

Secure Communications Doesn't Start With Phones From Home

July 2006



ON CYBER PATROL



If there were only a small number of combinations for safes, electronic door openers for cars or key designs for our house locks, our personal lives would be much less secure. Criminals would be able to break into our homes, drive away with our vehicles and steal our valuables with little trouble. Fortunately those keys and combinations are often difficult to reproduce or bypass, at least enough to offer an acceptable level of security. Like any security setup, all of them can be enhanced with additional or redundant systems that make getting past them that much harder. The personal consumer communication devices that we use at home have some of these safeguards, but most of them are very easy to bypass. A knowledgeable criminal could listen into your phone conversations and read your e-mail with only a little effort.

Obviously military communications, especially in a war zone, must be kept far more secure. The enemy can pick up valuable intel from even the most casual of conversations. That is why the military has gone to great lengths to ensure that approved communication devices are as secure as possible. A significant amount of technology, research, testing and financial resources go towards that effort. That is why using non-approved communication devices, especially consumer devices from home, to transmit potentially sensitive information puts everyone at risk.

It takes very little effort to listen in and intercept messages that could betray force strength, troop movement, and other information of strategic and tactical importance. It is difficult enough to keep that information secure with approved devices. That's why all military personnel should never use unsecured means to communicate anything that could aid the enemy. Well meaning gifts from home could end up putting soldiers' lives and military operations in danger.

Chapter 6 of AR 25-2 covers communication security. It is one of the most vital sections of the regulation and covers the requirements and use of Protected Distribution Systems (PDS), radio systems and telecommunication devices among other things. It specifically prohibits the use of commercial non-encrypted radio systems in the support of command and control functions. That's why the devices you received in that last package from home are potentially a direct link to an eavesdropping insurgent.

The bottom line is that soldiers should use only approved secured communication devices that transmit encrypted communications to discuss anything that deals with operations and related subjects. Not doing so could lead to a successful enemy ambush or the failure of a tactical operation because the targets had advance knowledge. Protect your fellow soldiers and yourself. Keep a secure lid on your communications.