Signalers Work *to* Change *how* Air Defenders Train, Certify *and* Fight

By MAJ Joshua Richey, CPT Charles Wilson,
CW2 Lucas Coffman and WO1 Alexis Martinez

As Signalers serving in an Air Defense Artillery (ADA) unit, it has been an eye-opening experience learning the importance of Air Defense and how to plan for the unique assets that Brigades (BDE) have. Unlike a typical Brigade Combat Team (BCT), ADA does not have any organic signal equipment but is very network communications heavy organization. This has fallen on the communications subject matter experts (SME) to come up with solutions to bridge the gaps to provide the Air Defender with the means to certify crews and ensure they are as prepared as we can get them. So, it starts with their training at home station and at the heart of that training, is how they communicate.

Patriot units have traditionally relied on the AN/GRC-245A radio at home stations as the backbone of their communication infrastructure. Establishing ultra-high frequency (UHF) radio links between their Information Coordination Central (ICC), Engagement Control Station (ECS), and Communication Relay Group (CRG), a Patriot unit can create their Local Area Network (LAN) with their UHF links known as Patriot Digital Information Link (PADIL) to support passing data internally (Figure 1).

While this training style provides Patriot units the rinse-and-repeat training they have been used to for years, it doesn't simulate the real-world fight they would traditionally see in the U.S. Central Command (USCENTCOM) Area of Responsibility (AOR) or another future combatant commands. Updates to the current system, most significantly the Combined Crypto Modernization Phase 1 (CCMP 1), open the door to breathing new life into the training conducted at home. 31st Air Defense Artillery (ADA) Brigade is looking at ways to squeeze every ounce of potential the systems have to increase training value. They currently look at this as a multi-phased process. The first step in that process is understanding what increased capabilities CCMP 1 provides.

CCMP 1 provides routers and network connections for all Patriot shelters, allowing unclassified and classified networks to be connected to each ICC, ECS, and CRG. This network connectivity also allows for a Beyond-Line-of-Sight (BLOS) PADIL capability enables Patriot units that are geographically disconnected to share information, commonly referred to as PADIL over IP (PoIP). Due to not having any organic communications equipment to support

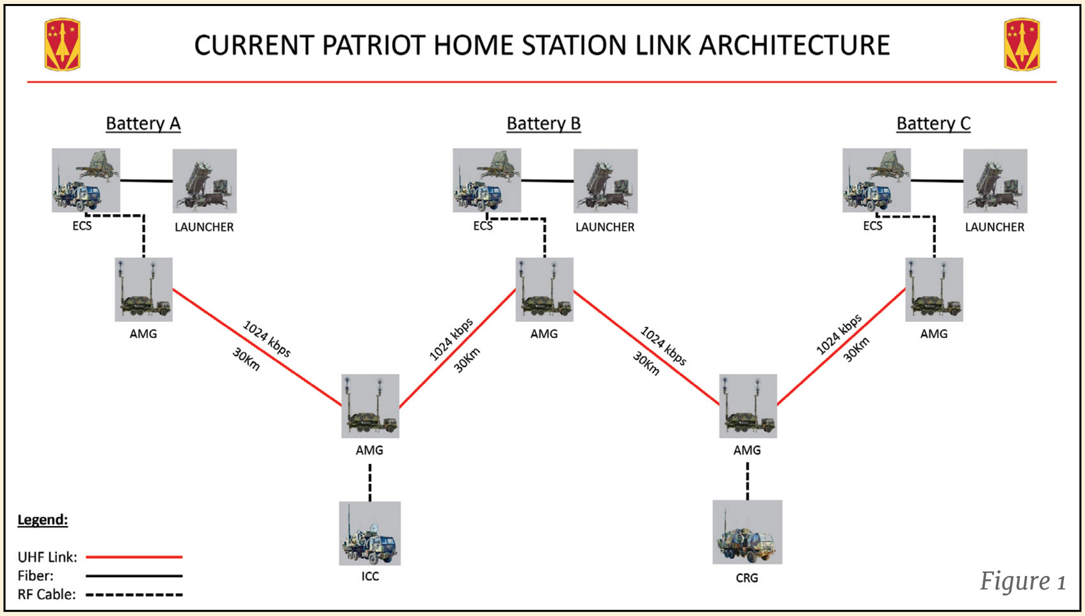

Figure 1

providing data and voice capabilities in Air Defense units, PoIP has traditionally only been used when deployed forward. This lack of organic communication assets to provide a BLOS backhaul solution has forced Patriot units to effectively fire and forget the shelter configurations they use deployed forward and revert to the home station training configuration they've been accustomed to for years until they're called upon once more.

During Roving Sands '22 at Fort Bliss, Texas 3rd Battalion, 2nd Air Defense Artillery Regiment was able to lay groundwork for improving the future of Patriot training at the 31st Air Defense Artillery Brigade by being the only ADA unit in the training event to successfully push Secret Internet Protocol Router (SIPR) services provided by a Command Post Node (CPN) from 86th Expeditionary Signal Battalion over their UHF links. This allowed the subordinate Battery's to connect and use SIPR services during the exercise. Although successful, additional testing was needed to find the optimal balance between the amount of data passed over the UHF links, without impacting the Patriot radar data, while providing the maximum distance between Patriot assemblages for training purposes. Armed with success from Roving Sands '22, the 31st ADA BDE took those lessons learned and attempted to increase the organization's capabilities.

With the help of Global Agile Integrated Transport (GAIT), like many units, 31st ADA has established its classified network infrastructure, often referred to as its tactical network or Archer Net. GAIT allows tactical units to access the greater Department of Defense classified network infrastructure and services with their organic fielded equipment from their headquarters (HQ). Combined with GAIT, units can host and maintain the same services traditionally hosted by their local installation Network Enterprise Centers (NEC) and provide connectivity to Army SIPR for their units. 31st ADA has utilized its GAIT connection, with help from the local Fort Sill NEC, to extend its Archer Net into the Fort Sill Mission Training Center (MTC). During Cumulative Training Event (CTE) 01-23, 31st ADA successfully conducted a training scenario that saw the Brigade HQ fight out of the Fort Sill MTC and its subordinate Battalions fighting out of the Brigade Operation Center (BOC), utilizing tactical services along with the Joint Training and Experimentation Network (JTEN) simulation feed to mimic the geographical separation they face when deployed forward. The next phase was to determine how to provide the same realistic training conducted during CTE to every Battalion during regular training events.

The current configuration Patriot units run in their shelters only tap into a small portion of its full potential. The current radio data rate configuration of 1024 kilobytes per second (kbps) allows for 512 kbps for their PADIL traffic and 512 kbps of overhead bandwidth to provide the path for their closed network IP services traditionally used while training at home. The AN/GRC-245A radio in the Patriot shelters can establish links with a data rate as high as 16,384 kbps providing up to 34 megabits per second (mbps) of full duplex traffic. Although the maximum operating distance of the radio is up to 40 kilometers (KM), operating the radios at higher data rates requires shorter distances between Antenna Mast Groups (AMG). Reconfiguring the radios to 8192 kbps will allow the optimal balance between maximizing the

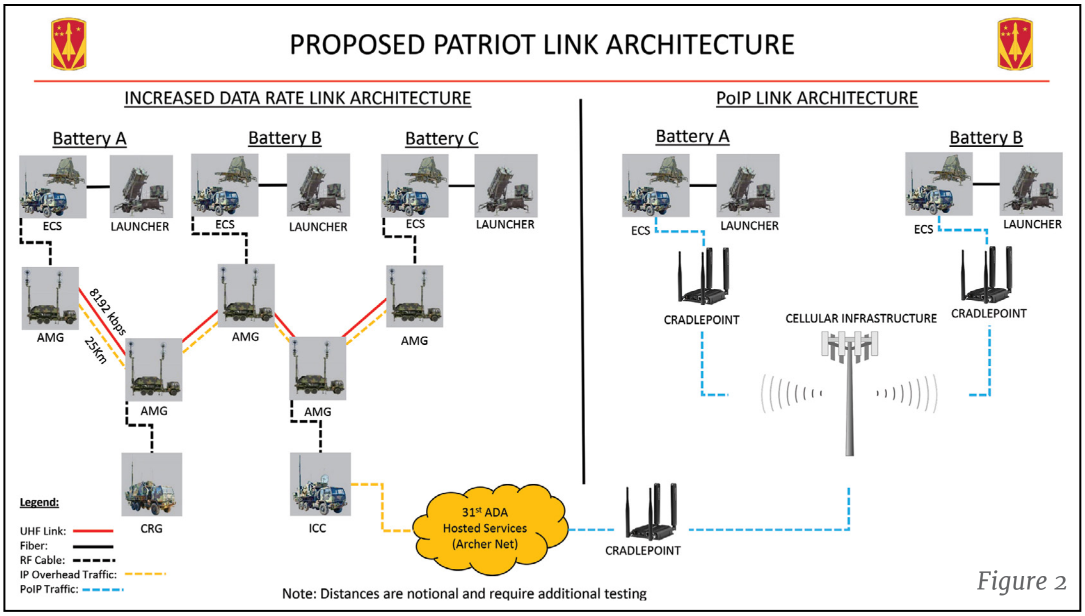

Figure 2

overhead bandwidth while, although shorter than they're used to, providing optimal distance between links for training. This increased overhead will allow Patriot units to utilize their UHF links to provide additional IP services, such as Archer Net services hosted at 31st ADA HQ, access to Army Enterprise Secret Internet Protocol (SIPR) network via GAIT, and provide simulation data from the Reconfigurable Table Top Trainer (RT3) Lab at 31st ADA HQ to the Battalion firing units (Figure 2).

PFC Harry Feliciano 25H of HHB, 3-2 ADA works on setting up the CRG for a pending certification exercise. Photo taken by CPL Yessenia Leahy 31st ADA BDE UPAR.

To provide the Patriot Battalions with access to Archer Net in the training areas of Fort Sill, 31st ADA is utilizing fiber pedestals installed in designated Training Areas (TA) as well as ingesting Archer Net services into a CRG located at 31st BDE HQ, passing these services over the Patriot units UHF links utilizing the additional bandwidth overhead provided by increasing the data rate of the AN/GRC-245A radios. Further testing is required, but the goal is to increase bandwidth to allow full SIPR connectivity, including email, Voice over Internet Protocol (VoIP), and Global Video Services Video Teleconference (VTC) ability. Along with SIPR services, 31st ADA is attempting to push simulation data from the RT3 lab at BDE headquarters over the UHF links and into the ECS shelters to provide a more realistic and challenging training environment.

Once simulation data is verified to consistently and reliably reach the ECS shelters, Flight Mission Simulator/Digital (FMSD) will be installed in each firing units ECS to pull in the simulation feed and push it into the radars to enhance user training. The FMSD system provides real-time simulation radar tracks to all Patriot radar systems within the scenario. The FMSD provides Patriot crews with a dynamic air battle that simulates the crew's real-world scenarios and requires rapid engagement decisions. This addition will allow the Soldiers to partake in rigorous training designed to stress their skills while providing an environment to perfect their skillset.

An Air Defense Artillery Brigade has the Air Defense Systems Integrator (ADSI) to provide real-time situational awareness in the AOR by integrating sensors on land, air, and sea sensors while delivering enhanced control of tactical units. Providing their common air picture in alternate ways enhances the ability to offer higher echelons timely, accurate information to assist decision-making. Since 31st ADA has enabled the simulation feed to be fed into Command Post Computing Environment (CPCE), the simulation feed from the RT3 lab would additionally reach the firing units and ADSI. This allows for multiple avenues to view the air picture locally, and the air picture can be fed to higher echelons via CPCE to provide Commanders with near real-time situational awareness.

With the potential increase in bandwidth, the opportunity exists to apply additional internet protocol (IP) based services, specifically network monitoring. 31st ADA is building a Cyber Defense Initiative (CDI) to utilize better the Cyber Network Defenders assigned to the organization. The Air Defense CDI aims to use the open-source software Security Onion to enhance network monitoring. Security Onion is a network security monitoring suite that enables both proactive and reactive monitoring of network devices; providing situational awareness of network activity. The Security Onion suite of tools coupled with Assured Compliance Asset Solution (ACAS), which scans devices for known vulnerabilities to ensure they get mitigated appropriately, will provide both a passive and active presence in Patriot Cyber Security. By installing sensor nodes in either the ICC or ECS, Patriot units could be able to send active network monitoring data to help prevent a malicious attack.

Using a simulated scenario, an insider threat were to gain access to the Patriot systems and alter the azimuth information of an incoming threat by 0.5 degrees without the operator knowing there's been any issue or change. In that case, the result could be the inability to neutralize the incoming threat, leaving the defended asset open and vulnerable to attack. That gap is what 31st ADA is looking to close at home, to take forward to the fight.

SPC Jonathan Colon 25H of HHB, 3-2 ADA turns on all the radios and equipment inside the CRG shelter for a pending certification exercise. Photo taken by CPL Yessenia Leahy 31st ADA BDE UPAR.

Providing Archer Net and simulation services to Patriot units is only one part of the hurdle in providing training enhancements that mimic their real-world mission. The ability to simulate firing units being geographically dispersed communicating via PoIP is a long-term goal of 31st ADA. A potential solution to provide the ability to train via PoIP could be using Cradlepoint routers to tap into the surrounding cellular network. Utilizing the ability to point Cradlepoint routers together by creating a Virtual Private Network (VPN) connection, you could connect a Cradlepoint to the signal entry panel of the Patriot shelters that connects to the KG-175D encryption devices that are a component of the CCMP 1 upgrade. This would provide a secure connection to a remote Cradlepoint at 31st ADA HQ to allow access to Archer Net services. If successful, this would enable the ability to provide Archer Net services and simulation while allowing the firing units to simulate being geographically dispersed, requiring them to establish their BLOS PoIP links to communicate.

The level of advanced training would alter the way large scale training events like Roving Sands are executed. With a home station PoIP solution, Patriot units at Forts Sill, Hood, Bliss, and Bragg could conduct large scale exercises from home while receiving simulation feed that is being fed into their ECS, and send their portion of the air picture to higher HQ. This would open the door for more creative training at all levels that does not rely on all units being collocated to conduct operations.

These changes would allow each unit to tailor their training to the specific environment they are about to encounter. Whether the unit will rely on UHF links, be tied to a CPN team for backhaul, or fibered into their PAT site, the ability to train at home station and mimic the situation down range would be a first for Air Defense. In lieu of historical assessment methods, this enhanced capability package would also lead to changes in the way Patriot crews certify. The new crew certifications could require ADA crews to certify based on the tailored operational environment, specific to mission variables and requirements allowing Air Defense to train as close as possible to how they fight while deployed, something they have only been able to partially replicate due to numerous limitations.

MAJ Joshua Richey is a Signal Officer, currently serving as the 188th Infantry BDE, S6/Senior Signal OC/T. He previously served as the 31st Air Defense Artillery Senior Signal Officer, 2d Security Forces Assistance Brigade and the Signal Company Commander for 5th Battalion, 2d Security Forces Assistance Brigade. MAJ Richey has deployed to Afghanistan, Iraq, and Qatar as the Top Notch S6 for 32d AAMDC with 31st ADA BDE.

CPT Charles Wilson is an Information Network Engineer currently serving in the 31st Air Defense Artillery Brigade as the senior Network Engineer. He has served in this position for over 4 years and previously served with 75th Field Artillery Brigade as a Fire Support Officer. CPT Wilson has deployed to the CENTCOM AOR twice.

CW2 Lucas Coffman is a Signal Warrant Officer currently serving in the 31st Air Defense Artillery Brigade as the Data Operations Warrant Officer. He previously served as the Automated Information Systems NCOIC for 3d Ranger Battalion, 75th Ranger Regiment and has deployed to the CENTCOM AOR twice.

WO1 Alexis Martinez is a Signal Warrant Officer currently serving in the 31st Air Defense Artillery Brigade as the Network Operations Warrant Officer. He previously served as the Deputy Branch Chief for White House Communications Agency, Special Missions Command Network Management Center and has deployed to the CENTCOM AOR four times.