

WHY CYBERSECURITY IS TOO IMPORTANT TO GET LOST IN SPACE

S**pace may indeed be the “final frontier” for exploration, as private companies strive to go where no human has gone before. But space is also ripe for exploitation.**

**Cybercriminals see lucrative potential in crippling satellite communications and even disrupting space flights, officials warn. Where they succeed, the consequences could be devastating – on an astronomical scale.**

**“Space is particularly susceptible to a range of cyber vulnerabilities and threats,” Gina Galasso, of The Aerospace Corporation UK, a member of the international Space Information Sharing and Analysis Centre, said recently.**

**With the emergence of new space, private space flights, which are just starting to take off, are certainly a concern: a cyber attack on one of these missions could endanger lives. But cyber threats to the thousands of satellites orbiting the Earth could have wide-ranging impacts.**

**Global Positioning Systems (GPS), for one, rely on satellites. A breach could disrupt shipping, distribution, military operations, air traffic, Wi-Fi and cellular service, weather forecasting, industrial internet-of-things, and more.**

**Satellites also take aerial images for intelligence-community surveillance – information that rogue nation-states may covet.**

**These threats aren’t hypothetical: they’re happening now. Malicious actors attacked the U.S. National Aeronautics and Space Administration, or NASA, nearly five times a day, on average, in 2020, the agency reports.**

**Over the past four years, NASA’s systems and networks weathered more than 6,000 cyber attacks. “Spacecraft without encryption or authentication are particularly susceptible,” NASA wrote in 2019.**

# WHAT COULD GO WRONG? A LOT, ACTUALLY.

**Some 2,666 operating satellites were orbiting the Earth in April 2020, according to the World Economic Forum. Of these, 1,007 were communications satellites and 97 were for GPS/navigation. Other satellites are used for surveillance, gathering and transmitting highly sensitive information. And tens of thousands of satellites will almost certainly join them in the next few years.**

**Securing all these systems is an increasingly complex and formidable task. These satellites were designed, largely, without security in mind. Governments struggle against the limits of legacy hardware, software, and systems, and frequently contract with private businesses for services. A plethora of private companies are rapidly entering the race into space on their own, as well.**

**Cyber attacks can occur at a number of points: on-the-ground systems, space station systems, or anywhere in between. These stations communicate using radio frequency (RF) signals.**

**A recent article in the International Journal of Information Security (IJIS) lists a number of forms that cyber-space attacks can take, including:**

* **Computer network exploitation (CNE). This is a breach of the network to which the ground station is connected.**
* **Cloud infrastructure attacks. Most of the ground station’s data storage and processing happen in the cloud.**
* **Data corruption or modification of unencrypted data at rest or in transit. Malicious changes in space-based data could cause software failure or errors, hardware failures, use of unauthorized software, or attempts to change data so even authorized users can’t access it. For instance, a corrupted spacecraft command could result in a command’s being aborted or the wrong action occurring, with potentially catastrophic results.**
* **Supply chain attacks. In the space domain as elsewhere, a supply-chain breach could inject vulnerabilities and exploits into the supply chain.**
* **Exploits of vulnerabilities in legacy software or equipment that hasn’t been updated or patched.**

**And then there are all the ways RF signals could be disrupted:**

* **Jamming, or blocking signal transmission, which could damage or even destroy critical infrastructure including electric grids and water networks.**
* **Eavesdropping, in which malicious actors “listen in” on or intercept data while it’s in transit. According to the IJIS article, data transmitted using RF may be unencrypted or use low-grade encryption.**
* **Hijacking, or overriding satellite communications to send out your own signal, as happened in Chicago in 1987 when a person in a “Max Headroom” mask interrupted the TV series “Doctor Who.”**
* **Spoofing, in which hackers send a signal that appears legitimate, as happened in 2017 when two NATO warships were reportedly tracked in the Black Sea near Russia when they in fact had not left their port 180 miles away.**

# GOVERNMENTS ARE PAYING ATTENTION. SO SHOULD THE NEW SPACE.

**As the threats increase to critical infrastructure and human safety, governments around the world are turning their attention to space-based cyber risks. In the US, some lawmakers are calling for space to be added as the 17th “critical infrastructure” sector along with energy, water, transportation, and others.**

**But companies in the space business will need to intensify their focus on security, as well. Governments often contract with private enterprise for manufacture of space hardware and software, all of which need strong data protection. Small satellite constellations in ‘newspace’ already face much risk, and that risk stands to increase as more entities join the race to space.**

# A SPACE-BASED SOLUTION FOR A SPACE-BASED PROBLEM

**CYSEC ARCA is the pragmatic solution to the challenge of cyber security in space, securing the entire satellite communications ecosystem: on the ground, in space, and in between. Using ARCA Trusted OS, commercial space companies can innovate securely with the data that they collect and transmit knowing their information is covered end-to-end.**

**Satellites are built to be robust and durable, but they’re not designed with security in mind – except for military satellites, which have been well secured for decades.**

**Knowing this, CYSEC is adapting its ARCA trusted OS to be ready to protect data in space. Its confidential computing technology provides high-grade protection of data at rest, in transit, and even in use.**

**ARCA Trusted OS will be used on a satellite computer for the first time in early 2022, in SpaceX’s Falcon 9 rocket. ARCA will protect all telemetry and tele commands as well as payload data, such as Earth observation data, from the moment these are generated on board until they reach mission control on the ground.**

**Recently, the company contracted with the European Space Agency (ESA) to develop end-to-end protection of governmental data exchanged over satellites, under ESA’s Strategic Programme Line Space Systems for Safety and Security (ARTES 4S).**

**Under this contract, CYSEC will improve the cryptographic key exchange protocol of ARCA trusted OS to be compatible with commercial satcom links. These links will be implemented on ARCA’s trusted execution environments to ensure end-to-end security.**

**The solution developed by CYSEC will allow govsatcom users to procure comsatcom services while benefiting from the highest level of security, without any negative effect on performance. CYSEC will fully lead this project with the technical support of the Cyber Defense Campus of armasuisse.**

# THE MOST POWERFUL SECURITY SYSTEM IN CYBER-SPACE

**As the race to space takes flight, ARCA is ready for launch.**

**The first-ever security system built especially for Low Earth Orbit (LEO) missions, ARCA provides a hardened operating system with a built-in cryptographic service and key management system. ARCA guarantees that the flight software executed on board has not been tampered with, and that all cryptographic secrets can be trusted. ARCA is a must-have for space missions collecting and processing sensitive data on board.**

**Sending a spacecraft up, up, and away can cause anxiety as it is: so much could go wrong. With ARCA on board, however, there’s no need to worry about security. You’ll know your secrets and your data, are safe with us.**