| Aviva Sternfeld

Beware: Your Plane Is Controlled By Computer Hackers

Over a year ago, Malaysia Airlines Flight 370 disappeared with 239 crew members and passengers, leaving no trace. Was it hijacked by ordinary computer hackers on the ground? Fantastic though the theory may seem, it has been raised more and more by security experts in recent months and has been discussed at urgent meetings of security agencies in the US and around the world. The possibility of computer hackers gaining control of an airplane or ship anywhere in the world is a critical topic that keeps some security officials from sleeping at night.

The First Round Is Fired—Stuxnet

One morning several years ago, the world woke up to the shocking news of the Stuxnet virus [see ***Zman*** 10—Kislev 5771]. Stuxnet was a project of the CIA working together with Israeli computer technicians. A rare form of computer virus, Stuxnet solely targeted the Iranian nuclear program. It was primarily noteworthy because it awoke the world to a new reality: the possibility of remote-controlling physical machinery through a computer virus.

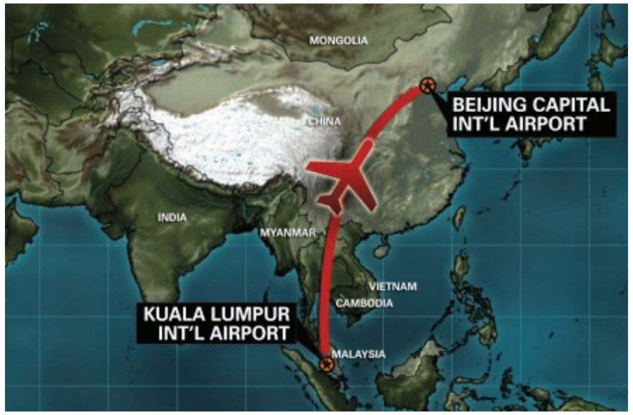
Stuxnet was created with the express purpose of sneaking into the secret computer program that controlled the centrifuges of Iran's nuclear reactor. It succeeded in disrupting the centrifuges by sometimes speeding them up and other times slowing them down. Despite the fact that Iran had been extremely careful not to connect the computers that control its reactors with the internet, Stuxnet was so advanced that it managed to pass from one computer to another until it reached the computers of the Iranian nuclear physicists. From there it passed itself onto the reactor's computer and got down to work.

Thanks to this super-sophisticated virus, the centrifuges did not function properly and broke down repeatedly. The Iranian operators could not figure out what was going on, since their computers indicated that everything was performing optimally. At first they assumed that the centrifuges had been victimized by a covert sabotage operation. It took more than a year until they realized that something was happening behind the scenes, and only after a massive search operation did they discover the Stuxnet virus buried deep inside the computer programs.

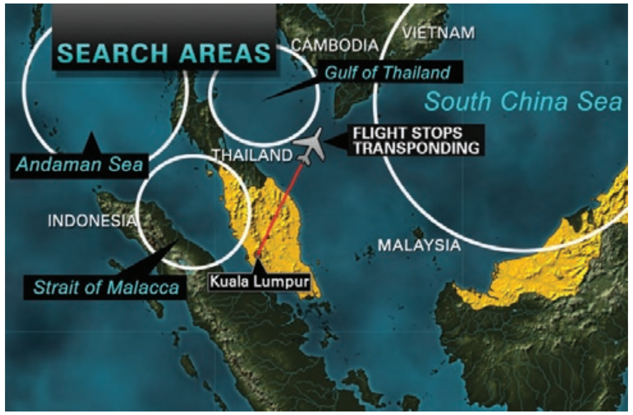
Though Stuxnet may have been the first prominent virus of its type, it did not remain alone for long. Years have passed since then and millions of new hackers have been initiated into the nefarious world of computer hacking, some even becoming masters of the field.

Hacking is responsible for hundreds of millions of dollars in direct damage each year and has turned into a major industry, spawning an equally large industry to protect against it. Two kinds of hackers usually make the news: the first are groups such as Anonymous, a group of computer geeks using their expertise to spread their ideology [see ***Zman*** 59—Cheshvan 5775]; the second are hackers who have broken into various computer systems and accessed bank accounts, credit card information, e-mail accounts, etc. These hackers cause serious damage—adding up to hundreds of *billions* of dollars each year when one includes the indirect costs incurred to protect systems from them. Every financial company must pay experts to create security nets to block online thieves.

A Boeing 777 belonging to Malaysia Airlines.



Scheduled flight path of the missing Malaysian airliner.



Huge areas of ocean that were searched unsuccessfully following the disappearance.

But these problems are only a minor headache compared to the threat of cyber attacks that security officials must worry about. The threat may come from terrorists, enemy governments, or even fanatical individuals who now have the ability to undermine the most powerful governments and elaborate industries.

Malaysia vs. Malaysia?

Just over a year ago, the shocking news broke that a Malaysian airplane en route to China had disappeared. The media kept the world fixated on the event for weeks, and to this day not a trace has been found of the airplane. There is no clear explanation of what caused it to stray from its flight path or where it eventually landed up.

Naturally, the absence of a simple explanation triggered all sorts of conspiracy theories. Several days after the disappearance, rumors began to circulate that the security community was unusually shaken by the incident. Officials began to seriously consider the possibility that a sophisticated hacker or group of hackers had managed to launch a remote-control attack that broke into the airplane's computer systems. It then ordered the computers to divert the airplane away from its preprogrammed flight path, with unknown consequences.

This theory would explain why the copilot sounded so calm just seconds before the airplane was diverted. He does not sound at all like someone who realizes that he is making his final journey. It also explains why ground control failed to hear any further communications from the pilots, even though the airplane probably continued flying for many hours. Even if they didn't fully comprehend the problem, at the very least they would be expected to radio that something was wrong. If the cyber attack theory is correct, the hackers may have isolated the pilots from their own communications equipment and instruments so they could neither remain in contact with ground control nor control their aircraft.

The cyber attack theory did not come from the twisted mind of some crackpot conspiracy theorist. The first person to mention this theory was a British security analyst who used to be employed in the British intelligence community. From there, the media quickly picked up the idea and it soon spread around the world. The analyst confidently stated that someone with the right knowledge and experience could conceivably use a smartphone to send electronic signals to an airplane's computers that would override the pilot's commands.

As expected, both the Boeing company and the US government emphatically denied that there was any such possibility of taking control of an airplane through ground-based computers. There are a few problems with their denial, however. First, in 2007, Boeing itself admitted that for years it had built

Hackers' conference in Amsterdam about to begin. Bottom: At the conference, a young security hacker demonstrated live how he took control of an airplane in the air from his smartphone!