THE WALL STREET JOURNAL.

http://www.wsj.com/articles/u-s-panel-aims-to-shield-planes-from-cyberattack-1435537440

TECH

U.S. Panel Aims to Shield Planes From Cyberattack

FAA advisory committee was scheduled to meet this month amid rising concern over vulnerability to computer hackers.

Operations at Warsaw Chopin Airport were disrupted earlier this month by what LOT Polish Airlines said was a cyberattack on flight-planning computers. *PHOTO: KACPER PEMPEL/REUTERS*

By **ANDY PASZTOR**

Updated June 29, 2015 2:33 p.m. ET

U.S. aviation regulators and industry officials have begun developing comprehensive cybersecurity protections for aircraft, seeking to cover everything from the largest commercial jetliners to small private planes.

A high-level advisory committee set up by the U.S. Federal Aviation Administration—including representatives of plane makers, pilots and parts suppliers from around the globe—was scheduled to meet for the first time this month amid rising concern over potential industry vulnerability to computer hackers. The panel's meetings are private.

On June 21, operations were disrupted at Warsaw Chopin Airport by what LOT Polish Airlines said was a cyberattack on flight-planning computers. Ten LOT flights were canceled and some 15 others were grounded for several hours, affecting roughly 1,400 passengers. Though airline officials said safety was never affected, LOT's chief executive was quoted saying that such a cyberattack "can happen to anyone, anytime."

The goal of the FAA initiative, according to Jens Hennig, the panel's co-chairman, is to identify the seven or eight most important risk areas and then try to reach consensus on international design and testing standards to guard against possible cyberattacks. "The industry needs a set of graduated requirements," he said in an interview, based on the types of software and various aircraft models.

The overall level of concern is reflected in Boeing Co.'s decision to pay outside experts dubbed "red hat testers"—essentially authorized hackers—to see if built-in protections for onboard software can be defeated. Mike Sinnett, vice president of product development for Boeing's commercial-airplane unit, said certification of the flagship 787 Dreamliner required Boeing to purposely allow such teams inside the first layer of protection to demonstrate resilience.

When it comes to protecting flight-critical software from hackers, Mr. Sinnett said, the systems can accept only "specific bits of information at specific preordained times, and it is all preprogrammed." As a result, he added, "there's no way for the flight-control system to pull in something" from an unauthorized source.

Such software and cockpit interfaces aboard commercial jets are tested extensively and have such a wide array of embedded safeguards that they are considered virtually impregnable to direct attack by industry outsiders, according to these experts.

Yet that hardly means airliners are beyond the reach of hackers. The biggest current risks, experts believe, stem from aircraft links to ancillary ground networks that routinely upload and download data when planes aren't flying—including information used for maintenance, sending various software updates and generating flight plans before takeoff like those that affected LOT earlier this month.

"Where we are weak," says Patrick Ky, executive director of the European Aviation Safety Agency, is in ensuring that a maintenance or air-traffic control system can't be hacked and used as a conduit to get at aircraft. "What is not being done today," he said, "is to have a view of aircraft operations in their entirety," recognizing all the potential outside hazards.

Airbus Group SE and most of its suppliers continue to rely on a secure computer platform to protect their manufacturing operations, with some European experts advocating more aggressive efforts to expand the network to additional companies. "Every time you introduce another connection" in the form of a new supplier, "it's another way to potentially attack the aircraft itself," says Alain Robic, a partner in Deloitte Consulting's French unit who works with industry clients on data security.

Mr. Robic says that ideally all of the different levels of security among suppliers to Airbus and Boeing would conform to an information-system policy self-regulated by industry leaders.

Neither LOT nor Polish authorities have identified the source of this month's disruption. Prosecutors may also be looking at internal-software failures or other explanations for the problem, which was resolved after roughly five hours.

Whatever the exact cause, the incident points to the kind of computer problem that security experts worry about most in aviation and consider among the hardest to prevent: Attacks on maintenance or air-traffic control systems, which routinely interface with aircraft, as opposed to direct intrusions by outsiders on computers aboard planes.

Ground-based computer networks, including those between traffic-control operations, are considered less secure against hacking than those installed on aircraft, largely because onboard flight-critical systems have more internal protections and multiple redundancies to filter out intrusions. Hardware used for passenger Wi-Fi connections and entertainment options, for example, is physically separated from onboard-safety-system servers, and even electrical conduits are designed so that information doesn't bleed between the two.

In interviews at the Paris International Airshow days before the Warsaw incident, more than a dozen international cyber experts and industry officials stressed that despite various high-profile and public allegations, they weren't aware of a single verified instance of hackers breaching flight-control or engine-control systems on any modern jetliner while it was in the air. The current system is "working pretty well" and aviation software generally has been "pretty difficult to infiltrate," Mr. Hennig, vice president of operations for the General Aviation Manufacturers Association, said.

But most cyberprotection systems for planes are certified using case-by-case risk assessments requiring regulators to expend a lot of resources, rather than the industrywide technical standards the FAA and Mr. Hennig foresee. European regulators are expected to eventually create a similar advisory board to coordinate future standards.

Still, with cybersecurity issues gaining more prominence throughout aviation, various initiatives are already under way. Michael Huerta, who heads the FAA, is stressing the importance of sharing details about cyber events the same way specifics of safety incidents are now distributed and analyzed world-wide. "One of the things that is absolutely critical is to have very robust mechanisms for information sharing" among regions, including threats, potential incidents and mitigations, Mr. Huerta said in an interview. "The specifics of the cyber threat require us to be sharing on a broader scale than we have done in the past."

Industry officials at all levels are increasingly vigilant about chasing down any suspicions or allegations of unauthorized attempts to penetrate computer systems.

Today, "people try to get in your cellphone ... they like to test the security of all kinds of electrical devices," according to Carl Esposito, a senior aerospace official at Honeywell International Inc., who emphasized that aviation designs understand that trend.

A major question is whether the global industry, which relies on software development cycles that sometimes stretch into years, can remain nimble enough to stay ahead of hackers who can shift quickly from region to region and work on much shorter timelines.

"I see a lot of sharing [of data security threats], maybe not between countries but at least within countries," said Marc Darmon, head of the cybersecurity unit for France's Thales SA, which helps safeguard banking and a huge chunk of the world's credit-card transactions. In the past, he said, aircraft makers and airlines believed it was enough to ensure that safety systems were isolated from accidental intrusions, but now almost

every industry has adopted identification and responses to cyberattacks as major design criteria. “That was not the case 10 years ago,” he said. “It has to be the case today.”

—Jon Ostrower contributed to this article.

Write to Andy Pasztor at andy.pasztor@wsj.com