STRATEGIC EXPORT CONTROLS:
THE IMPACT ON CRYPTOGRAPHY

A Response by

THE FOUNDATION FOR INFORMATION POLICY RESEARCH

to the

DEPARTMENT OF TRADE AND INDUSTRY

This paper was prepared for the Foundation by

Nicholas Bohm, *Solicitor*

Ian Brown, *University College, London*

Brian Gladman, *Information Security Consultant*

with assistance from other members of the Advisory Council of the Foundation

The Foundation for Information Policy Research

9 Stavordale Road, London N5 1NE

Tel: 0171 354 2333, Fax: 0171 827 6534

E-mail: cb@fipr.org, Web: www.fipr.org

STRATEGIC EXPORT CONTROLS: THE IMPACT ON CRYPTOGRAPHY

Executive Summary

The DTI's proposals, in a July 1998 White Paper, to extend export controls to the publication and communication of certain information would have a debilitating effect on cryptography. Yet availability of cryptography is vital for the emerging information age. This paper questions the value of existing export controls, and sets out the intolerable wider consequences for business, education and liberty of the proposed extension.

For the first time in history cryptography is accessible and important for all. DIY cryptography on personal computers can satisfactorily protect transactions over the Internet, which by itself is inherently insecure, unreliable and unaccountable.

Export of cryptographic products is controlled under UK law and EC Regulations. These in turn are based on the so-called Wassenaar Arrangement, intended to prevent dangerous concentrations of military weapons but not to damage civil commerce or legitimate self-defence. The rules cover cryptographic products, even though they are defensive, indeed they will be crucial to any nation's defences in the information age.

Military cryptography tends to be custom built and expensive. It could be distinguished in law from the new growing area of commercial civil cryptography. But the rules make no such distinction. The controls apply, contrary to the spirit of Wassenaar, to what is emerging as a vital area for civil commerce.

Are there other reasons why cryptography should be controlled?

The USA and UK have built up large organisations for intercepting electronic communications - NSA and GCHQ respectively - which would be greatly hampered by widespread encryption. Hence the desire to delay or prevent its adoption, in the interests of "national security". But a US National Research Council study pointed out how hard it was to take this pretext on trust. It concluded that the debate on cryptography should be open, and that the advantages of more widespread use of cryptography outweighed the disadvantages.

There is no independent, publicly accountable scrutiny of UK policy, and one suspects that UK policy would not survive open scrutiny.

The UK export control rules cover equipment or software designed or modified to use cryptography, or to provide protection from electronic eavesdropping, or to develop or produce the equipment or software listed. This covers precisely the equipment and software we need to make the Internet safe. It is not just military encryption, and not only encryption itself, but anything designed to work with encryption that is covered. Material already in the public domain is not restricted.

But businesses need good cryptographic products to protect their assets from competitors. Developed nations need secure information infrastructures. Constraints on cryptography, supposedly to protect us from terrorists, in fact make our make communications, power, transport and healthcare networks vulnerable to attack. Cryptography also protects citizens' privacy rights.

Attempts to apply a system of key escrow, under which government would ultimately have access to everyone's keys, involve demonstrable security risks and have aroused criticism, as the proposed safeguards are incapable of preventing grave abuses. Industry is also unenthusiastic.

So much for the present impact of export controls on cryptography. What effect would their extension into the realm of intangibles have?

The new proposals would effectively cover all cross-border research into cryptography. As proposed, they would make an export licence necessary for every fax and email on the subject (and those granting the licence would hardly be likely to understand the messages in question). It might control the education of non-UK residents including, for example, three quarters of Cambridge science and technology research students. UK participants would need a licence before submitting a contribution about cryptography to Internet mailing lists and news groups.

People might try to get around this by putting material into the public domain first, for example by publishing it on a web site. The White Paper accordingly proposes Government powers to prohibit transfer of any sort of restricted information orally or by demonstration, and to prohibit the publication of information relating to technologies for weapons of mass destruction.

Extension of export controls on cryptography would damage cross border research and invisible export earnings; education; and freedom of speech and publication. The existing controls are damaging to the emerging information society, and unjustified. Do they nevertheless serve a useful purpose?

They have prevented widespread use of cryptography, and it is easier for governments to continue to collect intelligence information. But there is no evidence that the restrictions have prevented criminals, terrorists or belligerent states from getting cryptographic software.

Government has failed to present a credible case to justify export controls on cryptography. If it has one, it should make it publicly.

One could argue that the DTI would apply the new rules benignly. But breach of the export controls is a serious criminal offence with mandatory imprisonment even for a first-time offender of previously good character. To have freedom of speech or publication dependent on an officials verdict on an export licence, based on complex controls set up under secondary legislation, is unjustified and intolerable.

Recommendations

1. There should be no extension of controls to intangibles without a full public justification by reference to actual harm caused by intangible exports of controlled technology as compared with properly evaluated burdens and losses involved in extending the controls.

2. If such a justification can be provided, any controls shown to be necessary should be limited to exports in the course of commercial transactions, and should not apply to communications or publications made for the purposes of research (whether basic or applied).

3. There should be free movement of all goods and intangibles within the European Community and the wider European Economic Area without any special treatment.

4. Information security products using cryptography for commercial purposes should be removed from the scope of control.

STRATEGIC EXPORT CONTROLS: THE IMPACT ON CRYPTOGRAPHY

In July 1998, in response to recommendations by Sir Richard Scott in his Report of the Inquiry into the Export of Defence Equipment and Dual-Use Goods to Iraq and Related Prosecutions, the Department of Trade and Industry published a White Paper on Strategic Export Controls. One of the proposals in the White Paper is that existing controls on the export of goods should be extended to control the publication or export of information. This proposal is presented as arising from the Government's "need to ensure that its strategic export control powers are brought up to date to enable it to deal with modern means of trading, such as transferring information via the Internet."

The extension of control over the export of goods to control over the publication and communication of information is much more radical in its effect than its presentation suggests. This paper examines one important controlled technology, cryptography, and the impact of extending the existing control in the way proposed by the White Paper

Cryptography

Cryptography, the art of secret writing, dates at least from classical times. But until quite recently the practical difficulties of using it on a large scale have limited its effective use to the rich and powerful, and primarily to the military and diplomatic arms of government.

Three recent developments have converged to change this picture out of all recognition. One is the discovery and publication in the 1970s of asymmetric cryptography, with its consequent enormous simplification in the management of encrypted communications. Another is the development of the Internet as a worldwide system for the exchange of digital messages. And the last is the widespread availability of personal computers and suitable software that enable only mildly computer-literate users to encrypt their communications using techniques which are capable of resisting the most powerful known methods of decryption.

The Information Society

It is widely recognised that we are approaching a period of social transformation. "As we prepare to enter a new century, our society stands on the threshold of a revolution as profound as that brought about by the invention of the printing press half a millennium ago", to quote "Communicating Britain's Future" (The Labour Party, 1995). A major element in this transformation will be the increasing use made, for a wide variety of purposes, of rapid digital communications over the Internet. Banking, commerce, industry and politics, as well as social life and leisure pursuits, will all be heavily affected. The computer and software industries themselves serve to illustrate the increasingly global character of industrial society, with research, development, component manufacture, assembly and sales divided between different countries and different continents collaborating through international networks.

The Internet is both well and badly fitted for the burdens it will be expected to carry. It has grown organically and without central management and control. One benefit is its resilient response to failures and breakdowns, and its independence of governments and corporate cartels. A weakness is its comparative insecurity: messages may pass over any number of different operators' networks, with no easy way of placing responsibility on any one of them for the security or reliability of the transmission. There are no physical means of being sure about who a message will reach, or who sent it, or whether the message received is the same as the one originated.

Surveys such as the Graphic, Visualization, & Usability Center's 8th WWW User Survey have identified security of the Internet as a widespread concern of members of the public contemplating its use. (See <www.gvu.gatech.edu/user_surveys/survey-1997-10/>) This concern is justified: the open nature of the networks comprising the Internet makes unauthorised access to its components a simple undertaking, and one well-documented in websites devoted to hacking. The threat of "Information Warfare", in which society is disrupted by attacks on its capacity to process information, is increasingly seen as a significant risk of coming developments.

These drawbacks might seem to place severe limitations on the suitability of the Internet for such serious purposes as banking, trade and politics. But the techniques of cryptography have been found to provide exactly what is required to enable an insecure medium to carry messages whose privacy, authenticity and integrity can be reliably ensured. That is why cryptography can rightly be seen as one of the key "enabling technologies" for the social changes that lie ahead.

The effective deployment of cryptographic technology to provide improved safety and security in Internet use is now a crucial step in achieving the public confidence on which its future benefits depend.

It is important to note that good data security, as well as requiring the implementation of good security practices, depends on well-designed computer equipment and well-designed software (a requirement which applies both to operating systems and to the special-purpose application programs which embody cryptographic techniques). Good data security is not an "add on" which can be applied effectively to any system irrespective of its underlying design. Its implementation depends significantly on the computer and software industries, and on their ability to develop and deliver systems which users can make reliably secure.

It is the central role which cryptography must play in the Information Society that justifies the detailed examination devoted to it by this paper. This begins with an examination of the existing legal controls on cryptography.

Controls

There are no general legal controls on the domestic sale, possession or use of cryptographic equipment or software in the United Kingdom. Information may be encrypted and stored, or sent by any means of telecommunication (through the post, or by telephone, telex, fax or electronic mail) to any destination in the UK or abroad, without any need for any licence and without incurring any general obligation to decrypt the information on the demand of any person. (There is one exception: amateur radio licences prohibit the use of cryptography)

Far from being prohibited, data security is increasingly becoming an obligation. The Data Protection legislation imposes statutory obligations on data users to protect the confidentiality of information held by them, and confidentiality agreements between private parties, usually in a commercial or industrial context, are a commonplace means of imposing similar obligations contractually. As methods of encryption become available with increasing readiness, failure to make use of them will come to be seen as a careless breach of the duty to take proper care in protecting the security of confidential information.

But there are controls on the export of products using cryptography, and given the globally distributed character of the industries on whose products data security depends, export controls can be seen to have a very special significance.

UK export control is imposed by statutory instruments made either under the Import, Export and Customs Powers (Defence) Act 1939 or under the European Communities Act 1972 pursuant to the requirements of the EC Dual-Use Goods Regulation (3381/94). The 1939 Act does not specify or limit the purposes for which its powers may be used. The EC Regulations reflect international export control agreements, now represented by an international agreement known as the Wassenaar Arrangement. It is a criminal offence to export goods specified in the controlled lists from the UK without a licence. The offence is punishable by up to two years' imprisonment; and in *R v Ludlam* (1985) 7 Cr.App.R.(S.) 154 the Court of Appeal held that immediate custodial sentences were necessary for offences involving exportation of prohibited goods, even where computers of no military use were concerned and the defendant was of previous good character.

The controls apply only to goods, i.e. tangible physical property. The 1939 Act gives no power to impose any wider controls, and the same is true of the EC Regulation. Where the controls apply to software, therefore, they apply only to software embodied in some tangible medium, such as an application-specific integrated circuit, a CD or a listing on paper of source code or machine code.

We begin by examining the justification for the present controls, before examining their scope in some detail.

The Justification for Export Controls on Cryptographic Products

The stated aims of the Wassenaar Arrangement are as follows:

1. The Wassenaar Arrangement has been established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations. Participating States will seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities.

2. It will complement and reinforce, without duplication, the existing control regimes for weapons of mass destruction and their delivery systems, as well as other internationally recognised measures designed to promote transparency and greater responsibility, by focussing on the threats to international and regional peace and security which may arise from transfers of armaments and sensitive dual-use goods and technologies where the risks are judged greatest.

3. This arrangement is also intended to enhance co-operation to prevent the acquisition of armaments and sensitive dual-use items for military end-uses, if the situation in a region or the behaviour of a state is, or becomes, a cause for serious concern to the Participating States.

4. It will not be directed against any state or group of states and will not impede bona fide civil transactions. Nor will it interfere with the rights of states to acquire legitimate means with which to defend themselves pursuant to Article 51 of the Charter of the United Nations.

From these aims it is evident that the intention of the Arrangement is to impede the development of concentrations of military weapons that might threaten regional and international security and stability. From paragraph 4, however, it is clear that implementation of the Arrangement should neither damage genuine civil commerce nor prevent states acquiring the legitimate means of self-defence.

Although cryptographic products are in no sense weapons they are nevertheless subject to controls under the terms of the Arrangement. This is surprising, since cryptographic products are defensive in nature and exist only to protect information from unauthorised access. In the modern information age, protecting information assets is no less important than protecting physical assets, and it seems inescapable that the right of states to implement effective defences, which the Arrangement recognises, must apply to permit states to acquire cryptographic technology.

There are indirect uses of cryptography in military and weapons programmes; for example it is normal practice to use cryptographic products to protect guidance and control telemetry for missile systems. It is also common for military command and control information to be encrypted. In both these cases, however, the products used will have little in common with their civil analogues, since military products have to meet stringent environmental and performance requirements that result in custom designs at unit costs that make civil use extremely unlikely. Products designed for military use could be subject to export controls without having any significant commercial impact.

States that use cryptographic products to protect their high value defence, diplomatic and intelligence information will use special custom-built devices produced domestically under very close scrutiny. States do not use commercial products for cryptographic information security applications. For these reasons there is no practical overlap between the military and civil cryptography markets, with the result that controls on cryptographic products having military performance characteristics could be implemented without affecting products intended for civil use.

Current export controls on cryptography, examined below, make no serious attempt to distinguish between products whose characteristics make them useful for offensive military applications and those intended for civil use. The reason is probably historical: civil applications of cryptography have been very limited in the past, and controls could have a wide scope without having any significant civil impact. However, with the growth of the Internet and the rapidly increasing interest in electronic commerce, cryptographic export controls have come to apply to apply to products of great importance to civil commerce. This raises a serious question about the compatibility of current export controls with the objectives of the Wassenaar Arrangement under which they are apparently justified. It is therefore necessary to consider the wider objectives which such controls may be thought to serve.

Since the end of the second world war a number of countries have built up very large organisations whose role is to intercept and exploit the electronic communications of other nations and organisations. Examples include the National Security Agency (NSA) in the United States and the Government Communications Headquarters (GCHQ) in the UK.

These organisations can deploy extensive resources and depend on being able to read the communications traffic being exchanged by other nations and organisations. They need to identify messages of interest to them by reading source and recipient addresses and by looking for "keywords" since the total volume of traffic involved is far too high to allow it all to be studied in any detail. Because of the very large volume of data involved, this filtering is an enormous task requiring huge collection and computing resources which puts it near the edge of what is economically feasible. But if even weak encryption were to be used to hide general communications traffic, a difficult but just feasible task would be turned into a truly impossible one.

Because of this the nations that deploy such capabilities are determined to maintain their value for as long as possible by slowing down the pace at which cryptographic products come into general and widespread use. This reason for trying to restrict the proliferation of cryptography is not made explicit, and it is usually hidden behind such terms as "national security" even though all informed observers know precisely what this really means. Such obfuscation is not helpful since it makes it practically impossible to determine whether there are valid reasons for maintaining such capabilities or whether secrecy is being used to hide a weak or non-existent case.

In a remarkable spirit of openness, the United States administration sponsored a National Research Council study of US cryptography policy, and allowed a number of respected US academics to have access to the classified information that it uses to justify the "national security" need for continued controls on cryptography. The study contains a nicely presented summary of the difficulties involved in using secret evidence to justify policies for which public accountability is necessary:

> "A common refrain by defenders of policies whose origins and rationales are secret is that 'if you knew what we knew, you would agree with us.' Such a position may be true or false, but it clearly does not provide much reassurance for those not privy to those secrets for one very simple reason: those who fear the government is hiding poorly conceived policies behind a wall of secrecy are not likely to trust the government, yet in the absence of a substantive argument being called for, the government's claim is essentially a plea for trust."

The resulting study (Cryptography's Role in Securing the Information Society: The Report of the US National Research Council Committee to Study National Cryptography Policy, June 1996) also presented two very significant conclusions:

- "the debate over [US] national cryptography policy can be carried out in a reasonable manner on an unclassified basis"
- "on balance, the advantages of more widespread use of cryptography outweigh the disadvantages".

While these conclusions are expressed indirectly, they seem to us to support the following inferences:

- There is no justification for conducting the cryptography policy debate in secret
- The secret arguments used by government to justify a policy designed to impede the widespread use of cryptography are unconvincing and are being used to sustain a policy that is precisely the opposite of that which is now needed.

Although these conclusions were reached in the United States, there is no obvious reason why they should not apply equally in the United Kingdom.

Some aspects of UK government policy on cryptography are now being more openly discussed, but the "national security" drivers for the policy, and the extent to which they are justified, remain shrouded in secrecy. Moreover, in contrast with the position in the United States, there has been no independent, publicly accountable scrutiny of these aspects of UK policy and this, combined with the US conclusions, must inevitably lead to a suspicion that the arguments for continued controls in the UK would not survive open scrutiny.

We now examine the scope of current UK export controls on cryptography, before assessing their practical impact.

Current UK Controls

UK export control regulations are amended quite frequently, but the Department of Trade and Industry publishes a helpful consolidated list of controls on its website at <www.dti.gov.uk/export.control/>. The details given in this paper are taken from that list as current at 15th December 1997.

The goods subject to control in connection with cryptography are specified in Category 5 of the list of Dual-Use goods, which is set out in full in Annex 1 to this paper, together with the relevant definitions.

The scope of controls on cryptographic and information security products is wide. Controlled goods include:

1. Equipment or software designed or modified to use cryptography to ensure information security or perform cryptanalytic functions.

2. Equipment or software designed or modified to provide protection from electronic eavesdropping or a warning of its occurrence.

3. Equipment or software designed or modified to provide multilevel security or user isolation at a level exceeding Class B2 of the Trusted Computer System Evaluation Criteria (TCSEC) or equivalent.

   (For this purpose "multilevel security" is defined as a class of system containing information with different sensitivities that simultaneously permits access by users with different security clearances and needs-to-know, but prevents users from obtaining access to information for which they lack authorization.)

4. Technology for the development, production or use of the equipment or software listed.

It will at once be seen that equipment and software providing functions which are essential to the safe use of the Internet are precisely those which may not be exported from the UK without a licence. The controls on cryptographic products are especially wide ranging in that:

- no attempt is made to encompass only products oriented towards military use;

- the definition encompasses not only cryptographic products but also any products specifically designed to work with such products ("modified to use").

In consequence, apart from exceptions discussed below, all civil cryptographic products are controlled, together with any products that are designed to incorporate encryption (even if they are sold without such capabilities).

The definition of "technology" is also very broad, covering not only specific technical material such as plans, engineering designs and specifications, but also "technical assistance" covering such activities as consulting, education and training. However, bearing in mind that the controls apply only to goods, the latter definition is so wide that it almost certainly falls outside the powers conferred by the current enabling legislation.

There are, however, a number of general limitations on the width of the controls:

1. The control on the transfer of technology does not apply to information in the public domain, to basic scientific research or to the minimum necessary information for patent applications (see the Annex for detailed definitions).
2. The control on software does not apply to software which is in the public domain, nor to user-installable software sold through retail channels.

Details of these limitations are contained in the General Technology Note and the General Software Note, which are set out in Annex 2 to this paper.

There are also a number of limited exceptions for specific equipment, designed to permit the use of cryptography for such applications as "pay-per-view" television, cash dispensers, copyright protection schemes, etc. These are shown in Annex 1; and their common feature is that they do not permit the encryption of messages by the user.

Goods subject to control on cryptographic grounds may not be exported from the UK to any destination without a licence (inside or outside the European Community). Licences are granted more readily, and with fewer conditions (relating to the scope of permitted use by the end user, for example), for exports to other member states of the European Community or to Australia, Canada, Japan, New Zealand, Norway, Switzerland or the United States of America. The European Commission has made proposals for amendment of the Dual-Use regime, and one effect would be to permit the free circulation of cryptographic products within the European Community, another (perhaps perceived by the Commission as the price to be paid for this relaxation) would be the extension of controls to intangibles. Even with this relaxation, however, cryptography exports within the Community would remain among those singled out for special treatment, since all such exports would have to be notified by exporters to their national export licensing authorities, who would retain control over subsequent export from the Community. Given the importance attached to the completion of the Single Market, these anomalies, whose legality under the Community Treaties must be questionable, amount to a reproach to the Community's competence in its proper sphere of operation.

Impact of Cryptography Controls on Civil Use

Since only a few states implement controls on the domestic sale or use of cryptographic products, it is sometimes argued that the controls on exports do not undermine civil applications. In practice, however, much modern business activity is international in character and purely domestic cryptographic solutions have little appeal. Multinational companies, for example, cannot afford to build their secure global networks on the use of a disparate collection of incompatible cryptographic solutions; they want to buy solutions that they can deploy freely on a world-wide basis, a requirement that is directly affected by export controls.

Building truly secure cryptographic security solutions is also a difficult and costly exercise requiring a large investment. Probably only one country in the world,the United States, has a domestic market that can justify the levels of investment needed; and even in the US it is evident that the inability to freely exploit international markets causes much concern in industry.

The lack of availability of cryptographic products suitable for widespread civil use has a number of consequences. First, businesses now need ways of protecting their critical information assets from their competitors, and they find it difficult to obtain the products needed to do this. Secondly, the economies of many developed nations are becoming ever more 'information based' and hence dependent on computer networks. Social and economic infrastructures such as communications, transport, power and healthcare now depend on networked computer infrastructures for their safe and secure operation. The limited availability of civil cryptographic products means that these infrastructures are vulnerable to attacks that could easily disrupt their operation. Constraints on cryptography, which are sometimes justified as necessary for the protection of society from criminal and terrorist activity, are now contributing to the emergence of information infrastructures that provide easy targets for criminals and terrorists. The United States is well aware of the importance of these issues: see

- *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63* <http://www.pub.whitehouse.gov/urires/I2R?urn:pdi://oma.eop.gov.us/1998/5/26/20.text.1>*,*
- *House Report 105-132 on Defense Authorization for 1998* <http://jya.com/hr105-132-iwd.txt> *and*
- *Report of The Defense Science Board Task Force on Information Warfare - Defense* <http://jya.com/iwd.htm>.

In most countries the privacy rights and needs of citizens are also respected in principle, and the widespread availability of cryptographic products and services is seen by many as an essential means of meeting those needs.

Governments are now coming to accept the need for widespread civil use of cryptographic products and services, but they have sought to balance these needs with their own need for information access by advocating 'Key Escrow' or 'Key Recovery': a means for providing government access to encryption keys under legal safeguards.

In practice such approaches have not achieved a great deal of success. First, they have been shown by the technical community to involve very significant security risks (see *The Risks of Key Recovery, Key Escrow & Trusted Third Party Encryption*, Hal Abelson et al, June 1998). Secondly, all civil liberty and privacy groups have been highly critical of such plans, since the legal safeguards proposed have been shown by past experience to be incapable of preventing grave abuses. And thirdly, much of industry has concluded that such solutions will not meet their own needs and will undermine their ability to sell products that consumers will be prepared to trust.

Because most research on cryptography is conducted through publication, meetings and electronic exchanges, export controls on cryptography have had no significant impact on pure academic research. The impact on applied research and on industrial development has been greater, however, especially when multinational programmes such as those funded by the European Commission have been involved. Here it has often been the case that EU member states have used their influence to ensure that the research programmes approved and funded by the Commission have not deployed cryptographic capabilities of the strength that would be needed to support real applications. A consequence has been that the credibility of significant elements of the research has suffered.

Having surveyed the justification for export controls and their impact in the context of the information society, we now examine the implications of the extension of export controls on cryptographic products to intangibles.

Extending the controls

The UK White Paper on Strategic Export Controls proposes that documents transferred abroad containing controlled technology should be subject to export licensing requirements, whether exported physically or by fax or electronic mail.

Current export controls assume that exports are made pursuant to contracts for the supply of goods, so that there is a specific customer as well as a supplier, and an invoice recording the goods exported. Record-keeping requirements are imposed on exporters which reflect this assumption. Where the only effect of the proposed extension of control is to cover the case where instead of sending tangible goods to the customer, such as a disc containing a computer program, the supplier sends the program to the customer by electronic means, it is fair to argue that a purely technical loophole has been closed.

But the proposed extension is not limited to such a case at all. It would apply control to all exports in intangible form of anything covered by the existing controls. So it would apply to all "technology", which, it will be remembered, means technology for the development, production or use of equipment or software using cryptography, and would also cover specific information necessary for the development, production or use of that equipment or software. The information in question take the form of technical data or technical assistance, and technical assistance may take forms such as instructions, skills, training, working knowledge and consulting services and may involve the transfer of technical data.

For the benefit of those who may be surprised that such a wide control is proposed, or indeed incredulous, we quote from section 3.2.1 of the White Paper:

> The Government therefore proposes that new legislation should provide it with the power to control the transfer of technology, whatever the means of transfer. This power would be used to introduce secondary legislation, which it is proposed should do the following: Given the ever increasing ease with which information can be transferred across national boundaries by electronic means, i.e. by fax or e-mail (E-mail includes transfers via the Internet and via organisations' intranets), the Government proposes to provide that documents transferred abroad containing controlled technology should be subject to export licensing requirements, whether exported physically or in electronic form. Information can also be passed on in non-documentary form (e.g. orally or through personal demonstration). The proposal to make it an offence to do something which it was known or suspected could assist a weapons of mass destruction or long range missile programme, described in paragraph 3.1.4, would catch transfers of information in non-documentary form. This offence would be implemented under the power to control the transfer of technology by any means. While this power would enable the Government, if need arose, to introduce the same controls on other types of technology, we propose for

> the time being, to limit this wider offence to technology related to weapons of mass destruction and long-range missiles. The Government considers that it is right that controls on the transfer of information orally or through personal demonstration should be limited to the areas of greatest concern, in view of the difficulties of licensing such transfers, both for applicants and for the licensing authority, and given also that there are sensitivities in relation to free speech and academic freedom.

The result is effectively to control all collaborative cross-border research in cryptography, since all exchanges of messages for the purposes of cryptographic research are liable to contain controlled technology as defined. Exchanges of ideas by fax or email cannot take place if each message must wait for an export licence; and since the content of the messages will often be unintelligible to those asked to grant the licence (at any rate without extensive and burdensome explanation), the operation of a licensing regime would itself be impracticably burdensome. The record-keeping requirements would also be impracticably burdensome. The UK is well-recognised as a valuable source of contributions to collaborative research, often for products developed and marketed elsewhere in the world, and this justified reputation is the reason for the UK's substantial overseas earnings from "invisible exports". If such exports are effectively prevented by the imposition of controls, the consequence will be the re-emergence of the "brain drain" notorious from pre-Internet times.

Given that technology is treated as being transferred through "instructions, skills, training, working knowledge and consulting services", i.e. education, there must also be a serious question whether control over the export of intangibles will imply control over the education of non-residents of the UK. The United States' export control regime is understood to treat disclosure of controlled technology to a "non-US person" as requiring a personal export licence. The impact of this control depends on the definition of "non-US person", which has varied from time to time. The White Paper offers no indication of the Government's thinking on this issue. If foreign students cannot enroll in University education without an export licence, the impact on University finances calls for some examination. Three-quarters of Cambridge University's research students in science and technology are foreign nationals, for example, and restrictions may be expected to have a significant impact on the University's research base.

The consequences for general freedom of discussion also deserve attention. Much serious discussion of cryptographic issues, sometimes in technical detail, takes place in the mailing lists and news groups of the Internet. ("ukcrypto" and "sci.crypt" are examples.) The membership of such groups and lists fluctuates, and it would be very difficult, and probably impossible, for anyone sending a message to such a list or group to know all the destinations. But it could hardly be practicable for UK participants to apply for an export licence for each intended message, or to maintain the necessary records.

Controls on intangibles may also create a regime whose real impact will be much wider than its formal scope, and therefore wider than what might be expected or may be intended. For all its inadequacies, the distinction between goods and intangibles has the merit of being relatively easy to understand and operate. But once controls are extended to intangibles it will be very difficult to set a precise dividing line between information that is controlled and that which is not. When this lack of clarity is combined with the threat of criminal prosecution it becomes inevitable that anyone who might possibly be affected will err on the side of caution by adopting a wide interpretation of scope in order to minimise the risk of a prosecution.

Current experience also suggests that officials will seek to apply the widest interpretation of scope that any legislation will allow. For example, even though current controls do not apply to intangibles, the DTI have nevertheless sought to extend this scope by suggesting that 'responsible companies would not export goods by intangible means if they would be subject to control in tangible form'. Since most UK companies want a comfortable relationship with government, the practical consequence has been that controls have actually been applied across a wider scope than the legislation permits. Once intangibles become controlled, with an ill-defined boundary, this experience suggests very clearly that official interpretations of scope will be as wide as the widest possible legal interpretation, if not even wider. And since companies and individuals will be reluctant to test the legal boundaries, the practical consequence of this will be a scope that is much wider and more severe than might be expected from legal considerations alone.

It must of course be noted that existing controls on technology and software are subject to an exception for material in the public domain. There is no proposal in the White Paper that this exception should be curtailed. The result is that a transfer by email for which a licence would be required under the proposed extension could be removed from the scope of control by prior publication on a website. It might also be argued that the sending of messages to mailing lists or news groups is in effect to place them in the public domain and so remove them from the scope of export control.

Just as the freedom of intangibles from control has come to be characterised as a loophole, so it seems likely that the "public domain" exclusion would in turn be treated as a loophole. This would justify attempts by the Government to close the loophole by taking powers to prohibit publication of all controlled technology and software. It is therefore not surprising to find that the White Paper does indeed propose that the Government should be granted the power to prohibit the transfer of information orally or by demonstration, and to prohibit the publication of certain information (e.g. on a website).

As shown from the extract quoted above, the power to prohibit personal transfers would be general, although intended to be used only in relation to technology related to weapons of mass destruction and long-range missiles. The power to prohibit publication would apply only to technology related to weapons of mass destruction and long-range missiles. Although this last limitation appears attractive, it is irrational on closer analysis: if it is an offence for me to convey an item of information to you, how can it not be an offence for me to publish it, thereby conveying it not only to you but to many others at the same time? And if prior publication is a defence, that will inevitably lead to it being seen as the exploitation of a technical loophole, requiring a further extension of control.

Consequences for Cryptography

We conclude that any general extension of export control on cryptographic products to intangible transfers would have adverse effects:

- on cross-border collaborative research and earnings from invisible exports
- on education
- on freedom of speech and publication.

We further conclude that the maintenance of export controls on civil applications of cryptography is damaging to the development of electronic commerce and the Information Society, and to the existing information security of many important sectors of the social and economic infrastructure of the UK. It is moreover unjustified on the basis of the international arrangements under which it is imposed. And perhaps most striking of all, it is wholly incompatible with the objective so recently expressed by Mr Peter Mandelson (in his new capacity as Secretary of State for Trade and Industry), of putting the UK in the forefront of electronic commerce by making it the best-regulated country for that purpose. (See his speech to the 5th Annual CEO Summit on Converging Technologies at <www.dti.gov.uk/Minspeech/spchfin.htm>)

It may reasonably be asked whether current or proposed controls serve a sufficiently useful purpose to justify them in the face of these conclusions.

Are Cryptography Export Controls Effective?

Export controls on cryptographic products have been very effective in impeding the widespread use of cryptography. Despite all the interest in better security on the Internet, only an insignificant proportion of the traffic involved is cryptographically protected, even though the need for this is now widely recognised. Government policies have thus been very effective in protecting their ability to collect intelligence information, but this has been achieved by impeding beneficial uses of cryptography as well as those that are undesirable.

There is no evidence to suggest that cryptographic export controls have had a major impact on the ability of criminals, terrorists or belligerent states to obtain cryptographic software products, since these are widely and easily available to those with the skills, motivation and resources for implementing security systems in a non-commercial environment. Neither have these controls prevented states of any persuasion from developing and using their own cryptographic hardware. It is possible that controls on cryptographic hardware will have prevented criminal and terrorist use, but it is by no means certain that this is the result of controls: such use might have been equally limited had no controls existed. And it is perhaps worth noting that the main terrorist threat which Britain has faced in the second half of this century has come from holders of British passports, to whom export controls are irrelevant.

There is also a conspicuous absence of evidence to show that closing the "intangibles loophole" would have any materially useful effect. Given the consequences of such an extension, it should not be implemented without a clear demonstration of its real necessity by the production of evidence of the adverse effect of abuse of the loophole.

Even those involved in operating export controls seem to accept their deficiency: William Reinsch, Head of the US Bureau of Export Administration, speaking at a recent Electronic Privacy Information Center cryptography conference in Washington, characterised them as "neither efficient nor fair, but at least available".

There are accordingly serious questions about the justification for existing cryptography controls and the benefits that they provide. Governments are increasingly recognising these concerns and are progressively relaxing these measures in order to allow for effective commercial use. Given such developments it is difficult to believe that it is sensible to propose extensions to cryptography controls at a time when there is a clear consensus for moves in exactly the opposite direction.

There must also be major cause for concern about the feasibility and the cost of implementing controls on intangibles, since it is far from obvious how these could be implemented without either large costs or the imposition of intolerable burdens on users and service providers. There needs to be evidence to show that there are definite and achievable benefits that are demonstrably worthwhile when judged against both the direct costs involved and the indirect costs resulting from any detrimental impact that they will have on desirable activities. The White Paper makes no attempt to address the matter at all, and therefore fails to provide a sound basis for this aspect of its proposals. Before these are carried forward there should be a proper study to identify:

- the specific, achievable benefits of extending controls to cover intangibles;
- the practical feasibility and cost of the organisational and technical mechanisms required to implement and operate effective controls on intangibles;
- the impact and indirect costs resulting from the detrimental effect that such controls will have on desirable activities.

Such a study would provide a rational basis for deciding whether the extension of controls to intangibles would provide net overall benefit for society.

Are Cryptography Export Controls Justified?

Given the adverse impact of existing and proposed export controls on cryptography, we conclude that no adequate case has been made by government to justify them. Furthermore, in the light of US experience, we also conclude that government has no acceptable excuse for failing to make that case in public if it can be made.

In considering any such case, if it is made, it is worth noting that the Internet and fax communications have been available for over 25 years. No comparable extension of controls was proposed, despite the fact that the international scene was dominated by the Cold War for much of that period: the protection afforded by the Official Secrets Acts for technology originated by government agencies was considered sufficient. Access to the Internet and fax is now widely available to ordinary people, not just to businesses or the rich: is that why controls need to be extended?

The evidence of law enforcement needs is certainly very sparse. Professor Dorothy E. Denning, of the Computer Science Department of Georgetown University, Washington DC, highly respected in this field, has published at <www.cs.georgetown.edu/~denning/crypto/cases.html> details of cases found by her or reported to her after a world-wide trawl for cases in which cryptography had been used in the context of crime. There are remarkably few cases, the majority of which involved stored data rather than intercepted communications. And in almost all cases the use of cryptography had no material adverse effect on law enforcement.

Wider consequences

The list of controlled goods is diverse, and it is very difficult for the non-specialist to understand the implications of its contents. This paper has concentrated on cryptography for two reasons. The first is that cryptography has now descended from the rarified and exclusive air breathed by military and diplomatic bodies into the province of the common man, and has emerged as a key enabling technology of the coming Information Society. The second is that by focussing in detail on a single technology, it becomes more readily apparent how to assess the impact of the current controls and the proposals for their extension.

It seems to us very likely that a similar review of the impact of current and future controls on other controlled fields will yield equally disturbing conclusions. We offer a few examples to show that cryptography may well not be a special case.

It must be remembered that much technology is controlled by reference to its possible relevance to weapons of mass destruction and long-range missiles. Many of the core curriculum subjects in the field of medicine, such as bacteriology, virology, toxicology, biochemistry and pharmacology, are central to a chemical and biological weapons programme. Other subjects whose technology is relevant to weapons of mass destruction or their delivery systems include not only nuclear physics and chemistry but also aerodynamics, flight control systems, navigation systems, and even computational fluid dynamics.

The effects of control can extend beyond the subject of research to the use of necessary equipment. Basic research in single-electron memories (not as such controlled) may use an electron beam lithographic machine to make prototypes, and this equipment is on the control list as it can also be used to fabricate masks for military semiconductors. Existing controls merely control the physical export of the machine, and so do not affect research conducted by its use; but if control is extended to limit access to its software, overseas students might need licences to use it.

Other fields in which teaching or research could become subject to controls include computer science (fast networks, high performance computing, neural networks, real-time expert systems, hardware and software verification, reverse engineering). Engineering departments would be affected by the listing of numerically-controlled machine tools and fibre winding equipment, robots, optical amplifiers, software radios and aero-engine control systems, as well as many lasers, gyros, accelerometers and similar components. The restrictions that previously only applied to physical hardware objects would be extended to the software used to design, test, control or operate them, or to integrate them into larger systems.

This brief reference to a number of affected fields is enough to demonstrate what widespread consequences could flow from an extension of control to intangibles. We conclude that it would be irresponsible to proceed with any such extension of controls without a thorough and extensive examination of the full consequences of such a step.

But the DTI is reasonable...

This paper has examined the application of control to exports. It should not be assumed that everything that is controlled is in practice prohibited, or even made very difficult. Although the licensing regime imposes inconvenient costs and delays on exporters, we have no reason to doubt that the DTI exercises its licensing functions with a clear appreciation of the importance of exports to the UK economy, and we believe that it is generally perceived by exporters as flexible and supportive in its approach. And in addition to its approach to individual licences, there are many open general export licences which effectively suspend most control over a wide range of goods.

It may be argued, therefore, that a similarly benign approach will be applied to the control of intangibles, and that the adverse consequences we have identified will not in practice follow from an extension of controls.

The weakness of this argument is that it proves too much. From the point of view of the administrator, there are always advantages in a system under which everything is prohibited except what is expressly permitted, especially where the administrator can withdraw and modify permissions easily. But the fact that the administrator is accountable to Parliament has never been regarded as a sufficient justification for departing from the well-established principle that the liberty of the subject requires that criminal sanctions should be imposed by legislation and not by administrative decree.

There are two particular reasons why this general principle should be applied to the extension of export controls to intangibles: the first is that breaches of export control are no mere administrative infractions, but serious criminal offences for which a sentence of imprisonment is required for a first offender of good character whose offence causes no particular harm; and the second is that, as the White Paper recognises, controls on intangibles cannot work without the support of controls on freedom of speech and publication.

In our view it is intolerable in a democracy that freedom of speech and publication should be subject to imprisonment depending on the granting or withholding by officials of export licences based on complex technical controls established by secondary legislation.

For similar reasons we regard it as unacceptable for the Government to justify the imposition of controls by reference to compliance with the UK's international obligations. Such obligations are not imposed by external forces over which the Government has no control; on the contrary, they are the result of decisions by the Government to bind itself to an international agreement. Where serious criminal consequences follow, affecting freedom of trade, speech and publication, the Government should not so bind itself without prior Parliamentary approval.

What should now be done: Recommendations

1. There should be no extension of controls to intangibles without a full public justification by reference to actual harm caused by intangible exports of controlled technology as compared with properly evaluated burdens and losses involved in extending the controls.

2. If such a justification can be provided, any controls shown to be necessary should be limited to exports in the course of commercial transactions, and should not apply to communications or publications made for the purposes of research (whether basic or applied).

3. There should be free movement of all goods and intangibles within the European

Community and the wider European Economic Area without any special treatment.

4. Information security products using cryptography for commercial purposes should be removed from the scope of control.

Annex 1

CATEGORY 5 and DEFINITIONS

5A2 Systems, Equipment and Components

5A002

a. Systems, equipment, application specific "electronic assemblies", modules and integrated circuits for "information security", as follows, and other specially designed components therefor:

1. Designed or modified to use "cryptography" employing digital techniques to ensure "information security";

2. Designed or modified to perform cryptanalytic functions;

3. Designed or modified to use "cryptography" employing analogue techniques to ensure "information security";

Note: 5A002.a.3. does not control the following:

1. Equipment using "fixed" band scrambling not exceeding 8 bands and in which the transpositions change not more frequently than once every second;

2. Equipment using "fixed" band scrambling exceeding 8 bands and in which the transpositions change not more frequently than once every ten seconds;

3. Equipment using "fixed" frequency inversion and in which the transpositions change not more frequently than once every second;

4. Facsimile equipment;

5. Restricted audience broadcast equipment;

1. Civil television equipment.

4. Designed or modified to suppress the compromising emanations of information-bearing signals;

Note: 5A002.a.4. does not control equipment specially designed to suppress emanations for reasons of health and safety.

5. Designed or modified to use cryptographic techniques to generate the spreading code for "spread spectrum" or the hopping code for "frequency agility" systems;

6. Designed or modified to provide certified or certifiable "multilevel security" or user isolation at a level exceeding Class B2 of the Trusted Computer System Evaluation Criteria (TCSEC) or equivalent;

7. Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion.

Note: 5A002 does not control:

a. "Personalized smart cards" or specially designed components therefor, with any of the following characteristics:

1. Not capable of message traffic encryption or encryption of user-supplied data or related key management functions therefor; or

2. When restricted for use in equipment or systems excluded from control under entries 1. to 6. of the Note to 5A002.a.3. or under entries b. to h. of this Note;

b. Equipment containing "fixed" data compression or coding techniques;

c. Receiving equipment for radio broadcast, pay television or similar restricted audience television of the consumer type, without digital encryption and where digital decryption is limited to the video, audio or management functions;

d. Portable or mobile radiotelephones for civil use (e.g., for use with commercial civil cellular radiocommunications systems) that are not capable of end-to-end encryption;

e. Decryption functions specially designed to allow the execution of copy-protected "software", provided the decryption functions are not user-accessible;

f. Access control equipment, such as automatic teller machines, self-service statement printers or point of sale terminals, which protects password or personal identification numbers (PIN) or similar data to prevent unauthorized access to facilities but does not allow for encryption of files or text, except as directly related to the password or PIN protection;

g. Data authentication equipment which calculates a Message Authentication Code (MAC) or similar result to ensure no alteration of text has taken place, or to authenticate users, but does not allow for encryption of data, text or other media other than that needed for the authentication;

h. Cryptographic equipment specially designed and limited for use in machines for banking or money transactions, such as automatic teller machines, self-service statement printers or point of sale terminals.

5B2 Test, Inspection and Production Equipment

5B002

a. Equipment specially designed for:

1. The "development" of equipment or functions specified in 5A002, 5B002, 5D002 or 5E002, including measuring or test equipment;

2. The "production" of equipment or functions specified in 5A002, 5B002, 5D002 or 5E002, including measuring, test, repair or production equipment;

3. Measuring equipment specially designed to evaluate and validate the "information security" functions specified in 5A002 or 5D002.

5C2 Materials

None.

5D2 Software

5D002

a. "Software" specially designed or modified for the "development", "production" or "use" of equipment or "software" specified in 5A002, 5B002, or 5D002;

b. "Software" specially designed or modified to support "technology" specified in 5E002;

c. Specific "software", as follows:

1. "Software" having the characteristics, or performing or simulating the functions of the equipment specified in 5A002 or 5B002;

2. "Software" to certify "software" specified in 5D002.c.1.

Note: 5D002 does not control:

a. "Software" required for the "use" of equipment excluded from control under the Note to 5A002;

b. "Software" providing any of the functions of equipment excluded from control under the Note to 5A002.

5E2 Technology

5E002

"Technology" according to the General Technology Note for the "development", "production" or "use" of equipment or "software" specified in 5A002, 5B002 or 5D002.

Definitions

"Basic scientific research" means experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective.

"Cryptography" means the discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification or prevent its unauthorized use. "Cryptography" is limited to the transformation of information using one or more 'secret parameters' (e.g., crypto variables) or associated key management.

N.B.: 'Secret parameter': a constant or key kept from the knowledge of others or shared only within a group.

"Development" is related to all phases prior to serial production, such as: design, design research, design analyses, design concepts, assembly and testing of prototypes, pilot production schemes, design data, process of transforming design data into a product, configuration design, integration design, layouts.

"Electronic assembly" means a number of electronic components (i.e., 'circuit elements', 'discrete components', integrated circuits, etc.) connected together to perform (a) specific function(s), replaceable as an entity and normally capable of being disassembled.

N.B.: 1. 'Circuit element': a single active or passive functional part of an electronic circuit, such as one diode, one transistor, one resistor, one capacitor, etc.

2. 'Discrete component': a separately packaged 'circuit element' with its own external connections.

"Fixed" means that the coding or compression algorithm cannot accept externally supplied parameters (e.g., cryptographic or key variables) and cannot be modified by the user.

"In the public domain" as it applies herein, means "technology" or "software" which has been made available without restrictions upon its further dissemination (copyright restrictions do not remove "technology" or "software" from being "in the public domain").

"Information security" is all the means and functions ensuring the accessibility, confidentiality or integrity of information or communications, excluding the means and functions intended to safeguard against malfunctions. This includes "cryptography", 'cryptanalysis', protection against compromising emanations and computer security.

N.B.: 'Cryptanalysis': analysis of a cryptographic system or its inputs and outputs to derive *confidential variables or sensitive data, including clear text.*

"Multilevel security" means a class of system containing information with different sensitivities that simultaneously permits access by users with different security clearances and needs-to-know, but prevents users from obtaining access to information for which they lack authorization.

N.B.: "Multilevel security" is computer security and not computer reliability which deals with equipment fault prevention or human error prevention in general.

"Personalized smart card" means a smart card containing a microcircuit which has been programmed for a specific application and cannot be reprogrammed for any other application by the user.

"Production" means all production phases, such as: construction, production engineering, manufacture, integration, assembly (mounting), inspection, testing, quality assurance.

"Required" as applied to "technology" or "software", refers to only that portion of "technology" or "software" which is peculiarly responsible for achieving or extending the controlled performance levels, characteristics or functions. Such "required" "technology" or "software" may be shared by different goods. "Software" means a collection of one or more "programmes" or 'microprogrammes' fixed in any tangible medium of expression.

N.B.: 'Microprogramme' means a sequence of elementary instructions, maintained in a special storage, the execution of which is initiated by the introduction of its reference instruction into an instruction register.

"Source code" (or source language) is a convenient expression of one or more processes which may be turned by a programming system into equipment executable form ("object code" (or object language)).

"Technology" means specific information necessary for the "development", "production" or "use" of goods. This information takes the form of 'technical data' or 'technical assistance'.

N.B.: 1. 'Technical assistance' may take forms such as instructions, skills, training, working knowledge and consulting services and may involve the transfer of "technical data".

2. 'Technical data' may take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memories.

"Use" means operation, installation (including on-site installation), maintenance (checking), repair, overhaul and refurbishing.

Annex 2

GENERAL TECHNOLOGY NOTE (GTN)

(To be read in conjunction with section E of Categories 1 to 9.)

The export of "technology" which is "required" for the "development", "production" or "use" of goods controlled in Categories 1 to 9, is controlled according to the provisions of Categories 1 to 9.

"Technology" "required" for the "development", "production" or "use" of goods under control remains under control even when applicable to non-controlled goods. Controls do not apply to that "technology" which is the minimum necessary for the installation , operation, maintenance (checking) and repair of those goods which are not controlled or whose export has been authorised.

Controls on "technology" transfer do not apply to information "in the public domain", to "basic scientific research" or to the minimum necessary information for patent applications.

GENERAL SOFTWARE NOTE (GSN)

(This note overrides any control within section D of Categories 0 to 9.)

Categories 0 to 9 of this list do not control "software" which is either:

a. Generally available to the public by being:

1. Sold from stock at retail selling points, without restriction, by means of:

a. Over-the-counter transactions;

b. Mail order transactions; or

c. Telephone order transactions; and

2. Designed for installation by the user without further substantial support by the supplier; or

b. "In the public domain".