Cook County ARES Net--Training--23 October 2013

Some Lessons Learned from the 2013 Statewide SET

The Illinois Statewide SET was conducted a few weekends ago. It was quite interesting, and the exercise reminds us of some realities of major disasters and other events that disrupt communications and other infrastructure.

The basic scenario of the SET was a "hack attack", in which the attackers disrupted conventional commercial telecommunications, including telephone and Internet. Broadcast media, and the electric power transmission and distribution network, and natural gas pipelines were also disrupted. A task announced before the event was to transmit a Winlink message to the state RACES station NC9IL over an RF path. Additional tasks were injected by announcements via the Illinois ARES HF net and via e-mail distribution lists (the Internet was deemed operational for that purpose.)

While that scenario, with several coordinated disruptions, may initially seem a bit contrived, on careful consideration the scenario is not far-fetched at all, and it seems highly likely that future terrorist attacks will be directed to several or all of these infrastructure elements. Many of them are believed to have signficant, unpatched vulnerabilities. Unlike many other types of attack against physical infrastructure, where the attackers must be present in the vicinity of the target, within hours or days of the attack, these vulnerabilities can be probed and catalogued by attackers (a) well in advance of an event, and (b) from remote locations. Moreover, such attacks may be initiated remotely. Thus, attackers may be emboldened by the view that such attacks are free of personal risk to them. Further, attacks against communications assets are especially effective because they hinder response and demoralize the civilian population.

So what can we learn, or be reminded of, based on the experience of this SET?

1. Simplex rules. Simplicity rules. Infrastructure, such as repeaters, the Internet, and the like may fail in ways out of our control. Simplex on VHF and UHF paths, direct HF, and other similar modes of communications that do not require intermediate infrastructure can be more reliable. Yes, it's true that our own equipment, antennas, feedline, and power sources are not impervious. But we usually have tools and expertise and may be able to work around those failures. We generally can't do anything about failed infrastructure in remote locations, or controlled by others.

2. Advance preparation helps. While we don't know what will happen or when, we can be far more effective if we have equipment assets prepositioned, and we have experience in

performing the various communication tasks we will be assigned. And we can be prepared in a number of ways, both traditional and non-traditional.

a. Know the skills of accessing (or running) voice and other nets on HF and on VHF/UHF. There are many opportunities to practice these skills.

b. Know the skills of originating, passing, and delivering both tactical and formal message traffic on behalf of your served agencies. If you are not affiliated with a served agency, there are a few basic message handling skills that you can learn and practice to be prepared for the agencies you are likely to serve. The ability to handle messages in ICS-213 and ARRL Radiogram formats is a commonly needed skill. And it **is** a skill, which you need to learn and practice in order to be be an efficient communicator.

c. Know how to use your equipment, and be able to do common tasks without consulting the manual. Modern radios, in particular, have lots of bells and whistles buried deep in menus or assigned to keys with multiple functions. If you will rely on those features, you should know how to enable, disable, and adjust them. For portable or mobile equipment you expect to deploy in the field, including generators, antenna supports, and the like, a few practice sessions will aid you in being familiar enough with the equipment to deploy it efficiently.

d. Know how to use whatever computers and software you expect to use, including any connections to radios and other equipment. When you're in the field trying to provide communications in a disaster (or even an exercise), that shouldn't be the first time you have ever used the software you need to send a message, do logging, record information in a served agency's application or database, or perform some other task. In this year's SET exercise, we were asked to send a Winlink message to the state RACES station via an RF path. For operators used to using Telnet message transport over the Internet, the instruction to use an RF path, and for those who elected to try it, an HF path, was something different, and for many, required practice and troubleshooting.

Those are a couple of lessons learned from the 2013 Statewide SET. We'll cover some other lessons in another net.