mybroadband.co.za

The South African who helped end apartheid with encryption and inspired a Hollywood movie

7–9 minutes

Former political prisoner and old-school hacker Tim Jenkin co-developed and built an encrypted electronic communications network in the 1980s that became a vital instrument in ending apartheid.

Years earlier, Jenkin and two other inmates had escaped from Pretoria Central Prison by reverse-engineering the keys of ten separate doors (and some extras) from wood.

Jenkin and university friend Stephen Lee landed in jail after joining the ANC in 1974 and setting off pamphlet bombs with anti-apartheid messaging in Cape Town between 1975 and 1978.

Former ANC spymaster Ronnie Kasrils said in the documentary *The Vula Connection* that Jenkin held the record for detonating 18 or 19 leaflet bombs in the Cape Town city centre in one day.

He said Jenkin and Lee weren't the usual intellectual types who joined the ANC as students. They combined brains with industriousness.

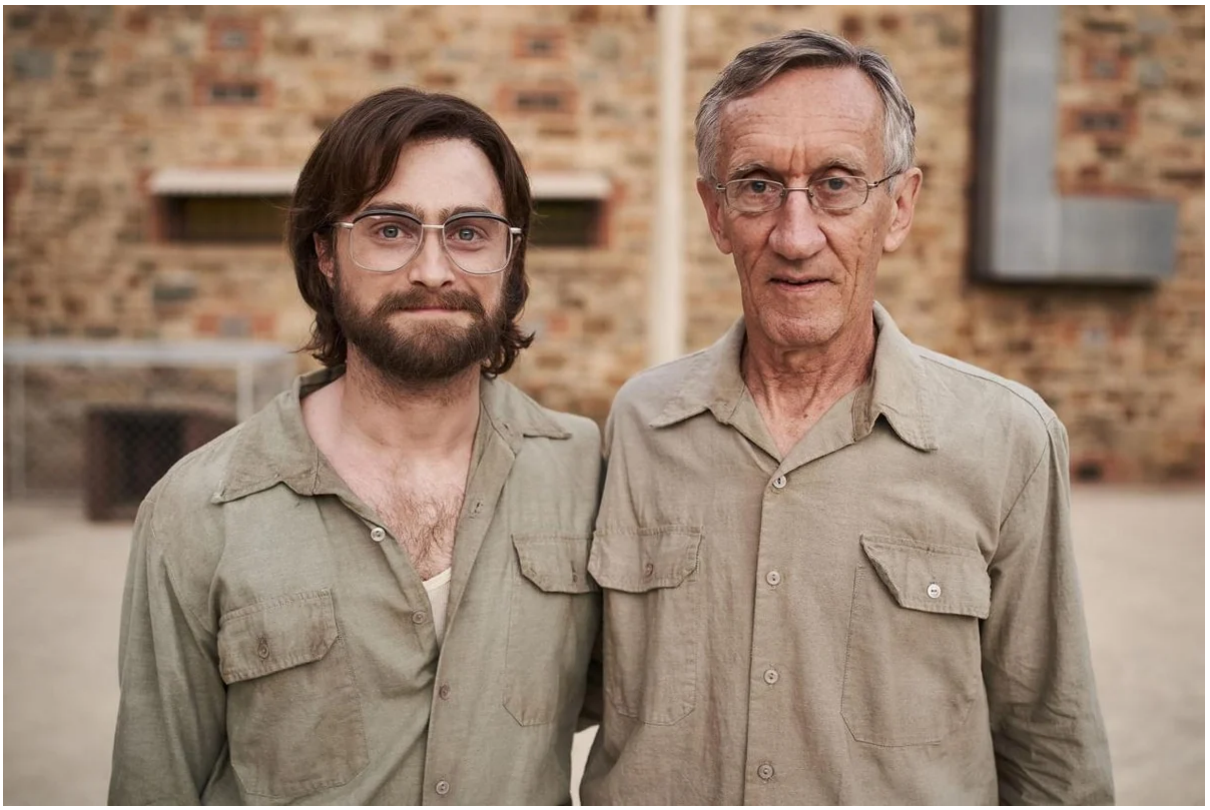
Jenkin had the extra advantage of being unassuming and almost withdrawn. "Which is exactly what you want," Kasrils added.

Unfortunately, the security police soon had the pair under surveillance. They were arrested at 03:00 on 2 March 1978 while moving their printing equipment.

Under legal advice, they pleaded guilty to all charges. Jenkin was

sentenced to twelve years in prison and Lee to eight.

Within 18 months, they had broken out. The caper became the subject of the 2020 film *Escape from Pretoria*, with Harry Potter star Daniel Radcliffe portraying Jenkin.



Daniel Radcliffe (left) with Tim Jenkin (right) during filming of *Escape From Pretoria*

By early 1980, Jenkin had relocated to London and was assigned to training operatives in the encryption techniques they needed in the field.

The ANC used a simple but effective paper-based one-time pad system for cryptography, which Jenkin trained recruits in.

One-time pad relies on single-use keys that must be pre-generated and issued to a group of communicating parties.

As messages are encrypted and decrypted, the keys are consumed and should not to be reused.

While the encryption itself is uncrackable, provided keys are properly randomly generated, one-time pad systems have several other vulnerabilities.

If an adversary gets their hands on the pre-generated keys and are able to intercept every message from then on, they can decrypt

them.

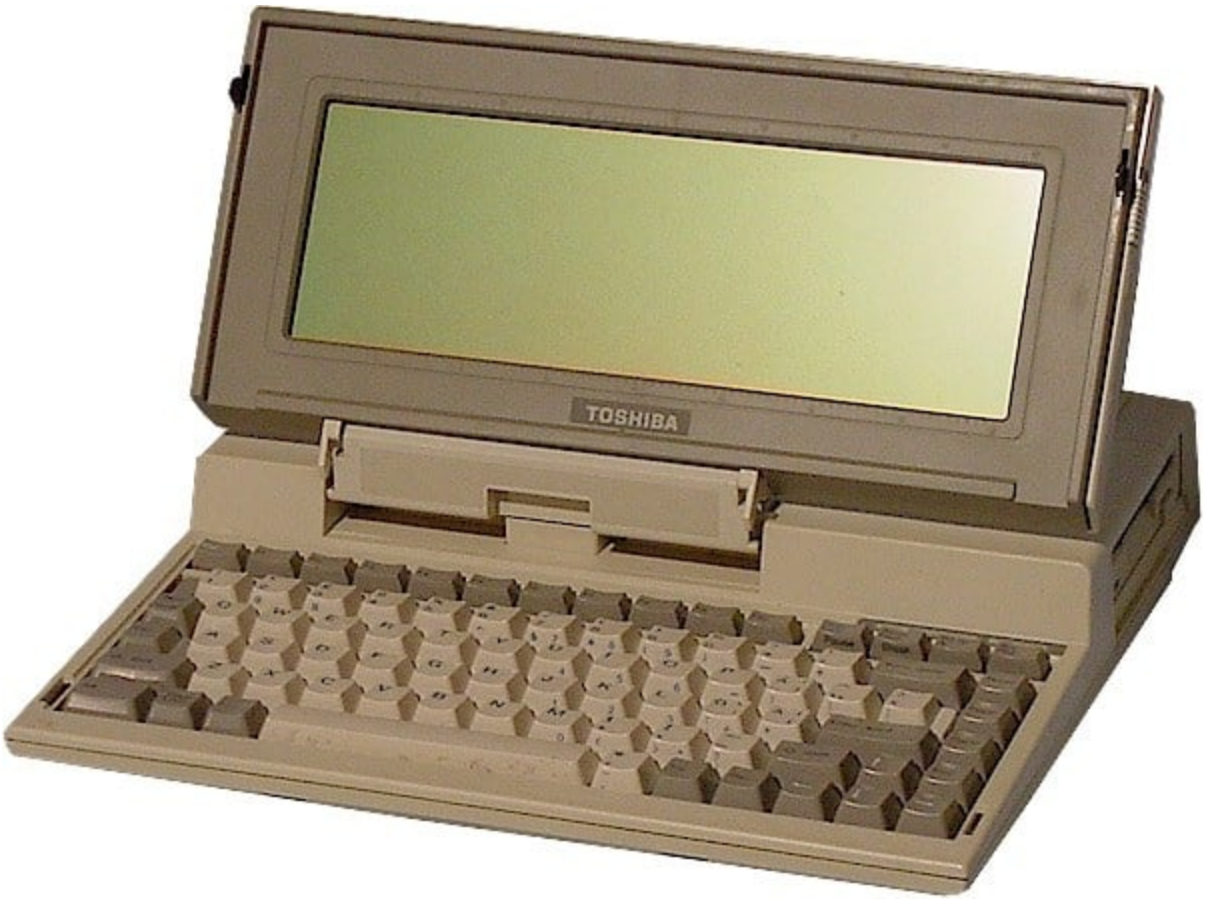
Operatives must also adhere to strict operational security protocols, such as destroying decrypted messages, old key pages, and old enciphered messages.

However, the main problem, Jenkin found, was that encryption and decryption was laborious.

“It took so much effort to say so very little and the responses, as few and far between as they were, contained little encouragement and advice,” he said.

“There were only instructions which usually lacked any connection with the reality they were experiencing.”

This quickly demoralised new operatives, and Jenkin said he could see their enthusiasm and activity rapidly die.



Toshiba T1000, personal computer of the revolution

In the early eighties, computers were getting cheaper, and Jenkin believed a program to automate the cryptography could solve their communications problem.

Together with new partner-in-crime Ronnie Press, they began work

on a system that would eventually become a fully-fledged underground electronic communications network.

“Off to the bookshops and libraries I went to find out about secure encryption algorithms,” Jenkin said.

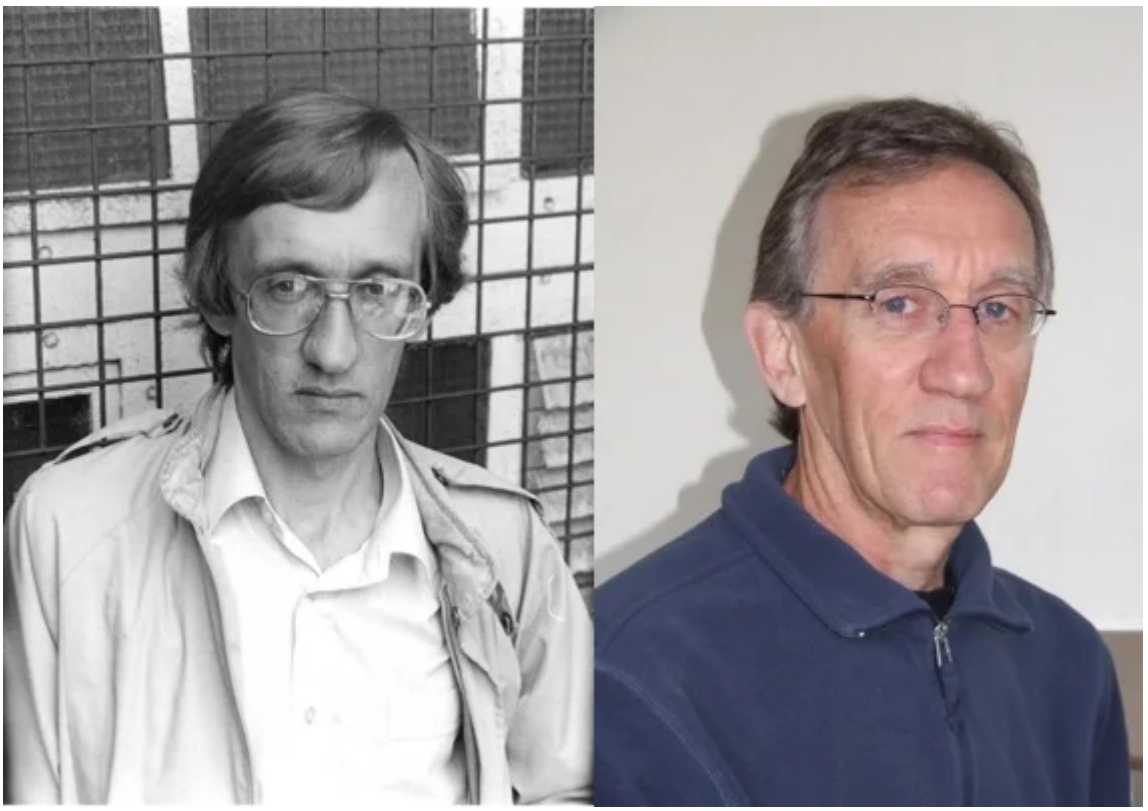
“Nothing impressed me very much and all I discovered was that cryptology was an arcane science for bored mathematicians, not for underground activists.”

While he did learn a few tricks they could use, he decided to keep it simple and digitise their existing one-time pad system.

Although their cryptography would remain simple, the whole communications system ended up having a lot more moving parts than just the software, as most of the Internet did not yet exist.

To transmit encrypted messages, they were encoded into a signal that could be played over a regular telephone call and recorded. This was to allow operatives to easily receive messages via public telephones.

The recorded message could then be played back into a computer via a modem and decrypted.



Tim Jenkin — then and now

However, keys had to be distributed to the two communicating

parties to encrypt or decrypt messages.

For this, Jenkin wrote random data to 1.44MB “stiffy” disks. These keys and the encryption program itself then had to be delivered to operatives in the field.

Enter Conny Braam, head of the Dutch anti-apartheid movement, who found a KLM air hostess sympathetic to their cause.

The hostess, Antoinette Vogelsang, helped smuggle the computers, disks, and other equipment ANC operatives in South Africa needed.

Vogelsang’s role was critical if the system was going to work. Had she provided copies of the disks to the South African authorities, the whole endeavour would have been compromised.

With everything in place, the ANC kicked off Operation Vula.

They infiltrated key leaders like Mac Maharaj, Siphiwe Nyanda, and Charles Nqakula back into South Africa with the ability to communicate with one another and the ANC headquarters in exile. Kasrils would later join them.

In 1989, the system and Operation Vula would achieve its greatest victory — re-establishing secure communications between Nelson Mandela in South Africa and ANC president Oliver Tambo in Lusaka, Zambia.

Mandela had been transferred to house arrest as part of negotiations to transition to a democratic South Africa.

However, the apartheid government kept Mandela isolated from the rest of the ANC in the hopes of securing more favourable terms by creating the impression they were negotiating solely with him.

While it was not possible to smuggle a computer and disks to Mandela, messages were relayed in the covers of books.

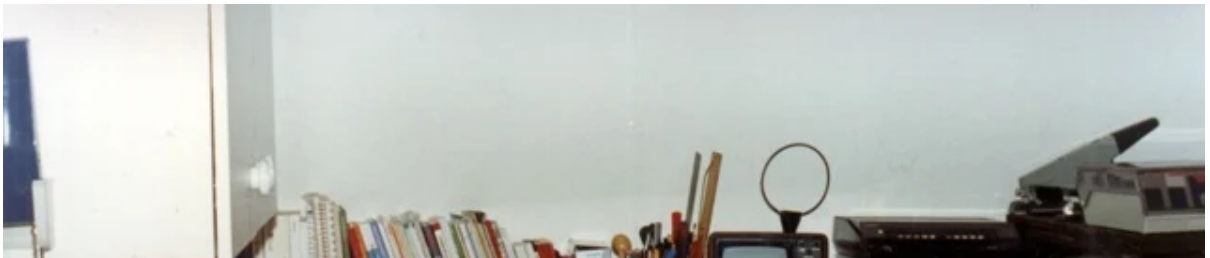
Mandela’s replies could then be smuggled out, encrypted using the software, and transmitted to Tambo in Lusaka.

“Messages from Mandela became a regular feature and in

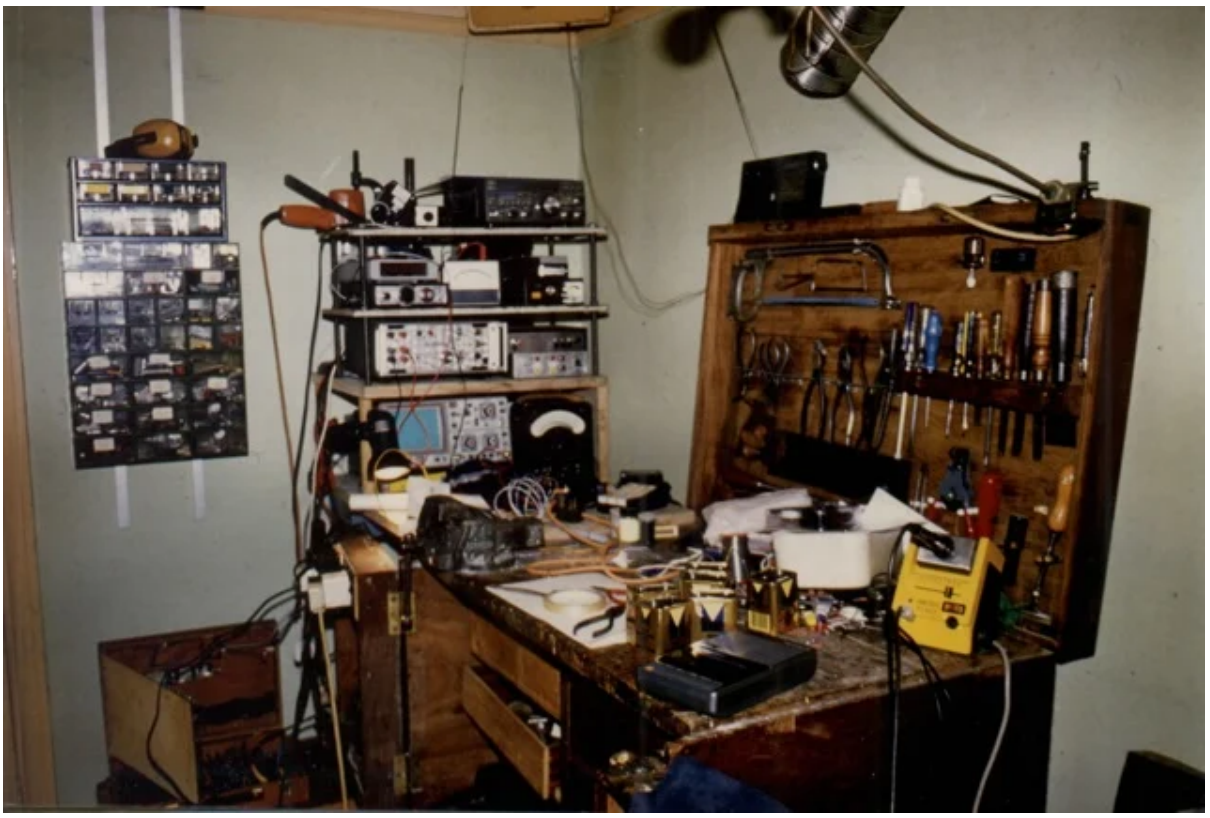
response there were long memos from Oliver Tambo in Lusaka," said Jenkin.

"The two were now talking in confidence for the first time since the early 60s."

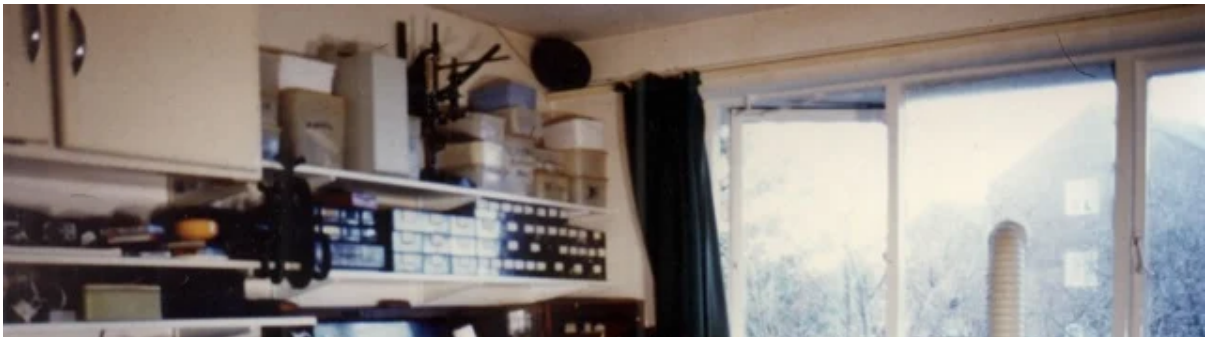
Another view of the ANC's ICT headquarters, nicknamed "GCHQ". Not visible in the scale image are various antennas sprouting from the roof. One of these was for a high-powered cellphone, used for sending and receiving messages via an electronic answering service ("voice bank") instead of answering machines. There were three phone lines in the flat: one for personal use, one for incoming Vula messages, and one for outgoing Vula messages. Adding more phone lines would have looked suspicious, so additional phone lines were installed at sympathisers' homes nearby. These were connected by (illegal) high-powered cordless phones. Aerials on the roof had line-of-sight with those at the other peoples' homes, so the reception was really good. Sophisticated commercial answering machines were installed that could be controlled remotely via the handsets in "GCHQ".

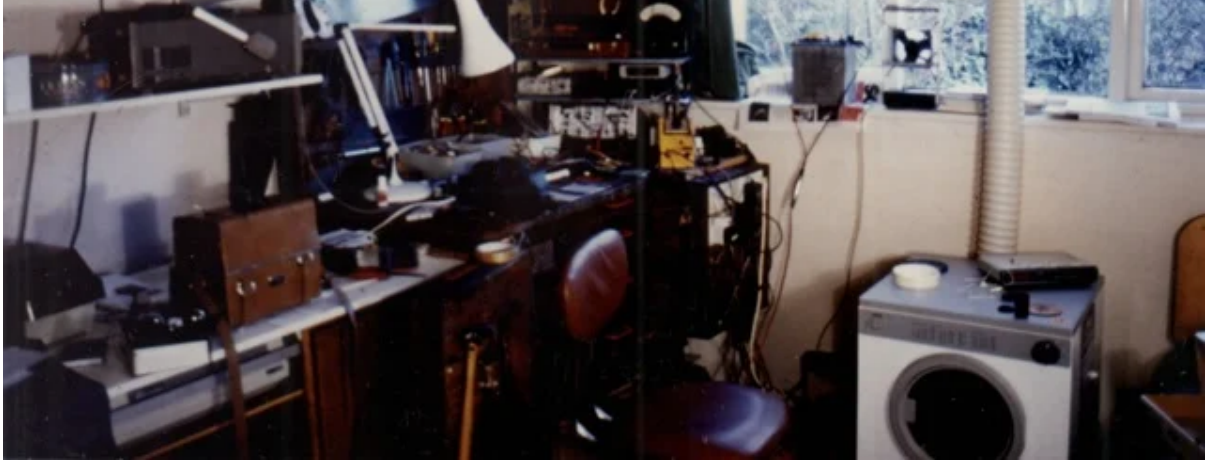


Operation Vula control centre at Ronnie Press' place. In the middle is the main Toshiba T3100 computer. Mounted on the wall are a pair of the incoming and outgoing answering machines. The acoustic modem is the white box under the bottom shelf behind the computer. On the first shelf at left are various radios used to communicate in London. In front, just to the right of the chair, is a home-made acoustic coupler attached to a mobile phone handpiece.

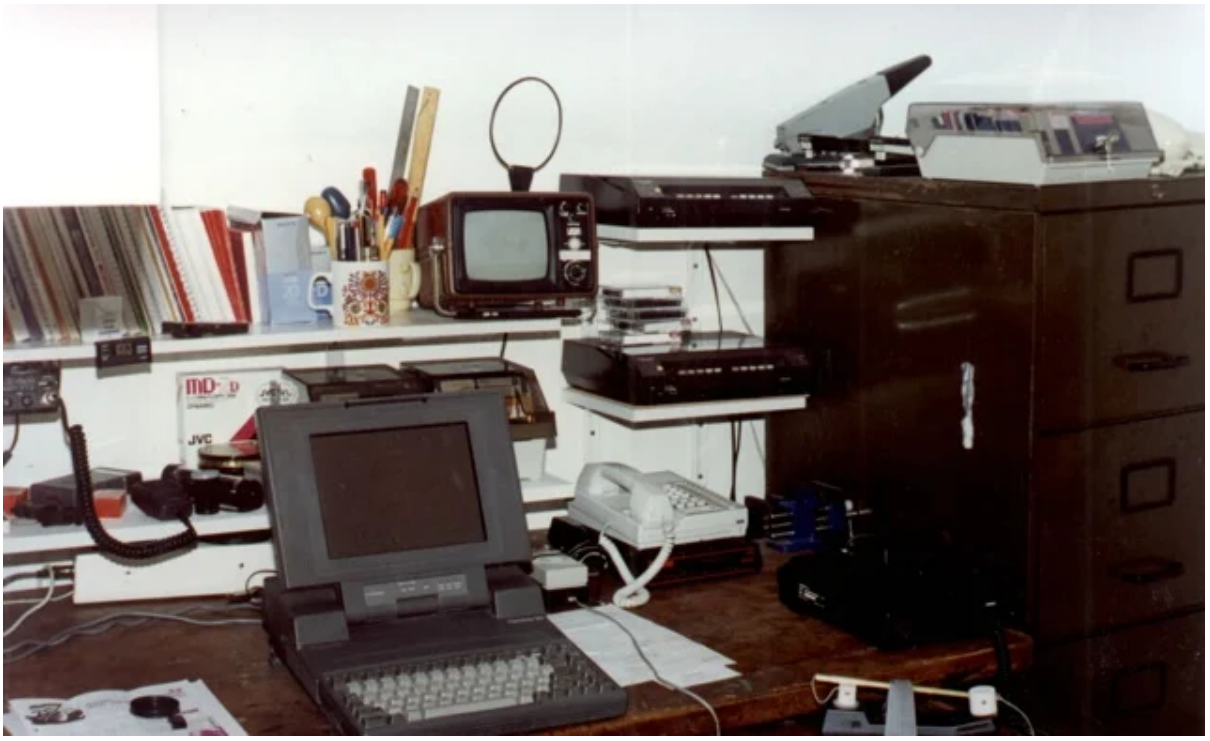


Operation Vula workshop

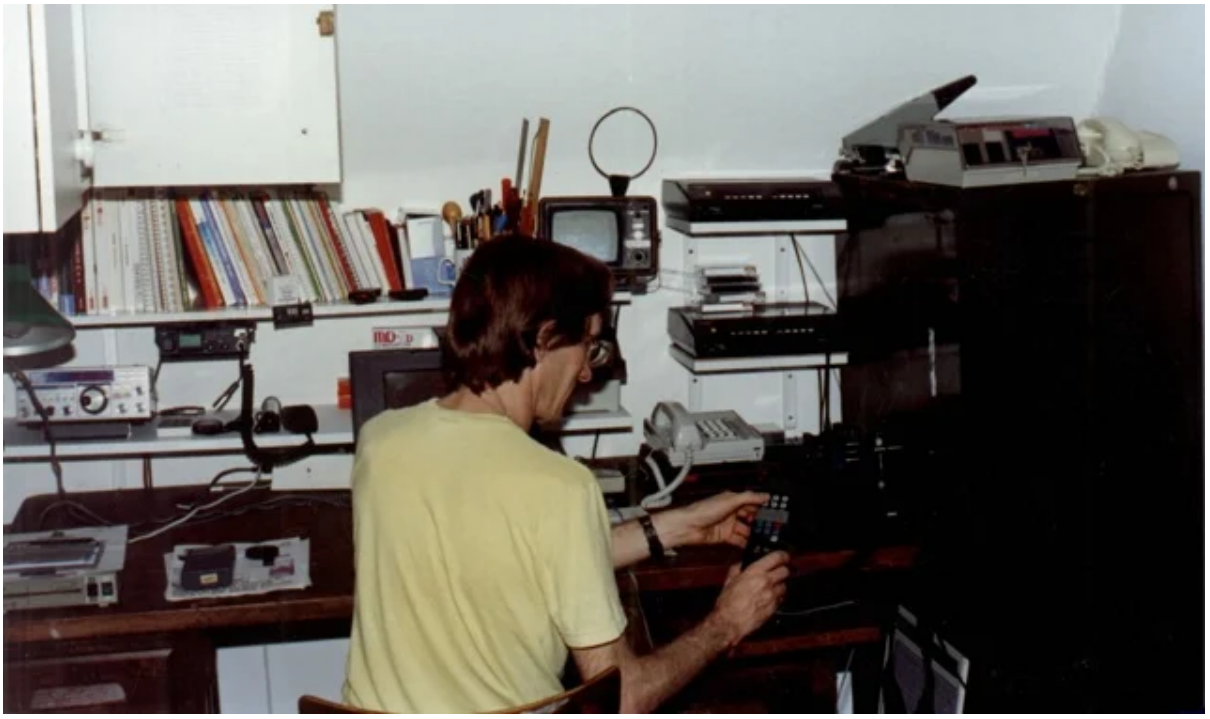




Operation Vula workshop



Close up view of the equipment



Tim Jenkin at his workstation in London