JUNE 1988

COMMODORE USER

£1.10

No1 For AMIGA GAMES

250 pta ■ HFL 5.90 ■ DM 5.50

GREAT GIANA SISTERS

❤ LOVE AT FIRST SIGHT

WIN A TRIP TO GERMANY

CYBERNOID MAPPED

REVIEWED: DREAM WARRIOR, INFILTRATOR II, HOPPIN' MAD, GAMES WINTER EDITION

FREE PULL-OUT POSTER

AMIGA PULL-OUT: WIZBALL
FA/18 INTERCEPTOR · GARRISON II

PIRACY

HACKING AT THE INDUSTRY'S ROOTS

by Mike Pattenden

'Europe is open for business in 1992.' That's what everyone from Margaret Thatcher to Alan Sugar is telling us at the moment. But try telling that to the network of hackers throughtout Europe. They've been trading cracked games and demos for *years*.

Once a month, maybe more, gangs of hackers meet up at a preset venue armed with blank disks which they use to copy every new release available on the circuit. Last month in Venlo, Holland you could have picked up *Street Sports Soccer, Aaargh!* and *Super Hang On*. That's pretty impressive when the first two are as yet unreleased and *Super Hang On* has been shelved.

Copy parties are simply the international gatherings for the crews and their friends to get together and swap ideas and games. Behind these occasions lies an organised hacking network of such technical ability and resourcefulness that the software industry is at a loss to stop it.

The map overleaf gives some idea of the enormity of the task that confronts them. No country is 'safe' and that only includes the best known names. Germany has nearly 50 gangs, whilst I tracked down a dozen in this country.

The main motive with the crews is games cracking. It's a test of contacts, technical skill, and speed. Many of the gangs have ways and means of getting hold of titles before they appear. Otherwise when a game's released, and games are always released on the Continent first, it's a race to see who can hack through the protection first and put it out on the network. It's all about kudos. And the competition is hot — Psygnosis' *Obliterator* was cracked within hours of its release, despite some of the toughest protection available on its loader.

It doesn't stop here. Games are cracked, given new loading screens, boasting the name of the crew, and frequently compacted so they load quicker. On occasion the games are even polished up, improved in a way clearly beyond the original programmer. From there they're displayed on billboards (non-official ones, naturally) where they're downloaded, copied manyfold and handed round to everymother's son who knows someone on the misappropriation merrygoround.

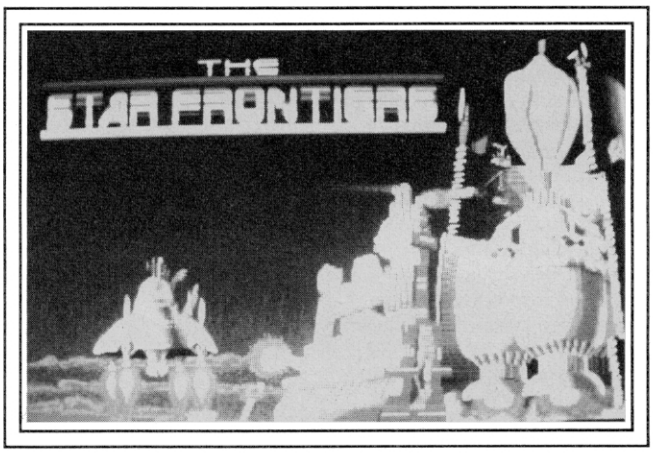
To some it's a game, but to most it's deadly serious. What they do is illegal. At best it is "distribution to the prejudice of the owner" — an offence under the Copyright Act that could involve the repayment of hundreds of pounds in damages and confiscation of hardware. At worst it could involve criminal proceedings with more serious consequences. Over in Holland and Germany the police raid PO boxes and have made numerous arrests. This country is fairly relaxed and life for the hackers is easy. But not if FAST (Federation Against Software Theft) have their way.

"The resultant loss of revenue through hacking is substantial . . . the problem is not exaggerated," says Bob Hayes, FAST's chief. It's not exaggerated, it's underestimated by many. Upper estimates of the cost suggest hacking/pirating costs companies up to 50% of their sales. And they don't like it. Most now build the costs into their price, and claim that price would come down if their profits weren't limited by these losses. The hackers dismiss that suggestion and say if games were good enough they'd buy them.

Do it for love

It is a fact that most hackers don't sell the games they crack.

"We're not making a profit," said one crew member. "We copy games simply because most software is not worth buying." Hackers consider most games poorly programmed and over-priced. The pricing of 16 bit software is a particular source of anger. Prices of £20-£25, they say, are simply not justified — an argument rejected by the companies who point to disk prices and extra development costs.



A typical Amiga demo.

In fact many crackers go as far as to say that they do the industry good, an argument difficult to justify, especially when many refuse to get involved legitimately in the business. Their abilities are not in doubt — one look at many of the demos they specialise in, with their slick visual effects and sampled sound is enough to prove that. But many are simply not interested in channelling their ideas creatively or even simply in making money through their proficiency, a fact that some software managers find hard to believe.

"There's a lot of talent out there, if only they could channel their energies legitimately," says FAST's Bob Hayes. That's an idea thrown out by many who view the whole industry suspiciously.

Aaargh! It's contagious!

One cracker who has made the transition is Christian Weber of the SCA (Swiss Crackers Association) — the man responsible for the infamous Virus. Swiss company Linel signed him up to write software for them. Ironically his first works will include a copy protection system and a virus protector! That's tantamount to treachery in the eyes of many of the crews.

"People said viruses similar to those on the VAX and IBM computers couldn't exist and I set out to prove them wrong," says Christian. "But I never wanted to destroy any software with it."

Christian Weber has gone over to the other side. There's a code of honour among crackers. You don't cooperate with the industry or provide information about fellow hackers.

If that all sounds pretty conspiratorial, that's because it is. The hacking network is organised. Although there is rivalry between teams, they collaborate in the circulation of games and demos. They even have their own publications. Photocopied fanzines like 'Delirious' and 'It's Illegal (But Who Cares?)' provide information about current goings-on on the hacking scene and flaunt illicit activities. April's issue of It's Illegal, the magazine published by Germany's TRIAD group carries news, interviews with hackers, a report on the Venlo copy party, a review of *Rolling Thunder*, a debate on the relative merits of 64 and Amiga, classified ads, news of the latest cracked games and charts. Basically it revels in its downright naughtiness, but at the same time it reaffirms the reasoning behind hacking. It holds the software industry in complete contempt and almost goes as far as to rationalise a kind of Robin Hood image for itself. In an interview in the March edition a guy called Ian from Brit hackers Fusion talks of his reasons for hacking: "To give people who can't afford to buy a game the chance to have it."

This view is backed up time and time again by anyone connected

PIRACY

with piracy. 'Software is overpriced, I wouldn't buy a tenth of the games I see. And I couldn't afford to either.'

Hacking is as old as the machines on the market. Demos on 8 bit machines have been around for years, and many still prefer the challenge of squeezing the best from their 64s. But as the 16 bit market begins to take off, so the crews start to put together more and more impressive demos, featuring multi-colour effects, wavy screens and slices of music sampled from records.

The danger however comes from the hacking. With the portability of 3½" disks, the fact that everyone with an Amiga and an ST has a disk drive, and the new stimulus provided by these machines, 16 bit hacking is reaching epidemic proportions. That's a source of concern, especially to the companies that have already made the transition to these machines.

Most vulnerable to this form of piracy are Psygnosis who only produce ST and Amiga Software. Their recently released *Obliterator* went the same way as the rest of their releases — on to the hacking circuit within hours of its release in Europe.

We give up!

"I'm not surprised," concedes programmer Dave Lawson. "The disk cannot be copied because there's so much protection on it, but it can be patched, there are areas where it can be disabled." When you consider that *Obliterator,* Psygnosis claim, cost £250,000 from inception to the moment it was shipped, estimates of 50% losses on sales because of the various forms of piracy must be pretty worrying.

"I don't think they damage us that seriously, we offer class packaging, posters, badges — extra incentives to make people buy."

Companies like Psygnosis and Rainbird have frequently resorted to providing novellas with passwords contained in them. The hackers just photocopy them. In *Carrier Command's* case they don't have to. Holding down the SHIFT key as it loads means that you can type in the same word every time.

That view is not echoed by others involved in the industry. Mirrorsoft who publish Cinemaware's 16 bit releases in this country are more concerned. Marketing Manager Tom Watson voiced his worries: "The real danger is we could go the same way as the ST market in the States where stuff went straight into public circulation through the bulletin boards. Now the ST market is dead over there and the hackers contributed towards that."

The American connection is important. Whilst the Euro crackers manage very nicely thank you with software releases on the Continent, the software theft chain extends right across the water, to the US. The Yank hackers are getting hold of US releases, phreaking the phone system (breaking into it) and downloading it within hours.

It's one thing games going round the circuit as soon as they're released, but much of the software that circulates is pre-release. So where the hell does it all come from?

- *European software retailers* — games are released abroad two weeks before they appear in this country, therefore many crackers in this country have them well before the UK release date.
- *US hackers* downloading American software way before its release.
- *Shops.* Some retailers, or their employees participate in feeding the hackers software on its release.
- *Programmers.* Many programmers are involved or are used unwittingly to provide their own games and those of their colleagues.

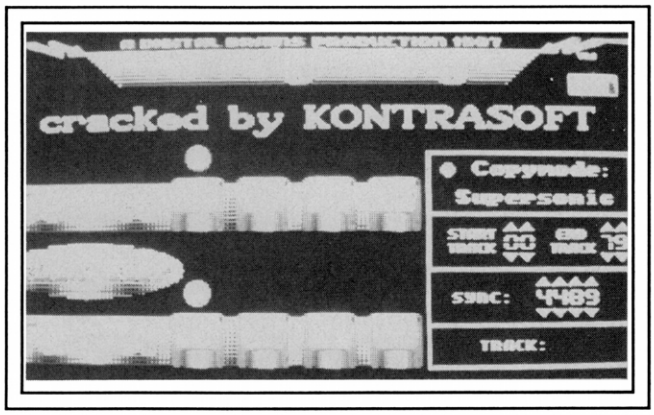
That may sound difficult to believe, but the disease runs right through the industry. So how is the industry attempting to cure it?

Protect and survive

System 3's Tim Best has his own ideas. "Software disks have become the new generation of swopsies, and it's difficult to know how to combat that, but it's their outlets which we must close. I know of a guy in Watford who went through 11 games in one day simply by taking them back to the shop and exchanging them. Shop assistants are contributing to the problem."

"We also need some kind of additional hardware, a sort of sophisticated dongle device. We tested one of our titles against the various cartridges on the market and only two failed."

The position over protection and back-up cartridges is a delicate one. As soon as protection is updated a new cartridge appears on the market. No-one is in a more delicate position to talk about this than



▲ *Cracked title screen from a copier.*

PHREAKING

This is a form of hacking particularly rife in the US where the crackers borrow the Alliance company's conference system and set up conferences all over the world for free. It's done by hacking out the codes by getting the computer to autodial each possible number until if finds the correct one. It costs the company millions of dollars.

Phreaking also allows pirates to modem trade cracked software for free. Mail trading however is still the most commonest form of dealing because there's less risk involved.

The US phone companies respond by:

- **Blasting fake carrier signals to the hacker's computer to waste their time.**
- **Tracing calls. Using ANI (Automatic Number Indicator) the service can trace all calls.**
- **TRAPping. The phone company sends out false codes to hackers. As soon as they dial the code they are traced and monitored until they have enough evidence to convict them. There is no way of telling whether a code is false or not.**

TOP FIVE EURO DEMOS

1 Think Twice V — The Judges
2 F.A.M.E. – F.A.M.E./TRIAD
3 Might – C64CG
4 Factory – CFR
5 Outspace – Orion

programmer John Twiddy who has, in the past, been responsible for writing both games and the notorious Expert cartridge software. I put one hacker's accusation to him that he was a "hypocrite".

"I don't think so, I developed the original Expert to help me program and that's what I intended it to be used for. Many programmers find it invaluable. Other companies jumped on the bandwagon."

The back-up cartridge is one avenue open that may soon be closed. The Copyright And Design Patent Bill currently going through Parliament contains an amendment to make it illegal to market or sell anti-spoiler devices like copiers. That of course won't stop the experts though. The basic tenet is still, as John Twiddy put it, "You can spend months developing protection for a game and someone will come along and crack it in a day. It's a matter of principle to them.

A disk CU was sent, said simply, "nice protection but the copy killer was killed". Honour has been satisfied.

Wouldn't it help matters if companies released games simultaneously in this country when they went abroad? Here the politics of the industry come into play. If you release on the same day all over Europe, English distributors will sell to the European market. Software houses *have* to build in a delay. If they don't foreign distributors won't agree to take as many copies and they won't sell as many. And who wants that?

The most deep-rooted problem seems to be the material that comes from within the industry. Many of the hacked games that appear are 75% finished and have come direct from a source closely involved with the business. For example there is a demo of a game called *Katakis* currently floating around the circuit which bears a close resemblance to *R-Type* and is currently being programmed by Rainbow Arts. We're not even supposed to know of its existence, but German hackers TRIAD are pouring out disks!

In another case copies of *Carrier Command* on the ST have turned up on the network and been traced back directly to a company doing conversion work for Firebird. They work in the offices above *CC*'s programmers Real Time. Someone got careless.

So what are Firebird going to do about it? Nothing. The company involved do conversion work and it would make things very awkward. But by this token they'll never stop it. As one Brit cracker put it "The industry's wrecking itself from inside."

The crackers point directly towards the companies and the programmers for encouraging it. "They definitely help us," said one. But the companies are at a loss to make games more secure. "It's difficult for us to know how much goes on," said Telecomsoft's Sean Brennan.

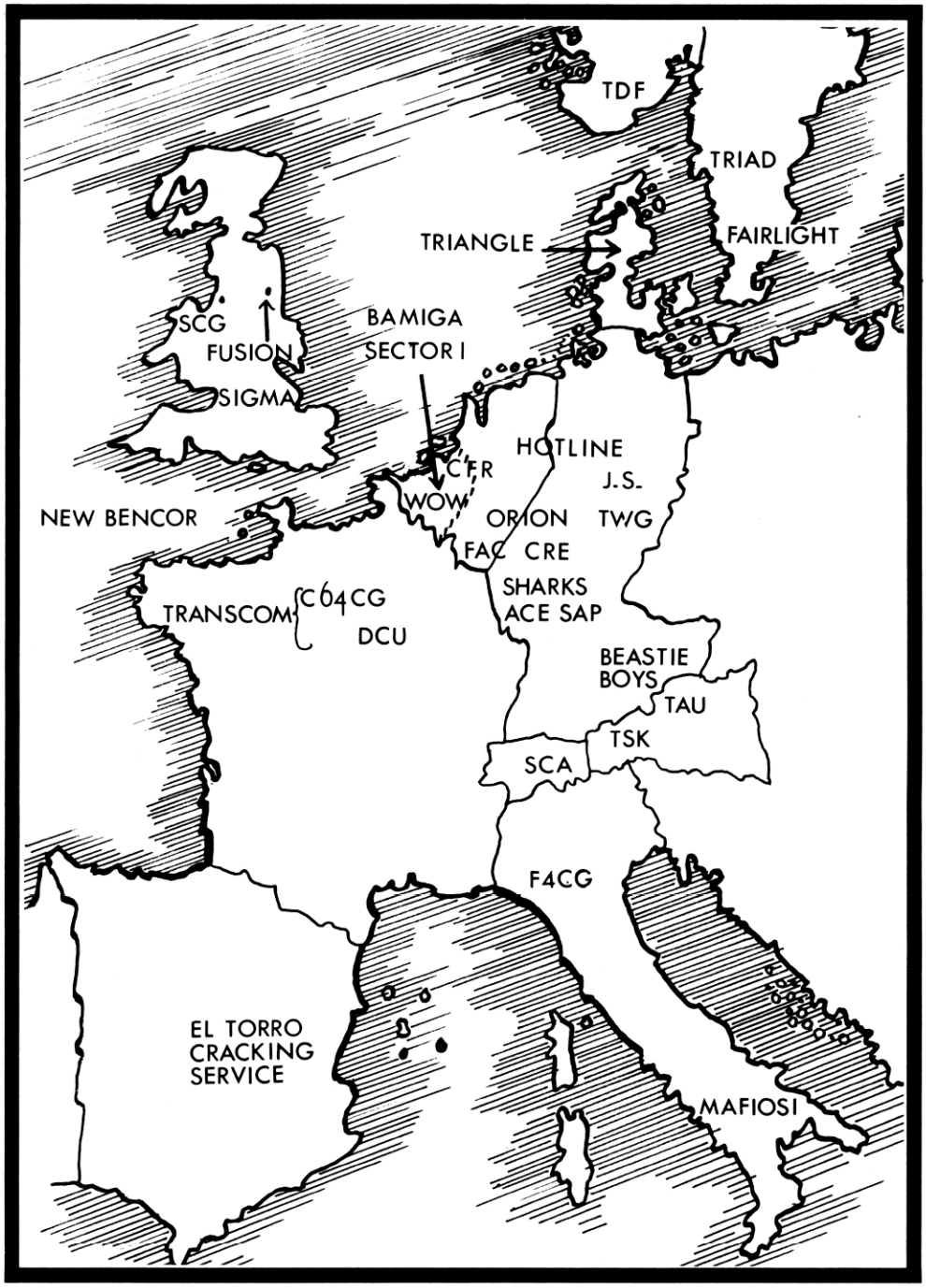
However most companies do take precautions with software that goes out. The most common method is 'fingerprinting', a technique which involves changing a line of code imperceptibly, so — should a rogue version appear — it can be traced back to the source. However that's only useful for closing the stable doors long after the software Shergar has bolted.

This is a particular problem for companies who use freelance programmers, but even companies with large in-house development teams have had problems. Elite have just spent more than a year assembling a complete internal squad and are anxious not to lose programs as they have before now.

"What's been a problem in the past is that people's mates were just walking straight into the place without our knowledge. Now that's not possible," says Marketing Manager Bernard Dugdale. But what if they take stuff home, you can't search people?

"There's no way of protecting against someone doing it wilfully, but programmers are under contract and they collect royalties, so they shouldn't want to lose out."

But practice suggests that some do and a number of hackers have pointed fingers. "Some of them just don't care," said one, a member of the *Ikari* team. However, rumours of chief programmers and top industry artists being involved are rife in the hacking network and are frequently unsubstantiated. Only those directly involved know for sure. And naturally, they're not saying.



The European hacking circuit.