(TS//SI) New CNO Capability Poised to Help Counter IEDs, Geolocate Terrorists

FROM: (C) [redacted]
Dragon Team Lead (S31211)
Run Date: 05/10/2006

(TS//SI) New capability allows for denial-of-service attacks against HPCP networks and the geolocation of specific HPCP users.

(U//FOUO) The S31211 Dragon Team

(TS//SI) Tucked in to a corner in the OPS 1 basement is a small Radio Frequency (RF) Screen room very few people remember how to find. This is where the S31211 Dragon team usually spends their days. Founded to provide Computer Network Operations (CNO) solutions to a wide range of Combatant Command and military service requirements, the Dragons focus on networks that communicate via the RF, rather than hard-wired IP technologies. They develop RF-based CNO capabilities against target networks ranging from VSAT to Trunked Mobile Radio to Personal Mobile Radio.

(TS//SI) "Tricking" Enemy Networks

(TS//SI) Any network that transitions the RF relies on Command and Control (C2) signals to establish, maintain, and protect the communications channel. The Dragon team's approach is to take advantage of such protocols by creating "legitimate" C2 signals and transmitting them into the RF. When the target network *hears* these signals, they respond accordingly. Depending on the Dragon command sent, the network may become visible in the network for geolocation, may end a communication session, or may even allow the insertion of a spoofed station into the network. Moreover, because these RF capabilities never physically "touch" the network or install network attack / exploitation software on the system, they are exceptionally hard to defend against or even to detect!

(S//SI) Focusing on HPCP Networks

(S//SI) As the global war of terrorism (GWOT) became an ever-larger task for everyone in the Intelligence community, the Dragon team was charged with developing capabilities to counter terrorist communications. Of special concern to the war fighters across multiple Combatant Commands was the prevalence of High Power Cordless Phone (HPCP) networks. HPCP networks (or Long Range Cordless Phones as they are sometimes known) presented our community with several challenges. They are cheap (under $1000.00 for many models), provide data, voice, and fax communications across very large areas (20-90km are common), and operate under absolutely no regulation. For a few thousand dollars, an individual can set up and run an HPCP network that provides service for over 100 square kilometers.

(S//SI) Moreover, as the insurgency in Afghanistan and Iraq came to rely heavily on Improvised Explosive Devices to attack US and Collation troops, HPCPs became a favored means of triggering these devices for several reasons. Unlike garage door openers or key fobs, HPCPs provide a strong, clear signal over a great distance. Because the user owns the network, there is no risk of dialing registries, billing records, or licenses to identify the attacker and because there are no competing users on the network, there is no risk of call blocking or delays to interfere with the timing of the explosion.

(TS) Key terrorist high-value targets (HVTs)

(U//FOUO) The Mission: Help Find the Bad Guys and Help Stop Them

(S//SI) The Dragons were charged with providing clean, surgical, and controllable CNO effects against HPCP networks to assist Force Protection missions by stopping the HPCP networks from communicating and to assist in the geolocation of High Value Targets (HVTs) by providing surreptitious pinging for geolocation assets.

(U//FOUO) HPCPs used as triggering devices for IED attacks

(U//FOUO) The Solution: FIRESTORM

(TS//SI) The FIRESTORM Capability is the first Radio Frequency (RF)-based Computer Network Operation (CNO) Capability designed to provide the war fighter a plug-and-play attack capability against High Powered Cordless Phones. Among the capabilities provided by this tool is the ability to run denial of service (DoS) attacks against HPCP networks and to assist in the geolocation of specific targeted users. Operational applications of this capability include preventing specific target networks from communicating, preventing some classes of Improvised Explosive Device (IED) attacks where the HPCPs are used as the triggering device, and supporting "Find and Fix" missions seeking to locate and apprehend high value enemy users. The FIRESTORM capability to actively ping a known HPCP network supports one of the most critical efforts in the GWOT - locate high priority targets - by forcing the targeted HPCP to emit an RF signal that can be geolocated by any asset in the area. A FIRESTORM operator can decide when the HPCP will be visible and will even designate the frequency!

(S//SI) The FIRESTORM CNO capability is poised to support a wide variety of customers and the Dragon team has been eagerly working with potential users to move this capability out of the development lab and into the fight. USSOUTHCOM has requested that a FIRESTORM capability be available "on all platforms supporting this" Area of Responsibility. To this end, the Dragon team is working with the [redacted] to integrate and test a FIRESTORM on the SHULA PAVON platform and is working with the Navy to integrate and test a FIRESTORM on the EP-3 DOLPHIN EAGLE. Additionally, they are supporting a Navy request for FIRESTORM effects on alternate platforms by providing technical assistance to ongoing research efforts at the Naval Postgraduate School.

(S//SI) Finally, as this article "goes to press" (with a short stop at the inbox of our friendly Classification Advisory Officer), several of the S31211 Dragons are packing their bags and heading down to Quantico, Virginia. The [redacted] US Marine Corps is currently deployed in Iraq and asked the Dragons to assist them in preparing for a Test and Evaluation of the FIRESTORM to determine its suitability for their mission. It seems that our Marines know of some bad guys in "The West" and would really like to speak with them. How could the Dragons refuse?
