AEROSPACE

ORBITER NEWS

News, announcements, and more.

Aerospace's 2022 Annual Report: Fostering an Integrated Vision for Modern Space

At a pivotal moment for the space domain, shaped by significant challenges and immense opportunities, we at The Aerospace Corporation are accelerating our innovation and expanding our impact across a growing set of partners to drive integration throughout the space enterprise.

Working alongside our government partners, Aerospace is shaping the next generation of resilient space systems, with a focus on speed and agility to outpace the threats facing our nation and ensure integrated capabilities are reliably delivered across warfighting domains.

Aerospace also played key roles supporting flagship civil space missions, while enabling future ecosystems that will support a new era of space exploration and commercialization.

We invite you to explore the 2022 Annual Report to learn more about how Aerospace is responding to meet the evolving needs of our partners and further U.S. leadership in space. It speaks to our unwavering commitment to deliver on our vision: The nation's trusted partner, solving the hardest problems for the preeminent space enterprise.

*Explore the **2022 Annual Report here**.*

Video: Aerospace's New Waterjet is Literally Cutting-Edge Technology

January 24, 2023

In this video (**Watch on YouTube**), Aerospace's Alfredo Aguilar shows off the new Flow Mach500 Waterjet. The technology can cut a variety of materials by pumping a mixture of water and abrasives at high pressure to create a piercing effect for precision cutting and shaping. These kinds of capabilities enable Aerospace's experts to push innovation forward, advancing concepts and prototypes, such as with DiskSat technology.

One Aerospace: Providing Meaningful Change on MLK Day

January 16, 2023

In the spirit and remembrance of Martin Luther King Jr.'s lifelong service and dedication in creating a more equitable society, MLK Day is the only federal holiday also designated as a National Day of Service. Occurring annually on the third Monday of January, individuals across the nation are encouraged to take action and give back to their communities.

"I hope the numerous acts of service employees demonstrated last year — which was also the inaugural year of Aerospace designating MLK as a corporate holiday — will be repeated on Jan. 16 and continue throughout 2023," said Ed Swallow, Aerospace's Chief Operating Officer. "I encourage all at Aerospace to consider engaging in a meaningful opportunity to act in service to their community."

This year, Aerospace is offering opportunities for employees to address ending hunger in their local communities.

This year will be the corporation's first National MLK Day of Service and employees are encouraged to focus on efforts towards ending hunger. This issue affects more than 34 million people in the United States, including nine million children. Aerospace has partnered with multiple organizations to provide opportunities to become engaged and help address this nationwide problem.

For opportunities to give back beyond MLK Day, please consider:

- VEX Robotics Competition (Virginia)
  - Become a part of the largest and fastest growing middle school and high school robotics program by signing up as a member of the planning team, judge or event volunteer.
- Science Olympiad US! (California)
  - Support first-time competitors by providing mentorship, serving as a guest speaker or judging on competition day.

- Aerospace Cares
  - Employees can search for current and upcoming opportunities or create their own volunteer initiative on the company giving and volunteering platform; Aerospace Cares. (To find other opportunities that suit your preference, please use Volunteer Match and track your time on Aerospace Cares.)
- Aerospace's Mentoring Initiative
  - January is National Mentoring Month and through Aerospace's Mentoring Initiative, employees can contribute to personal growth and professional development within the corporation. Other STEM mentorship opportunities are also available on Aerospace Cares.
- Become an Aerospace Volunteer
  - Sign up to receive email updates from Aerospace about new and upcoming volunteer opportunities.

Introducing SPARTA: Cyber Security for Space Missions

January 11, 2023

In 2013, MITRE created the ATT&CK framework to document common tactics, techniques, and procedures (TTPs) used by adversaries against enterprise networks. While the framework assists organizations in better understanding, visualizing, anticipating, and defending against cyber-attack, its taxonomy of offense and defense also provides cybersecurity disciplines, from threat intelligence to network defense, with a common language.

The SPARTA framework is a living document; through a combination of space-cyber community input, and aggregation of unclassified research from both academia and Federally Funded Research and Development Centers (FFRDCs), it will evolve and advance over time.

A similar and growing need exists for identifying, categorizing, and sharing space-cyber TTPs — with the same "adversary perspective" and context that ATT&CK offers. In response, The Aerospace Corporation has created the Space Attack Research and Tactic Analysis (SPARTA) framework to meet this need. SPARTA intends to provide information to space professionals about how spacecraft and space missions may be compromised via cyber means and builds a taxonomy of defined activities that can contribute to spacecraft compromises. But like ATT&CK, SPARTA defines mitigations too — meaning that SPARTA as a whole can help guide space professionals in activities that range from space-cyber threat modelling and assessments, to subsystem design and building space-cyber resilience.

The “new space” evolution — more players, new technology, and a dramatically reduced barrier for entry — has only underscored the critical gaps that SPARTA serves to address, as all these factors now collide with our modern and substantially adversarial information environment. These gaps range from lapses in harmonization between far-flung catalogues of potential threats and incomplete TTPs, to a lack of information dissemination and ways to communicate information in a machine-digestible manner (i.e., STIX-compliant). In the same way that Information Technology and Operational Technology stakeholders have done before, the growing number of space-cyber practitioners from all sectors can learn from the past, and use SPARTA as a means to normalize taxonomy, countermeasures, and best practices across the community.

The SPARTA framework offers space professionals a taxonomy of potential cyber threats to spacecraft and space missions, such as NASA’s Lunar Gateway.

As with ATT&CK, the SPARTA framework is a living document; through a combination of space-cyber community input, and aggregation of unclassified research from both academia and Federally Funded Research and Development Centers (FFRDCs), it will evolve and advance over time. But unlike ATT&CK, SPARTA takes a view to the “art of the possible” — and will include TTPs of potential attack utility, not just observed or likely behavior. This fundamental difference enables a shift from retroactive analysis into proactive analysis — one of Aerospace’s key goals with SPARTA. The space community will be better positioned to understand TTPs, identify associated countermeasures, and defend spacecraft and space missions. SPARTA can also be used as the basis for testing the efficacy of security solutions in development environments, ground systems, and spacecraft subsystems.

What is SPARTA?

Like the ATT&CK framework, SPARTA is organized around the pre-attack, attack, and post-attack stages: reconnaissance, resource development, initial access, execution, exfiltration, persistence, defense evasion, lateral movement, and impact. Each step lists several techniques and sub-techniques for providing more specific information about the various stages of an attack. It also includes information on the tools and infrastructure that might be used to support an attack.

- **Tactics:** These represent the “why” of a SPARTA technique or sub-technique — the threat actor’s tactical goal, and the reason they are performing a technique. For example, a threat actor may want to achieve initial access on a spacecraft via cyber means.
- **Techniques:** These represent “how” a threat actor achieves a tactical goal by performing a threat action. For example, a threat actor may exploit trusted relationships to achieve initial access.
- **Sub-techniques:** These represent a variation or more specific instance of the threat actor’s behavior used to achieve a goal. Sub-techniques typically describe behavior at a lower level than a technique and are considered children of the parent technique. For example, a threat actor may compromise mission collaborators (academia, international partners, suppliers, etc.) to achieve their initial access.
- **Procedures:** These represent specific implementations the threat actor uses for techniques or sub-

techniques. Procedures are the step-by-step descriptions of how the threat actor plans to go about achieving their purpose. It details how the general techniques/sub-techniques will be carried out.

- **Pre-Attack:** The Pre-Attack phase includes information about the reconnaissance and resource development activities that attackers typically conduct before launching an attack. This includes gathering relevant space system design information, social engineering, malware research/development, and compromising initial infrastructure.
- **Attack:** The Attack phase includes information about the different types of attacks that can be carried out, as well as the tools and techniques that are typically used. For example, these attacks may involve leveraging initial access, such as through a compromised ground station or hosted payload, to execute an attack, such as denial-of-service, arbitrary code execution, or data exfiltration.
- **Post-Attack:** Once an attacker has begun an attack, the Post-Attack phase includes information about the persistence, evasion, and movement techniques an attacker may employ. This may consist of compromising memory or installing a backdoor, disabling fault management systems, and/or moving to a new target in a constellation.

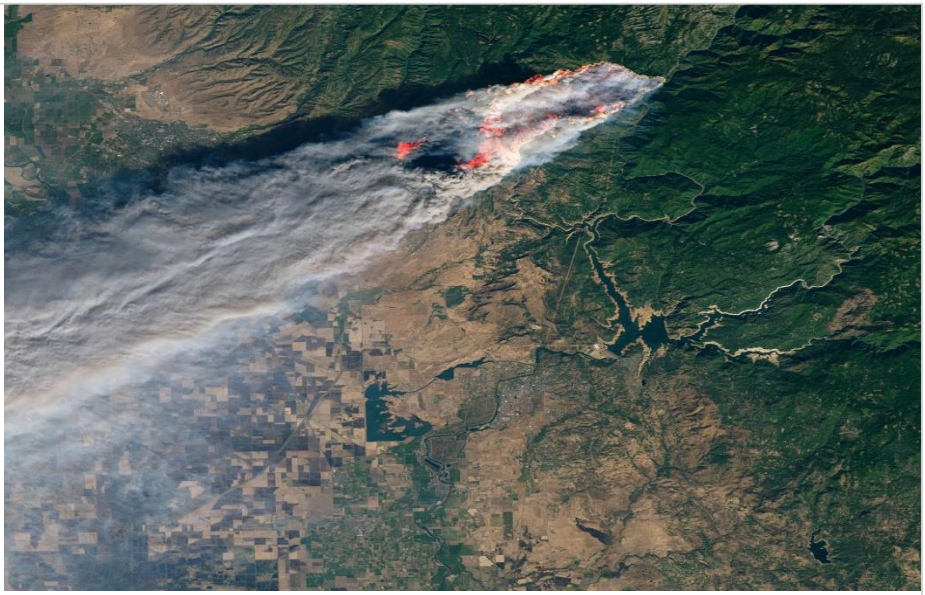
The SPARTA team recently provided an example on Aerospace's Medium publication of how the framework can be used by space professionals as a taxonomy of potential cyber threats to spacecraft and space missions. The example describes an attack dubbed PCspooF, which targets the vulnerability in and exploit of Time-Triggered Ethernet (TTE). TTE is used as a bus service for a variety of spacecraft including NASA's Orion capsule, NASA's Lunar Gateway space station, and ESA's Ariane 6 launcher — among others.

*To read more about what this attack chain would look like and how SPARTA can serve to strengthen resilience for space, read the full article on **Aerospace's Medium channel**. Cybersecurity-focused news media have also begun picking up on SPARTA, including DarkReading and CyberScoop.*

The Medium article is authored by Brandon Bailey and Brad Roeher of the Cyber Assessments and Research Department at Aerospace.

How Aerospace is Advancing Sensor Capabilities for Wildfires

January 05, 2023



With the effects of climate change becoming more prominent, Aerospace is leveraging technology and lessons learned to improve wildfire detection and monitoring.

In 2021, more than 2.5 million acres burned due to California's wildfires—aggravated by drought and intensified temperatures. The estimated economic loss was between $70 billion and $90 billion in the United States, with over half of

that attributed to California's wildfire season alone. Boosting space surveillance abilities can help improve response time and understanding of how these wildfires develop.

The Aerospace Corporation is addressing this growing area of need by identifying opportunities to improve wildfire detection and monitoring capabilities. These proposed efforts could ultimately protect biodiversity, infrastructure and human life, as well as mitigate wildfires' financially damaging effect.

"Although Aerospace has done previous wildfire monitoring-related work, with the rising number and gravity of California's wildfires, we sought to conduct a more comprehensive study on this topic to not only understand current wildfire remote sensing but also locate technological areas that could be improved upon," said Dr. Rob Stevens, Director of Aerospace's Model-Based Systems Engineering Office. "This effort was made possible by bringing different experts across Aerospace into a room and providing them the digital engineering tools to work concurrently, which ultimately saved time in building a solution."

The Aerospace Corporation is identifying opportunities to improve wildfire detection and monitoring capabilities, efforts that could ultimately protect biodiversity, infrastructure and human life, as well as mitigate wildfires' financially damaging effect. (Credit: U.S. Forest Service)

Determining What's Possible

Current satellites that can detect wildfires often have a gap in their capabilities, ranging from a lack of spatial resolution to low revisit frequency times or other essential qualities needed to provide in-depth and up-to-date information. A team at Aerospace is leveraging previous research—including a summer 2022 intern memo on existing architecture options and learned remote sensing principles and techniques—to provide a more comprehensive space vehicle design solution.

"The Overhead Persistent Infrared (OPIR) architectures team, which studies cutting-edge technology and approaches aimed at hard problems, applied their expertise to the wildfire problem," said Dr. Dee Pack, Principal Scientist in Aerospace's Space Science Applications Laboratory. "Our experts provided insight on architecture and sensor designs for fire monitoring and detection, information that was taken into account as the project progressed."

Read the full article on Aerospace.org.

January 2023 Obituaries

January 01, 2023

Sincere sympathy is extended to the families of:

- **Eileen Cross**, office of technical support, hired July 21, 1964, retired Nov. 1, 1988, died Nov. 25, 2022
- **Miguel De Virgilio**, member of technical staff, hired July 2, 1973, retired Oct. 1, 2019, died Nov. 28, 2022
- **William Faust**, member of technical staff, hired April 23, 1967, retired April 1, 1998, died Sept. 3, 2022
- **Gerald Finn**, member of technical staff, hired March 10, 1980, retired Feb. 1, 2012, died Sept. 3, 2022
- **Patrick Heming**, office of technical support, hired July 30, 1990, retired Sept. 1, 2000, died Nov. 9, 2022
- **Martha Miles**, office of technical support, hired May 1, 1961, retired Oct. 1, 1984, died Sept. 4, 2022
- **Eduardo Rodriguez**, member of technical staff, hired Oct. 8, 1973, retired Jan. 1, 2004, died Dec. 3, 2022
- **Marilyn Shaw**, office of technical support, hired Oct. 7, 1991, retired May 1, 2005, died Sept. 18, 2022
- **Christine Spria**, office of technical support, hired Sept. 14, 1976, retired July 1, 1988, died Dec. 2, 2022

These articles are reprinted from The Orbiter, a publication of The Aerospace Corporation 2310 E. El Segundo Blvd., El Segundo, CA 90245-4691 310-336-5000
Visit: Aerospace.org
Contact Orbiter staff: Orbiter@aero.org