Hiding Within the Spectrum

SFC CHRISTOPHER M. RANCE

T*he sun begins to rise over the white sun-bleached hilltops of northern Syria. Without silhouetting against the orange sky, a sniper team lies softly behind some low brush, nested below the hilltop crest, with eyes fixated on the town roughly a kilometer away. Meanwhile, an electronic warfare support team (EWST), whose mission is to support the sniper team by finding the enemy through electromagnetic reconnaissance, is ready to act a few kilometers away.*

EWST Soldiers scan the targeted area from their observation post. First, they determine the line-of-sight bearings of frequencies used by the enemy. Then, over a secure channel, they contact the adjacent sniper team, talking them onto enemy positions so the snipers can begin to collect critical information, which is essential to answering the specific priority information requirements (PIR)/commander's critical information requirements (CCIR) laid out by the commander. With the correct information, the commander can now act. This "blended" reconnaissance method allows the sniper team to take action on the objective differently; perhaps well-placed precision fire on the key targets or the calling in of indirect fire assets. In turn, this completes the cycle of find, fix, and finish.

The concept of pairing intelligence enablers with a sniper team or a forward observer isn't new, but on today's modern battlefield, this tactic is seeing a re-emergence. If the goal of intelligence is exploitation, then pairing one asset with a precision asset like a sniper team which will be making the kill only makes sense. In recent wars in Iraq and Afghanistan, the electronic warfare threat was limited. In today's fight, drones and ground systems conducting electromagnetic surveillance and jamming against satellite, cellular, and radio communications will be the new normal.

To be detected is to be targeted is to be killed.

The flip side of that story is that your radio can kill you. Communications equipment is bright (spectrum-wise) and loud. The vast majority of our infantry battalion emissions are voice and data. We boast bandwidth and power, but our adversaries can easily detect these emissions. Even down to the company or platoon level, our radios, mapping services, and even portable electronic devices such as the smart watch on your wrist emit some form of

A Soldier assigned to the 173rd Airborne Brigade engages targets during a live-fire exercise in Slovenia on 26 February 2020. (Photo by Paolo Bovo)

electromagnetic signature or leave some digital footprint for the enemy to sniff out and find.

Hiding within the spectrum requires you to collect your unit's own-force electromagnetic emissions signature from the adversary's point of view. First, have your EWST measure the baseline signals in your area of operation. Then, with tools like a spectrum analyzer, measure your unit's signals. Second, schedule strict communications windows to blend behind "normal" background signal noise. Enforce radio discipline. Keep communications brief. Use terrain masking and communicate on the lowest power setting possible. Finally, analyze your unit's electromagnetic signature. What are you emitting? When and why?

The bottom line is that well-trained units communicate less. Have a robust signature management plan and learn to accept that the next fight you find yourself operating in will be an electromagnetic environment under near-continuous EW observations. Learn to hide within the spectrum.

References

EP EMCON SOP, Intelligence Training Enhancement Program, November 2020.

Martin Egnash, "US Marines in Norway Pair Electronic Warfare Team with Snipers to Test New Concept," *Stars and Stripes*, 3 July 2019.

SFC Christopher Rance currently serves as a senior drill sergeant in 2nd Battalion, 29th Infantry Regiment, 197th Infantry Brigade, Fort Benning, GA. He previously served as an instructor/writer with the U.S. Army Sniper Course as well as in a variety of sniper-specific roles.