

FOREIGN HACKERS IMMUNE FROM UK JUSTICE

Source: The Times On-Line

A case involving two Russian companies accused of hacking into a London computer system can be heard in English courts, a High Court judge has ruled. The allegations make for an exciting story of corporate espionage in the internet age, but the case serves as a reminder that, even today, cross-border lawsuits are anything but point-and-click operations.

The bitter dispute ranges across a number of cases and jurisdictions. It involves three companies: TadAz, a state-owned company in Tajikstan; Rusal, a the Russian company that happens to be the third biggest aluminium producer in the world; and Ansol, a company based in Guernsey.

Ansol and its UK advisors, Ashton, claim that Rusal and TadAZ stole its business assisting Tajikstan in producing aluminium.

Ashton's computer system in London was broken into from an internet address belonging to Rusal, as well as from a number of other addresses, including many in Russia. Ashton and Ansol claim that Rusal is behind the digital break-ins, and that it was trying to obtain information that would be of use in the court battles. Rusal denies accessing Ashton's system and says that the IP address could have been used by someone outside of the company via the firm's Wi-Fi network, which at that time was not secure.

Rusal's legal team argued that there was no serious case to be tried because the claim that a Rusal employee had hacked into the system could not be sustained. In order for the court to try the case, there must be a "serious case".

Jonathan Hirst, QC, sitting as a deputy judge of the High Court, disagreed. He said: "The Claimants are making extremely serious allegations against the Defendants, involving conduct which would be criminal under sections 1 and 2 of the Computer Misuse Act 1990, and which would constitute an outrageous attempt to gain access to privileged information held by the other party to litigation, and will have to produce commensurate proof," he wrote. "I am satisfied that the Claimants have shown that there is a serious issue to be tried. They have done more than just scrape over the hurdle."

A crucial question for the court was whether the acts took place in England or Russia, and therefore whose law and jurisdiction applies. Mr Hirst said that the actions did take place in England.

"Ashton's computer server was in London. That is where the confidential and privileged information was stored," he said. "The attack emanated from Russia but it was directed at the server in London and that is where the hacking occurred. The fact that it was transmitted almost instantly to Russia does not mean that the damage occurred only in Russia. If a thief steals a confidential letter in London but does not read it until he is abroad, damage surely occurs in London."

"I also consider that substantial and efficacious acts occurred in London, as well as Russia. That is where the hacking occurred and access to the server was achieved. This may have been as a result of actions taken in Russia but they were designed to make things happen in London, and they did so," wrote Hirst.

"Effectively the safe was opened from afar so that its contents could be removed. It would be artificial to say that the acts occurred only in Russia. On the contrary, substantial and effective acts occurred in London."

So Mr Hirst said the English court is the right venue for the case. This is consistent with other cross-border internet disputes. I've no idea what will happen in this case, but generally when courts rule in civil cases against companies based overseas, enforcement is at best inconvenient, at worst impossible. Our network of international treaties — and their application in practice — could really do with an upgrade.