Moonlight Defender – Purple Teaming in Space

Ben Hawkins,
Cyber Engineering Specialist
Engineering and Technology Group

February 2024

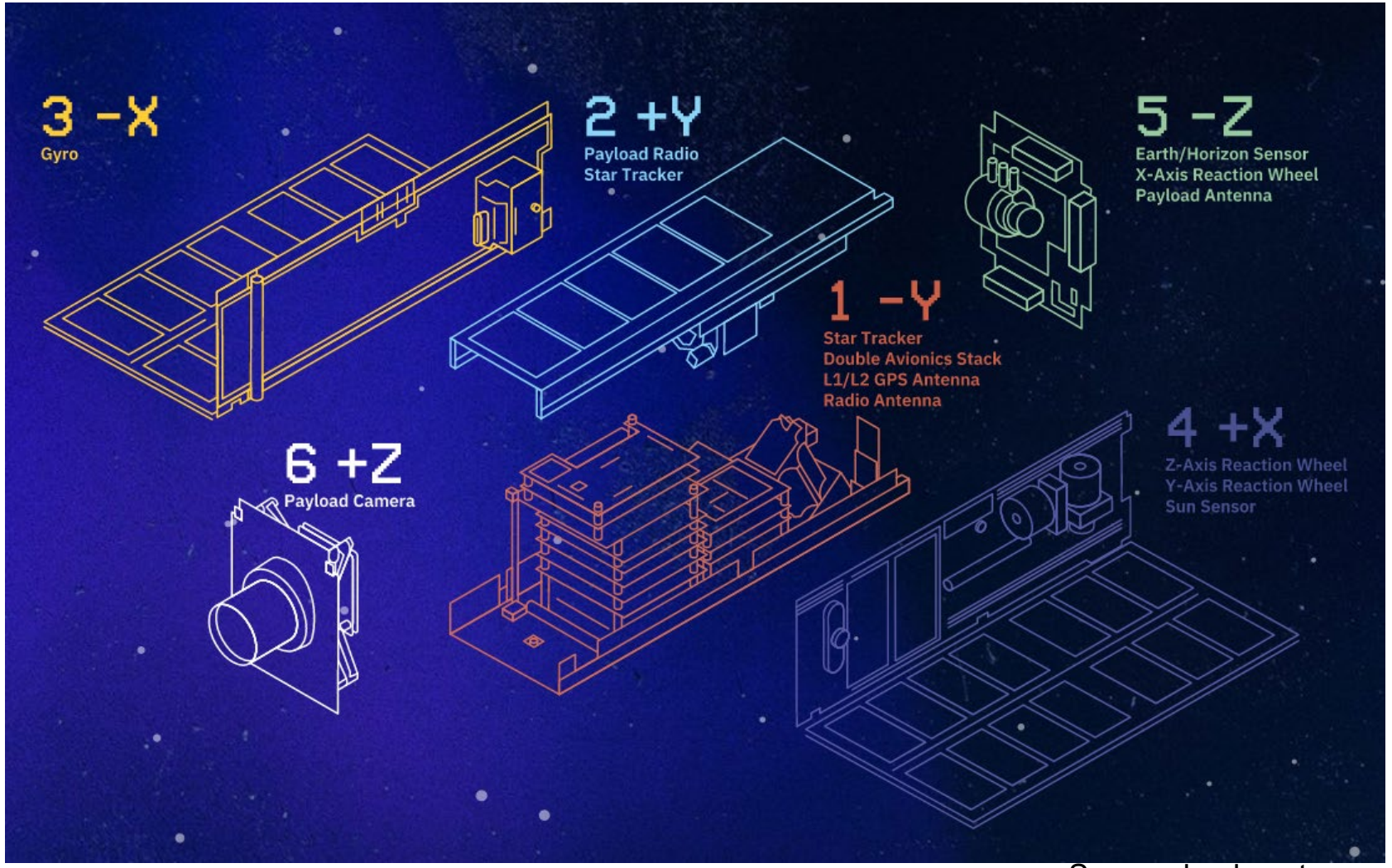
Scenario Briefing

Overview of Intelligence and Exercise Scenario

- Multiple intelligence sources have indicated credible threats to the mission related to ground system and satellite payload exploitation.
- There are no specific APTs identified in the intelligence reports, however it is suspected the group is focused on cloud systems exploitation and supply chain compromise.
- The Blue Team is tasked with protecting all systems associated with Moonlighter and ensuring the availability of it’s imaging capabilities.

Moonlighter Overview

Decomposition of Satellite

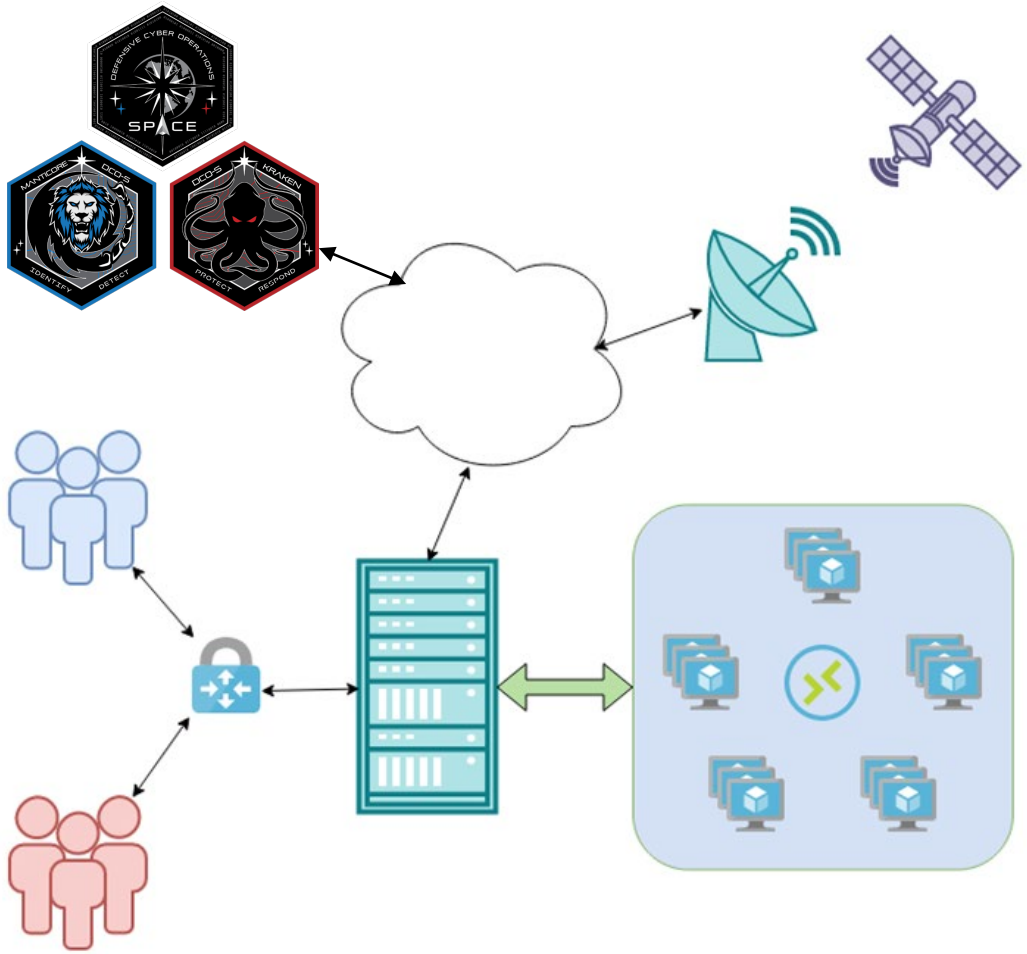


Source: hackasat.com

This satellite is ON ORBIT, the exercise will use the actual vehicle as the mission system.

Dark Sky Cyber Range

Lightweight, highly customizable virtual environment



Pre-Exercise Training

TTP development, Tool Familiarization, Space Fundamentals

- **Blue Team training event conducted at MITRE, Colorado Springs**
  - Over 20 Participants from USSF attended remote or physical.
  - Operators participated in a space-centric “Capture the Flag” game where they were able to apply the skills and knowledge gained during the training.
- **Red Team training conducted at Aerospace, Colorado Springs**
  - Initial training discussed cyber and space fundamentals along with defensive and offensive TTPs.
  - Cromulence and Aerospace SMEs delivered advanced space-cyber exploitation including reverse engineering, exploit development, traffic compromise, and cloud systems exploitation.

Both teams gained crucial hands-on training to prepare them for space system attack and defense.

Key Takeaways

- Exercises utilizing live satellites must consider the sometimes-unreliable nature of contact windows and payload bugs.

- The Kraken system proved to be extremely capable in identifying malicious behavior and allowing DCO operators to rapidly respond on the compromised system.

- The utilization of virtual infrastructure allowed for on the fly scaling and configuration changes which made dynamic operations possible such as intelligence injects, scenario and objective modifications, and deploying fixes to compromised systems.

Questions?

Ben.Hawkins@Aero.org