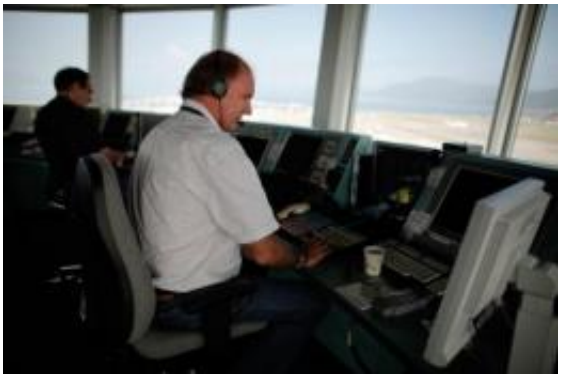
Airliners fly in face of cyber attack scares

November 3 2010, by Adrian Addison



Air traffic controllers monitor flights at Hong Kong's international airport. Almost five billion passengers were transported by airplane in 2009, but experts are concerned that a computer attack on aviation control systems could wreak havoc with the finely-tuned network.

Around the world, around the clock, circles of flickering screens keep aircraft apart in the air, ease them gently down to the ground and guide their precious human cargoes off the runway.

This finely choreographed global ballet of speeding metal, fuel and flesh moved almost five billion passengers in 2009, according to data from Airports Council International.

But what if all those screens went blank?

Inside the hot and stuffy glass bulb of the Hong Kong airport control tower, a dozen staff watch the dots on their computers transform into

planes rapidly descending from a clear blue sky.

A few floors below, more staff sit at screens in a room with no windows and keep digital tabs on all of the city's airspace, from the tip of the tower to far out over the South China Sea.

Computers everywhere.

Radar. Navigation and weather data systems. Radio communications.

All work together to bring hurtling aircraft to the point where the black rubber lips of the airbridge kiss the doors and weary passengers can safely shuffle off the plane and get on their way.

Then ground control systems cut in to turn the plane around and get fresh passengers in the air until, finally, it exits Hong Kong's airspace and registers as a blip on some far away air traffic controller's screen.

But computers are vulnerable to cyber attack -- and that worries the world's intelligence community.

The head of Interpol, Ronald K. Noble, issued a stark warning to the international police agency's first ever cyber-threat conference in Hong Kong in September.

"We have been lucky so far that terrorists did not -- at least successfully or at least of which we are aware -- launch cyberattacks," he told 300 of the world's top law enforcement officials from 56 countries.

"One may wonder if this is a matter of style. Terrorists may prefer the mass media coverage of destroyed commuter trains, buildings brought down.

"But until when?"

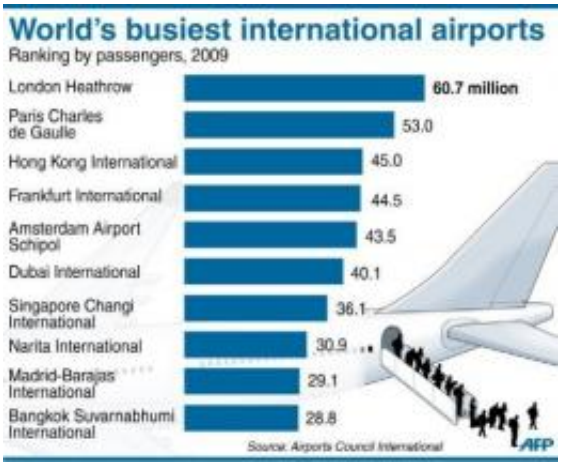


Chart showing the world's busiest international airports including Hong Kong's Chek Lap Kok

Within weeks of Noble addressing the conference, news broke of the world's first 'cyber superweapon' which was said to be targeting Iran's nuclear facilities as well as infrastructure systems in China.

The Stuxnet worm could break into computers that control machinery at the heart of industry, allowing an attacker to assume control of critical systems like pumps, motors, alarms and valves.

It could, technically, make factory boilers explode, destroy gas pipelines or even cause a nuclear plant to malfunction.

A worm is piece of malicious software (malware) which copies itself and sends itself on to other computers in a network, usually without the computers' operators even knowing it is there.

But at Hong Kong's Chek Lap Kok airport, nobody seems particularly worried.

Carl Modder is the senior man on deck in a control tower that handles a take-off or landing every minute of the day.

"Our system runs on rails really," Modder told AFP. "And we have multiple layers of contingency procedures and fall-back systems that can cut in when required to minimise risk of failure to the air traffic control system.

"For instance, we have four separate radar systems. They can all work independently. If one were to go down the others would still work.

"Plus," he says, gesturing to the controller in charge of the runway used for landing. "The human element is also very much part of the system.

"The final decision to allow an aircraft to take-off or land is taken by a human, not a computer."

He waves a hand out over the vast state-of-the-art facility built on flattened islands and land reclaimed from the sea as yet another plane gently touches down, brakes and exits the runway.

"We even have a back up control tower," he smiles. "We often have drills where we simulate an evacuation from the main tower and 'use the spare'. We have to be prepared to the best of our ability for any eventuality."

And Ir Leung Ping-keung, the man in charge of the airport's 50 technical systems, is certain that there is no risk from cyber attack.

"It is a closed system," he told AFP. "There is no connection between

our systems and the Internet nor is there USB access."

Yet computer security experts are not convinced.

Air traffic controllers monitor flight traffic in the control tower of Hong Kong international airport. Staff watch screens in a room with no windows and keep digital tabs on all of the city's airspace, from the tip of the tower to far out over the South China Sea.

Alan Paller, director of research at US-based computer security organisation the SANS Institute, says there is a fundamental weakness in the "not connected to the Internet" argument.

The average air traffic controller cannot email or surf the web from the control systems, he explained.

"But when most managers say there is no connection to the Internet, they are unaware of maintenance connections," he told AFP.

"Behind the scenes there are almost always semi-direct connections through routers shared between the control system and business systems that can be exploited. Worms and attackers can find them easily."

In January 2003, he said, the Bank of America reported that its ATMs had been disabled by an Internet worm -- that was after the banks assured the world that their ATMs were 'not connected to the Internet'.

The most serious cyber attack on the US military came from a tainted flash drive in 2008 inserted into a military laptop in the Middle East which released malicious code that spread undetected in classified and unclassified systems.

It established "what amounted to a digital beachhead, from which data could be transferred to servers under foreign control," Deputy Defence Secretary William Lynn said in August.

But the threat is even greater now, Paller says.

"One of the most virulent new vectors is smartphones -- especially Android-based (the Google operating system) smartphones," he said.

"People plug them into their computers, even computers not connected to the Internet, not for data transfer but to recharge the battery -- not knowing that behind the scenes their phones have been infected and are a carrier between the Internet and the better protected networks."

But in the skies there is still, ultimately, a human in charge: the pilot.

Hong Kong airline Cathay Pacific trains their pilots to face all eventualities they can think of, including a sudden collapse in the air traffic control system.

Blank screens could cause massive disruption but not necessarily disaster.

"Pilots are still trained to fly visually," a Cathay spokesman told AFP.

"We also have communications with our aircraft and can keep them informed with what is going on."

(c) 2010 AFP