The Australian Financial Review
Thursday 14 February 2008 • www.afr.com

The murky world of pay TV pirates

A missing hard drive is the key to a $1 billion industrial espionage case, writes **Neil Chenoweth**.

Former Scotland Yard commander Ray Adams slipped from public view with barely a murmur. A single paragraph in a British newspaper in June 2002 recorded that the former policeman had stepped down a month before from his job as NDS Group's head of operational security for Europe.

NDS, a News Corp subsidiary which has its head office in England but is in effect based in Israel, makes the smartcards that encrypt and secure News Corp's global satellite network. Adams's job was to police the murky world of hackers and counterfeiters who produce forged smartcards that defraud pay TV networks around the world of more than $US5 billion ($5.5 billion) each year.

This secret world had hit the headlines in March 2002, when French media group Canal Plus launched a $US1 billion lawsuit accusing NDS of industrial sabotage — hacking the Canal Plus smartcards and posting their source codes on a Canadian piracy site.

It was the start of a welter of accusations from satellite broadcasters around the world complaining of NDS actions — EchoStar and DirecTV in the US, Sogecable in Spain, ITV Digital in Britain and Astro in Malaysia — from which NDS would eventually emerge unscathed and undiminished.

If few remarked on Adams's departure in May 2002 during the hullabaloo, no one noticed a minor incident involving his vehicle. According to NDS, someone broke into the family car that month and stole the hard drive from his laptop. The hard drive contained some 26,000 pages of confidential NDS documents, including hundreds of pages of internal NDS emails detailing the activities of its covert operations group.

In a global hunt to retrieve the documents, NDS lawyers appeared in a Vancouver court last September, where they claimed the hard drive had been obtained by Plamen Donev, a Bulgarian hacker who had been on the NDS payroll. He had passed copies of the documents to Canadian satellite pirates on two CDs.

The Vancouver hearing was just an outlying skirmish related to a much larger case due to go to trial in April in the California District Court, where EchoStar (and its smartcard provider, NagraStar Corp) is claiming $US1 billion damages against NDS for industrial espionage in a trial.

The EchoStar lawsuit quotes extensively from an explosive series of NDS emails that NDS says came from the missing hard drive. EchoStar says it obtained the emails from a range of sources.

The issue of source seems beside the point. The bottom line is that on NDS's own account, the innermost secrets of its undercover ops are on CDs being hawked around the world in a boxed set.

How did it come to this? And what do the emails say?

One answer is to follow the money. Satellite piracy is the perfect cash business. It has similar profit margins to the drug-running industry and sometimes runs alongside it to launder drug money.

There are up to three stages in hacking a smartcard. It begins with tracing the circuitry of the microprocessor on the card layer by layer, with a combination of electron microscope photography, acid etching, micro probes and ion beams. The circuitry plans allow the discovery of the card's source codes. Finally, a hacker finds a backdoor around the software to unlock the card.

Once that is done, a pirate can mass-produce his own forged cards offering free access to pay TV. Selling 100,000 cards can raise $10 million or more. It costs the broadcaster five times as much in lost revenue.

Hacking is a nerd's game, for programmers and the tech-savvy. But as a business it is a shadowy world associated with big money, deception, drugs, violence and sex.

What would a satellite company or its security provider be prepared to do to stop the billion-dollar money drain from piracy? The question is central to EchoStar's damages case against NDS in California.

NDS says EchoStar has concocted a far-fetched international conspiracy based on ''inadmissible hearsay and unauthenticated documents awash in attributes that highlight their unreliability, evidence of activities by third parties in Canada outside the statute of limitations, and legal anti-piracy activities undertaken by NDS''.

''Given the supposed scale, scope and at least five-year duration of the alleged distribution network, the complete absence of physical evidence or testimony from any even somewhat reputable source is truly remarkable,'' NDS lawyers argued in a submission to judge David Carter last week.

Its lawyers told the court no one at NDS was able to authenticate the documents quoted by EchoStar, which they said were ''highly suspicious''. NDS and News Corp did not reply to written questions from *The Australian Financial Review* this week.

The roots of the dispute date from 1996, when DirecTV and BSkyB faced a wave of piracy of their NDS smartcards.

NDS appointed Reuven Hasak, a former deputy head of Israel's formidable internal security force, Shin Bet, to beef up its security. Hasak's role has led to ongoing speculation over possible links to Mossad.

For the US operations, Hasak headhunted former naval counter-intelligence officer John Norris from cable-box builder General Instruments, where he had been running elaborate stings to trap pirates. In Britain, Hasak hired Adams.

The NDS team soon made its presence felt. In June 1996, police in the US, Canada, Bermuda and Cayman Islands staged simultaneous raids against suspected pirates and DirecTV launched civil actions against 22 people, including high-profile Canadian pirates such as Norman Dick and Gary Tocholke in British Columbia, and Ron Ereiser in Saskatchewan.

With the pirate networks in disarray, Ereiser hired a young American hacker called Chris Tarnovsky to reprogram the pirates' existing ''battery'' smartcards.

Tarnovsky, who used the nickname ''Biggun'', had become a hacker while in Germany with the US Army, working with a group of hacker enthusiasts called TVCrypt, founded by German university student Markus Kuhn.

NDS now targeted Ereiser. In an affidavit in EchoStar's Californian court case, Ereiser says Norris told him NDS and DirecTV would drop charges against him and allow him to continue hacking DirecTV if he testified against Norman Dick. He says Norris also tried to persuade him to hack EchoStar. Norris denies this.

Ereiser's affidavit says he has seen a video tape of Norris and Hasak meeting Tocholke at an outdoor restaurant where they ''unequivocally threatened Tocholke [that] in the event that NDS ever caught him in Mexico again, they would apprehend him, bind him, put him in the trunk of a vehicle and haul him across the border''.

They also said that it does not seem possible that a commercial company would take such drastic steps just to save its product. (Yossi said: 'There's a limit to how far I will stretch my neck out for Rupert Murdoch.')

Ereiser also claims to have heard a tape of Norris offering $25,000 — with advice on how to evade any tax — to the secretary of another Canadian pirate, Herb Huddleston, if she copied Huddleston's computer files.

NDS has denied all of Ereiser's claims.

In mid-1997, as DirecTV switched to a second generation of NDS smartcards called P2, the pirates counter-attacked. EchoStar says Tarnovsky introduced Ereiser and Huddleston to two Bulgarian ex-military hackers, Plamen Donev and Vesselin Nedeltchev, who agreed to reverse-engineer the P2 cards.

According to a later court case, the two Bulgarians flew to Manitoba on July 14 before they were given forged papers and smuggled over the US border into Montana. They used an electron microscope at the University of Montana to extract a detailed map of the H2 circuitry, before analysing the source code in Cayman Islands.

Ereiser says the codes were turned over to Tarnovsky who had found a ''back door'' into the H2 card within a week. By the time DirecTV completed its card swapover, the new cards had been hacked.

The remarkable thing is that Tarnovsky had been working for NDS since at least early 1997. While the moves appear part of an elaborate scheme to trap pirates, DirecTV allegedly was not always informed.

In fact Tarnovsky was part of a two-pronged strategy. In Europe, NDS had hired celebrated hacker Oliver Kommerling (code-named Alex), but neither Tarnovsky nor DirecTV knew this, according to NDS internal correspondence cited in the EchoStar case.

To hide its links to Kommerling, EchoStar says NDS sent equipment to him in several parts to different addresses in Germany, which he then reassembled.

Meanwhile NDS had moved Tarnovsky to California, though he would pretend when online to be living in the east. In late 1997 Norris described Tarnovsky to DirecTV security chief Larry Rissler as an NDS consultant called ''Mike''. In a December 1 email to Adams, Norris referred to placing Tarnovsky in Ereiser's pirate group with NDS's support, and said Tarnovsky had concerns about NDS protecting him.

Another Canadian pirate, Marty Mullen, says in an affidavit in the EchoStar case that at this time he was obtaining updates from a European hacker with a German accent who used the name Lorenzo Palma, who Mullen says was able to provide fixes for DirecTV electronic counter measures (ECMs) before they happened.

Around December 1997, Mullen says he became aware that Palma was an NDS employee when Palma called to warn him that DirecTV was about to release an ECM. Mullen says that although Palma attempted to cover the phone, in the background he could hear a loudspeaker announcement, ''Would all NDS employees report to the boardroom''.

NDS says Mullen is an unreliable witness who has an axe to grind because NDS tipped off US authorities when he made a secret trip to Florida in June 2003, resulting in a seven-year prison sentence.

Meanwhile NDS was working on a new project. An NDS executive wrote on July 11, 1997, in internal correspondence tabled in court by EchoStar: ''Why not for example, let Alex [Kommerling] and Mike [Tarnovsky] run together on this one. Why separate them? I am prepared to let JN [John Norris] run the operation.

''. . . For some time there has been speculation about Kommerling and the fact that he is no longer acting with the pirates. His withdrawal from the USA scene will serve to confirm the suspicions. He is supposed to be a pirate and should therefore act like one . . . In one simple move we would get the operation moving and protect Kommerling from exposure . . . he [Swiss hacker and security consultant Jan Saggieri] knows that Kommerling is with NDS.''

It's not clear what the new project was. But in August 1997, EchoStar claims in its lawsuit, Kommerling contacted Mullen and told him that ''he would soon be in possession of EchoStar's ROM code that was being extracted in Europe''. Mullen has phone records showing he made a 50-minute return call to Kommerling's mobile on August 23, 1997.

EchoStar and NagraStar say their problems began in May 1997, when Rupert Murdoch walked away from an agreement with EchoStar founder Charlie Ergen to merge their US satellite interests. They quarrelled over which conditional access system to use.

Murdoch was insistent that NDS was more secure while Ergen preferred the Nagra cards made by Swiss firm Kudelski. To prove his point, Ergen reportedly used a pirated smartcard to play a DirecTV program during a meeting with Murdoch. The merger talk ended acrimoniously and EchoStar sued News for $US5 billion damages.

Whatever the reason, by mid-1997 Kommerling had set up a high-tech laboratory for NDS in Israel in Building No. 20 in the MATAM Advanced Technology Center in Haifa, one of only six such laboratories in the world.

Kommerling worked with NDS's chief technical officer, Yossi Tsuria, who had his own colourful history — he took up technology

His withdrawal from the USA scene will serve to confirm the suspicions. He is supposed to be a pirate and should therefore act like one . . . In one simple move we would get the operation moving.