http://www.worldcrunch.com/tech-science/espionage-in-academia-how-to-stop-spies-and-thieves-from-swiping-top-research/copyright-university-spying-cnrs-technology/c4s9644/#.UGM8mHmDmSp

Worldcrunch
all news is global

Monday 8 October 2012

news | crunch it | videos | images | your world | about us | advanced search mode | search

world affairs | business & finance | culture / society | tech / science | opinion / analysis | eyes on the U.S. | food / travel

Home > Espionage In Academia: How To Stop Spies And Thieves From Swiping Top Research

Le Monde

Share | Tweet | Recommend

ESPIONAGE IN ACADEMIA: HOW TO STOP SPIES AND THIEVES FROM SWIPING TOP RESEARCH

A Stasi Snooping Device At The DDR Museum. - (ptwo)

By David Larousserie
LE MONDE/Worldcrunch

PARIS - Pirates, spies, moles, thieves: those who want to steal the scientific treasures of French research laboratories had better be careful.

With a new measure to protect the "nation's scientific and technical potential," in the next few months every organization, university and engineering school will be receiving instructions on how to protect themselves. Indeed, spying on national or foreign competitors is not limited to industrial espionage: fundamental and applied research are also targeted.

"This is not imaginary. You would have to be naively optimistic not to know that there research is a target of international information-gathering strategies," says Jean Marimbert, secretary general and security chief of the French education and research ministry.

No doubt there are few espionage scandals as bad as that of "Farewell," the code name of a French double agent who worked for the KGB and its French counterpart of the time, the DST, during the 1970s and 1980s; nor as serious as the case of Rolf Dobbertin, a French researcher accused of spying for East Germany in 1979. He was finally acquitted in 1991.

But the threat exists. Certainly, preventing the proliferation of nuclear, chemical or bacteriological weapons is still a priority, but with globalization and economic competition, attention is also turning toward laboratories researching for patents, start-ups, and other innovative products. There have been leaks, although the people we interviewed did not want to discuss them. "A research scientist is not going to brag that someone stole his computer or his idea. A laboratory will not be proud of having been burglarized," we were told. But several enlightening stories are already making the rounds.

Ties dipped in laboratory beakers

The most popular story is the one about the foreign delegation visiting a chemistry lab, whose delegates carelessly let their ties hang into the beakers. A more serious example is the case of a foreign scientist in a French laboratory who filed for patents in his home country without mentioning the institution he was affiliated with. Another case is that of a foreign student caught twice stealing files on his director's computers, and allowed to leave without any trouble, except for being sanctioned by the university.

One chemist told us that his foreign competitors had been able to make up time by seizing data he had naively posted in a grant proposal for funding for his laboratory. One French computer executive caught a foreign delegation in the act of lending its hosts a thumb drive loaded with spy software.

In fact, the form of espionage varies widely. Computer attacks, a classic, remain quite common. The French Commissariat for atomic and alternative energies (CEA) estimates that 97 % of requests for access to its servers are rejected. Most of these are from abroad. Other threats include computer and telephone thefts, a quarter of which are "targeted," or linked to their content rather than to the computer or telephone itself, according to those we interviewed. In the Thalys trans-Europe express train, 400 computers are stolen each year. At the French National Center for Scientific Research (CNRS), more than 50 computers were stolen in 2008.

Thefts and conflicts relating to intellectual property are also an important category, which often take much longer for a resolution. The CEA took almost ten years to win a lawsuit against Samsung over flat screen technology. Less well known are attacks on image or reputation through hijacking or takeovers of websites.

Another category of threat has created a great deal of anxiety in people's imaginations: "financial infringement." The expression means equity participation or purchases by foreign investors, which can be a way of getting access to secret or patented information. The suspicion is difficult to confirm. It is also true that not all valuable information needs to be stolen. It could be public already; the trick is knowing how to find and use it.

Access to restricted zones

France, therefore, is getting ready to counter the threat. "The new measure is less about the form than about legal issues," explains Jean Marimbert. Since 1993, security has been under the ministry's "instruction," a measure that is less effective than the law that is now in place. Intrusion into "ZRR" restricted zones can now be punished according to the penal code. Until now, all that could be done was to ask an intruder to leave an area with controlled access.

The number of these zones, obviously, is confidential. There could be "between 100 and 1000" among the 2200 laboratories whose activities are listed in the July decree; these include mathematics and mathematical interactions, astronomy, and theoretical physics. As before, requests for internships, theses, and post-doctoral research regarding these zones will be examined by the 120 officials in charge of defense and security for French universities, organizations and engineering schools, whose main activity is to filter such requests. The CEA for instance deals with tens of thousands a year, and refuses less than 1 % requests.

Another innovation is that the decree applies to all nationalities. Earlier, European Union citizens were not affected. Moreover, the term "visit" will apply not only to work encounters, but to any "temporary" presence, which increases the number of people being monitored.

"The aim is not to keep our scientists from working. We are protecting ourselves so that thefts do not occur," explains Edwige Bonnevie, director of risk prevention at the CEA.

The task is more difficult in the research world than in the economic sphere. "A scientist needs to interact with the outside world. He listens, he talks. He shows in order to receive. But transparency does not mean naïveté," says Jacques Lewiner, president of the ESPCI Georges Charpak fund, which promotes research.

In spite of all efforts, our sources say, the number of attacks on French science is rising. The 2010 audit that led to the current reform showed a "disquieting level." A report by Claude Rochet for the Ministry of the Economy in July 2011 reported that "economic security was not a priority" in the competitive poles, or laboratories grouped by themes, of enterprises of any size. In response, the inter -ministry delegation for economic intelligence published a guide in March for French laboratories. Before the end of the year, it plans to offer software for laboratories to evaluate their own level of protection. The defense and security officials have one more task, a demanding one: raising awareness of the threat.

Some basic security principles :

- Put property marks on personal documents.

- Keep laboratory logs up to date.

- Make back-up copies.

- Use only computer hardware and software that is of known origin, trusted and tested.

- Encrypt data when necessary.

- Make interns and visitors sign confidentiality agreements before they enter a laboratory.

- When going abroad, take only indispensable documents. Take a computer only if absolutely necessary.

Read the article in the original language.

Photo by - ptwo