Africa Command

A data sharing network

by Maj Benjamin J. Hawthorne

>Maj Hawthorne was assigned to the Combined Joint Task Force - Horn of Africa CJ-63 when he wrote this article. He has previously deployed to Operation Iraqi Freedom (2005–06) and to Operation Enduring Freedom - Horn of Africa (2014–15). Maj Hawthorne is currently assigned as the Operations Officer, Marine Wing Headquarters Squadron 2.

During a commencement speech to the graduating class of 2014 at West Point, President Barack Obama stated:

> … for the foreseeable future, the most direct threat to America, at home and abroad, remains terrorism, but a strategy that involves invading every country that harbors terrorist network is naïve and unsustainable. … We need partners to fight terrorists alongside us. And empowering partners is a large part of what we have done and what we are currently doing …

For Combined Joint Task Force–Horn of Africa (CJTF–HOA), enabling our multinational partners to neutralize violent extremist organizations is a daily activity involving a broad scope of organizations. This is a cooperative effort between Joint services, interagency, intergovernmental, and multinational teammates. CJTF–HOA's Commanding General, BG Wayne Grigsby, USA, refers to this great combined force as the JIIM team—joint, interagency, intergovernmental, and multinational team. This article will focus on enabling our multinational partners in an effort to strengthen the JIIM team by providing a secure means to collaborate together in order to render our adversaries incapable of disrupting peace and stability in Eastern Africa.

Conducting operations within Africa comes with a set of unique challenges. Each challenge is met with a unique solution to overcome those challenges. One such challenge is being able to share information securely between U.S. forces and troop contributing countries (TCC) to African Union Mission in Somalia (AMISOM). The Africa Command Data Sharing Network (ADSN) has been developed to meet the need to securely pass data communications between U.S. Forces and TCCs. The ADSN also provides an opportunity for U.S. forces to interface with their African counterparts, which has the potential to improve the relationships between U.S. forces and our multinational partners.

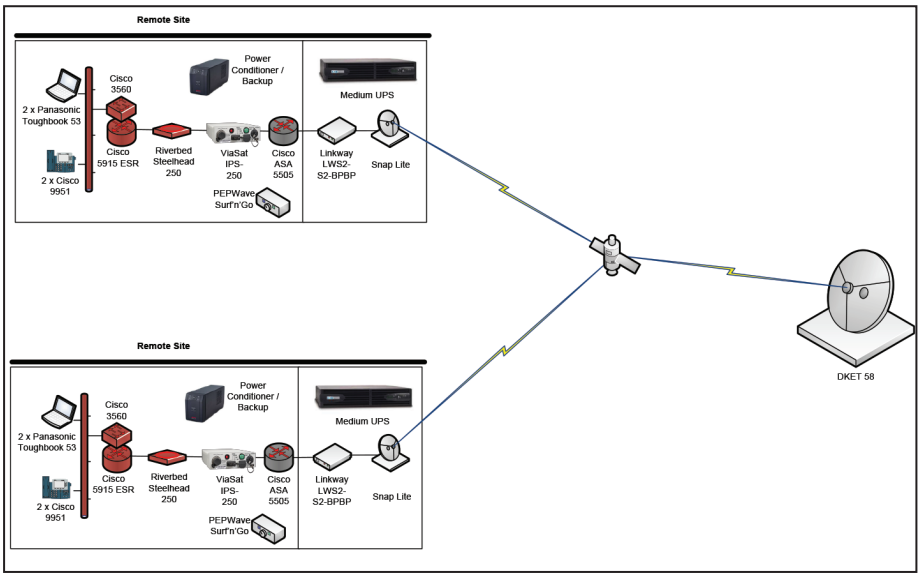

Figure 1.

So what is the ADSN? The ADSN is a closed network, provided by the United States to select TCCs. Currently, Kenya, Djibouti, Uganda, and Burundi have been recipients of an ADSN terminal. The terminals are Secure Internet Protocol Router (SIPR) Network Access Point (SNAP) 1.2 meter lite systems that provide secure voice and data. These terminals are packed in six ruggedized transit cases for a combined weight of 600 pounds. The equipment is easy to transport for the TCCs as all six boxes fit in the rear of a sports utility vehicle. Each ADSN terminal comes with two voiceover Internet protocol (VOIP) phones and two laptops. The setup of the terminal is fairly simple and quick, taking a trained operator approximately 30 minutes to establish the node. Once in place, the satellite dishes will automatically acquire the satellite. Figure 1 is a depiction of the equipment string of the SNAP Lite. It is very basic: modem to router, router to encryption device, encryption device to router, router to switch, and switch to user end equipment. This provides a simple package that will allow the

user access to SharePoint and secure phones.

Located within the same satellite footprint is the hub, a Deployable Ku-band Earth Terminal (DKET), which houses the various services for the network. The SharePoint server and Cisco call manager reside at the hub. Currently, there is no exchange server as all communications products are exchanged via SharePoint. This enables all the distant sites to tie together on one network and share information. Lastly, the hub allows U.S. personnel to push the cryptographic keys to the distant terminals. This is important because there is no provision which will allow our TCCs to handle and manage Type 1 cryptographic keying material. For the purposes of this article, this is all that will be reviewed. This is the basic network layout which supports information sharing between U.S. Forces and TCCs.

Installing an ADSN system

Before the physical installation, permission must be gained from the host nation and the U.S Government. The first step in the process is to agree to share information between the United States and the host nation. Once approval for information sharing has been met, a release in specific dissemination control will be staffed and validated by the Joint Staff and then sent over to the National Security Agency so that the new cryptographic keying material can be developed. The two nations will then sign an information security equipment agreement. This accomplishes two goals: one, the host nation agrees to safeguard the equipment and not tamper with the cryptographic equipment; and two, it acts as a hand receipt between the United States and the host nation. Except for the cryptographic device and the hard drives, the rest of the equipment is now the ownership of the host nation. Neither of these tasks is a simple exchange between the two countries; however, this may be viewed as the initial stages of cooperation and sharing. These initial steps have great potential to create an environment of trust and good will between the two countries.

As soon as there is an information sharing agreement between the United States and the host nation, United States forces can train qualified individuals. A qualified individual is a host-nation member who has been Leahy vetted. The Leahy amendment was sponsored by Senator Patrick Leahy in 1997, and was put in place to prohibit the United States from providing military assistance to foreign military units that have violated human rights unchecked. The Leahy vetting is applicable to foreign units, not necessarily to individuals. It is important to note here that this is the only requirement to receive training. This is a challenge as instructors engage with various levels of student capabilities—past experience, baseline knowledge, rank, age, language, and military specialty. We are very familiar with our MOS selection process. A physically and morally qualified individual takes an Armed Service Vocational Aptitude Battery (ASVAB) which will determine his career options. From there, individuals are basically trained and attend an in-depth MOS school. For example, a data network specialist (0651), is physically qualified to join the Marine Corps, is morally qualified to attain no less than a secret clearance, obtains a general technical score of 110, receives 13 weeks of Marine Corps recruit training, completes 22 days of Marine Combat Training, then finishes his data and network training within 72 days at MOS school in a structured environment. The East African trainee may not have any networking experience at all. As it stands, the Internet is not widely available to the average citizen throughout Eastern Africa. For example, only 1 out of 10 Burundians have ever experienced the Internet. The students may have been placed in the class due to technical ability, but they also may have been selected due to social standing, ethnic affiliation, rank, or other factors that may not have made them the best choice for technical training.

Typically, once a vetted group of individuals has been identified, a mobile training team (MTT) will travel to the host nation's desired location. The MTT consists of two servicemembers from a communications background who have been thoroughly trained on the ADSN. This training consists of a 4-day course, taught by contractors, to U.S. servicemembers who have a background in satellite communications and data networking. The other team members are U.S. servicemembers from operations and those who have a background in intelligence to instruct the host nation on how to post intelligence products. The course is designed to last 4 days. This is not due to lack of materials, but to a realistic approach to funding the training. On day one, the host nation is introduced to the equipment. Days two and three are spent establishing the terminal, learning how to power it on properly, programming the modem, remotely controlling the antenna, and analyzing how to assist in remote troubleshooting. The switches and routers are preconfigured by U.S. servicemembers. This is somewhat out of necessity as adding training material for routing and switching protocols/commands to the course would exceed the 4-day training course. For this reason, the host nation does not receive the username and passwords to their routers or switches.

Before the physical installation, permission must be gained from the host nation and the U.S. Government. The first step in the process is to agree to share information between the United States and the host nation.

Maintaining the ADSN

In order to maintain the ADSN, some basic requirements must be met. The ADSN terminal requires a dedicated 30 amp circuit or a dedicated 3,100 kilowatt generator. The terminal also requires an environmentally controlled

room, capable of maintaining temperatures less than 85 degrees Fahrenheit. The length of the receive, transmit, and monitor and control cables are 100 feet, so a satellite dish needs be to within 100 feet from where the backside equipment will be staged. The dish needs to be placed on flat level ground, free from vehicle and foot traffic, and in a 12-foot-by-12-foot area. Also, the satellite dish needs to have a clear line of sight to the satellite, but special consideration has to be made to ensure that it is not emanating into anyone's workspace, such as a guard shack. For U.S. forces, these requirements can all be met in short order; however, these considerations present unique challenges to some of the host-nation recipients. Power is a premium in most African nations, which makes it challenging to find a dedicated 30 amp circuit. Once procured, it becomes a challenge to ensure that circuit is not used for other equipment which draws a considerable amount of power, such as the air conditioner that is required to keep the room at or below 85 degrees Fahrenheit. This is a challenge in itself since temperatures in most areas where ADSNs operate have an average of 100 degrees Fahrenheit throughout the summer. If shore power is not readily available and a generator is required, it presents a whole new challenge—providing a steady stream of fuel to keep the generator running. This can put a considerable strain on the logistic capability of the host nation. It also dictates the hours of operation for the terminal. Most nations will turn the system on when they need to pass data and turn it off when they no longer require it. This makes two-way communications difficult, particularly when trying to contact the distant end via phone. Lastly, having a basic understanding of the host-nation's engineering capability is important. If a level surface is not available in the desired location, the host nation must have the capability to create such a surface. These are planning factors that are well understood and are attainable by U.S. forces; however, the introduction of satellite and expeditionary data equipment is foreign to the majority of African nations, which means the supporting requirements for this capability have not been established or may not be present.

Very frequently, components of the ADSN may not be able to survive the harsh environment of East Africa, the daily set up and tear down, or the lack of consistent clean power. There have been a variety of component failures on the ADSN terminals. Block-up converters have failed because faulty fans became clogged due to dust and rain. Lawn mowers have run over transmission cables. Power surges have damaged the uninterrupted power supply on several occasions. Improper start up and shut down procedures have burned out the satellite dish's tracking motor. Some TCCs have run the

system off the uninterrupted power supply before being able to perform a graceful shutdown, which affects the system and prevents the satellite dish from being properly stowed. Having the satellite dish improperly stowed will affect the systematic boot up process and will affect the auto-acquire feature of the satellite. These systems are under warranty; however, getting the parts to their respective ADSN terminals is not a speedy process, particularly within conflict zones where U.S. forces are not allowed to operate freely. Receiving permission from the U.S. Embassy and then coordinating with the host nation's military delays the ability to send a contact team to repair the equipment. Typically, with an expedited process, permission from the U.S. Embassy and the host nation can be achieved in 96 hours. The primary mode of logistics is U.S. airlift. U.S. airlift provides the speediest means to send repair parts and personnel down range.

There have been several challenges that have been addressed when it comes to maintenance and installation. The first set of challenges that should be addressed is installation. The installation of an ADSN system takes effort from different elements of the staff. The J-2 (intelligence) is primarily responsible for the user end training. The J-6 (communications) has been responsible for conducting the site surveys, determining if the physical location would be suitable, and training the technicians. The J-2 has always met with their counterparts and the J-6 has met with theirs. However, the J-4 (logistics) has never accompanied the MTT on training for site surveys. This is problematic because a significant portion of ADSN reliability is directly connected to power and environment control. This will also allow the utility subject matter expert to interface with his host-nation counterpart to reemphasize the need to maintain a suitable temperature for the ADSN and to never overload the circuit. This information is already part of the training package, but perhaps it is given by the wrong trainers to the wrong audience who may not be able to affect power requirements. If using a generator, the utility operators and the ADSN technicians require close coordination. ADSN shut down should occur before the generator is turned off, and not repeatedly rely on the uninterrupted power supply on a daily basis. This will ease the wear-and-tear on the equipment and allow the shut down to be more methodical instead of trying to shut down the equipment within a small window of time. This has two desired effects: one, it will help solidify the engineer requirements for the ADSN terminal; and two, it increases staff coordination within the host nation.

With the training challenges that are presented, one factor that is persistently not an issue is the willingness and desire to learn.

With the training challenges that are presented, one factor that is persistently not an issue is the willingness and desire to learn. Due to time restrictions, the instructors could not possibly cover anything beyond how to turn the ADSN on and how to turn it off. However, instructions can be broken down into elements that they can fix and elements that they can control. For example, along with the ADSN, we can provide them with a thermometer with the 85 degree mark highlighted. This is their tool to monitor the health of the network. This provides them with a useful tool to make an informed decision and empowers them control their maintenance. Likewise, it is not enough to teach the host-nation partners how to turn the ADSN on and off. A maintenance package needs to be included. Another example of preventive maintenance is teaching the host-nation partners how to use a can of canned air and how to apply air pressure properly in order to keep the equipment free from debris. Instructions on how and when to replace the batteries and how to order batteries from various vendors will also aid in the maintenance cycle. Lastly, a thorough understanding of each piece of equipment and how it functions will greatly aid the contact team's effectiveness once they reach the equipment and will assist the contact team in bringing the right replacement equipment and tools for the job. This type of pre-coordination makes the host nation an active member in the contact team instead of a bystander.

Finally, the movement of personnel and equipment should also involve the host nation as much as possible. There are several reasons for this. One, the host nation may have more on-the-ground assets than U.S. forces as well as greater flexibility to operate in their own country or conflict zones. Two, the requirement to request permission to have a U.S. member enter the country is no longer there, saving 4 to 5 days. Three, and most importantly, it injects the host nation into solving its own maintenance issues.

It is hard to predict what our future involvement on the content of Africa will look like, but it is safe to say that events in Africa will continuously be tied to our national security strategy. Groups such as Boko Haram and Al Shabab have replaced headlines once held by the Taliban. Since 1960, when the majority of East African and Central African countries received their independence, the region has been defined by instability. Being able to enable responsible governments to counter violent extremists and improve regional stability will most likely be an enduring mission of the U.S. Government. The ADSN is just one tool that is currently being used to enable our partners. However, the fielding, training, installation, and maintenance are equally important in increasing our partners' capacity to integrate the ADSN into their arsenal.