it with its speed, precision, and adaptability. This article, the first in a two-part series, offers a concise guide into the complexities and innovations defining the field today. We start with an overview of the current state, setting the stage for a deeper exploration into the transformative role of test and measurement tools. Part 2 will discuss the paradigm shift brought forth by cognitive radar and AI's integral role in electromagnetic dominance.

The Current Landscape of Spectrum Operations

Military and government entities, as well as non-government actors and civilians, contend for access and control of the electromagnetic spectrum (EMS), which brings its own set of challenges and complexities to effective spectrum operations. These are outlined below.

Increased Spectrum Congestion

Commercial allocation of new frequency bands for telecommunications and other civilian uses continues to grow. Bands previously reserved for satellite communication and military radar now serve cellular services. And bands that had been reserved and sparsely used are now designated for unlicensed Wi-Fi use, while new commercial cellular services seek to take advantage of mmWave bands, operating in the vicinity of high-bandwidth satellite and radar systems.

RF designers working in this contested environment must ensure that their designs and the radio systems that they're working with stay within their allocated channels, minimizing the amount of energy that they spill on other bands.

Regulators and spectrum operations specialists must use sensitive, wideband RF receivers to monitor the spectrum continuously and ensure that all actors are respecting their allocated frequency bands. They must also detect contested use of the spectrum for pirated use, jamming, and other forms of unauthorized electromagnetic applications.

The Dynamic Nature of Spectrum Change

The pace of change of the EMS has accelerated. To achieve multiple advantages in the use of the spectrum, and to enable better decision-making, engineers and other spectrum users must maintain continuous EMS awareness through a larger number of more capable EMS sensors. Test and measurement equipment with higher dynamic range and wider instantaneous bandwidth enables them to improve their operations as well as outpace adversarial forces in the creation of EMS effects.

The Growing Sophistication of Adversarial EMS Tactics

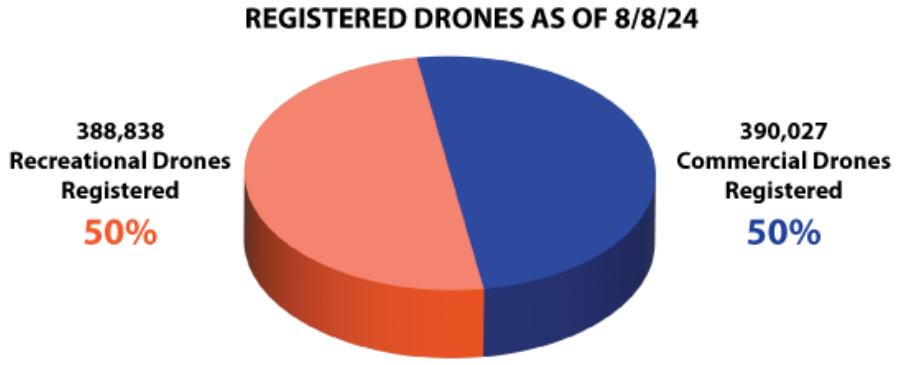
The sophistication of jamming and spoofing techniques used by adversaries is concerning. This is particularly the case when it comes to the relative ease of acquiring and deploying software-defined radios (SDRs) with cutting-edge FPGA capabilities and wideband front ends. Researchers need high-precision waveform generators and signal analyzers to model, simulate, and replicate these RF environment threats and stay one step ahead of malicious users.

The Greater Integration in Unmanned Aerial Systems

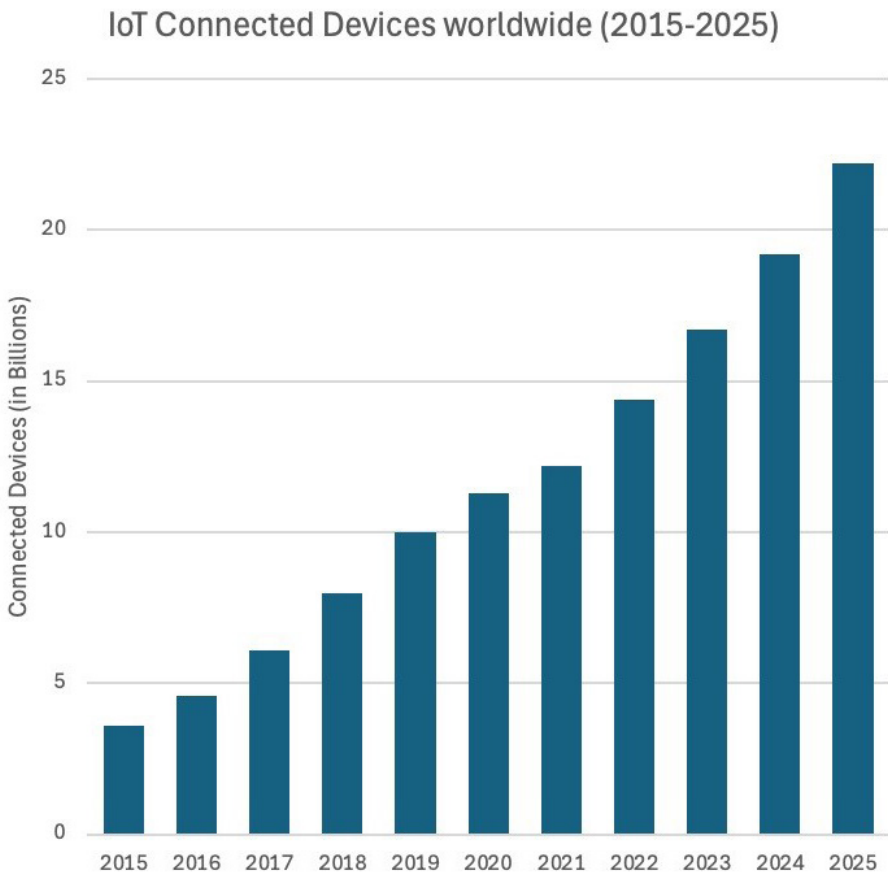
The last 20 years have seen a proliferation of both military and commercial unmanned aerial systems (UASs),

commonly referred to as drones *(Fig. 1)*. These drones have numerous legitimate and beneficial applications, but also unscrupulous and illegal uses.

UASs are readily available to consumers, which presents a challenge in managing spectrum usage and ensuring security against threats posed by swarms of these devices. RF signal analyzers and signal generators need lower noise, improved frequency selectivity, and advanced triggering to detect, identify, monitor, and take countermeasures against these threats.



1. This graphic represents the numbers of registered UASs in the U.S., broken out by commercial and recreational. (Credit: U.S. Federal Aviation Administration)



2. Shown here is a graph of the number of IoT-connected devices worldwide contending for RF spectrum access. The graph begins with 2015 and projects forward through 2025. (Credit: https://iot-analytics.com/number-connected-iot-devices/)

Cyber-Electromagnetic Activities on the Rise

While electronic attacks rely on the physical effects of electromagnetic energy to disrupt or deceive, cyber-electromagnetic activities (CEMA) leverage cyber techniques to infiltrate, manipulate, or damage systems at a data or network level. This combination increases the effect of the attacks, allowing for more precise and targeted disruptions, often with a broader strategic scope.

The integration of cyber and electromagnetic operations tactics is a sophisticated endeavor. However, just like SDRs are commercially available and affordable, the tools for cyberattacks are increasingly accessible to users with a moderate level of technical expertise.

Increasing Density of Connected Devices

The commercial communications industry continues to drive the development and mass deployment of both high-bandwidth cellular standards and narrowband Internet of Things (IoT) services, causing the number of users and devices per area to grow exponentially *(Fig. 2)*. Arbitrating contention for RF access and improving the quality of service to all of these connected devices requires opening new bands, such as mmWave bands for 5G, and devising new radio access mechanisms.

Tools for Assessing, Researching, and Advancing Spectrum Operations

Instruments such as Tektronix's arbitrary waveform generators (AWGs) and real-time spectrum analyzers (RSAs) are pivotal in navigating these complexities. High-bandwidth AWGs enable the generation of complex, real-world RF environments with precise modulation and timing characteristics, essential for testing and simulating dynamic radio behavior and electronic countermeasures.

Together with RSAs for spectrum analysis, signal interception, and environment scanning, AWGs enable researchers to replicate dense, dynamic spectral environments for developing adaptive, intelligent systems. With these advanced tools, researchers can effectively analyze spectrum usage, identify vulnerabilities, and enhance the resilience of communication, radar, guidance, and other RF systems against sophisticated denial, jamming, and spoofing techniques. As a result, they help ensure secure and efficient spectrum utilization in both military and civilian applications.

The second article of this two-part series will discuss the paradigm shift brought forth by cognitive radar and AI's integral role in electromagnetic dominance, signifying a leap toward more sophisticated and efficient spectrum management. Through examples of real-world applications, the discussion touches on the practical implications of these advances. Also addressed are the inherent technical challenges that accompany the course toward a more secure and technologically adept future in the realm of spectrum operations.

Alejandro Buritica has worked in the RF test and measurement industry for nearly 20 years, with experience spanning R&D, test engineering, and marketing management. He currently serves as an RF product manager at Tektronix. Alejandro holds a degree in Electrical Engineering from Universidad Javeriana de Bogotá and a Master's degree in Wireless Technologies from Politecnico di Torino, Italy.

References

Del Monte, L. A. (2018). *Genius weapons: Artificial intelligence, autonomous weaponry, and the future of warfare*. Prometheus Books.

Federal Aviation Administration. (2023). "Drones by the Numbers." Retrieved January 9, 2024.

Haigh, K. Z., Andrusenko, J. (2021). *Cognitive electronic warfare: An artificial intelligence approach*. Artech House.

O. M. Khodayer Al-Dulaimi, M. K. Hassan Al-Dulaimi and A. M. Khodayer Al-Dulaimi, "Cognitive Radio Technologies and Applications in Dynamic Spectrum Access Method," 2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), Kharkiv, Ukraine, 2022, pp. 9-14, doi: 10.1109/PICST57299.2022.10238684.

S. You, M. Diao and L. Gao, "Deep Reinforcement Learning for Target Searching in Cognitive Electronic Warfare," in *IEEE Access*, vol. 7, pp. 37432-37447, 2019, doi: 10.1109/ACCESS.2019.2905649.

U.S. Air Force. (2023). "Electromagnetic spectrum operations" (AFDP 3-85). Retrieved January 12, 2024.

An Overview of Cognitive Radar: Past, Present, and Future.

Statista. (2023). "Number of IoT Devices."