Low-Cost Unclassified Intelligence

The case for low-level open-source SIGINT/cyber technicians

by GySgt Andrew Guthart

>GySgt Guthart is an Intelligence Watch Officer at Central Command. He has deployed to Afghanistan four times, in 2010–11 as an augmentee with the 101st Airborne Division, as a High Value Targeting Analyst in 2013 and 2014 with Special Operations Task Force, and in 2016 as an Airborne Tactical System Operator. He also deployed to Iraq in 2017 serving as a Detachment SNCOIC and Airborne Special Missions Operator. He holds a master's degree in Intelligence Studies from American Military University with a focus in Cyber and is also a Nationally Certified Emergency Medical Technician. His master's thesis was titled "Electromagnetic Spectrum Dominance in the Second World War."

The United States faces strategic competitors, transnational terrorists, and criminals—all of whom seek to level the playing field through technical ability and equipment. In recent years, opponents have utilized low-cost and open-source means to manipulate battlefield outcomes in their favor. The United States has made some effort in pushing low-cost commercial off the shelf (COTS) gear to its forward deployed forces, but this practice could be greatly improved upon. This article demonstrates how low-level, open-source signals intelligence/cyber technicians embedded across deploying units could provide a low-cost unclassified intelligence platform, providing parity against opponents and situational awareness to commanders.

Low-cost, open-source COTS solutions are increasingly utilized on the modern battlefield. In 2017, Ukrainian militia were able to identify electronic warfare equipment operating onboard Russian military helicopters during fighting in Eastern Ukraine. They were able to do this with a 300 dollars Software Defined Radio called the "Hack RF One."[1] Similarly, in 2009, Shiite militants in Iraq, using a $26 Software Defined Radio add-on, gained access to the video feeds of overhead U.S. Predator Drones.[2] With access to the video feeds, insurgents could accurately predict where U.S. special forces would strike next and plan accordingly.[3] The United States has also utilized COTS gear for intelligence purposes. In one documented instance during the 2011 fighting season, Marines deployed to Helmand Province, Afghanistan, were able to monitor Taliban insurgents through COTS radio scanners and make swift tactical decisions based on that intelligence. In this instance, they informed a patrol that an attack was imminent from a well-armed group approaching their position. The Marines set up an ambush and waited, unleashing a fierce barrage on the surprised Taliban who retreated after a short firefight.[4]

> *... COTS solutions are increasingly utilized on the modern battlefield.*

Proposal

This article proposes that the "Every Marine a Collector" concept be expanded into the signals intelligence and cyber realms with the use of open-source COTS gear and that the Marine Corps formally establish a Low-Level Open-Source Support (LLOSS) program to apportion unclassified signals intelligence and cyber capabilities, personnel, and equipment to every deployable unit. LLOSS technicians will continue to fulfill their standard job responsibilities while providing support when the mission allows or is necessitated. Technicians can also be a conduit for formalized intelligence support and will create a pool of interested and tactically proficient personnel to draw on for the growing cyber intelligence field. Marines who performed well in this role could be identified for lateral move into the 17xx cyber or 26xx signals intelligence fields upon re-enlistment.

This new program could stand on its own or be incorporated into existing structures. The Marine Corps currently features a program where non-intelligence Marines are instructed on tactical intelligence, called the Company Level Intelligence Cell Course.[5] LLOSS adds low-level passive SIGINT and Cyber, building upon the concept of "Every Marine a Collector" as outlined in the

Marine Corps Warfighting Publication 3-11.1. This documents states:

> The ability to maximize the observation and reporting skills of the individual Marine is critical to successful patrol execution. Every patrol member observes critical information during every patrol and successfully captures those observations because of proper training and disciplined debriefing techniques.

The Basic School Guide to Intelligence: Road to War describes the "Every Marine a Collector" concept as:

> The individual Marine, whether an infantryman, truck driver, or aviator—goes everywhere and sees everything. Due to the needs of timeliness, *every Marine must be an information collector on the battlefield.*

Capabilities of LLOSS Operators

Commercial, amateur, and hobbyist signals intelligence and cyber equipment can provide situational awareness and information of immediate tactical value to supported units. One of the easiest to use and widely applicable is the COTS handheld radio scanner. These devices can monitor the upper high frequency and very high frequency radio bands commonly used by insurgents.[6] Marines operating in RC South used these to characterize enemy activity and callsigns to their advantage, providing information of immediate value to troops in the field. These radio scanners are not only light weight but inexpensive, costing under 200 dollars, with basic very high frequency radios with single channel monitoring available for $24 online.

Augmenting the unencrypted radio transmission interception capability, civilian amateur radio direction finding gear could be furnished or built to provide locational information on detected signals. Around the United States, amateur radio "Fox Hunting" clubs routinely conduct direction finding against beacons in the form of an electronic scavenger hunt. These clubs also participate in search and rescue operations and assist with communications support during natural disasters. With the ability to direction find on radio emissions used by the enemy, it is not only possible to conduct situational awareness but to identify the transmitters for follow on offensive operations. These setups can be purchased online for about $70.

Soldiers from the 101st Airborne Division conduct Wolfhound training in Afghanistan. *(Photo by 1stSgt Matthew Veasley.)*

To obtain a broad spectrum of awareness of activity in the electromagnetic spectrum, Software Defined Radios (SDR) can be used to observe a wide range of signals from 100 KHz to 6 GHz. While not as powerful as dedicated spectrum analyzers, SDRs can observe a wide range of activity, some of which—if unencrypted—can be heard or viewed with the software. This is the same type of hardware that allowed Iraqi insurgents to gain access to drone feeds. Surveys can also be made of other signal sets, to include passively detecting Automatic Dependent Surveillance Broadcast (ADS-B) from commercial and military aircraft, which can plot the aircrafts location with additional open-source software. This technology has already been exploited by security researchers to track NATO aircraft in Afghanistan.[7] In addition to aircraft, seagoing ships can also be monitored via their Automatic Identification Systems (AIS). Other applications include pulling down weather satellite data, listening to commercial and amateur radio, and receiving GPS satellite signals. SDRs can be purchased online for under $50. LLOSS technicians would also have a limited passive cyber capability provided by open-source Operating System Kali Linux. This could be provided for as little as ten dollars to mount a USB image of Kali for use on laptops. Combined with a $30 wireless interface card, passive monitoring of nearby 802.11 (Wi-Fi) routers and devices can be achieved. Swapping out the omnidirectional antenna for a directional one, rough direction finding could be conducted by measuring received signal strength. By using a wireless network card in conjunction with an open-source packet sniffer, it is possible for a technician to characterize the Wi-Fi activity and users in their area of operations. Nearly any modern commercial laptop can run Kali Linux as a dual boot option. Finally, with wireless packet sniffing, it would be possible to conduct a limited computer network defense capability to observe if packets are being spoofed to deny service or other malicious uses. Alfa wireless cards and antennas retail for about $30 online.

One extremely relevant and timely application of this support capability would be to aid in the fight against enemy drones on the battlefield. Many drones are Wi-Fi enabled, essentially functioning as flying routers controlled by a client device controller. With the packet sniffing capability mentioned above, it would be possible to detect some of these drones at a distance based off their MAC addresses (unique to the devices manufacturer) and prepare defenses, either kinetic or electronic. Replaying a de-authentication packet using the wireless card and Aircrack suite on Kali Linux could temporarily disable some drones or force them to return to home. If the password of the drone's router is known, the drone can potentially be disabled and brought down.

The aforementioned capabilities complement each other, building a broad situational awareness, and can be deployed modularly depending on the mission. It should be noted that these signal sets that the COTS gear collects are freely available and will remain easily accessible; the choice is only to exploit it or willfully choose to deploy units with a minimum ability to gain situational awareness of their electronic surroundings. For isolated units in the mountains of Afghanistan, the Islands of the Pacific, or elsewhere, LLOSS operations could significantly augment their ability to understand their battlespace.

Another advantage of the LLOSS program would be the ability to share information broadly with U.S. allies and partner nations without formal intelligence sharing agreements. This program could serve as a platform for enabling partner forces to standup their own low-level, open-source operations at little cost and without classification or intelligence sharing issues. LLOSS could also serve as plausible cover for higher-level intelligence operations. Finally, LLOSS operations would have a completely absent signature footprint to detect while operating abroad, being wholly passive and using commercial equipment.

Cost and Training

To purchase all the above-mentioned gear and accessories (to include an average priced laptop of $632) totals $992. A comparable purpose-built electronic surveillance system costs approximately $130,000 according to U.S. General Services Administration Federal Supply Schedule Price List.[8] The latter system is superior in many measures but requires that users hold a security clearance and other restrictions that heavily limit its deployment and utilization. It also requires specialty maintenance and is subject to U.S. export restrictions. *LLOSS operators could utilize the COTS gear in an unclassified environment requiring no security clearance and for less than one percent of the cost.* However, the intent of LLOSS is not to replace the specialized equipment but to augment current equipment and organizations for a larger collection footprint. This will allow commanders to maintain situational awareness and focus their dedicated intelligence units on higher priority objectives.

The personnel required for training could be sourced from the signals intelligence and cyber fields. 1st Radio Battalion runs a month-long entry-level course for newly graduated Signals Intelligence operators known as the Initial Training Course. This course could be tailored to meet the LLOSS baseline capability standard and be offered at any tactical signals intelligence unit at an unclassified level. Alternately, this course could be integrated into the Company Level Intelligence Cell Course hosted at the Regional Intelligence Training Center. This would have the added benefit of familiarizing non-intel personnel with the intelligence support capabilities and organizations available to them.

Precedent and Parallels

Combat lifesaver training has been a pre-requisite for deployment workups since 2008, "The CLS [combat lifesaver] course was developed to *bridge the gap* between self-aid or buddy aid until care could be provided by the platoon 68W combat medic," according to a peer reviewed article in the *Journal of Military Medicine*. The intent was to improve patient outcomes by providing basic medical training in treating traumatic injuries to those who would be on scene before higher levels of care were available. As a result of better frontline medical training, rapid transport, and enhanced rear echelon care, U.S. battlefield casualties have a very high rate of survival.

... the intent of LLOSS is not to replace the specialized equipment but to augment current equipment and organizations for a larger collection footprint.

Similarly, human intelligence efforts also necessitate involvement by personnel not formally billeted as human intelligence collectors. While detaining enemy combatants, trained service members conduct Tactical Questioning to "identify individuals for immediate evacuation to a higher echelon facility for detailed questioning," according to *Army Field Manual 2-22*.[9] Tactical questioning is also used to obtain information of immediate tactical value that may trigger a follow-on raid or inform friendly forces of impending danger.

Signals Intelligence may seem like an esoteric art; however, its first practitioners were far from professionals. During the First World War, the Russian Imperial Army were early adopters

***Signals Intelligence Marines learn their trade at Goodfelllow Airforce Base.** (Photo by LCpl Jose VillalobosRocha.)*

of mobile radio to support its offensive operations. German Army radio operators in Prussia realized the Russians were broadcasting in plain text and passed this critical intelligence to their commander, Field Marshal Hindenburg. "We were always warned by the wireless messages of the Russian staff of the positions where troops were being concentrated for any new undertaking," remarked one senior German commander.[10] With this emerging form of signals intelligence, German forces were able to secure a key victory over the Russians at the Battle of Tannenberg. These German radio operators were not formally trained in signals intelligence but applied their innovation to make a significant contribution to the commanders' situational awareness.

Conclusion

During the Second World War, American armored forces were tied down in the Normandy countryside—unable to get through the thick hedgerows without exposing their tanks to enemy fire. GEN Eisenhower described how a small unit leader solved this urgent problem:

> There was a little sergeant. His name was Culin, and he had an idea. And his idea was that we could fasten knives, great big steel knives, in front of these tanks, and as they came along they would cut off these banks right at ground level—they would go through on the level keel—would carry with themselves a little bit of camouflage for a while. And this idea was brought to the captain, to the major, to the colonel, and it got high enough that somebody did something about it—and that was General Bradley—and he did it very quickly.

For a very little cost and training expenditure, the Marine Corps can provide open-source low-level signals intelligence and cyber support to deploying units. Individual LLOSS trained Marines will serve as valuable extra electronic eyes and ears to their units and can fill vital information gaps when isolated from formal intelligence support. The application of this proposal will expand our ability at the lowest level to collect information critical to the commanders' understanding of the battlespace and will allow all Marine Corps units to understand the electronic battlespace around them.

Notes

1. Sergey Sukhankin, "Russian Electronic Warfare in Ukraine: Between Real and Imaginable," *The Jamestown Foundation*, (May 2017), available at https://jamestown.org.

2. Siobhan Gorman, Yochi J. Dreazen, and August Cole, "Insurgents Hack U.S. Drones," *The Wall Street Journal,* (December 2009), available at https://www.wsj.com.

3. Siobhan Gorman, Yochi J. Dreazen, and August Cole, "Insurgents Hack U.S. Drones," *The Wall Street Journal,* (2009), available at https://www.wsj.com.

4. Associated Press, "Afghan Transition Tempered by Continuing Violence," *Desert News,* (July 2011), available at https://www.deseret.com.

5. Jerrick Griffin, "Every Marine a Collector," (Camp Pendleton, CA: February 2011).

6. "Afghan Transition Tempered by Continuing Violence."

7. David Cenciotti, "U.S. Airborne Communication Plane Could Be Tracked on the Web For 9 Hours During Air Strike that Killed Taliban Leaders in Afghanistan," *The Aviationist*, (August 2014), available at https://theaviationist.com.

8. General Services Administration, *2020 Authorized Federal Supply Schedule Price List*, available at https://www.gsaadvantage.gov.

9. Headquarters Department of the Army, *FM 2-22.3 (FM 34-52), Human Intelligence Collector Operations*, (Arlington, VA: September 2006).

10. Michael Warner, "Reflections on Technology and Intelligence Systems," *Intelligence and National Security,* (Milton Park, UK: Taylor & Francis, February 2012).