

Dies ist der [Zwischenspeicher](#) von [Google](#) für <http://www.globes.co.il/DocsEn/did=376767.htm> nach dem Stand vom 31. März 2005 06:18:20 GMT.

[Google](#)s Cache enthält einen Schnappschuss der Webseite, der während des Webdurchgangs aufgenommenen wurde.

Unter Umständen wurde die Seite inzwischen verändert. Klicken Sie hier, um zur [aktuellen Seite](#) ohne Hervorhebungen zu gelangen.

Diese Seite im Cache bezieht sich eventuell auf Bilder, die nicht länger zur Verfügung stehen. Klicken Sie hier, um nur den [Text im Cache](#) anzuzeigen.

Um einen Link oder ein Bookmark zu dieser Seite herzustellen, benutzen Sie bitte die folgende URL:

[http://www.google.com/search?q=cache:a_wX6rz-](http://www.google.com/search?q=cache:a_wX6rz-ywsJ:www.globes.co.il/DocsEn/did%3D376767.htm+%22ray+adams%22+scotland+yard&hl=de)

[ywsJ:www.globes.co.il/DocsEn/did%3D376767.htm+%22ray+adams%22+scotland+yard&hl=de](http://www.google.com/search?q=cache:a_wX6rz-ywsJ:www.globes.co.il/DocsEn/did%3D376767.htm+%22ray+adams%22+scotland+yard&hl=de)

Google steht zu den Verfassern dieser Seite in keiner Beziehung.

Diese Suchbegriffe wurden hervorgehoben: **ray adams scotland yard**

[Market prices](#)

[Site map](#)

[Newsletters](#)

[Israel links](#)

[About us](#)

[Support](#)

[Advertise](#)

[Archive](#)

עברית



Freertext

Search in



Sunday January 15, 106

Israel

18:35

New York

11:35

Hacker Hunter

After years with the General Security Service, its only natural for Reuven Hazak to have ended up in NDS, which wages electronic warfare on pirates and hackers throughout the world.

Ronny Lifschitz 25 Jul 99 17:57

When it comes to intelligence, Reuven Hazak has considerable experience. He served many years in the General Security Service (GSS), holding the post of deputy GSS head until 1985, when he resigned over the Bus 300 affair, which badly rocked the organization. Hazak then proceeded to set up security company Shafran. Four years ago, Shafran seconded Hazak to NDS, to provide NDS with an active security umbrella.

NDS sells security products: encryption cards enabling television companies (via satellite or over cable) to provide pay television services. "But were also providing them with an active security service that is based on the assumption that any security product can be broken into. Its only a question of when. Even if we take the best protected spot in the world, Fort Knox, where all US gold is stored - if someone takes the time and makes the effort, he will succeed in breaking into it. In order to protect Fort Knox, you must have an active and aggressive security system," says Hazak.

The phrase "active security umbrella" conceals a 17-member organization run from its Jerusalem headquarters. Sub-units operate in various parts of the world. The British unit, based in Heathrow, is led by former **Scotland Yard** deputy chief **Ray Adams**, and the US unit, based in Los Angeles, is headed by John Norris, a former high-ranking US Naval Intelligence officer.

"Globes": What is, in fact, active security?

Reuven Hazak: "We protect NDSs secrets from pirates and competitors. We look out for pirates, track them down, and handle them through recourse to the law, disinformation, manipulation of the demand curve, and other methods. For instance, NDS is the only company in the world with an updated data base on pirates and hackers, the connection between them, and their capabilities.

"The problem is that, nearly everywhere in the world, law enforcement arms have neither the means nor the motivation to fight white collar crime. To overcome this problem, we provide them with all the necessary information. Our role is to furnish them with the information. They take care of the rest."

If intelligence and prevention activities have taken place abroad so far, this "idyllic" situation is apparently about to change soon. "I believe piracy problems will soon surface in Israel as well," Hazak estimates, in view of recent statements by Matav and DBS Satellite Services.

It was recently reported that NDS will provide Matav with a comprehensive system for digital transmission over Matavs cable infrastructure. Under the \$7 million project, NDS will supply the digital infrastructure for cable broadcasts, and Korean company Sansung will furnish the terminal units through which subscribers will be able to receive the new services. DBS Satellite Services also plans to use NDSs encrypted card, which enables the decoding and reception of dozens of television channels in the home.



When are Israeli pirates expected to get going?

"I expect a problem in Israel, just as we have cable broadcasts piracy at present. I've no doubt it's going to be a hot issue. There are also some figures to corroborate this assumption. For instance, as long as there are only 50,000 subscribers, it's not worth while to counterfeit a card. But when it comes to a market of 250,000 subscribers, it's worth it. In some countries, it's worth while to manufacture counterfeit cards only when the market reaches the half million figure.

"Generally speaking, it's better for the pirate to be present in the market before the card is out. That's the ideal. This is why pirates will try to break into NDS and ferret out its secrets. NDS currently employs more than 1,000 staff at its production plant and in various offices throughout the world. The development center at Har Hotzvim employs 400 people. That's also why NDS is a highly protected place.

"It's possible to get hold of secrets at the production stage. Much of the production is done by large sub-contractors whose identity is also kept under wraps. We get them to comply with security regulations that bar pirates from access to the secrets with which we entrust sub-contractors."

How do you discover that a certain card is counterfeit?

"Someone sells the counterfeit card, which is why it leaves a trace. We track down ads on the Internet, and sometimes even in the printed press. But my goal is to unearth hacker activity before the hackers go out into the market. In most cases we know when an operational plan for card breaking is being cooked up."

And what happens after a counterfeit card has already been distributed and sold on the market?

"The minute a code-broken card hits the market, it can be killed with electronic counter-measures. The engineers know how to take it out of action with a death ray - a special signal transmitted from a satellite. But to do that they need technological intelligence from the field that makes it possible to assess the number of cards and their geographic deployment. Usually this is done at peak-viewing time, in order to hit as many counterfeit cards as possible and hassle illegal customers. There's also a technology for destroying fake cable television cards, but it's still in the bud."

Do pirates and hackers have ties with the underworld?

"Up to two years ago, the market was strictly local, but it has recently gone international. For instance, we tracked down East European hackers who were shipped to North America to provide piracy services. We know that drug dealer groups in America launder their money by financing pirates. In this way they reduce the gravity of the offense for which they may be charged. We unearthed such an organization in Mexico, and we immediately notified the US authorities."

Is your method also effective for information systems protection?

"The common denominator in both cases is that, in order to provide a security system, you can't confine yourself to the product only. The product requires baby-sitting. Someone has to watch over it, and it's clear that this philosophy applies to the whole of the high tech world that is involved with protected products. In the last three years, none of our products in Europe has been broken into. Our current product in the US has been broken into, but the measures we're taking prevent the tampered-with card from turning into a widely distributed commercial product on the market. The pirates know us. We're not hiding away. The fight we're waging has an economic impact in the sense that some pirates are wary of messing with us, and attack our competitors instead."

Reuven Hazak admits he prefers to work from home. He reluctantly goes abroad when it's a must. In his spare time, he likes to live among the statues he sculpts and the objects he fished out from the sea-bed, and to listen to classical music. He is particularly fond of a mechanical piano linked up to a computer. It's a piano to all intents and purposes, whose keys are operated by software. You put in a jazz disk, and the piano gives a performance for you alone. You insert a disk with the performance of a celebrated pianist, and all of a sudden you have a virtuoso giving you a private concert at home. And it all sounds genuine enough. Not - perish the thought - like some pirated or counterfeit copy.

Published by Israel's Business Arena July 22, 1999

[Save article](#)[Send to a friend](#)[Print article](#)[Home](#)[Back to top](#)

