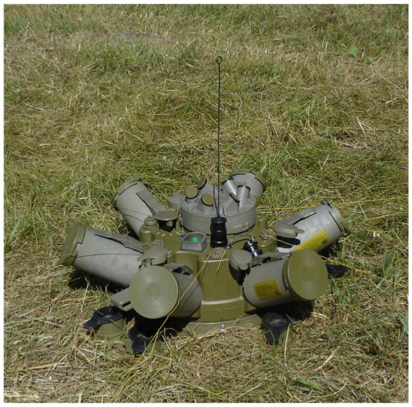
Spider Increment 1A M7E1 Network Command Munition

Executive Summary

- The Army conducted the Spider Increment 1A (I1A) IOT&E in October 2018, at Fort Campbell, Kentucky.
- DOT&E published an IOT&E report in August 2019, with the following assessment:
  - Spider I1A is not operationally effective. The system contributed to the test unit's response to enemy activity 60 percent of the time, which is less than the original Spider Increment 1 munition contributed during its final operational test in 2012.
  - Spider I1A is not operationally suitable. The system's Remote Control Station (RCS) completed 59 percent of the test missions without an Essential Function Failure (EFF). This is below the Army requirement of 91 percent. Soldiers found the system difficult to use and leaders did not trust the system because of its reliability problems and complexity.
  - Spider I1A possesses both electronic warfare and cybersecurity vulnerabilities.
  - The Army should demonstrate fixes in developmental testing and verify operational effectiveness, suitability, and survivability in FOT&E.
- The Army is developing a plan to improve software reliability and solider usability prior to a full materiel release in 4QFY21. The plan includes early soldier involvement and operational testing.

System

- The Army uses Spider as a landmine alternative to satisfy the requirements outlined in the 2004 National Landmine Policy that directed the DOD to:
  - End use of persistent landmines after 2010
  - Incorporate self-destructing and self-deactivating technologies in alternatives to current persistent landmines
- A Spider munition field includes:
  - Up to 63 Munition Control Units (MCUs), each housing up to 6 miniature grenade launchers or munition adapter modules (the modules provide remote electrical firing capabilities).
  - An RCS consists of a Remote Control Unit (RCU) and RCU Transceiver. An operator uses the RCS to maintain "man-in-the-loop" control of all munitions in a field. The RCU is the component upgraded in Spider I1A.



  - A repeater or communications relay device for use in difficult terrain or at extended ranges.
- Spider incorporates self-destructing and self-deactivating technologies to reduce residual risks to non-combatants and has the capability to use non-lethal munitions, such as the Modular Crowd Control Munition that fires rubber sting balls.
- The Army fielded Spider Increment 1 systems in FY09 under an urgent materiel release. The system reached Initial Operational Capability in FY11 and obtained its full materiel release in FY13.

Mission

Brigade Combat Team commanders employ engineer units equipped with Spider to provide force protection and counter mobility obstacles using lethal and non-lethal munitions. Spider functions either as a stand-alone system or in combination with other obstacles to accomplish the following:

- Provide early warning
- Protect the force
- Delay and attrite enemy forces
- Shape the battlefield

Major Contractor

Command and Control hardware and software:
Northrop Grumman Information Systems Sector,
Defense Systems Division – Redondo Beach, California

Activity

- The Army conducted the IOT&E from October 9 – 31, 2018, at Fort Campbell, Kentucky, in accordance with the DOT&E-approved Test and Evaluation Master Plan and test plan.
- The IOT&E record test consisted of four anti-personnel perimeter missions, four anti-personnel ambushes, and eight counter-mobility missions. The test unit was an engineer platoon attached to an infantry company.

- DOT&E published the Spider I1A IOT&E report in August 2019.
- The Army delayed the full materiel release based on IOT&E results. The Army will conditionally release Spider I1A to a limited number of units.
- The Program Office is developing a plan to support full materiel release that consists of early solider involvement in developmental testing, to include usability studies. The Army intends to conduct an FOT&E prior to a full materiel release in 4QFY21.

Assessment

- Spider I1A is not operationally effective. Spider I1A contributed to the unit's response to 60 percent of threat intrusions during the IOT&E. Spider I1A contributed less during its 2018 IOT&E than Spider Increment 1 did during its 2012 Follow-on Operational Test 2 (FOT2).
- Spider 1IA is not operationally suitable. The Army requires the RCS to operate 91 percent of the missions without an EFF. The RCS completed 59 percent of the IOT&E missions without an EFF. Soldiers found the system difficult to use and leaders did not trust the system because of its poor reliability and complexity. In addition, the test unit reported the equipment required to transport the system and recharge its batteries made it not suitable for a light infantry company.
- The Spider I1A software is not mature. Both developmental testing and the IOT&E uncovered new software deficiencies, including an inaccurate safety warning concerning system status. The RCU is required to operate for 30 days, but after 15 days of continuous use during developmental testing, the RCU's response time slowed to the point where the system was not effective in responding to intruders.
- The IOT&E and previous operational tests exposed vulnerabilities of the system in an electronic warfare environment. Operational testing exposed cybersecurity vulnerabilities if a threat has physical access to the RCU.

Recommendations

The Army should consider the following recommendations:

1. Update the system software prior to fielding Spider I1A. The software should be updated to mitigate reliability, cybersecurity, and safety failures found in developmental and operational testing, rather than relying on soldier training.
2. Increase the usability of the system by decreasing software complexity.
3. Adopt a test-fix-test approach. Fixes should be demonstrated through realistic testing with soldiers before software is locked.
4. Conduct an FOT&E after fixes are verified in developmental testing.
5. Reconsider fielding tested configuration of Spider I1A to light infantry units.