

Defining AFRICOM's Mission

By Hamlin Tallent and Cameron Matthews

December 2008



A key goal for the new U.S. Africa Command (AFRICOM) is to facilitate information sharing between the continent's militaries and governments. The command seeks to ensure the interoperability of national communications systems, such as this Ugandan officer's radio, with other nations' equipment for humanitarian, peacekeeping and disaster relief operations.

Combatant commands are vital to the protection and preservation of U.S. interests. However, in today's dynamic, volatile global environment, they may need to evolve their "product" to best suit the environment they intend to shape. In the case of U.S. Africa Command, it may be more relevant and effective for the organization to support the region's fledging democracies. These nations need assistance in establishing their ability to openly share information with each other and international allies. In doing so, U.S. combatant commands can prove invaluable in helping nations grow and prosper to become better service providers to their people and achieve greater positive outcomes as a result.

As the newest combatant command (COCOM), U.S. Africa Command (AFRICOM) must be able to define its mission. This main theme has run through national media articles, the March 2008 Congressional Research Service report on AFRICOM, and the congressional testimony of various experts offering insight into the

challenges and opportunities facing the command. A central line of questioning running through all of this dialogue centers on what AFRICOM's mission is and therefore its "product." While the primary product of other COCOMs historically has been war plans, AFRICOM might consider an alternate approach. Instead of extending U.S. capability into a foreign environment, the command instead could use U.S. capability to enhance that environment.

This approach allows AFRICOM to develop the sovereignty of African nations by enabling governments and other leadership entities to provide services to their people and, by doing so, to strengthen their societies. While not a direct military role, the benefits of taking on such a responsibility could foster even greater regional security and stability by exhibiting a large-scale show of force.

Perhaps AFRICOM's initial thrust should be to enhance African national information gathering, analysis and sharing, as well as its planning and execution capabilities—because without information, there can be no knowledge, and without knowledge, there can be no real sovereignty. Without sovereignty, there is no core of responsibility for the host of challenges that face national populations. In this scenario, AFRICOM does not provide information—rather, it assumes the role of enhancing the collection, sharing and use of the data already resident within a society. This is where the information to fight the Global War on Terrorism resides. As the late Speaker of the U.S. House of Representatives, Tip O'Neill, once said, "All politics is local." The same is true for the Global War on Terrorism because "all terror is local." Those who are terrorized must define the nature of the threat, and the way to fight it must be defined by those doing the fighting.

AFRICOM can lead in helping sovereign nations defend themselves by increasing their ability to collect information from disparate open sources and by analyzing the data for meaning in context to providing services. This capability includes security from terror and rampant criminality. The COCOM also can help nations share this information both internally and to a wider audience when appropriate, as well as help transform the data into plans and operations.

The creation of such a capability will allow African decision makers to query databases, gain situational awareness, understand the environment, develop plans to affect that environment and then administer activities to support those plans. It is possible to envision a proactive decision maker applying this system to counter terrorism and criminal activity, but also using it to counter the spread of HIV-AIDS or even to develop and administer a multiyear agricultural project.

While it may be argued that African nations are too suspicious to share information, failure to develop the capability will doom the region to a dangerous ignorance. AFRICOM's regional predecessor, the U.S. European Command (EUCOM), was a noble provider of services and support to much of Africa. This assistance included some Internet access and communications equipment, some English-language training and a huge dose of advocacy before Congress.

EUCOM also provided filtered information from classified sources to support the Global War on Terrorism. However, EUCOM did not take the next step to help Africa develop a comprehensive system sovereign to each nation that also connects to and supports regional and continental spectrum groupings such as the Regional Economic Councils (RECs) and the African Union (AU). Ideally, such systems would be developed and owned—with assistance—by the nations themselves and the technologies selected based on the processes Africans find most useful. National systems will be cooperative, and the plan would combine them to support a REC or AU goal.



AFRICOM may develop information-sharing networks that would enable African nations to share unclassified data. One area that would benefit from such a system is maritime security because it would allow nations to operate in regional coalitions, such as this exercise off of Equatorial Guinea, to combat pirates, terrorists, smugglers and human traffickers.

A central piece of the African vision is to provide stability to the continent by using regional standby brigades. Each of the five African regions is responsible for developing the capability whereby nations pledge forces, and a central, regional headquarters plans operations to provide a range of services across the region. However, none of the regions has the ability to identify and characterize the readiness of pledged forces, let alone plan and actually conduct operations with them.

This envisioned information-sharing system would be designed to allow U.S. entry and data flow as appropriate. Such a capability is critical, as most of the desired information regarding impending terrorist activities is “known” in the local environment but not necessarily on U.S. classified databases. It is the type of information known by ordinary people as they observe what is happening around them. Information and the communications systems that analyze and forward it must be supported by unclassified technology systems, such as geospatial mapping and virtual chat applications. These means of communication will foster collaboration and real-time response to situations occurring in an area of operation. The unclassified nature of these networks and systems would alleviate the concern of providing African governments access to secure U.S. Defense Department Internet protocol networks while providing these moderate ruling parties access to valuable information to help them counter insurgents and terrorists within their borders. Moreover, such a system would go beyond merely providing a collaboration center. It also would enable wide coalitions such as the 1,000-ship navy—a proposed international alliance for maritime security—the operational means to plan and conduct activity.

In essence, this system would be a communications portal based on the open-source server, Web services and other common Internet applications that can process and disseminate

information across everything from fiber optic connections to the slowest cell-phone data networks. Such flexibility is important in Africa as well as other developing nations where basic infrastructure support, such as reliable satellite and wireless connectivity and access to stable power, may be limited or nonexistent.

These scenarios are becoming more commonplace as the Global War on Terrorism requires more U.S. government and military personnel to operate in remote areas for longer periods of time. Forward-deployed assets will undoubtedly deal with regular power outages, sporadic Internet connectivity and high-packet latency. This does not mean that information sharing is impossible under such circumstances. However, program managers and engineers must understand how data exchange can occur with units and individuals operating in remote areas. Two potential solutions involve resolving the “small pipe syndrome” and overcoming intermittent connectivity.

For issues where remote operations are preventing forward-deployed assets from downloading large amounts of data before timing out, administrators should consider implementing policies and practices to move data along, such as using compression software on Web service call payloads or transport-level compression (for example, GZIP over hypertext transfer protocol), re-examining the system’s communication infrastructure and generally reducing the amount of messages that are sent, and batching information together where possible to reduce call overhead. Other solutions to low bandwidth include using longitudinal communication encoding—never sending the same full message twice—and designing the system to be event-based with server push, rather than client polling, to eliminate update detection traffic.

To better serve end users operating in locations with unstable or unreliable power and Internet access, agencies may want to employ tactics such as using a graphical user interface client package with Web service calls to service-enabled back ends, designing both client and server to be event-oriented and evaluating using an overall event-driven architecture for proper fit.

Additional solutions for circumventing intermittent connectivity include designing both the client and server to be asynchronous message-based rather than using synchronous Web service calls, thus preventing either side from hanging up when a connection is impossible; pushing as much intelligence as possible into the client (making it a “smart” client), because it is closer to the user and will retain functionality even if the connection drops; and understanding the issues with cache coherency and reconciling differences once the connection is regained.

Rear Adm. Hamlin Tallent, USN (Ret.), is the vice president of C4ISR systems at Sentek Consulting and former director of operations for U.S. European Command. Cameron Matthews is the chief technology officer for Sentek Consulting.

Web Resources

U.S. Africa Command: www.africom.mil

Sentek Consulting: www.sentekconsulting.com