PlugFest Scenario

West 2015

SITUATION: An expeditionary Division-sized Task Force is operating on a large island in the western Pacific. The Task Force has many elements with their equipment that are continuing to arrive by air and by ship and, once arrived, must maneuver quickly to establish footholds against a determined enemy over high-hilly terrain. Satellite communications are the primary means of digital communications due to the hilly terrain and distances between units. Because of the Task Force' dependency on satellite communications and the technical capabilities of the enemy, there is concern that the usage of commercial and military satellites could be denied through cyber or electronic warfare methods or that the data transiting them could be compromised. Hardening of satellites and transiting data needs to be done and alternate digital communications methods need to be available.

BACKGROUND: US Army expeditionary forces, from Corps to Battalion, are equipped with Ku and Ka satellite communications systems to facilitate digital communications between headquarters. These systems provide great flexibility because they are not dependent upon line of sight existing between headquarters. Regional Hub Nodes are located globally in strategic locations and are well-connected to the DoDIN for backhaul to CONUS and other strategic services.

Task: Imagine you are in a Command and Control Cell as a part of the NSA or the U.S. Army. Electronic Warfare is an asset that can protect U.S. infrastructure. Considering the unclassified nature of PlugFest, your task is to provide means or methods that would be utilized to protect and defend or respond to Corps to Battalion satellite communications assets. What are the options and immediate action to ensure assured command and control? Provide a presentation that clearly communicates the problem and your proposed solution!

Questions for consideration:

1. What is the architecture?
2. What is the threat (broad band, sun spots, jamming, etc.?)
3. What circuits are lost?
4. What circuits can be exploited?
5. What my alternate means of communication?
6. What are mitigation strategies?
7. What resources do I need?
8. What is your next course of action?

<u>Actions by PlugFest Team</u>

- Come out of comfort zone to create the exercise- What is the data needed?
- Need a notional map? (Needs to be Unclassified)
- What's being attacked and what is the response?
- Develop a platform to support the teams
- Seek sponsors to support the event
- Data, things that turn data into answers, what are the interfaces process or actions
- What are security requirements (Could do compliance testing)
- Determine the three PlugFest teams
    - Government - Chief Winter Coord
    - Industry - Bob Damon Coord
    - Academic - Bob Damon Coord

NIST Cyber Security Framework for Consideration

Identify: What assets need protection? Satellites, mobile satellite terminals, regional ground stations (RHN), spectrum, baseband, common information services, mission critical systems...

Protect: What safeguards are available? Cyber (IA) Security Stack (TLA), firewalls, IPS, failover equipment, COOP, adjust power, change frequencies, change polarization, leverage terrestrial networks, harden communication equipment, enforce DAPE, limit P/P/S, access technique (TDMA, FDMA, NCW) as well as Modulation (QPSK, 8PSK, etc) and FEC(1/2, 2/3, 3/4 etc.). Note: The way that you accesses and the profile of the carrier can be modified at times to overcome issues.

Detect: What techniques can identify incidents? IPS/IDS alerts, loss of transport, latency, availability, confidentiality, configuration changes, spectrum analyzer monitoring, active space segment monitoring.

Respond: What techniques contain impact of incidents? Configuration adjustments, modify P/P/S, modify router ACLs, increase power, switch satellites, implement COOP, "hot swap" satellite terminals, launch Cyber Protection Teams, collect forensic data, modify bootfiles, geolocation to identify and locate/destroy the enemy EW assets.

Recover: What techniques can restore capabilities? Configuration adjustments, modify P/P/S, modify router ACLs, increase power, switch satellites, implement COOP, restoral priorities.