52nd IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cyber-security threats to space missions and countermeasures to address them (4)

Author: Dr. Jeremy Straub
North Dakota State University, United States

# SOFTWARE ANTI-SATELLITE CAPABILITIES: DEVELOPING SOFTWARE TOOLS TO COUNTER NEFARIOUS AND ROGUE STATE SPACECRAFT

**Abstract**

A variety of offensive uses of spacecraft have been proposed, in Earth orbit and beyond. Some have suggested space as the 'ultimate high ground' just for sensing. Others have gone further, proposing the use of satellites for munition deployment. The impact of an electromagnetic pulse (EMP) in low-Earth orbit has also been recently considered.

To counter uses like these, anti-satellite technologies have been a subject of considerable interest. Demonstrations of ballistic anti-satellite munitions showed how problematic this type of an approach can be, cluttering a significant area of orbital space.

This paper proposes an alternate solution to this challenge: a software-driven approach to attacking the command and control mechanisms used by spacecraft. The paper describes and evaluates the proposed system.

The proposed system has four phases. First, a goal (e.g., disablement or relocation of a spacecraft) is identified by controllers. Then, this goal is provided to a software system which, using a basic model of spacecraft control (ideally already as close to the target spacecraft's as possible) identifies relevant subsystems to target.

Next, the system collects data related to these targeted subsystems and their command and control decision making processes. If the spacecraft uses a common or well-documented command system, then this can serve as a starting point. Alternately, if a unit (e.g., a captured unit) is available this can also be used for testing. If not, then tests must be carefully run on the targeted unit, applying small changes to sensor inputs and such to see how the craft responds. In this type of testing, there is a clear tradeoff between better understanding the targeted craft and alerting it to the fact that it is being targeted. Ideally, potential future targets could be analyzed long before the information is needed to attack them.

Finally, with a basic decision-making model for the targeted craft identified, the system must identify the best approach to use to manipulate this model to achieve the desired goal and implement it.

The design and operations of the system are described and evaluated. The system uses an expert system (which supports code embedding) to store the model of the target system. It uses an expert system-like Blackboard Architecture for decision making and command capabilities to plan, execute and evaluate the effectiveness of the attack. The paper concludes with a discussion of the potential uses of this type of a system and its efficacy for these uses.