Satellites as a Susceptible Databank to Hackers and Artificial Intelligence

Key Judgements

With the ever-growing world of technology, the cybersphere has been developing exponentially. Cybersecurity can barely keep up with the constant development of cyberattacks created to hack into government, business, and personal information. What remains an even greater threat is the security of the satellites that receive and send and store all the digital data this world has to offer. Broken into commercial, civil, governmental, and military categories, there are a lot of satellites that remain at risk. Hackers are now employing the use of Artificial Intelligence and Machine Learning to learn ways to breach through satellite security and get access to information and intelligence.

- Artificial Intelligence is already being used to interpret geospatial images to determine threats.
- Artificial Intelligence is used to navigate orbital routes.
- Satellites are a databank that could be seen as a soft target to hackers who are more knowledgeable than the inexperienced cybersecurity worker.
- Adversarial Machine Learning programs are being developed to deceive/manipulate AI systems that help maintain satellites.

Introduction

The ongoing creation and evolution of Adversarial Machine Learning (AML) algorithms presents an exponentially growing threat to homeland security in the United States of America. Modern warfare is more asymmetrical than ever, and predictive models of future warfare can't underestimate the danger artificial intelligence and machine learning will play. Intelligence community relies heavily on satellites for reconnaissance information and intelligence collection to create strategic military decisions; neglecting these systems' defense mechanisms leaves them prey to cyberattacks that could prove detrimental to the USA's process of intelligence collection.

Background

Artificial Intelligence (AI) is already at use in the foundation of society to better aid and equip the way day-to-day life functions. Private medical companies and insurances use AI to prevent data leaks. The stock market uses it for trend prediction. The algorithms are at use through social media businesses to learn individual human beliefs and worldviews. AI is being used as a data miner to compile and compress information at an alarmingly fast rate. The Department of Defense spends billions of dollars to use satellites operated with AI for intelligence collection and image compilation. There are already dozens of AI programs that

have passed the Turing test.[1] And machine learning learns exponentially, not linearly. Scientists predict that AI will reach singularity by the year 2045. The first covalent bond is being forged between humans and AI in the year 2020; the company NeuraLink, backed by Elon Musk, is moving on to human trials to implant AI into the brain to observe the brain's processes.

Adversarial Machine Learning (ML) programs are being developed to tamper with United States' defense systems. There are a multitude of approaches any attacker can take: evasion attack, equation solving attack, path finding attack, model inversion attack, member inference attack, member inference attack, black box attack (just to name a few). These attacks are meant to reduce ML confidence and cause them to mis-classify information. Satellites, like all other technology, are vulnerable to cyberattacks. And because machine learning is an exponential process, the vulnerabilities are only getting more vulnerable as time progresses. It has been mentioned that AI can be used to breach health/medical companies, the stock market, oil and gas companies, and even the government, but the greater risk is the thing that helps these companies run: satellites. The seemingly limitless cloud of endless data we can access on our phones, and all information of the internet, all goes through satellites, one of the anticipated next targets of hackers.

Analysis

There are a lot more satellites orbiting Earth than you probably know. In total, there are 2,218 satellites currently in orbit. 1,007 of those belong to the United States. 323 belonging to China. 164 belonging to Russia. 700+ belonging to a categorical nominal titled: Other. A breakdown of the United States' 1,007 satellites follows: 35 civil, 620 commercial, 163 government, and 189 military. Although commercial vastly outnumbers the amount of government and military satellites, there have been talks that the United States government will contract with commercial companies for use of satellites.

There is evidence that Artificial Intelligence is a tool being used by hackers. It's factual that AI programs are in charge (in part) for the orbital navigation of satellites. SpaceX, a privately owned satellite company, has AI in place to ensure satellites don't collide with other satellites in orbit or with spacial debris. Other private companies of the same caliber are currently hiring cybersecurity positions, which may inference that they are struggling to keep their defenses up to par with the amount of cyberattacks they are receiving.

There are a vast possibility of goals hackers could have in breaching satellites. Aside from the obvious fact that they could cause tremendous damage by manipulating the orbital route of satellites, there are other advantages to hacking into satellite databases. Like a hacker who cracks into someone's laptop computer, they can then observe everything going on in a certain location, a form of intelligence collection. Like a much bigger laptop, a satellite serves a plethora of attractive qualities for adversarial intelligence agents. If a cyberattack successfully breached a government/military satellite, it would not only be hard to detect, but it would be one of the

[1] The Turing test, developed by Alan Turing in the 1950s, is a test for artificial intelligence programs where an interrogator interacts and questions a machine. If the human interrogator is unable to differentiate the machine's responses from those of a human, the machine has passed the Turing test.

largest data leaks ever. Important locations, communications, names, files, and much more information is sent over email servers every day. Hack into a government satellite and that secured information is no longer hidden from the open, and even worse, it's in the hands of the enemy.

Outlook

The technological field is growing exponentially, and the cybersecurity that surrounds it is struggling to keep up. With the free market dominating the United States, the private/business sector has had a quick race to get satellites in orbit. It's more than just cell phone and wireless companies launching satellites. But the IT positions in charge of running cybersecurity on these satellites is struggling to maintain the knowledge to withstand constant cyberattacks coming from domestic/foreign enemies.

War is becoming more asymmetrical as technology continues to develop, and the military must change with it. Being engaged in war now consists of remotely piloted drones and targeted killing, something that wasn't a concept twenty years ago. Like that evolution in combat, warfare is getting increasingly outsourced to the cybersphere. Hackers are interested in stealing information from businesses, government databases, universities, anything they can get their hands on. China has been discovered in these attacks multiple times. The security overseeing these satellites must evolve, or put their main security in the hands of Artificial Intelligence to run defenses. Algorithms that detect adversarial intelligence efforts (hackers) could be developed to also learn from the attacks being witnessed.

Intelligence needs to be predictive in anticipating the current trends in technological advancement. AI is much more efficient in analyzing geospatial images from satellites (in comparison to a human searching the images). But this level of helpfulness could easily be flipped to harmfulness if in the wrong hands. Therefore, it's better to have the defenses ready and not need them, than to need them and not have them.

Sources

Michael O'Hanlon, "The role of AI in future warfare," *Brookings EDU*.
Vasisht Duddu, "A survey of adversarial machine learning in cyber warfare," *Indraprashtha Institute of Information Technology*.
Robert Lemos, "Cybersecurity Experts Worry About Satellite & Space Systems," *Darkreadings*.
Mark Holmes, "AI Elevates Cyber Threat to New Level," *ViaSatellite*.
Mike Wheatley, "US restricts export of AI software used to analyze satellite images," *Silicon Angle*.
Union of Concerned Scientists, "UCS Satellite Database."