Paper ID: 49642
oral

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: Prof. Alex Ellery
Carleton University, Space Exploration and Engineering Group, Canada, aellery@mae.carleton.ca

HYBRID ARTIFICIAL INTELLIGENCE AS A DEFENCE AGAINST CYBER-INTERFERENCE OF MILITARY SATELLITES

Abstract

The military satellite fleet is the backbone of the modern battlefield – it provides communications, navigation, weather forecasts, strategic intelligence, telemedicine and, potentially in the future, logistic supply in the field (through 3D printing). It is also the backbone of the drone's capability to project power remotely without endangering friendly forces. The drone of course has become the cause celebre of recent revolutionary military affairs. Traditional threats to satellites imposed technological barriers to entry to space warfare – anti-satellite missiles, hunter-killer interceptors, stealth cubesats, etc. The cyber-attack imposes no such barriers representing an asymmetric threat from any non-state aggressor against a crucial military technological infrastructure. Cyber-attacks may impose simple denial-of-service, convert the satellite into a source of elint, cause expensive mission failure (e.g. Stuxnet on reaction wheels) or physical destruction (e.g. ignition of propellant), subvert satellite channels to broadcast propaganda (e.g. Tamil Tigers hacking Intelsat in 2007) or infect all recipients with malware, re-direct drones to friendly targets (e.g. South Korean reconnaissance drone crash into ground control station by North Korean jamming of its GPS signal), etc, many of which may be disguised as accidents. Stuxnet has demonstrated that computer viruses are a form of munitions. A multi-layered immunisation strategy is required. We propose isolating the spacecraft from the TTC uplink by imposing a high degree of Bayesian network-based artificial intelligence implemented on FPGA-based hardware neural network circuitry. The key to this capability is the mapping of Bayesian networks onto neural networks. There are several ways to achieve this but deep learning neural networks offer a potential solution. In neural network form, the AI is immune to logic bombs as there is no software code logic as it is distributed through the neural network. Neural network implementation on FPGA platforms ensures that no software can be uploaded without full prior access to the AI code. Although this is a radical solution, it may be the only means to harden military satellites against cyber-threats.