

L'Ecole de guerre économique dans le New York Times !

19/08/2009 : Suite au scandale d'espionnage informatique dont a souffert dernièrement Greenpeace, le New York Times consacre un long article sur les pratiques d'espionnage en France, en faisant appel à l'expertise de Christian Harbulot et de l'Ecole de guerre économique dans le domaine de l'intelligence économique et stratégique.

In French Inquiry, a Glimpse at Corporate Spying

par David Jolly, August 1, 2009, The New York Times

[lien vers l'article original](#)

PARIS — The story has the elements of a corporate thriller : a cast of characters that includes former French spies and military men, an American cycling champion, Greenpeace activists and a dogged judge whose investigation takes him from a sports doping laboratory outside Paris to a Moroccan jail and to some of the top corporations in France.

Like installments in a serial novel, new revelations have been dripping out since March. And while the climax is still probably many months away, the story is providing a rare glimpse into the shadowy and potentially lucrative business of gathering what corporations refer to as “strategic intelligence.”

“For most companies, on a daily basis there are many more things going on than can possibly be handed off to the police,” said Christian Harbulot, director of the École de Guerre Économique, or School of Economic Warfare, in Paris.

The companies they turn to for “extra help,” Mr. Harbulot said, include everything from corporate security giants like Kroll to what he terms “small operators,” ranging from ex-intelligence agents to computer hackers.

The sprawling case unfolding in France involves a mix of the latter and some of the biggest French companies, including Électricité de France, the world's largest operator of nuclear power plants, and Vivendi, the media and telecommunications conglomerate.

According to a case file compiled by the investigating judge, Thomas Cassuto, and reviewed by the International Herald Tribune, investigators stumbled on to the case almost by accident, in the wake of a doping scandal at the Tour de France in 2006.

The American cyclist Floyd Landis was stripped of his victory that summer after testing positive for elevated levels of testosterone. Not long afterward, in November 2006, the French anti-doping agency filed a criminal complaint charging that confidential documents related to Mr. Landis's drug tests had been stolen and sent to the news media and other labs. The documents had been altered in what lab officials said appeared to have been an effort to discredit or embarrass

them by casting doubt on the handling of test samples. Investigators concluded that one such e-mail message was sent from a computer using the same Internet protocol address used by Arnie Baker, then Mr. Landis's coach.

A search of computers in the lab in Châtenay-Malabry, a suburb of Paris, turned up a Trojan horse program that allowed an outsider to remotely download files.

No evidence has surfaced to connect Mr. Landis or Mr. Baker to the hacking, and both have vigorously denied any involvement. They did, however, make use of the pilfered documents in their unsuccessful campaign to overturn Mr. Landis's cycling ban, on the grounds that the documents had entered the public domain.

The trail, picked up by a special cybercrime unit of the French Interior Ministry, led to a French computer specialist, Alain Quiros. He was caught in Mohammedia, Morocco, and questioned by French and Moroccan officials there (It is not clear from the case file exactly when).

Mr. Quiros initially denied any knowledge of the lab hacking, but when presented with incriminating evidence found on his computer, he confessed, telling investigators he had been paid €2,000 to €3,000, or \$2,800 to \$4,000, for hacking into the lab. He identified Thierry Lorho, head of Kargus Consultants, a corporate intelligence company in Paris, as having instigated the computer attack.

Then things got complicated. As the French authorities delved more deeply into Mr. Quiros's computer, they found a copy of the hard drive of Yannick Jadot, the former campaign director of Greenpeace France, as well as that of Frédéric-Karel Canoy, a French lawyer and shareholder rights activist who has battled some of the country's largest companies, including Vivendi and European Aeronautic Defense & Space, the parent of the aircraft manufacturer Airbus.

Mr. Lorho, a former French intelligence agent, acknowledged his role to the French officials. He told them that he had handed off the lab data to another man, Jean-François Dominguez, who had paid him for it. Both men are being formally investigated. Mr. Lorho also admitted that he had collected data on Greenpeace. His client that time, he said, was Électricité de France, which had paid him for "strategic intelligence" on anti-nuclear campaigners.

Mr. Lorho has said his contacts at E.D.F. were "perfectly aware" of the hacking and that such activities were understood to be included under the two one-year contracts he signed with the company.

One, signed in April 2004, paid Mr. Lorho's company €12,000 a month; a second, signed in November 2006, provided for €3,900 a month.

The investigation found that in addition to information on Greenpeace in France, E.D.F. obtained data on the environmental organization's activities in Spain, Belgium and Britain, where E.D.F. last year agreed to buy the largest nuclear power company there, British Energy.

E.D.F. has denied any knowledge of the cybertheft and has portrayed itself as a victim of illegal acts by Kargus Consultants.

But Judge Cassuto, who took over the three-pronged investigation in April 2008, has declined to grant E.D.F. civil party status in the case. The decision was upheld on appeal. Instead, the judge has declared E.D.F. an "assisted witness," one step short of being placed under formal investigation, and the chief executive of E.D.F., Pierre Gadonneix, has been called in for questioning.

Alexis Gublin, the attorney who is representing E.D.F. in the case, said the company was cooperating "totally" with the inquiry.

Through their lawyers, Mr. Quiros, Mr. Dominguez and Mr. Lorho declined to comment. Astrid Granoux, a spokeswoman for the prosecutor's office, said Judge Cassuto and the prosecutor, Philippe Courroye, would not discuss the case while

the investigation was under way.

Spying by corporations on their perceived enemies is not new. In the mid-1960s, General Motors sent private detectives to dig up dirt on the consumer activist Ralph Nader when he began to criticize the auto industry's safety record.

In 2006, top executives of Hewlett-Packard, infuriated by damaging leaks from corporate insiders, hired investigators to spy on journalists in an effort to learn their sources.

And over the past two years, some of the biggest companies in Germany, including Deutsche Telekom, Deutsche Bank and the national rail operator, Deutsche Bahn, have been caught overstepping the line regarding surveillance of critics and their own employees.

People in the field of corporate intelligence say information in the public domain is considered fair game. Theft of a computer hard drive would normally be understood as a step too far, they said. But it might not even be necessary as the technology advances: Experts say the Trojan horse attack is giving way to automated targeting of the "cloud" of information that people and organizations generate through their online activities.

In the Cassuto investigation, the connection to E.D.F., which is 85 percent owned by the French government, has touched a nerve in France, whose intelligence agents bombed and sank the Greenpeace ship Rainbow Warrior in 1985 in Auckland, killing a photographer on board.

However, there has been no evidence to suggest that the French government was aware of or involved in the hacking.

In an interview with an intelligence Web site, Lerenseignement.com, Mr. Lorho said he assumed "full responsibility" for hacking into the Greenpeace computer, but he added that "I would like to see E.D.F., which sponsored the operation, take responsibility for its part."

On April 10, E.D.F. said that, after an internal investigation, it had terminated its relationship with Kargus Consultants and, as a "precautionary measure," temporarily removed from their posts two corporate security employees who had been dealing with the firm.

The two — Pierre-Paul François, an site protection engineer and former police officer, and his superior, Pascal Durieux, a security manager and former French Navy admiral — have been placed under formal investigation by Judge Cassuto. They have been transferred to other duties but continue to work at E.D.F. and to draw their salaries, their lawyers said. Both maintain their innocence.

E.D.F. also said it had terminated a contract with another corporate intelligence company, Securewyse, based in Lausanne, Switzerland.

The French newspaper *Le Canard Enchaîné* reported that Securewyse had been retained to monitor the French anti-nuclear group *Sortir du Nucléaire*, whose spokesman, Stéphane Lhomme, has been under investigation in France since 2006, when he passed confidential company documents to the media.

Securewyse did not reply to numerous requests for comment, but a company official told *Le Canard Enchaîné* that it had done nothing illegal.

Mr. Jadot, who has since left Greenpeace and was elected June 6 to represent western France in the European Parliament, said the case showed "a systematic policy of spying by E.D.F."

But E.D.F. defends its need to keep an eye on activist groups.

"We have a duty to be vigilant," Jean-Marc Sabathé, the company's security director, said in an April interview with Le Monde. "It's important to know, for example, if this or that group is in the radical extreme or if it is above board. But we have no need to pay hackers to find out!"

Meanwhile, the investigation goes on, with Judge Cassuto alternating among the threads as resources and scheduling allows.

In the doping lab case, Mr. Dominguez, who has been described in the French media as a photographer with links to French intelligence, told investigators that he had acted only as a middleman, passing on the data he received from Kargus to another man, who has not been located.

Judge Cassuto summoned Mr. Landis and Mr. Baker to Paris in May for questioning, but neither appeared for the hearing.

The judge has the power to issue international arrest warrants for both men, although he has not indicated yet whether he intends to do so.

Mr. Landis did not respond to requests for comment through Team Ouch, his new cycle-racing squad.

But he told Cycling News in November 2006, when rumors of the computer hacking first surfaced, that "any claims attributing these actions to me or my defense team are baseless, untrue, irresponsible and another example of the character assassination that I have faced since the initial allegations surfaced."

In an e-mail message, Mr. Baker denied any involvement in hacking into the drug lab's computer, or in hiring anyone to hack into it. "If the L.N.D.D. computer system was hacked, I do not know who did this," he wrote, referring to the drug-testing lab, Le Laboratoire National de Dépistage du Dopage.

In the case of Mr. Canoy, the shareholder activist, investigators raided the office of Jean-François Dubos, Vivendi's general counsel, in June. Antoine Lefort, a spokesman for Vivendi, confirmed that Mr. Dubos "has been heard as a witness and his office was searched." But he said that neither Mr. Dubos, who has not been placed under formal investigation, nor the company had sought to hack into Mr. Canoy's computer.

Since 2002, Vivendi has fought 13 different lawsuits brought by Mr. Canoy, and filed two countersuits against him, Mr. Lefort said.

Mr. Canoy said the hackers stole data about his finances and even his family. "My son has a rock band, and everything including his songs and poems was stolen," he said. "It is a complete violation of my personal and professional privacy."

Mr. Harbulot, the expert on economic intelligence, said the most curious thing about the whole case to him was why a company like E.D.F. would get involved with "these kinds of people" in the first place.

"All of E.D.F.'s security needs should be taken care of by the state, because it's strategically important," he said.

Still, hackers like Mr. Quiros seem to be proliferating, he said, estimating there were "a few dozen" in France alone. "Not that he was very expert," Mr. Harbulot said. "Like most hackers, he was undone by some really stupid blunders."