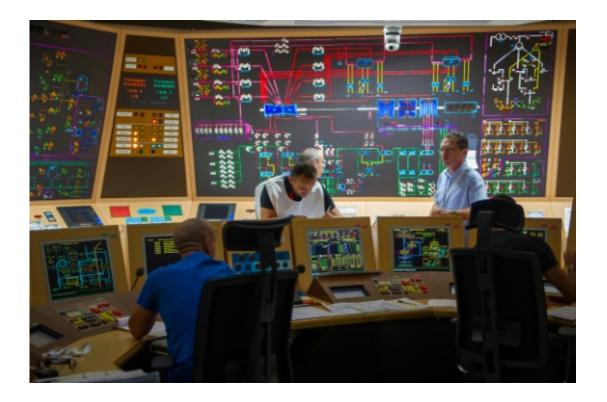# Nuclear power plants warned on cyber security

October 5 2015

Technicians are pictured as they work on the simulator control panel during an exercise on nuclear security at the Civaux Nuclear Power plant, 34 kms southeast of Poitiers, western France, on September 22, 2015

Operators of nuclear power plants worldwide are "struggling" to adapt to the increasing and potentially dangerous threat of cyber attacks, a report warned Monday.

The [nuclear industry](#) "is beginning -– but struggling -– to come to grips with this new, insidious threat," the Chatham House think-tank in London said in a study based on 18 months of investigation.

Its findings suggest that [nuclear plants](#) "lack preparedness for a large-scale cyber security emergency, and there would be considerable problems in trying to coordinate an adequate response."

It highlighted insufficient funding and training, a "paucity" of regulatory standards, increasing use of digital systems and greater use of cheaper but riskier commercial "off-the-shelf" software.

In addition there is a "pervading myth" that [nuclear power plants](#) are protected because they are "air gapped"—in other words not connected to the Internet.

In fact, many nuclear facilities have gradually developed some form of Internet connectivity, and computer systems can be infected with a USB drive or other removable media devices.

This was the case with Stuxnet, a virus reportedly developed by the United States and Israel—and implanted with a flash drive—which caused Iran's [nuclear facilities](#) major problems in 2010.

Chatham House added that Stuxnet, which it said is also believed to have infected a Russian nuclear plant, has had the unintended effect of teaching cyber criminals how to improve their techniques.

"Once Stuxnet's existence became publicly known, hackers around the world took inspiration from the way it functioned and incorporated some of its features into malware to suit their own purposes," it said.