AEROSPACE
AMERICA

2022 YEAR IN REVIEW

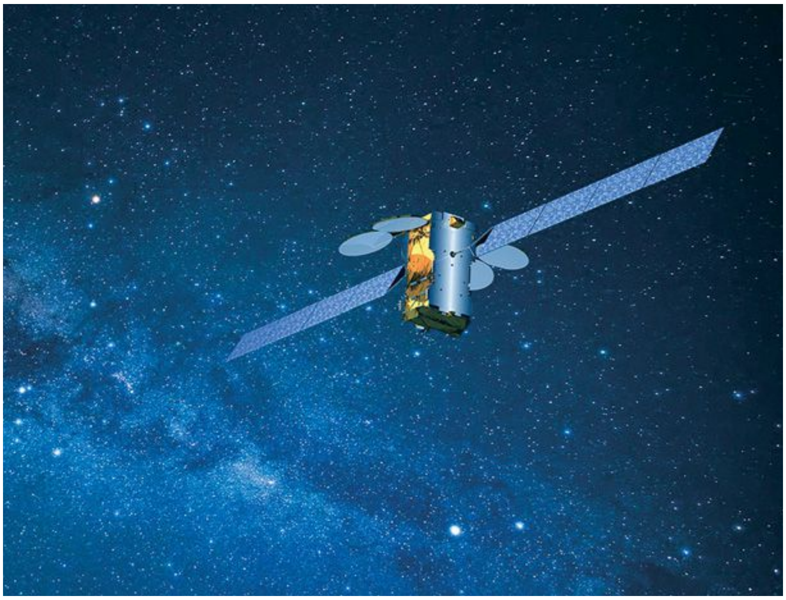
The Pillars of Creation from the Webb telescope

NASA'S DART MOVES AN ASTEROID

NASA'S SLS ROCKET NAILS ITS DEBUT

DECEMBER 2022 | A publication of the American Institute of Aeronautics and Astronautics | aerospaceamerica.aiaa.org

AIAA
SHAPING THE FUTURE OF AEROSPACE



Space and aviation sectors take steps to guard against increased cyberattacks

BY ARUN VISWANATHAN

The **Aerospace Cybersecurity Working Group** provides awareness, education and standards development to help protect aerospace's digital infrastructure.

▲ Accounts differ on the exact sequence of events in the February Viasat hack, but all agree that the company's KA-SAT was an unwitting conduit for an attack on thousands of modems.
Viasat

Cyberattacks targeting the space and aviation sectors have been on the rise for several years, but this year started with a vivid illustration of their real-world consequences. On Feb. 24, hours before Russian forces invaded Ukraine, a cyberattack interrupted **Viasat's satellite broadband service**. Several thousand modems in Ukraine and tens of thousands across Europe were disconnected from the **KA-SAT network** after an attacker sent commands to these modems via the satellite's spot beams. Viasat's overview document published in March says "high volumes of focused, malicious traffic" prevented the modems from staying online, but researchers at **Johns Hopkins University** in Maryland theorize that the attacker uploaded wiper malware to the modems. The network remained offline for several days. The attack also caused collateral damage, including the outage of wind turbines operated by **Tobi Windenergie Verwaltungs** in Germany.

In August, a group of researchers hacked a satellite dish on **SpaceX's Starlink network** with a homemade circuit board costing only $25 to demonstrate the network's vulnerabilities. SpaceX days later introduced a bug bounty program, encouraging hackers to find bugs for a hefty reward.

In February, researchers with California-based cybersecurity company **Proofpoint** tracked a persistent cybercrime threat actor, called **TA2541**, targeting organizations in aviation and aerospace among other sectors. The threat group used various means to deliver malware to targeted organizations, which is then used to gain remote control of infected machines and steal data. In June, cybersecurity company **Pen Test Partner**s, based in the U.K., presented the results of its attempts to hack a decommissioned airliner. The company focused on vulnerabilities introduced by **electronic flight bags**, which are tablets or other mobile devices pilots usually take home. Pen Test found that EFBs are insecure, and the lack of hardening of these devices may pose a significant security risk to flight operations. Throughout the year, airports reported an increase in cybersecurity attacks, including the **distributed denial of service attack** in May that temporarily disabled the website of **Bradley International Airport** in Connecticut.

The Viasat hack, among others, may just be the beginning as such attacks become more frequent, warned **U.S. Rep. Don Beyer** in July during opening remarks of a **House Science Committee hearing**.

This rise in cyber activity spurred the U.S. government and industry to acknowledge the cyber risks in their next-generation, highly autonomous systems. In August, the **Association for Uncrewed Vehicle Systems International and Fortress Information Security** announced they will develop an enterprise cybersecurity model and standards to "address cyber risks specific to uncrewed systems and robotics." The **National Institute of Standards and Technology and the Cybersecurity and Infrastructure Security Agency** began writing guidance on authentication among agencies, contractors and citizens.

Amid the urgency created by Russia's invasion of Ukraine, **U.S. President Joe Biden** in March signed into law the **Cyber Incident Reporting for Critical Infrastructure Act of 2022**, tasking CISA with developing and implementing regulations requiring covered entities to report covered cyber incidents and ransomware payments. In May, NIST released **SP-800-161 Rev1**, a significant upgrade to the **800-161 document**, containing guidance for securing enterprises against supply chain hacks such as the **2020 SolarWinds hack**. Also in May, the **U.S. Space Force** rolled out the **Infrastructure Asset Pre-Approval program** to assess the cybersecurity of commercial satellite operators that do business with the Defense Department.

Real-world cyberattacks and research this year have demonstrated the relative ease with which motivated attackers can compromise ground systems and networks used to operate critical infrastructure. While the threats are increasing, it is promising to see government and industry acknowledge the risk and increase efforts to secure and defend our critical assets. ★