Back to the Future

By John Haystead

For reasons not completely clear, in recent years a perception developed within the SIGINT industry – as well as in some circles of the military and intelligence communities – that with the emergence of cellular phones, satellite links and other newer forms of communication, the use of the High Frequency (HF) portion of the spectrum and HF communication systems, in general, were becoming substantially less important, even "dead," as a significant signals intelligence (SIGINT) environment. The reality, however, is that just the opposite is true, and a number of voices in industry and the military are beginning to call attention to this fact and the dangers posed by not paying adequate attention to this part of the spectrum. For example, James Kilgallen, President of COMINT Consulting (Bozeman, MT), points out that "The telecom industry apparently didn't get the memo that things had slowed down in HF, so they didn't. The major manufacturers and even some of the smaller creative manufacturers have continued their development and also spent a lot of R&D money in HF."

Rather than HF going away, Kilgallen says that what actually happened is that the SIGINT community just largely decided to look away, focusing on other parts of the spectrum instead. "But, people always have a need to communicate and there are a lot of places in the world without the communication infrastructure of a Public Switched Telephone Network (PSTN) or whatever." In fact, there are many reasons why HF has remained uniquely viable, such as the demands of rugged terrain, long-distances, mobility, etc

The notion of HF going away may have started in the '90s with the breakup of the Soviet Union, the then principal threat to the West and a heavy user of HF. Russia, today, however is still a major user of HF, as are the military forces of other large nations. Says Kilgallen, "Both militaries and militants are using the technology, and there isn't a modern military in the world that isn't an extremely heavy user of HF with users depending on HF as a crucial element of their battlefield and fleet-level HF networks. Today, the problem is that, when we looked away, we lost track of things, and we're now in a position of playing catch-up." Worse still, Kilgallen says that many SIGINT companies haven't yet realized just how far we've fallen behind and so continue to lose ground.

ADVANCING TECHNOLOGY

Many advances in communication technology that have emerged and been implemented in systems using other parts of the RF spectrum are also taking firm hold in the HF universe. Although the majority of commercial technology development activity has been in the higher, UHF, VHF and SHF frequency ranges – primarily because of the greater availability of bandwidth requiring less precise modem technology and the availability of a greater variety of commercially available protocols – there has also been a tremendous amount of technology development in HF as well. Today there are not only stealthier forms of HF transmissions including burst, spread spectrum and frequency-hopped waveforms (especially by special ops forces), but advanced HF technology is being used by regular military forces as well. On the data-exchange side, the technology has also advanced tremendously. For example, Kilgallen says, "Just think about the processing power in our cell phones, and you can imagine what purpose-built chips can do. And now there are also batteries available for HF that give satellite communications a run for their money and can be just as reliable."

Victor Wollesen, Founder of Per Vices Corporation (Toronto, ON, Canada), agrees, observing that, setting aside unique military frequency range requirements, the demands of civil telecommunications technology are generally far more stringent than those for defense. "Your cell phone, for example, with 3G or 4G LTE requires 25 MHz of very complex (both frequency and time domain) protocols in order to allow the rather simple experience of downloading an application or checking the Internet while walking down the street. Those kinds of capabilities far exceed those of traditional military requirements, which generally focus on cryptographic strength, which is its own box of worms and places its own demands on hardware, but that is very different than the actual radio receiver front-end demands."

Per Vices is pursuing a business and technology approach aimed at applying the hardware/application-software development paradigm used with personal computers and other personal communication devices to the broader radio receiver universe. Says Wollesen, "You'd never think of buying a different computer for every application you run, but when it comes to wireless hardware, that's often exactly what you see – dedicated hardware for a dedicated purpose."

While Wollesen agrees that, in some cases, there are very good reasons for this approach, especially for very tightly integrated systems, at the same time, he also points out that there are also very good reasons to decouple these two design aspects, "to achieve to the best of your ability, a generic radio receiver

with HF SIGINT

platform together with an application or applications that turn that platform into something more specialized. Just as depending on their processing technology requirement, some users will invest in a more powerful computer or server to run their applications, the majority of users can get away with a less expensive generic system, while the application(s) can run across all of the platforms."

Very much related to this, one particular technology development posing challenges for SIGINT systems operating across the entire spectrum is the widespread use of Software Defined Radio (SDR). Noting that while there are many different architectures called SDR, Wollesen says they define it as, "a separation, as best as possible between the digitization and tuning of a radio signal and the processing or information extraction method of that signal." As such, Wollesen says, "SDR gives you the freedom to do things, at least conceptually, that would be traditionally impossible using dedicated silicon and dedicated processing."

Of course, like most things in the EW/SIGINT world, the SDR technology sword cuts both ways, making the signal detection and processing challenge exponentially greater even for extremely sophisticated SIGINT systems. Says Kilgallen, "today anyone can write software to create a modem that can be uploaded into some firmware, and all of a sudden, there's a new mode on the network. Imagine what the arrival of systems that completely reprogram themselves in milliseconds does to the intercept challenge. And, then there are networks now that will implement a mode, use it for a few days to do an operation, and then it goes away and we'll never see it again. We have no response to that."

As observed by Wollesen, the difficulty is not due to a shortage of smart people to address the challenge, but rather that "the problem they are trying to attack is itself very hard. And, the other thing about the military domain versus the civil domain, is that you're not working in a permissive environment; people are actively trying to deceive you and are actively trying to deny your ability to receive their information. These are challenges that remain constant, whether you're working with SDR or dedicated analog electronics."

CALLING SYSTEMS

An additional challenge facing both the modern HF SIGINT system designer and the SIGINT analyst is the use of advanced calling systems in the HF arena. Similar in some ways to the way cell phone communication links are established, these are sophisticated and automated communication connection systems that establish a link between communication stations in milliseconds, while taking into consideration numerous factors such as antenna type, range, propagation inversions, ionosphere and atmospheric conditions, noise and other factors (such as jamming) prior to even transmitting message signals. (For more on the HF region, see "HF SIGINT Battles the Ionosphere" on p. 32.)

Calling systems have been in use in HF for nearly 20 years now, with some extremely advanced versions now available that can frequency hop and adapt to changing parameters in the middle of a transmission, switching to a different channel and reestablishing the link right where they left off. As observed by Kilgallen, "You can imagine the problems this can pose. For example, if you don't know who called who, how do you know what modem got set up afterwards? Sure, you might stumble into the modem, but you won't have a full understanding of how that network works."

WIDEBAND VS. NARROWBAND

Not unique to HF, but certainly a major factor for SIGINT system designers, is whether to focus on wideband or narrowband collection systems. Obviously, wideband systems can collect signals over a wider bandwidth, and for that reason they are primarily used to broadly survey an operational environment to determine what is out there. Narrowband systems with higher-quality processing are then used to examine specific channels of interest in more detail.

As described by Wollesen, there are some very fundamental tradeoffs between wideband and narrowband approaches with a tight mathematical relationship between bandwidth and processing of dynamic range. From his personal experience, Wollesen says he believes it's generally more difficult to design wideband systems. "For narrowband systems, there are a great number of specialized components that are perfectly tailored for very particular military communications bands and that offer amazing value and performance. Achieving this same performance with wideband components is an ongoing challenge. Still, having said that, there are systems out there that can act as both a broadband and narrowband platform."

Some wideband collection systems are in fact themselves also capable of a fair degree of the higher-level processing found in their narrowband counterparts. These "digital drop" receivers are essentially software-implemented narrowband receivers that automatically select individual channels and "drop them down" for further processing. Says Kilgallen,

"They may not provide the same quality as a full rack-mount, purpose-built receiver but they're good enough to process most of what is out there."

Even so, more powerful and sophisticated signal processing capability is becoming increasingly important as the complexity of modems dramatically increase, and with higher-order modulation schemes, like Orthogonal Frequency-Division Multiplexing (OFDM) and Quadrature Amplitude Modulation (QAM), becoming common in HF. Kilgallen points out that these higher-order modulation schemes are not just the province of modern military systems, but in fact are readily available commercially. "Anybody can write software, upload it to firmware. Boom, you've got a new capability."

Jim Taber, Director of Sales and Marketing for X-COM Systems (Reston, VA) agrees noting that "before you can address the threat, you must know it exists, and many IQ collection systems are either too narrow-band or too low signal fidelity or don't have 100 percent probability of intercept. Unfortunately, modern threats are pushing the performance boundaries on all three dimensions."

X-COM makes broadband RF record and analysis systems ranging from a few MHz of IQ band to 6000 MHz bandwidth of continuous uninterrupted recording for many minutes. The data can then be offloaded to a workstation or PC, for more detailed fingerprinting and analysis using the company's "SPECTRO-X" tool.

Taber says they see their role as helping, not the warfighter directly, but the designer of the tool for the warfighter to understand what the threats are. "The value we provide the COMINT guys is in our ability to take inventory of all emissions in the HF, VHF and UHF bands no matter how elusive they might be." For COMINT, X-COM is focusing their attention primarily on narrowband systems where they see the greater requirement. "Some of our wideband stuff is relevant for COMINT, but not many customers require that much bandwidth. The value of narrowband is that you're buying a recorder that is an incremental expense over what you already have in your lab. Everyone has spectrum analyzers, generators. Now you have a recording piece that is very high fidelity."

Rather than HF going away, Kilgallen says that what actually happened is that the SIGINT community just largely decided to look away, focusing on other parts of the spectrum instead.

Ultimately, Kilgallen says that, "At the brute level, the wideband systems need to advance in terms of their ability to classify the environment, because they're blind to a lot of it right now." But he adds that with some of the new technology now being developed and deployed, systems may soon be able to operate at speeds where the distinction between narrowband and wideband collection becomes moot. "You're essentially collecting and cataloging so fast, you can drop everything to a collection channel where the user can pick and choose what they want to look at further, and determine how to react to it – jam, destroy, listen etc."

INCREDIBLY COMPLEX SIGNALS ENVIRONMENTS

The process of fully classifying a signals environment can involve sweeping through an enormous part of the spectrum and identifying perhaps a million different signals. By defining a specific subset of signals and modulation types of interest, this may be reduced to around 10,000. As Kilgallen explains, however, while this "is a start, and it's useful, it's also useless at the same time because the analyst still has way more than they can deal with in that moment. What's needed are wideband systems that work as well as they do now with collection but that can also do a better job of classifying the environment." Kilgallen says the problem remains that the systems are hamstrung by the limits of modulation recognition technology – "which is the first level of classification, and if you ask users in the civilian intelligence community or military if they need more and better tools, they will all give you an unequivocal 'yes.'"

X-COM's Taber says, "Big IQ data collection is only the first step. Once users have collected their mountain of data, they need to know how to sort it to locate their signals of interest. Perhaps more to the point is that they need to find their needle in a mountain of needles."

Wollesen says a big part of the solution may be found in open-source, commercial software that wouldn't necessarily jump out as applicable to the problem. For example, he points to commercial "SHAZAM" mobile device application software that automatically recognizes music and TV by creating a digital fingerprint of the audio within seconds and matching it to a database of millions of tracks and TV shows.

Wollesen observes that there's no reason why the same principles can't be applied to the RF SIGINT task. "There are a lot of parallels, and it would allow far better signal and signature libraries to be built, and, because it's software-defined, you can really decouple the raw sensor input from the processing." In addition, Wollesen notes that because you can record the data, "analysts would no longer be stuck in the analog domain with real-time scopes where transient signals are lost. Here you actually have the ability to correct your mistakes."

LISTENING TO THE LISTENERS

One additional, and perhaps the most important element, of the HF SIGINT system design equation is finding ways to better correlate the requirements and desires of the collection system users with the capabilities and interfaces being provided to them by system designers. Although all, or at least most of the technical parameter data collected and processed by HF SIGINT systems is needed to allow them to fully and efficiently identify and categorize signals and modulation types, this level of technical detail is not needed by the users themselves, at least not those in the field. In fact, it serves to

complicate an already overwhelming task even further. Says Kilgallen, "Commanders and decision makers aren't looking for PRI data. What they want, and have been requesting for years, is the rapid and efficient provision of useable tactical information about the emitter – what it is, where it is, what it is doing?"

Wollesen agrees with this assessment adding that, "This disconnect between what a SIGINT system engineer is going to want to design into a system and what the user actually wants, isn't any longer a technology problem, which was historically the case with analog radio, but a user-interface and user-experience problem." Wollesen observes that it's also certainly an ironic situation given that modern "mobile phones deliver a wonderful experience to their users, yet the users of SIGINT systems, who are operating in a far more stressful environment where they have to make far more timely decisions, and whose decisions have far more import than anything in the civil domain, are often dealing with arcane receiver structures. It's not the paradigm you want."

HF IS NOT AN OUTLIER

Clearly HF remains a vibrant and active segment of the military communication spectrum, and therefore, also remains of critical importance to the SIGINT community. Kilgallen observes that some SIGINT decision makers might benefit from reflecting on the obvious point that no reasonable seeker of tactical intelligence information would ever start out by deciding up front where they were going to find the information they sought and ignoring all other potential sources. This adage applies to modulation types as well as frequency bands. "You can't look at an environment and say 'okay, we don't have to worry about this signal or that modem because it's operating in a legitimate role,' when we really don't know what we don't know. If you've got 30 or 40 more new modes in some band per year, and you start out with the assumption that you don't need to worry about 15 to 20 of them, you're bringing the wrong mindset to the table. We need systems that can keep us aware of everything."