Crypto in Europe — Markets, Law and Policy

Ross J Anderson
Cambridge University Computer Laboratory
Email: rja14@cl.cam.ac.uk

Abstract. The public debate on cryptography policy assumes that the issue is between the state's desire for effective policing and the privacy of the individual. We show that this is misguided.
We start off by examining the state of current and proposed legislation in Europe, most of which is concerned with preserving national intelligence capabilities by restricting the export, and in cases even the domestic use, of cryptography, on the pretext that it may be used to hide information from law officers. We then survey the currently fielded cryptographic applications, and find that very few of them are concerned with secrecy: most of them use crypto to prevent fraud, and are thus actually on the side of law enforcement.
However, there are serious problems when we try to use cryptography in evidence. We describe a number of cases in which such evidence has been excluded or discredited, and with a growing proportion of the world economy based on transactions protected by cryptography, this is likely to be a much more serious problem for law enforcement than occasional use of cryptography by criminals.

1 Introduction

The US Clipper chip initiative has fuelled extensive and acrimonious debate on the privacy versus wiretap issue, and this has spread to other countries too. At this conference, for example, an official from the Australian Attorney General's office has proposed that banks should use escrowed crypto, while ordinary people and businesses should be forced to use weak crypto [Orl95].

We provide an alternative view by looking at the state of play in Europe. We will firstly describe the political situation, then look at what cryptography is actually used for, and finally discuss the real problems of cryptography and law enforcement. Along the way, we will challenge a number of widely held beliefs about cryptology which underpin much research in the subject and condition the public policy debate. These include:

1. the primary role of cryptology is to keep messages secret. So if it is made more widely available, criminals will probably use it to stop the police gathering evidence from wiretaps;
2. its secondary role is to ensure that messages are authentic, and here it provides a useful (if not the only) means of making electronic evidence acceptable to a court. It is thus indispensible to the future development of electronic commerce.

2 Euopean Law and Policy on Cryptography

Some European countries, including Switzerland, Belgium and Germany, used to supply considerable quantities of cryptographic equipment to developing countries. This trade appears to have been tightened up recently as a result of American pressure, and now all European countries appear to enforce export controls on cryptographic hardware. Some even control its use domestically.

The country taking the hardest line is France. There, the "decret 73-364 du 12 mars 1973" put cryptographic equipment in the second most dangerous category of munitions (out of eight); any use required authorization from the Prime Minister, which could not be given to criminals or alcoholics. The "decret 86-250 du 18 fevrier 1986" extended the definition to include software, and specified that all requests be sent to the minister of the PTT with a complete description of the "cryptologic process" and two samples of the equipment. The "loi 90-1170 du 29 decembre 1990" states that export or use must be authorized by the Prime Minister unless used only for authentication [Gai92].

Few people in France seem to be aware of these laws, which are widely ignored. A hard line is still taken by SCSSI, the local signals agency, according to whom the use of PGP even for signatures will never be permitted [Bor95]; but when one looks at the actual text of the Loi No 90-1170 as it appeared in the Journal Officiel on 30th December 1990[1], it is unclear that digital signatures are covered at all.

Germany has no legal restraints on the domestic use of cryptography [Heu95]; indeed, Dirk Henze, the chief of the BSI (the information security agency), recommended that companies which cannot avoid sending data over the Internet should encrypt it, and the interior minister sees encryption as a precondition for the acceptance of electronic communication. However, Henze's predecessor Otto Leibrich took the view that security should rather be provided as a service by network operators in order to stop crypto equipment being available to villains [CZ95]; and a number of politicians, such as Erwin Marschewksi (home affairs spokesman of the CDU), argue for an outright ban [Moe95]. Meanwhile a law has just been passed forcing all telecomms companies to provide wiretap access to government agenices, including various call tracing services [Eis95].

Denmark, Finland, Sweden and Latvia have no domestic restrictions at present [Bor95] and no particular controversy which has come to our attention. But not all northern European countries are so relaxed; the Norwegian government is introducing its own encryption standard called NSK, which will be tightly licensed; Norwegian Telecom will manage the keys of line encryptors which use these chips and will be able to provide access to the intelligence services [Mad94].

Russia seems to be reverting to the policing traditions established under the Tsars and continued under the Soviets; a recent decree by President Yeltsin has

[1] Art 28. - On entend par prestations de cryptologie toutes prestations visant a transformer a l'aide de conventions secretes des informations ou signaux clairs en informations ou signaux inintelligibles pour des tiers, ou a realiser l'operation inverse, grace a des moyens, materiels ou logiciels concus a cet effet.

made cryptography illegal without a licence from the local signals agency [Yel95]. At the other extreme, the traditionally liberal Dutch government tried to impose a ban on civilian crypto in 1994 but was forced to back down at once by banks, petrol companies and other business interests.

The UK is mildly liberal at present. Prime Minister John Major stated in a 1994 parliamentary written reply to David Shaw, the member for Dover and Deal, that the government does not intend to legislate on data encryption. However, a spokesman for the opposition Labour party — which appears likely to form the next government — said that encryption should only be allowed if the government could break it [Art95]. This caused a storm on the Internet, and a subsequent policy document backed down on this issue; it did however propose to make warrants for the interception of communications much more easy to get. At present, these are only available to investigate serious arrestable offences; a future labour government would make them available for all offences, for 'racism' and for the 'protection of minors' [Lab95].

Even without a change in government, there is still occasional confusion in government policy. On the one hand, GCHQ permitted the export of over $35m worth of tactical radios to Iraq, which used them against allied forces in the Gulf War; on the other, it has made efforts to suppress academic research in cryptography. Interference with research is also common with the EU in Brussels, whose crypto policy is driven by SOGIS, the Senior Officials' Group (Information Security), which consists of signals intelligence managers. A typical EU project was Sesame, a Kerberos clone supposed to provide authenticity but not secrecy, and to be adopted by European equipment manufacturers. However its many flaws make this unlikely [ano95]: at the insistence of SOGIS, DES was replaced with xor, but the implementers did not even get a 64-bit xor right. Sesame also generates keys by repeated calls to the compiler's random number generator. Another project was RIPE (the RACE integrity primitives project), whose researchers were paid to devise a hash function (since attacked) but forbidden to do work on encryption. Close observers say that defective projects are approved deliberately to provide an excuse to refuse funding for more worthy proposals.

So the overall picture in Europe is one of confusion. Governments, and in particular by their signals intelligence agencies, claim to be concerned that the growth of commercial and academic cryptography might threaten intelligence and law enforcement capabilities. These fears are rarely articulated coherently; in addition to the contradictory behaviour of GCHQ, we would note that the current conference's paper from the Australian attorney general (cited above) says on the one hand that the use of encryption by criminals is not seen as a threat, but on the other hand that controls on crypto should be imposed.

Is there a real case here, or are we just seeing a panicky defensive reaction from bureaucratic establishments for whom the end of the Cold War means the loss of jobs and budgets, and who are looking for something to do? In order to assess the threat to law enforcement operations, we shall have to look first at what cryptography is actually used for.

3 European Applications of Cryptography

Many research papers on cryptography assume that two parties, traditionally called Alice and Bob, are sending valuable messages over an untrusted network. The idea is usually to stop an intruder, Charlie, from finding out the content of these messages. This application, message confidentiality, has historically generated perhaps 85% of research papers in the field.

Confidentiality has indeed been important in the government sector. The available information suggests that the NATO countries' military communications systems have about a million nodes, with the USA accounting for over half of this. This would appear to make governments the main users of cryptology, and they conduct the debate in these terms: for example, a recent report on crypto policy, one of whose authors is Assistant to the Director of the NSA [LKB+94], says '*cryptography remains a niche market in which (with the exception of several hundred million dollars a year in governmental sales by a few major corporations) a handful of companies gross only a few tens of millions of dollars annually*'.

This assessment is just plain wrong. The great majority of fielded crypto applications are not concerned with message secrecy but with authenticity and integrity; their goal is essentially to assure Bob that Alice is who she says she is, that the message he has received from her is the one she sent, or both. Here Charlie may try to impersonate Alice, or Alice might try to avoid paying for services rendered.

The main commercial cryptographic applications include the following.

Satellite TV decoders: There are tens of millions of these worldwide, with BSkyB having fielded 3.45 million in the UK alone by mid 1994 [Ran94]; they may be the largest single installed base of cryptographic terminal equipment. They are also the one nonmilitary application of cryptography which has attracted sophisticated and sustained technical attacks.

Automatic teller machines: ATMs have been around since 1968, and worldwide there are somewhere between 300,000 and 500,000 of them; over 100,000 are installed in Japan and 70,000 in the USA [AP94]. Many ATMs are networked together, and cryptography is used to manage personal identification numbers (PINs) — in fact this was the first large scale commercial application of cryptography [MM82]. The European ATM population is of the order of 100,000 [CI94].

Electronic funds transfer at point of sale (eftpos) . There is a lot of overlap between ATM, eftpos and credit card systems. In some countries (such as France and Australia) the ATM and eftpos networks are well integrated, with customers using PINs rather than signatures in shops; in others (like Britain), signatures are used to authorise retail transactions, but cryptography is still used to make the cards themselves harder to forge. The installed base of eftpos terminals has overtaken that of ATMs in most countries.

SWIFT: Based in Belgium, this is probably the oldest high security commercial computer network. For the last twenty years, it has transmitted payment instructions between the several thousand banks which own it, and its primary use of cryptography is to calculate a message authentication code (MAC) on each payment message [DP84]. The MAC keys used to be exchanged manually, but are now managed using public key protocols [ISO11166].

Telephone cards: These range from prepaid cards for public telephones to the much more sophisticated 'subscriber identity modules' (SIMs) used in GSM digital mobile phones. The SIMs are smartcards which identify the user of a telephone to the network for billing purposes, manage keys for encrypting the conversation [Rac88], and may even let the subscriber perform banking functions [Rob93] and place bets on horse races [Llo94]. Although only 4 million GSM phones are in use — mostly in Europe — the market is growing at 70% per annum, and 61% of new mobile phone subscribers in the UK now opt for GSM rather than the analogue alternatives [New94]. The market should grow even more quickly once GSM is fielded in countries such as China and India whose land based telephone systems are inadequate.

Utility tokens: The UK has about 1.5 million prepayment electricity meters, using two proprietary cryptographic schemes, and 600,000 gas meters using DES in smartcards. They are mainly issued to bankrupts and welfare claimants. Other European countries have smaller installations; France, for example, has about 20,000. However, prepayment meters are a growth industry in developing countries; technical information on such systems can be found in [AB94].

Computer access tokens: The market leading supplier of software protection dongles, Rainbow Technologies, has sold seven million units since 1984; from this business base, it took over Mykotronx, the manufacturer of the Clipper chip [Rai95]. There are also several vendors of one-time password generators. We have no overall figures for the total European sales of dongles and other access tokens, but they must be in the millions of units.

Building access control tokens: Although many early devices (from metal keys to magnetic cards) do not use cryptography, smartcard vendors are starting to make inroads in this market [Gir93].

Burglar alarms: Under draft CENELEC standards, class 3 and 4 alarm systems must provide protection against attacks on their signaling systems [Ban93], and some manufacturers are already taking steps in this direction. The market leading burglar alarm product in the UK claims to use 'high-level encrypted signalling' [BT93].

Remote locking devices for cars: These are starting to incorporate cryptographic techniques to thwart the 'sniffers' which can intercept and mimic the signals of first generation locking devices [Gor93].

Road toll and parking garage tokens: Some countries may issue these tokens to all their motorists [Sin95]; others may use multipurpose tokens, as with a German scheme to enable road tolls to be paid using the subscriber identity modules of car telephones [SCN94]. As well as a number of pilot schemes there are some fielded systems, including municipal parking garages in Glasgow [Tol93].

Tachographs: The European commission wants the current system for monitoring transport drivers' hours and speed to be replaced with a smartcard system which would be harder to tamper with [Tor94].

Lottery ticket terminals: The UK national lottery uses encryption to ensure that vendors cannot manufacture valid tickets after the draw or otherwise manipulate the system [Haw94]. Similar systems are used in other countries, and remote gambling terminals are becoming popular in the Far East.

Postal franking machines: The latest designs can be replenished remotely, thanks to cryptography: the user can use a credit card to buy a 'magic number' over the phone which lets her machine dispense a certain amount of postage.

Embedded applications: For example, some 40 million users of Novell NetWare use encryption embedded in the authentication protocols with which they log on to the system [Ber94].

These retail applications dwarf the world's military systems. An indication of overall sales figures comes from a French smartcard manufacturer which shipped 53m microprocessor cards last year and estimated that the total world market was 250 - 280m, and set to grow to 600m by 1997 [Rya94]. These microprocessor cards are more expensive than simple memory cards, and are typically used when some kind of crypto protocol needs to be supported. It would therefore seem reasonable to estimate that, whether we measure the size of a secure system by the number of nodes or the number of users, the retail sector is about two orders of magnitude larger than the military sector.

This economic fact is starting to loosen the traditional government control of the technology. On at least two occasions in the past decade — in South Africa in 1986 and the Netherlands in 1994 [Rem94] — a government has tried to ban civilian cryptography, and on each occasion it was forced to back down by pressure from banks, utilities, broadcasters, oil companies and others. So a lot of companies are coming to rely on cryptology, But is it in fact reliable? Does it really do what its advocates claim?

4 The Legal Reliability of Cryptography

In previous articles, we have discussed how cryptographic systems fail. We first looked at automatic teller machines, and the various frauds which have been carried out against them; it turned out that the attacks were not particularly high-tech, but exploited blunders in system design and operation [And93]:

- one bank wrote the encrypted PIN on the card strip. They got away with this for years, until villains found that they could change the account numbers on their own cards to other people's account numbers, and then use their own PINs to steal money from those accounts;

- villains would find out PINs by looking over their victims' shoulders, and then make up cards using the data on discarded tickets. This kind of fraud has been going on for years and is easy to stop, yet some banks still seem vulnerable to it;
- most fraud exploited much simpler blunders, such as insecure card delivery or poorly designed support procedures. For example in August 1993, my wife went into a branch of our bank, and told them that she had forgotten her PIN; they helpfully printed a replacement PIN mailer from a PC behind the counter. This was not the branch at which her account is kept; no-one knew her, and the only 'identification' she produced was her bank card and our cheque book.

We found much the same pattern with prepayment electricity meters. These allow the customer to buy electricity units at a shop and take them home in the form of a coded token, which is inserted into the meter; once the units run out, the supply is interrupted. Here too, most frauds exploited design blunders in simple and opportunistic attacks [AB95]:

- it was possible to insert a knife or a live cable into the card throat of one meter type and destroy the electronics immediately underneath, which had the effect of giving unlimited credit;
- another type of meter could have the tariff code set to a minute amount, so that it would operate almost for ever;
- another would often go to maximum credit in a brownout (a voltage reduction to 160 - 180V). This bug was due to one wrong assembly language instruction in the meter controller; its effect that customers threw chains over the 11KV feeders in order to 'credit' their meters. The manufacturer had to replace and re-ROM over 100,000 units.

A similar failure pattern has been found with satellite TV decoders as well, where, despite using an encryption algorithm which is vulnerable to analysis [And90], the majority of systems have been attacked by manipulating the key management mechanism. We conclude that cryptography does not provide any 'silver bullet' solution for the old problem of software reliability [Bro75]; systems which use it are just as likely to fail in unexpected ways as any other computer system.

This brings us on to the legal reliability of cryptographic systems — after all, as the above list shows, an increasing proportion of GNP is tied up in contracts which are enforced by crypto. If these contracts are broken in some way, the evidence needed for a civil suit or criminal prosecution may depend on crypto. Yet if crypto mechanisms are not reliable, then how can a judge tell whether the system was working at the time of the disputed transaction or not? Of course the system's owner — and his security consultants — will claim that the system is secure, but how is this claim to be tested?

This problem was illustrated by a recent series of court cases about disputed banking transactions. The typical pattern in such cases is that someone has a 'phantom withdrawal' from their account; they go to the bank and complain; the bank says that as its systems are secure, it must be the fault of the account holder, who must have been defrauded by a friend or relative; the victim goes to the police and lays a complaint; and some unlucky person gets arrested.

In years gone by, that was effectively the end of the matter; for example, one Janet Bagwell was accused of stealing money from her father, and was advised to plead guilty as it was her word against the bank's. She did so and then disappeared; much later, the bank manager in charge of the cover-up confessed that it had all been an administrative error. By then, Janet's lawyer could no longer trace her, and we can only speculate at the effects which this incident had on her life.

However, in the last three years, defence lawyers have started to challenge the banks' claims that their systems are secure. In the first such case, charges of theft against an elderly lady in Plymouth were dropped after our enquiries showed that the bank's computer security systems were a shambles, and we demanded full information about their security systems. The same happened in a number of subsequent cases [And94].

The most notorious case so far is that of John Munden. John was a constable at our local police station in Bottisham, Cambridgeshire, with nineteen years' service and a number of commendations. However, his life came apart after a holiday in Greece; he returned to find his bank account empty, and went to the manager to complain.

The manager asked how his holiday in Ireland went; apparently the information he had in front of him indicated that ATM withdrawals had been made in Omagh. When John told him that he had been in Greece, the story changed; the bank claimed that six withdrawals totalling £460 had been made from his home branch just before he had gone on holiday. When he persisted with his complaint, the bank complained to the police that he was trying to defraud them. He was arrested, tried for attempted fraud and — to the surprise of many — convicted.

The description of the bank's systems which came out at the trial was more reminiscent of Laurel and Hardy than of ISO 9000:

- The bank had no security management or quality assurance function. The software development methodology was 'code-and-fix', and the production code was changed as often as twice a week;
- the manager who gave technical evidence claimed that bugs could not cause disputed transactions, as his system was written in assembler, and thus all bugs caused abends;
- he claimed that as ACF2 was used to control access, it was not possible for any systems programmer to get hold of the encryption keys which were embedded in application code;
- he had not investigated the disputed transactions in any detail, but just looked at the mainframe logs and not found anything which seemed wrong (and even this was only done once the trial was underway, under pressure from defence lawyers);

- there were another 150-200 disputed transactions which had not been investigated;
- in the branch itself, the security cameras were conveniently not working, and the branch manager had since left the bank's employment.

An appeal was launched, and a week before it was due to be held, the bank produced a thick expert report from a partner at its auditing firm claiming that its systems were secure. The defence team promptly went to court and asked for the time and the access to prepare their own report as well. The court responded with an order that the defence expert have full access to the bank's 'computer systems, records and operating procedures'.

After five months in which the defence repeatedly demanded this access, and in which the bank refused it, a further application was made, and the judge has now ruled that the prosecution will not be allowed to call expert evidence at the appeal. The date for this has still to be set at the time of writing; it remains to be seen whether the Crown will offer any evidence at all.

This underlines a conclusion which we already drew in [And94]:

Security systems which are to provide evidence must be designed on the assumption that they will be examined in detail by a hostile expert.

It remains to be seen how the other systems listed above will stand up to the rigours of a trial. One suspects that few if any of them were designed with the above principle in mind; and the lesson does not appear to be getting through.

For example, the Bank of England is building a system called Crest which will be used to register all UK equities. When its security was publicly criticised [Inm95], the Bank's reaction was to keep the design secret; and despite repeated criticism it has evaded the question of how its system will withstand a legal challenge [Boe95].

5 How Realistic is European Public Policy?

Most crypto is about authenticity rather than secrecy, and an increasing proportion of economic activity relies on it to some extent. Thus more and more prosecutions are likely to depend on cryptographic evidence, and law enforcement agencies should be concerned at the difficulty of relying on current systems in court. However, the only official interest so far in liability was in a US Commerce Department study which looked at whether the government could have its cake and eat it too; the idea was that the government could manage everybody's keys without assuming too much liability when things go wrong [Bau94].

The policy debate continues to focus on secrecy, with civil rights groups saying that crypto is important for freedom and privacy in the electronic age, and governments claiming that good crypto would make law enforcement more difficult by making it harder for the police to gather evidence using wiretaps.

This debate misses the point. Quite apart from the liability problem, it is not true that villains will use crypto; it is not true that wiretaps are important to the police; and it is not true that cryptography is important to individual privacy.

1. Clever crooks don't use crypto for secrecy. They are aware that the main problem facing law enforcement is not traffic processing, but traffic selection [LKB+94]: in layman's terms, a ten minute scrambled telephone call from Medellín, Columbia, to 13 Acacia Avenue, Guildford, is an absolute giveaway. Instead, a competent villain will try to bury his signals in innocuous traffic. One common modus operandi (in the USA and increasingly the UK) is to use an address agile system — cellular telephones are repeatedly reprogrammed with other phones' identities. In Paris, villains use cordless telephone handsets to make calls from outside unsuspecting subscribers' homes [Kri93]; and in Britain, villains have tapped domestic phone lines in order to make outgoing international calls.
2. The official use of wiretaps varies substantially from one country to another, and even from one local police force to another. In the USA, three states forbid wiretaps completely, and in 1993 there were 29 others that did not use any; 73% of state wiretaps were in the 'Mafia' states of New York, New Jersey and Florida [Han94]. There is similar variation in Europe. Many wiretaps were carried out unlawfully in France by the President's henchmen, and this was one of the scandals which dogged the last years of the Mitterrand administration. In the UK, on the other hand, all legal wiretaps have to be authorised by a minister, and the number reported (both to parliament and by our police informants) is low. The clear conclusion is that wiretaps are not essential, or even very important, for policemen; many admirable police forces function perfectly well without them.
3. Even if crypto were banned, it still does not follow that wiretaps would remain a feasible option for the police. It is very expensive to provide a wiretap capability in a modern digital network; if it is mandated in the USA, phone companies say it could cost $5bn in the first four years alone. Yet US police agencies only spent $51.7 million on wiretaps in 1993 — as close as one can get to an estimate of their value [Han94]. Forcing phone companies to subsidise 96% of the cost of wiretaps makes no more sense than forcing Westland to sell helicopters to the police for the same price as cars. This may become an issue in Europe as well as the USA; senior managers in the European telecomms industry have complained to the author that a similar provision would add to costs, stifle competition and be a disaster for business generally.
4. The real threats to individual privacy have little to do with crypto but are rather concerned with the abuse of authorised access to data.
   - All US police forces have access to the FBI's criminal records system through gateways, and it has proved impossible to impose effective controls on them. As a result, criminal records can be obtained through private detective agencies who in turn buy them from local police officers.

These records have been used on occasion to discredit political opponents and troublemakers [Mad93]. UK criminal records are no different, and the consolidation of European criminal records in the Schengen system will make the problem worse;
- Most of the big UK banks let any teller access any customer's account (one bank even boasted about this when their system was recently upgraded). The effect, as widely reported in the UK press last year, is that private eyes get hold of account information and sell it for £100 or so [LB94];
- a banker on a US state health commission had access to a list of all the patients in his state who had been diagnosed with cancer. He promptly called in their loans [Bar93];
- a study at the University of Illinois found that 40 percent of insurance companies disclose medical information to others, such as lenders, employers and drug salesmen, without the patient's permission; and over half of Fortune 500 companies use medical records in hiring decisions [Con94]. Although the situation is not yet as bad in many European countries as it is in the UDSA, it is rapidly heading the same way [And95].

The fight against such abuses is political rather than technical. For example, the British Medical Association has recently threatened to boycott a new medical network being installed by the government [Jac95]. Although the doctors want encryption (which the government is resisting), their primary complaint is not about mechanisms but about policy — namely that the system must not repeat the mistakes of the banks and the police; it must limit the number of people who can access any patient's record.

We conclude that the privacy versus police debate is misguided; neither the libertarians nor the policemen have a serious case. Yet this debate continues to wend its weary way across the world; and since about March 1995, there appears to have been a concerted effort by many of the developed world's secret policemen to introduce laws and regulations facilitating wiretapping of digital communications, key escrow, mandatory weak crypto, and various other measures whose ostensible purpose is protecting law enforcement capabilities but whose real purpose may be to hinder the uptake of cryptography by industry and commerce, to preserve employment at signals intelligence agencies, or both.

6 Conclusions

The politics of cryptology is often viewed as a Manichaean struggle between the privacy of the individual and the ability of the police to detect crimes such as money laundering and child pornography. While this perception may drive the actions of legislators, it is at odds with the facts. Villains do not use crypto; wiretaps are almost irrelevant to police work; and there are many much more immediate threats to privacy, such as the wholesale trading of credit records, medical records and other information with the power to do harm.

The real law enforcement problem is that neither prosecutors nor civil litigants can rely on cryptographic evidence, and in an information based society, this kind of evidence is likely to figure in more and more trials. Within the next two to three years, we expect that arguments about whether the crypto was working (and whether the defence experts can examine it) will spread from disputed ATM transactions to investigations of securities fraud and other serious white-collar offences.

This is not inevitable. It can be tackled by insisting that cryptographic systems be built to withstand examination by hostile expert witnesses, just like the alcohol intoximeters and radar cameras used by traffic policemen. If governments are serious about preserving their law enforcement capability, then they should not harrass crypto manufacturers but rather encourage them to get their products up to this standard — whether using government purchasing power in projects such as Crest, product development subsidies such as those currently wasted by the EU in Brussels, or national standards bodies.

But if the real goal is to preserve the payrolls and influence of the secret policemen and their favoured suppliers, then this policy may be painful. The infrastructure built up by GCHQ and its overseas counterparts is of little relevance to commerical crypto. For example, the ITSEC/ITSEM procedure typically takes a year and a million dollars to evaluate a security product, while underwriters' laboratories might do the job in a month for twenty thousand dollars [ESO94]. We can see no reason why military crypto suppliers should be any more able to beat swords into plowshares than the similarly bloated and inefficient suppliers of tanks, warships and missiles turned out to be.

So the challenge facing Europe's crypto policymakers is a hard one. It is not just a matter of sacking a few thousand civil servants at GCHQ, and letting a few CLEFS and equipment vendors go to the wall. It is the challenge of adapting to a major paradigm shift: from intelligence to evidence, from protecting lives to protecting money, from secrecy to authenticity, from classified to published designs, from tamper-proof hardware to freely distributed software, from closed to open systems, and from cosseted suppliers to the rough and tumble of the marketplace.

Every aspect of this change is likely to be alien and threatening to the signals security establishment. On past form, we expect that the securocrats will fail to adapt. Their attempts to retain control of cryptographic technology appear doomed to fail, and if they continue to fight market forces, then they risk public humiliation, with resulting cuts in their organisations' budgets and influence.

Acknowledgement: The final version of this paper was written while the author was a guest of the Information Security Research Centre, Queensland University of Technology.

References

[And90] RJ Anderson, "Solving a class of stream ciphers", in *Cryptologia* v **XIV** no 3 (July 1990) pp 285–288

[And92] RJ Anderson, "UEPS — A Second Generation Electronic Wallet". in *Computer Security — ESORICS 92*, Springer LNCS **648**, pp 411–418

[And93] RJ Anderson, "Why Cryptosystems Fail", in *ACM Conference on Computer and Communications Security* (Nov 1993) pp 215–227; journal version in *Communications of the ACM* v **37** no 11 (Nov 1994) pp 32–40

[And94] RJ Anderson, "Liability and Computer Security: Nine Principles", in *Computer Security — ESORICS 94*, Springer LNCS v **875** pp 231–245

[And95] RJ Anderson, "NHS-wide networking and patient confidentiality", in *British Medical Journal* v 311 (1 July 1995) pp 5–6

[ano94] anonymous, "SESAME", posted to Internet newsgroup `sci.crypt` as message <`154315Z07111994@anon.penet.fi`>, 7th November 1994; and followup postings

[Art95] C Arthur, news article in *New Scientist*, 11th March 1995; when accused by a labour spokesman of misquoting, he supplied the tape of his interview to the net. See 'Re: Britain to outlaw PGP - whats happened so far', posted as article <`D60F7L.KvH@exeter.ac.uk`> to `sci.crypt`, 25 Mar 1995.

[AB94] RJ Anderson, SJ Bezuidenhout, "Cryptographic Credit Control in Prepayment Metering Systems", in *1995 IEEE Symposium on Security and Privacy, pp 15–23*

[AP94] Associated Press, "BANKS-ATMS", wire item **1747**, 30 November 1994, New York

[Ban93] KM Banks, *Kluwer Security Bulletin*, 4 October 93

[Bar93] ED Bartlett, "RMS need to safeguard patient records to protect hospitals", in *Hospital Risk Management* v 15 (1993) pp 129–133

[Bau94] MS Baum, *'Federal Certification Authority Liability and Policy — Law and Policy of Certificate-based Public Key and Digital Signatures'*, U.S. Department of Commerce Report Number NIST-GCR-94-654

[Ber94] T Berson, *private communication*

[Boe95] Bank of England, "Crest's security", in *Crest project newsletter, April 1995*

[Bor95] S Bortzmeyer, "Data Encryption and the Law(s) — Results", *available from* `http://web.cnam.fr/Network/Crypto/survey.html` (15/12/94);

[Bro75] FP Brooks, *'The mythical man-month: Essays on software engineering'* (Reading, Massachussetts, 1975)

[BT93] *'RedCARE — The secure alarm networks'*, British Telecom, 1993

[Con94] "Who's Reading Your Medical records?", in *Consumer Reports* (Oct 1994) pp 628–632

[CI94] *Cards International* has country surveys about once a month; similar information can be found in *Banking Technology*

[CZ95] Report of 4th Deutschen IT-Sicherheitskongreß, Bad Godesberg, 8–11 May 1995, in Computer Zeitung no 21 (25th May 1995) p 21

[Eis95] S Eisvogel, posting about German 'Fernmeldeanlagen Ueberwachungs-Verordnung' of May 4th 1995 to tv-crypt mailing list

[ESO94] Conference debate on security evaluation, ESORICS 94

[Gai92] JL Gailly, "French law on encryption", *posted to Internet newsgroup* `sci.crypt` *as message* <`831@chorus.chorus.fr`>*, 28 Oct 92 by* `jloup@chorus.fr` *(Jean-loup Gailly)*

[Gir93] Y Girardot, "The Smart Option", in *International Security Review Access Control Special Issue* (Winter 1993/1994) pp 23–24

[Gor93] J Gordon, "How to Steal a Car", talk given at 4th IMA Conference on Cryptography and Coding, December 1993

[Han94] R Hanson, "Can wiretaps remain cost-effective?", in *Communications of the ACM v 37 no 12 (Dec 94) pp 13–15*

[Haw94] N Hawkes, "How to find the money on lottery street", in *The Times* (8/10/94) weekend section pp 1 & 3

[Heu95] A Heuser, writing on behalf of BSI to U Möller, copied at `http://www.thur.de/ulf/krypto/bsi.html`

[Inm95] P Inman, "Bank of England share system 'open to fraud' ", in *Computer Weekly*, 23rd March 1995, pp 1 & 18

[ISO11166] 'Banking — Key management by means of asymmetric algorithms — Part 1: Principles, procedures and formats; Part 2: Approved algorithms using the RSA cryptosystem, *International Standards Organisation, 15th November 1994*

[Jac95] L Jackson, "NHS Computer is 'Paparazzi's Dream' ", *Press Association* report 1520, 1st June 1995.

[Kri93] HM Kriz, "Phreaking recognised by Directorate General of France Telecom", in *Chaos Digest 1.03 (Jan 93)*

[Lab95] Labour party policy on the information superhighway, at URL `http:www.poptel.org.uk/labour-party/content.html`

[Llo94] C Lloyd, "Place your bets while on the hoof", in *the Sunday Times* 2nd October 1994 section 2 p 11

[LB94] N Luck, J Burns, "Your Secrets for Sale", in *Daily Express*, 16th February 1994 pp 32–33

[LKB+94] S Landau, S Kent, C Brooks, S Charney, D Denning, W Diffie, A Lauck, D Miller, P Neumann, D Sobel, "Codes, Keys and Conflicts: Issues in US Crypto Policy", *Report of the ACM US Public Policy Committee June 1994*

[Mads93] W Madsen, "NCIC criticised for open security and privacy doors", in *Computer Fraud and Security Bulletin (Oct 93) pp 6 - 8*

[Mad94] W Madsen, "Norwegian encryption standard moves forward", in *Computer Fraud and Security Bulletin (Nov 94) pp 10–12*

[Moe95] Ulf Moeller, "Kryptographie: Rechtliche Situation", at `http://www.thur.de/ulf/krypto/verbot.html`

[New94] M Newman, "GSM moves past analog", in *Communications Week* issue **135** (28 November 1994) p 40

[Orl95] S Orlowski, "Encryption and the Global Information Infrastructure, An Australian Perspective", *this volume*

[Pat95] N Pattinson, Schlumberger, *personal communication*

[Rac88] Racal Research Ltd., "GSM System Security Study", 10th June 1988

[Rai95] "Counterfet Software Operations", press release no. OTC 06/27 1135 on CompuServe.

[Ran94] J Randall, "BSkyB set for record £5bn stock market debut", in *The Sunday Times* (2nd October 1994) section 2 p 1

[Rem94] MNR Remijn, "Tekst van de memorie van toelichting van de wet tegen crypto", posted to Internet newsgroup `nlnet.cryptografie` as message <1994Apr15.124341.20420@news.research.ptt.nl>

[Rob93] D Robinson, "Cellular phones offer chip opportunity", in *Cards International* no **98** (24th November 1993) p 10

[Rya94] I Ryan, "Market diversity points way forward", in *Cards International* no **111** (13th June 1994) p III
[Sin95] Discussion at Singapore National Computer Board, 30th June 1995
[SCN94] "German Motorway Toll Trial is GSM-Based", in *Smart Card News* v **3** no 3 (March 94) pp 41–44
[Tol93] Discussions with staff of Tollpass Ltd., Edinburgh
[Tor94] A Torres, "Commission wants black box, smart cards to enforce road safety", *Reuters RTec* 09/02 **0804**
[Yel95] B Yeltsin, Decree no. 334, 3rd April 1995; English translation at `http://www.eff.org/pub/Privacy/`