

25 May 2009

By: Lucian Constantin, Web News Editor



The military looking for ways to weaponize cyberattacks
United States Air Force

[U.S. Military Developing Hacking-for-Dummies Cyber-Warfare Device](#)

Move some sliders, push a button and you're in

U.S. Defense Department officials were so impressed with the level of coordination between ground military ops and cyberattacks against strategic targets during the recent conflicts, that they are now looking for ways to weaponize hacking. Aviation Week glanced at such a device and [reports](#) that it is being designed to be easily used even by non-techy soldiers.

The recent armed confrontations, such as the one in the Gaza Strip between Israel and Hamas or the earlier one between Russia and Georgia, were accompanied by Denial of Service and other types of attacks targeting governmental networks and servers that shocked the IT experts. It certainly did not take long for everyone to realize that this was the future of warfare and get the military to send its researchers looking for efficient ways to apply similar tactics.

Apparently, there are several devices currently being developed behind closed doors specifically for such purposes, but the one Aviation Week talks about is intriguing. It is basically a highly complex hacking tool designed for the unexperienced that is to turn soldiers into veritable script kiddies. Granted, script kiddies with a lot of firepower.

This expensive hacking gadget can be carried around in the backpack on the battlefield and used to assist in missions that might require breaking into wireless networks, such as the ones used for VoIP or satellite communications. However, the icing on the cake is the ability to hack into SCADA (Supervisory Control and Data Acquisition) systems. These systems are used to administrate industrial equipment at power and chemical plants, nuclear facilities, oil refineries, etc., so one can easily imagine how that would be extremely valuable.

The device is easily able to map out all the nodes of a given wireless network and, if necessary, cause them to disconnect, then watch them getting back online in order to identify weak spots. Once the best target is determined, the soldier (slash hacker) is presented with several attack attributes and can adjust their respective level by using sliders on a touch-screen. These attributes include, but are not limited to covertness, speed, or collateral damage.

For example, depending on the situation, one might be OK with a high level of collateral damage in exchange for a more speedy attack. At other times, when remaining undetected is vital, the covertness slider can be maxed out, but the attack can take days. Depending on the selections, the device decides what combination of hard-coded hacking algorithms to use.

The attack techniques are implemented by using both publicly available code, from projects such as Aircrack-ng or MadWifi, as well as proprietary one. The device can also be used for penetration testing purposes or to gather blueprints of possible targets from the battlefield, which are then taken back to more specialized personnel, who can execute the attacks.