

# Perspectives on the State of Electronic Warfare Expertise, Technology, and Culture

By John Haystead

Signals Intelligence (SIGINT) has long provided the US and its allies with a major advantage in all manner of conflicts from all-out warfare with near-peer adversaries, or even superior forces, to the Cold War, to asymmetric conflicts with paramilitary and terrorist foes. Today, however, the detection, identification and location of RF emitters, whether communication signals (collected the communications intelligence – COMINT) or the emissions of other electronic systems such as radars (collected via electronic intelligence – ELINT), has reached an entirely new level of importance. In fact, for today's military forces, superior SIGINT capability provides not just an advantage or force multiplier, but is an absolute necessity for success on the battlefield.

Despite this reality, it's not at all clear that "the West's" SIGINT forces are adequately prepared to deal with potential tier-one adversaries equipped and trained for modern electronic warfare operations, and who are also, themselves, intent on achieving EMS superiority.

For example, observes Nicolas Vafiadis, Director/Chairman, Communications Audit UK (Cheltenham, UK), "The Russians have been spending a lot of money on EW, and the main thing they're spending it on is electronic attack (EA). They've also been fighting and learning in Ukraine how to fight a modern and sophisticated war. In contrast, the West doesn't know how to do it. Because the West has been largely fighting asymmetric warfare, we have no experience, we haven't trained enough operators, and those that have been trained haven't been up against a Russian-type threat, with the exception of maybe in Syria."

Jim Kilgallen, President of COMINT Consulting (Denver, CO), concurs. "From the early part of the '90s, at the end of the Cold War, everyone really relaxed their guard and focus on RF SIGINT, in favor of a 'nothing-but-net' approach. The problem with this is that the commercial telecommunications industry kept making better radio equipment with more and more capability. And, at the same time, our RF SIGINT intelligence organizations closed up a lot of field sites around the world, meaning we lost a lot of the up-front and personal insight and expertise that had been cultivated on a daily basis focusing on everything being done remotely. The result is that we lost a lot of people with extensive RF SIGINT expertise."

Although Kilgallen adds that, in the early 2000s, "some people were brought back as sort of a stop-gap measure, we just don't have the RF talent we once had. There are still some pockets of expertise, but in general, the kids that come in now are net-savvy, computer-savvy and social-network-savvy, but they don't have an RF-savvy guy working alongside them."

## NEW AND EMERGING CHALLENGES

Even as the capabilities and relative skill level of potential adversaries advance, so do the challenges posed by new and rapidly-proliferating technologies, such as software-defined radios (SDRs) that can be rapidly reprogrammed with new and potentially previously unknown waveforms. Says Nicholas Cianos, Executive Staff Scientist at WGS Systems (Frederick, MD), "With SDR, you can change a parameter that a SIGINT operator might not be aware of, and they may not even know that something

has changed until, or if, they look at the details of the waveform."

Martin Atanassov, Director of Marketing, Monitoring and Network Testing Division, Rohde & Schwarz (München, Germany) adds that, from an intelligence-gathering perspective, the impact can be even greater. "SDR is a game changer. In the classical duplex or simplex operational mode, you have a lead node requesting an answer and getting a response. From that alone, you can actually derive information and analyze the behavior; maybe even be able to evaluate the hierarchy from the positions, the type of network you're dealing with, the type of forces you're up against, etc. Just from the metadata, without even touching the content, you can make assumptions about intent and objectives of that unit." In contrast, with SDR, the operational mode is changed. "Now it's going directly to IP and whenever you need to transmit something, it could be over a military ad hoc network," he explained. "In that situation, all of the transmitters are on and communicating all of the time, which is good for detection, but this also makes it more difficult to determine who is talking with who. You're still getting the locations, and can still derive information from that, but its more effort to analyze the entire situation."

New cognitive radios, that can search for and rapidly shift their signals to open spaces in the spectrum, are also posing a major challenge. Says Cianos, "If the radio is sophisticated enough, it can do that frequently, as well as hop into segments of the spectrum where you didn't expect to see it before. Especially for short-duration transmissions, this makes them much harder to be seen."