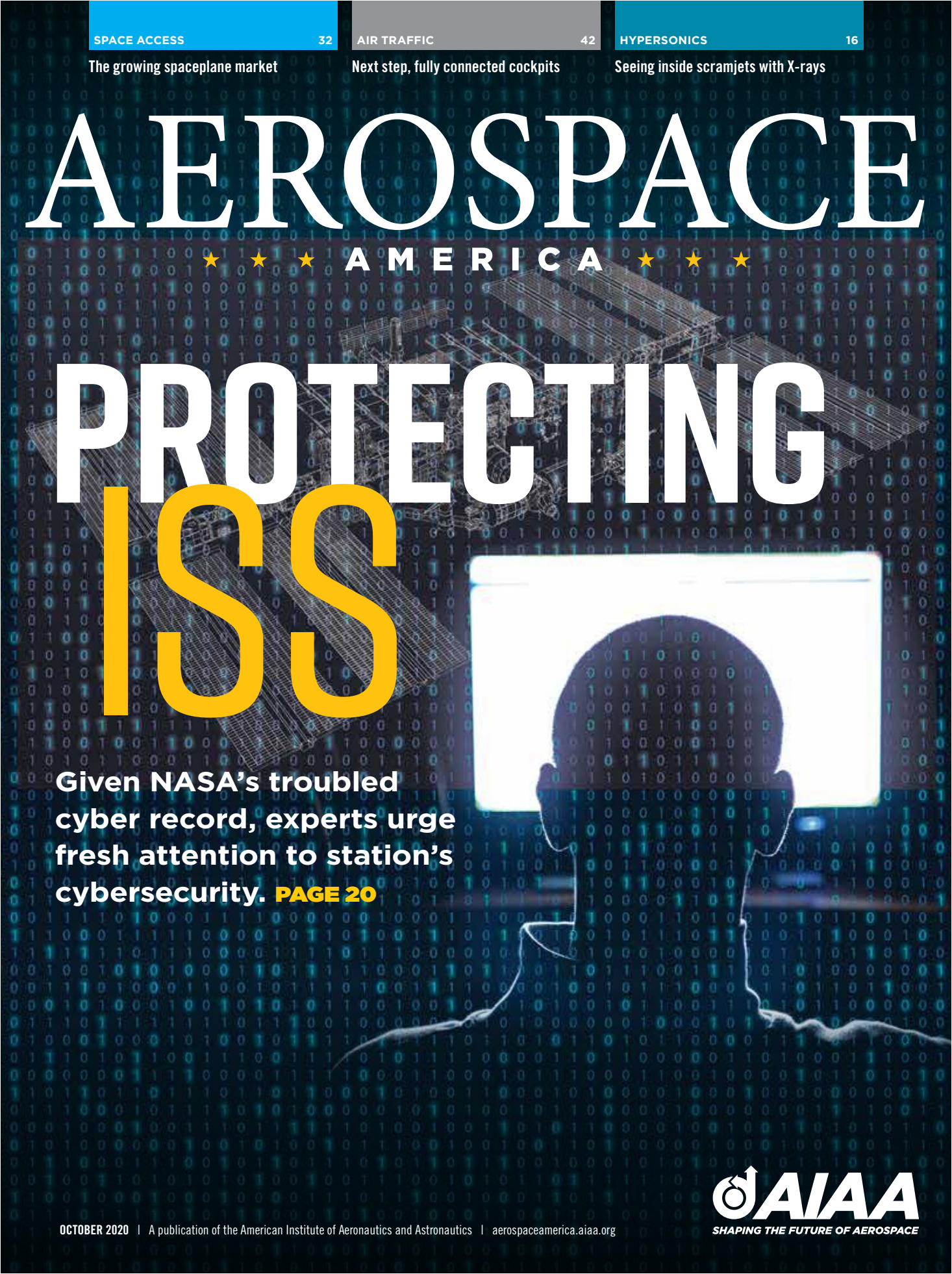
AEROSPACE

AMERICA

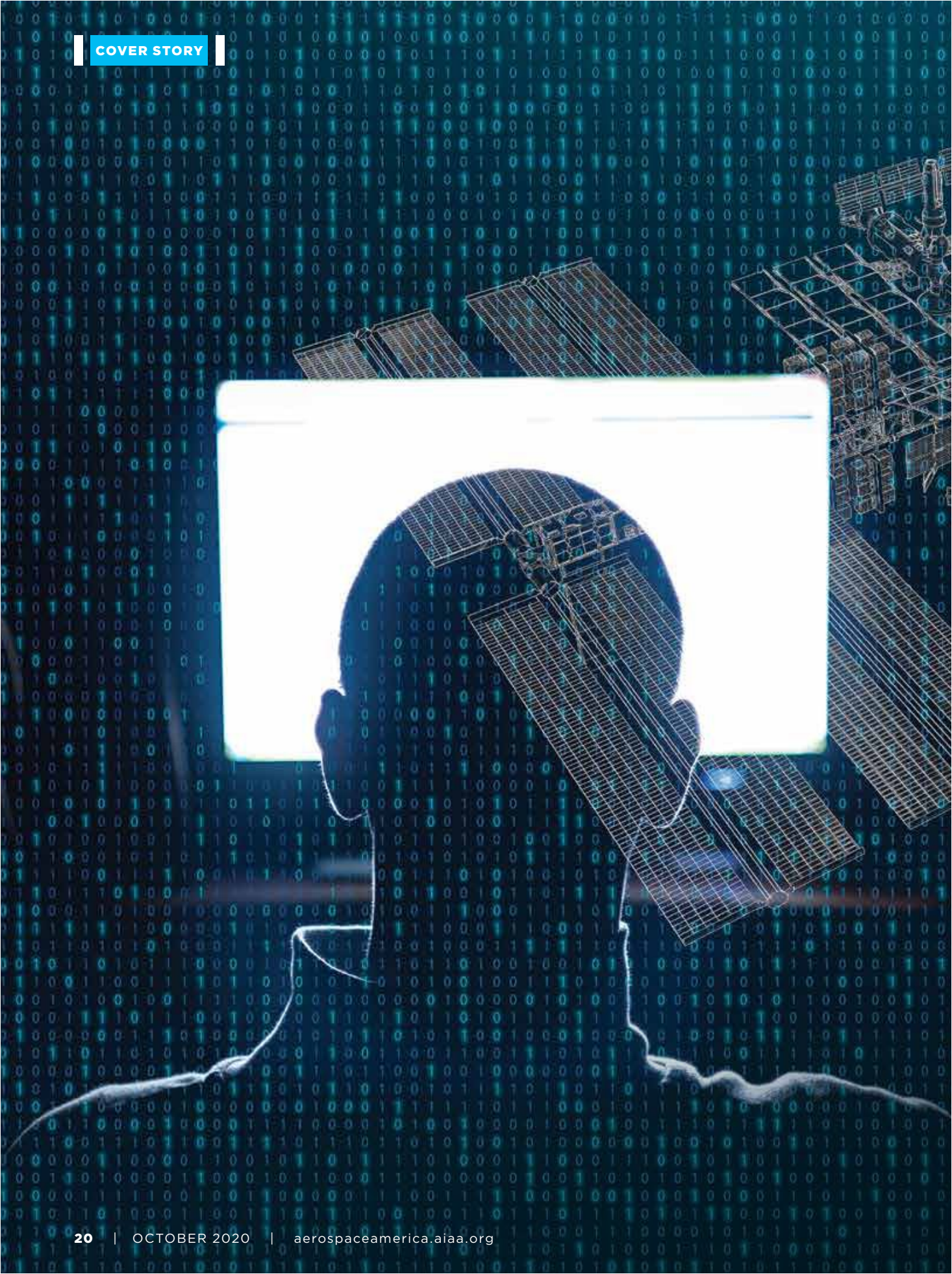
PROTECTING ISS

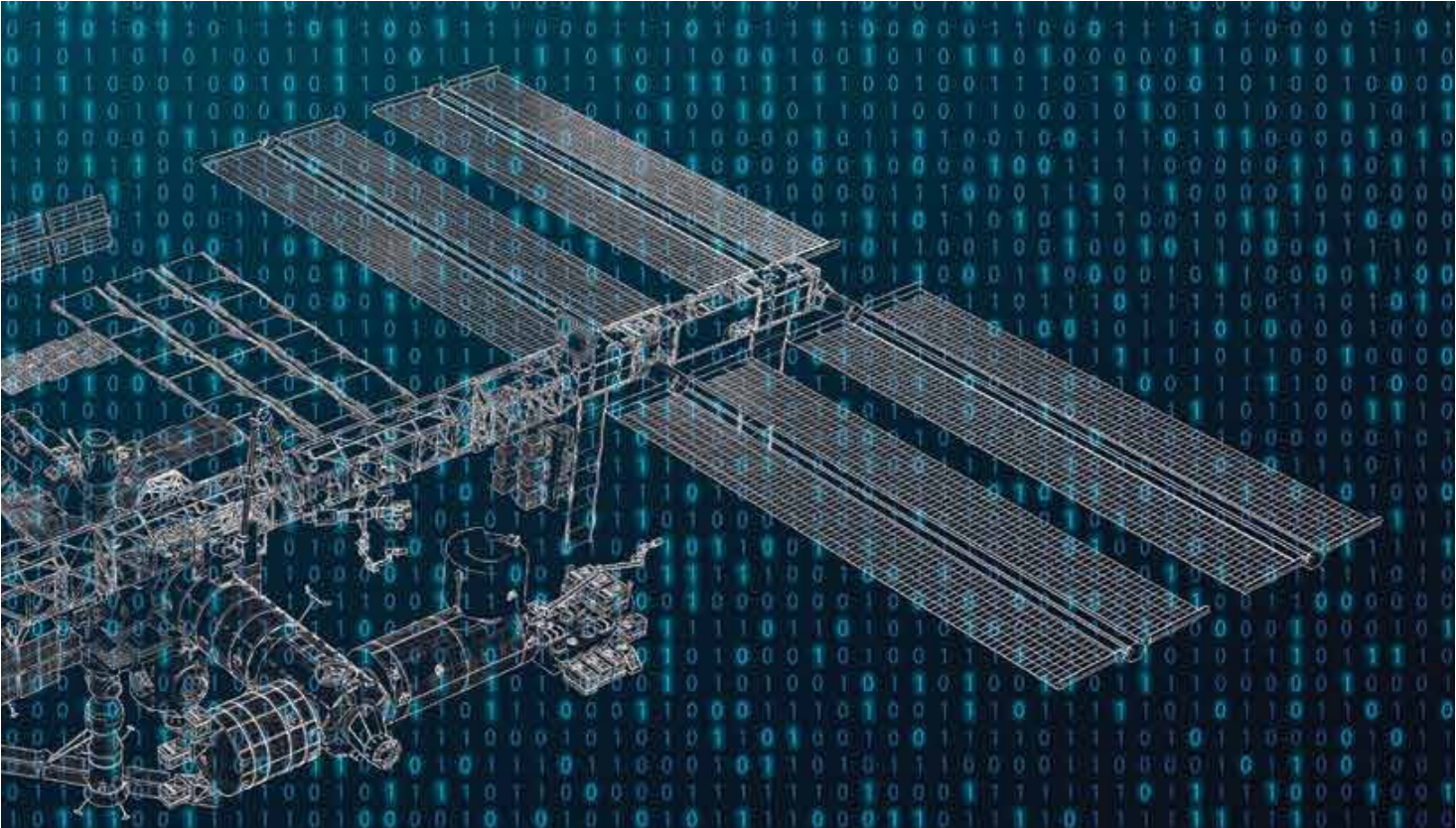


Given NASA's troubled cyber record, experts urge fresh attention to station's cybersecurity. PAGE 20

OCTOBER 2020 | A publication of the American Institute of Aeronautics and Astronautics | aerospaceamerica.aiaa.org

AIAA
SHAPING THE FUTURE OF AEROSPACE





PROTECTING ISS

NASA's cybersecurity track record has been a troubled one, but as far as the public record shows, the troubles have not reached the International Space Station. What should NASA do to keep it that way? Sarah Wells spoke to cybersecurity experts to find out.

BY SARAH WELLS | sarahes.wells@gmail.com

While it is easy — and even romantic — to imagine the International Space Station as a safe haven from Earthly pressures, the orbiting lab is, in reality, digitally connected to our terrestrial world, and therefore vulnerable, at least in theory, to the kind of targeted and malicious cyber threats we face on Earth from anyone with a grudge and a keyboard.

Of course, ISS is not connected directly to the internet. Before birthday wishes, photos and social media are allowed into NASA's network and bounced to the station via the geosynchronous Tracking Data Relay Satellite System, they are checked by NASA and mirrored by a computer at NASA's Johnson Space Center in Texas. With their NASA-provided laptops, U.S. crew members can remotely view this computer's desktop and control it via the laptop's track pad.

Still, the public prominence of the station has made the ISS a potentially juicy target for hackers worldwide — though likely not in the catastrophic, careening-out-of-orbit way that we might see in an action movie. More likely, experts believe, are data thefts and efforts to undermine the prestige of the ISS partner nations, probably carried out by finding a way around this secure computer.

The closest to anything like that came in 2011, when an unencrypted notebook computer containing ISS command and control algorithms was stolen, though NASA maintained that there was never an operational risk to the station. Nevertheless, NASA's poor cybersecurity record throughout other parts of the agency has independent experts and retired officials counseling even greater vigilance to protect ISS, especially with 90% of the workforce working remotely since March.

"We must recognize that while basic cyber hygiene practice is relatively doable under normal circumstances, these are not normal times," said Diana Burley, a cybersecurity researcher at American University in Washington, D.C., in a September congressional hearing.

Even before the pandemic, internal audits and reports by NASA'S Office of the Inspector General and the congressional Government Accountability Office indicated that NASA had repeatedly fallen short on cybersecurity of its computer networks and the proper data hygiene of its employees.

After repeated attempts for comment from NASA's associate chief information officer for cybersecurity and privacy, Mike Witt, and others in the Information Security Office in charge of NASA's cyber posture, I was able to connect with Renee Wynn, who was on the receiving end of some of those reports before

▲ **NASA astronaut** Mike Hopkins (foreground) and Japan Aerospace Exploration Agency astronaut Koichi Wakata monitor the situation as a cargo spacecraft unberths from the International Space Station in 2014.
NASA

retiring in April after five years as NASA's chief information officer.

Arriving as NASA's CIO in 2015, Wynn says she found independent scrutiny essential for identifying where NASA's corporate information technology has fallen short, and she acknowledges that it has indeed fallen short.

"One of the big challenges for NASA is that it invented some of the IT [the agency] needed to launch super cool science missions," she explains. And some of that IT, for example, communications software for receiving data from the Voyager space probes, has continued to be used well after what many would consider its prime. In the 1970s when these probes were launched, cybersecurity was not a top concern, says Wynn.

As for technology not tied up in nearly half-century long missions, Wynn says the importance of shoring up — or introducing — cybersecure technology and policies has become a priority in recent

▲ **The International** Space Station photographed from a Soyuz spacecraft after undocking. On board the Soyuz were two NASA astronauts and a Russian cosmonaut. The international delegations that work on ISS add another layer of complexity to preventing cybersecurity intrusions. NASA/Roscosmos

years. But devising the best way to do so has not been without its challenges.

To understand how to best plug NASA's cybersecurity holes, Wynn says that under her watch the agency took a risk-based-assessment approach and began to evaluate a variety of scenarios and risks of all programs, including the human spaceflight program that operates the ISS.

"We certainly found a green field of opportunity" for improving security, she says.

Despite Wynn's efforts, in 2018, the NASA-funded Jet Propulsion Laboratory in California had 500 megabytes of undisclosed data stolen through an unsecured and unmonitored Raspberry Pi, a credit-card-sized hobbyist computer. NASA and cybersecurity reviewers from other agencies have released little information about the incident, but we do know the hacker used the Raspberry Pi to access NASA's Deep Space Network, which routes commands to spacecraft beyond Earth orbit and receives scientific data back from them. They also penetrated an internal communications network that connects JPL with other NASA centers and contractors. A 2019 NASA audit report says that Johnson, the center responsible for ISS, disconnected from the infected internal network altogether.

"Johnson officials were concerned the cyber attackers could move laterally from [the internal network] into their mission systems, potentially gaining access and initiating malicious signals to human space flight missions that use those systems," according to the report, "Cybersecurity Management and Oversight at the Jet Propulsion Laboratory."

While NASA reports that no serious damage was done during this breach, records suggest that the agency has continued to struggle with cyber threats. In an independent review of federal records between 2018 and 2019, Atlas VPN, an online privacy company based in New York, reported that cybersecurity incidents at NASA were up 360% from 2018, with a total of 1,468 cyber incidents in 2019. This assessment is echoed by concerns voiced in a NASA inspector general report issued in June, "Evaluation of NASA's Information Security Program," which cited the agency for poor implementation and maintenance of cybersecurity infrastructure and protocols at its various centers.

NASA's Office of Inspector General explained to me in an email that these shortcomings threaten "the confidentiality, integrity, and availability of NASA information maintained in those [computers and databases.]"

Source of the problem

Although analyses to date have not specifically named the ISS as a concern, cybersecurity researchers I

spoke to say there could be as-yet-undiscovered weaknesses at the root of the agency's tangle of information computer networks, software and personnel, that might leave the station vulnerable.

As for how NASA amassed a poor cyber record, Emmanuel Lesser, a software product assurance engineer at the European Space Agency who researches cybersecurity solutions for satellites and deep space probes, thinks he knows, and it has to do with history.

"The kind of security implemented in space systems was security through obfuscation," he says. Lesser explains that major science and technology organizations, like NASA, that were building advanced hardware, software and craft for space exploration simply believed that malicious actors would find it too hard to obtain the communications protocols or appropriate transmitters necessary to hack their computers, let alone to understand the information once they got it. "They really believed [they were] not worth the effort to hack."

But, while the sheer complexity of spacecraft and their communications networks may have been enough to safeguard them in the past, hackers can learn a lot about those technologies from information that's available online, and they can add to that knowledge with each breach. This has left NASA rushing to catch up to modern cyber threats that stretch from its ground-based operations all the way, at least in theory, to the ISS.

In the June report, NASA's Office of Inspector General contends that this lack of security does not necessarily come from a lack of funding or lack of overall infrastructure capabilities, but instead from a more human problem: inconsistent management.

Part of the cause for this, says Wynn, is the diversity of protocols and organizational structure in different parts of the agency itself. During her tenure, she recognized that she would need solutions tailored for the specific needs of the different programs.

While some offices proved to be challenging to work with, the station managers were not.

"I immediately found partnership with the human space program," says Wynn, including managers of the ISS. When coming to discuss the cyber risks of the program, Wynn says she was prepared for resistance but instead "found people were already thinking about it and really putting some great ideas into practice."

Part of what drove this early adoption of cyber posture, Wynn suggests, is the concern for astronaut safety among those in the human spaceflight program. For them, cybersecurity was another critical element of that safety.

Challenges ahead

Of course, a desire for security is one thing, finding it is another. Bhavani Thuraisingham, who directs the Cyber Security Research and Education Institute at the University of Texas in Dallas, says that securing a spacecraft such as ISS is far more complicated than, for example, securing a retail store.

"The retail industry, like many industries, uses computers, iPads, and smartphones that are all integrated into databases and your operating system," says Thuraisingham. Targeting one piece of technology within a network of devices, say the microprocessor of a single iPad, is equivalent to an attack on the whole information network — from the iPad fleet to the financial databases they might be connected to — because of its interconnectivity, she says. This means that these networks are truly only as powerful as their weakest link.

So, retail stores are continually updating their software and devices for security. That's much harder to do with spacecraft far from Earth whose weaknesses might be outdated code or low-memory capacity for cybersecurity upgrades, says Gregory Falco, a security researcher at Stanford University.

The good news is that ISS is close to Earth, relatively speaking, and astronauts can regularly update its computers.

Teleworking targets

NASA is already contending with delays to its missions because of the widespread teleworking prompted by the coronavirus pandemic. Now, the agency must also contend with how that teleworking affects its cybersecurity, agency Inspector General Paul Martin told the House space subcommittee in September.

About 90% of NASA's employees and contractors have been working remotely since March, Martin said during the hearing. He said, "phishing attempts have doubled and malware attacks have increased exponentially."

This increase is not unique to NASA, said Diana Burley, a cybersecurity researcher at American University in Washington, D.C. Larger numbers of employees logging in from their home networks increase the number of points through which hackers can attempt to gain information from government agencies and companies, and employees who may be "distracted, frightened, and fatigued" with juggling work and personal responsibilities may be easier targets.

"Employees are worried about meeting their basic needs and are less likely to attend to seemingly lower priorities like cybersecurity," Burley told lawmakers.

— Cat Hofacker

▲ **Linking the** International Space Station to Earth requires flight controllers, software and hardware at NASA's Johnson Space Center in Texas.
NASA

In fact, ISS is certainly not stuck in the 1960s — or even '90s — when it comes to technology, says Pamela Melroy, a retired Air Force colonel and NASA astronaut who piloted or commanded three space shuttle missions to ISS. Melroy, now director of space technology and policy at Nova Systems in Australia, spoke during the virtual DefCon in August in a session titled "Cybersecurity Lessons Learned From Human Spaceflight." Hardware and software updates have even been made in recent years to accommodate new commercial spacecraft, she noted, the first of those being Northrop Grumman's Cygnus cargo capsules and SpaceX's Dragon and Crew Dragon capsules.

But with added complexity and capability, points out Thuraisingham, comes the possibility of cybersecurity breaches or mishaps. For example, the process from designing specialized hardware and software for a new spacecraft all the way through docking it at ISS can mean the participation of not only many NASA centers but private-sector partners as well. Any misstep in the process can create weak points, says Thuraisingham, and assigning blame can be nearly impossible.

And, of course, there is the international aspect of the space station. Nations aboard the station include Canada, Japan, Russia and those represented by the European Space Agency. While the astronauts do work together to transport cargo and crew to and from the station and share dinners together in com-

> **"It can sometimes be challenging for scientific institutions like NASA to look beyond their bigger mission — the advancement of science — to see how specialized hardware or software might be used nefariously for other purposes."**
>
> **— Gregory Falco,** Stanford University

mon areas, scientific experiments are carried out in separate, national modules and follow information security protocols from their respective agency CIOs, says Wynn, the former NASA CIO.

While comradery and respect among these international space agencies is critical to the station's overall mission of peaceful scientific cooperation in space, these differences in security protocols could nonetheless leave room for miscommunication or accidental introduction of nefarious code to ISS.

But, as Melroy explained in her DefCon talk, even if infected software were to be introduced to the station, say through a computer laptop, this wouldn't likely lead to stationwide infections because computers on ISS are never connected to other station networks or computers. In fact, this is true for many communications and scientific devices on the station for just these security reasons.

This similarly makes it unlikely for a phishing email with malware hidden in its links to infiltrate the station. These emails and personal communications are originally accessed through a secure computer on Earth and mirrored safely to laptops on the space station, similar to how you can trick your internet provider into thinking your computer is located in the United Kingdom by using a VPN. The next thing you know, you're watching another country's Netflix selections. Likewise, by using the station's laptops to remotely access the proxy computer on Earth, astronauts can check their email or other personal accounts a few times a day, says Melroy.

The threats

Wynn says that phishing attacks do not necessarily keep those in the CIO office up at night worrying about threats to ISS and human spaceflight. But that does not mean the station is completely out of harm's way, either.

When it comes to the actual damage these hackers could do to ISS, Steve Lee, AIAA's aerospace cybersecurity program manager, says there are three main types of attackers to look out for.

"I would say, if you had a pie chart of this sort of thing, some significant portion, maybe a quarter or a third, would be [industry] insiders and com-

petitors." Lee says these types of bad actors, which may likely be behind the data breach at JPL in 2018, are not in the hacking game for chaos or prestige, but instead to steal trade secrets and make money. Similarly, Lee says another big piece of the pie is opportunistic hackers armed with ransomware or malware to corrupt or steal information. And the remaining sliver, no more than 20%, is terrorists and nation states, says Lee.

Regarding nation states, "What they're doing is super strategic, super targeted and, frankly, super surgical," says Lee. China and Iran, two nations not represented on ISS, are often top suspects for threats like these, he says.

No wise person entirely disregards the possibility of terrorists trying to hack ISS, but as yet there is no evidence that they would have motivation for such an attack, Lee says.

What seems more likely than a catastrophic attack would be one that undermines the integrity of NASA and ISS partners by stealing or corrupting experiment results, says Falco. Even if not aimed directly at the ISS, a breach that threatens data accuracy or NASA's reputation could result in an overall loss of public trust, funding and, ultimately, NASA's place in space leadership, worries Falco.

▲ **The Canadarm2** robotic arm, guided by an astronaut on the ISS, prepares to capture a Cygnus supply spaceship made by Northrop Grumman. Hardware and software aboard ISS have been updated in recent years to accommodate new commercial spacecraft.
NASA

"I think the biggest risk is that we lose trust in the organizations trying to make space exploration real," says Falco.

It can sometimes be challenging for scientific institutions like NASA to look beyond their bigger mission — the advancement of science — to see how specialized hardware or software might be used nefariously for other purposes, Falco says. Hiring cybersecurity experts who can see around and through this mystique will be essential to protecting it.

While Thuraisingham says that this tug of war between hackers and the guardians of technology is destined to be eternal, there are steps that can be taken to secure space communication networks, spacecraft and computers.

In addition to better management from NASA, Lesser, the ESA researcher, says that it will also be important to future-proof security upgrades such as encryption. Even though today's modern encryption techniques can go toe-to-toe with hackers, the rise of quantum computing suggests that, without innovations, tomorrow's hackers will be able to cut right through conventional encryption. But, if ISS is indeed decommissioned in 2028, Lesser says this threat is unlikely to reach the station.

For ISS, Thuraisingham also suggests implementing security strategies that do not rely on encrypted communication signals to transmit commands to and from space, but instead depend on physical data available only on the station itself, for example, exact positioning or velocity measurements. Physical, immutable data like this would make spoofing encryption keys much harder. This, along with artificial intelligence algorithms designed to learn and anticipate hackers' patterns, could be another step forward.

Ultimately, putting more tools in NASA's cybersecurity toolbox is about more than protecting communications, data and science. It's about maintaining the public's trust — and funding — for scientific endeavors that aim to expand the understanding of our universe and ourselves.

"There's going to be a lot of players in the coming decade," Falco says. Those players will include private companies seeking to shuttle tourists and scientific instruments into space and national organizations like NASA and the space agencies of other nations. Falco says these players must work together to ensure they "have the security toolsets" to build these critical safety nets. ★

*Staff reporter **Cat Hofacker** contributed to this report.*