Perspectives on the Stat
Expertise, Technology, C

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 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."

e of SIGINT Readiness – apabilities, Threats

MILLIMETER-WAVE AND 5G TECHNOLOGY

Just over the horizon looms another major technological challenge for the SIGINT world – the arrival of 5G cellular communication technology and the increasing movement of signals into the millimeter-wave (MMW) region of the spectrum. As described by Cianos, "If you look at the internet of things in terms of the concepts being discussed, there are a number of applications in the millimeter-wave portion of the spectrum. The challenges associated with detection of these signals are multi-fold, but first, you have to deal with the physics of signals operating in millimeter-wave frequencies. Your spread loss will be higher, hence for a given transmitter power, the signal will decay over a shorter distance, and your antenna beamwidths can be relatively narrow, making detection difficult."

Rohde & Schwarz's Atanassov, says 5G will be a massive game changer just in terms of the connectivity of various systems already operating in VHF, UHF, satellite phones, frequencies in the Ku- and Ka-bands as well. The number of subscribers is rising exponentially, and the amount of data transmitted through mobile networks is increasing exponentially. In order to meet these requirements, the bandwidth requirements of SIGINT systems will continue to grow and to cover additional areas of the spectrum such as millimeter-wave. In particular, we're expecting a dramatic increase in the frequency ranges used in urban environments.

SIGNAL DETECTION

Choosing the right path to SIGINT superiority, let alone executing it, is not a simple exercise, however. But, regardless of the course chosen, the first task will always necessarily be signal detection, and system designers are already working to improve their systems' detection capabilities in a number of ways to pace the increasingly challenging requirement.

One approach is providing wider instantaneous bandwidth. As described by WGS Systems' Cianos, "COMINT tuners have clearly increased their instantaneous bandwidth over the past several years, with on the order of 80-100 MHz of instantaneous bandwidth, and these tuners also have dramatically-increased frequency range coverage. Typically, they can cover up to 6 GHz, reaching into the radar band, and many suppliers are also offering frequency extenders. The next generation of COMINT tuners will essentially have the capability to cover from HF up to 18 GHz and still provide 100 MHz of instantaneous bandwidth."

Cianos also sees traditional microwave or ELINT receivers moving to wider instantaneous bandwidth. "It's not yet happening as rapidly, but microwave receivers typically have on the order of 500 MHz of instantaneous bandwidth and you can get tuners today providing 1 or 2 GHz with good performance in terms of dynamic range, phase noise, etc."

In fact, the required tradeoff in dynamic range in exchange for wider instantaneous bandwidth can be a potential drawback of the approach for all SIGINT tuners. Says Cianos, "Dynamic range will be critical because as the bandwidth of the tuner increases, and you are looking at more signals that are illuminating that receiver, effectively all those signals will behave like Gaussian noise. If you don't have a properly designed receiver, all that noise will give rise to a dramatic increase in spurs and that increase will limit your ability to detect signals."

One company, S2 Corporation (Bozeman, MT) is taking a different approach to the wide instantaneous bandwidth requirement. Preferring to identify themselves as a spectrum awareness and signal identification/geolocation business rather than as a traditional SIGINT system provider, the company's CEO, Kris Merkel, says they're working to break the conventional paradigm of SIGINT receiver capability.

As he describes it, "Basically, what we do is take snapshots of time and see the energy in the frequency domain manifest over time. We don't always get the pulse-descriptor words, we get energy-descriptor words that you can use to get SIGINT-like fingerprints (center frequency, bandwidth, POPS, modulation – chirp vs. quadrature phase shift etc.,) that you can then use to cue other receivers." Known as spatial-spectral (S2) holography, the system uses unique photonic and crystalline material technology that can currently provide 40 GHz of instantaneous bandwidth, and the company plans to extend this to 110 GHz by the end of this year. Says Merkel, "We're an energy detector and integrator with very fine precision frequency resolution providing instantaneous spectrum awareness and allowing you to know certain signal classes are there and up, and then use traditional receivers to get into the fine detail."

CONVERGENCE OF COMINT/ELINT

As can be seen from the above discussion, there is clear convergence going on between what were once considered distinct COMINT and ELINT system technologies. As explained by Rohde & Schwarz's Atanassov, "From a technology-provider point of view, this convergence is not something that is particularly difficult to do," but he adds, however, that when it comes to the organizational structures of the user community, it's a different story. "The operational CONOPS [concept of operations] still differ quite a lot from COMINT and ELINT, and the operations people still have the mindset that 'this is ELINT and this is COMINT,' and we want to separate them. Also, the training and skillsets of the operators differs quite a bit because of the different requirements they have to process. In order to get the best results, you have different operators with different techniques. So, from our perspective, the only reason we're not selling fully-converged SIGINT systems that can do both is because customers don't want it, not yet."

Ultimately, however, Atanassov thinks other factors will come into play as well. "In the end, instead of having two systems in the field that need to be logistically maintained, that need specialized training, and all the costs that are accompanying the system life cycle, you can streamline your logistical tail, train on the same system, and deploy personnel who can conduct either COMINT or ELINT on the same system. You can and use that as an advantage for your operations."

For operators, the increase in instantaneous bandwidth is also not necessarily a panacea, given the much wider breadth of signals they will be seeing at once. As noted by Cianos, "The increase in bandwidth is good, because you're increasing

continued on page 33

continued from page 28

your probability of intercept, but within the large number of signals detected, the signal of interest may be missed."

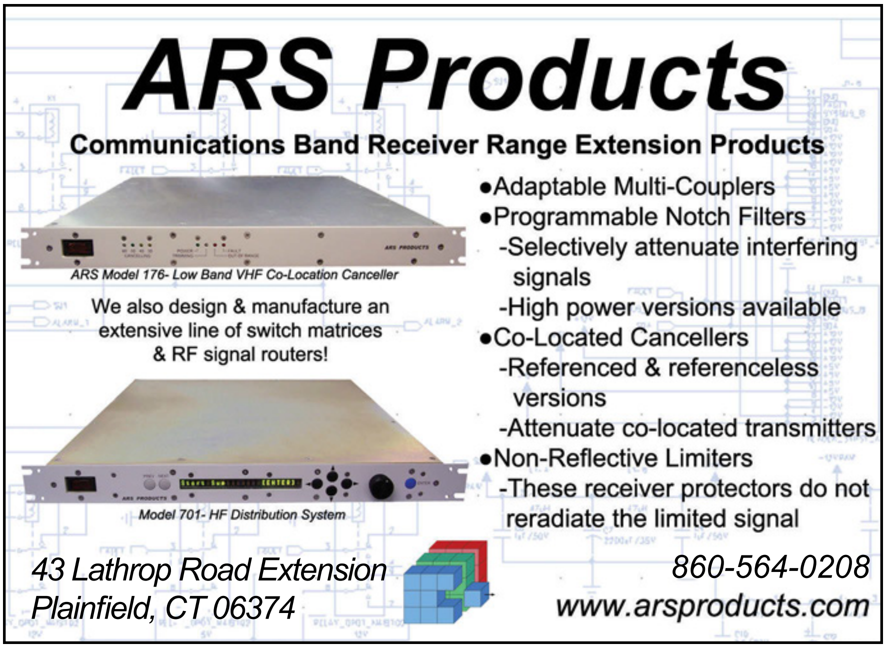
Cianos notes that this is one challenge area where advanced machine-learning or artificial intelligence (AI) algorithms can help. "These tools can help the operator cull out the signals of interest." Machine learning aids may also help with the problem of software-definable radios. Says Cianos, "The best way to address the challenge is to start leveraging tools that will quickly identify and alert an operator when changes are taking place. Those change notifications can potentially serve as a wake-up call."

BACK-END PROCESSING/ COGNITIVE EW

Having solved the detection problem, designers must now deal with the results of their success. Data – lots and lots of data. Says CommsAudit's Vafiadis, "With the data quantities generated from the move toward wider instantaneous bandwidths, you absolutely have to use some form of artificial intelligence to help handle it. Otherwise you can't cope with it, you don't have enough people."

Rohde & Schwarz's Atanassov agrees. "Even without talking about content, the amount of metadata you're analyzing is massive. The challenge is to separate the relevant from the irrelevant." Atanassov points to the benefits that automation and cognitive systems can bring to the challenge by helping sort out that relevant data. Even so, he still sees a clear need for skilled operators as well. "At the end of the day, even with modern AI algorithms and cognitive approaches, you'll still need experienced and skilled operators to put everything into context." In fact, Atanassov says he's sensing the need for a paradigm change that will bring more skilled operators to the front to provide a pre-evaluated and pre-prioritized data set for later stages of the evaluation process. "They, together with intelligent filtering systems up front, even with vast amounts of data to evaluate, can reduce the load dramatically. And, by using skilled operators, who are not only collectors but also evaluators, you can actually have better and more relevant data quicker."

Not all software-based pre-filtering tools need to be incredibly complex or sophisticated in order to provide significant advantages to the processing task. Zeta Defense (Gebze/KOCAELI, Turkey), for example, provides such software tools capable of running efficiently on standard microprocessor and FPGA cores. Ibrahim Basaran, Zeta Defense Business Development, points out that one of the biggest challenges associated with the detection and identification of modern frequency-hopping, and short-burst communications, is the need for rapid identification. To accomplish this automatically without the need for massive amounts of processing power, Zeta's software focuses exclusively on this signal-recognition task. As Basaran says, "It's not getting bogged down dealing with modulation types or other complex analysis. As soon as a signal appears, it is de-



tected and goes through the channelizer for analysis. Yes, as bandwidths get wider, the more signals you need to process, but a computer can have many cores, and if you share the processing load over many CPUs, it becomes very manageable.

Similarly, S2's technology doesn't avoid the data crunching challenge either, particularly for complex analysis, but it can help make it more manageable down the line. Says Merkel, "Almost every time someone talks about extending their instantaneous bandwidth, they're going to create a ton of data. So, for example, if they get 4 GHz of bandwidth, they will create 10 GB of data per second or more that will have to be processed. Our approach provides this extra bandwidth with very high dynamic range and very high sensitivity, without creating extra data where there is no signal, and allowing digitizers to just digitize the signals, not the trash." Signals that are present, however, must still be collected and analyzed, and as Merkel acknowledges they still "create an overwhelming amount of data in real time." Like others, he also sees the potential benefit of applying smart/cognitive processing capabilities. "There's still a lot of human-in-the-loop – going in and looking at the display – and we need sophisticated/cognitive spectrum awareness capabilities to change that."

CHALLENGES AHEAD

One of the results of the diminishing base of operational RF SIGINT expertise, is that the user and procurement communities often don't have a strong understanding of what they need to meet their SIGINT goals and requirements. Says COMINT Consulting's Kilgallen, "It's not a question of budget, it's a question of users not being able to specify what they need." Kilgallen says industry also needs to accept a part of the blame for the problem in that the business paradigm of providers "often leads to exploiting this lack of expertise and experience with overstatements of system capabilities, and in some cases, the sale of obsolete and useless technology relative to the current threat."

CommAudit's Vafiadis raises another very worrisome issue for SIGINT system designers. "The other piece is the fusion between SIGINT and cyber, and the potential of using electronic attack against your SIGINT systems. What if the opposite side suddenly decides to attack you with a cyber weapon born on RF signals and waveforms designed to get into your processing and disrupt your SIGINT systems. You also have to guard against this."

From his perspective, S2's Merkel sums up the SIGINT challenge as follows. "The EW community is definitely talking like they're interested in pursuing cutting-edge technologies to deal with future threats – early adopters, etc., but we need much more rapid prototyping, more accelerated testing and field-demonstration of capabilities. If we're really going to stay ahead in the global, threat-driven marketplace, we have to keep pushing these development processes. When we're doing that, we're remaining cutting edge."